بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

مقاوم‌سازی امنیتی Oracle

فهرست مطالب

پیشگفتار

در این مستند، مقاوم‌سازی امنیتی سیستم مدیریت پایگاه داده‌های اراکل نسخه 12c مورد بررسی قرار می‌گیرد. به این منظور، نحوه وارسی و ایمن‌سازی مقادیر و تنظیمات مربوط به صد و شصت پارامتر تاثیرگذار در عملکرد اراکل معرفی می‌گردند. در مورد هر پارامتر، کاربرد آن پارامتر به طور مختصر بیان می‌شود، ارزش امنیتی پارامتر ذکر می‌گردد، نحوه آگاهی از مقدار کنونی پارامتر مشخص می‌شود، و در نهایت چگونگی مقداردهی امن پارامتر نشان داده می‌شود.

بررسی پارامترهای مربوط به مقاوم‌سازی اراکل در پنج بخش متمایز صورت می‌گیرد. در بخش اول، نیازمندی‌های مرتبط با حساب‌های کاربری موجود در اراکل ارائه می‌شود. بخش دوم به تشریح پارامترهای نصب و پیکربندی اراکل می‌پردازد. بخش سوم به معرفی محدودیت‌هایی اختصاص دارد که باید بر روی فرآیند اتصال و ورود کاربران به اراکل اعمال گردد. پارامترهای مربوط به کنترل دسترسی و مجازشماری در بخش چهارم بررسی می‌شوند. در خاتمه، در بخش پنجم، رویدادنگاری امن مورد توجه قرار می‌گیرد.

لازم به ذکر است که قبل از اجرای دستوراتی که مقداردهی امن پارامترهای مختلف را برآورده می‌کنند، ابتدا باید اطمینان حاصل گردد که هیچ‌کدام از برنامه‌های کاربردی وابسته به پایگاه داده اراکل و یا برنامه‌های مختلف مربوط به نظارت و مدیریت اراکل، به مقادیر قبلی وابستگی نداشته باشند. در چنین وضعیت‌هایی باید پس از مقداردهی امن پارامترها، وابستگی‌های موجود نیز با توجه به مقادیر جدید بروزرسانی گردند. همچنین کلیه دستورات SQL موجود در این مستند باید با حساب کاربری SYS اجرا شوند.

۱ امن سازی محیط اجرا

در زمان نصب اراکل، بسته به نحوه نصب و انتخاب گزینه‌های مختلف، تعدادی حساب کاربری به طور خودکار ایجاد می‌شود که برای اجرای گام‌های مختلف نصب و نیز مدیریت سیستم نصب شده مورد استفاده قرار می‌گیرند. گذرواژه‌های بسیاری از این حساب‌ها به طور خودکار و با مقادیر پیش‌فرض مقداردهی می‌شوند و گذرواژه‌های تعداد اندکی نیز از کاربر نصب کننده دریافت می‌گردد. با توجه به این‌که حساب‌های کاربری مذکور معمولا مجوزهای پر قدرتی دارند، آگاهی از گذرواژه‌های پیش‌فرض‌شان ممکن است منجر به سوء استفاده از آن‌ها گردد. به منظور مقاوم‌سازی اراکل در برابر این تهدید، لازم است گذرواژه‌های پیش‌فرض حساب‌های کاربری تعویض شوند.

همچنین در زمان نصب اراکل، بسته به نحوه انتخاب گزینه‌های مختلف، ممکن است تعدادی حساب کاربری نمونه به منظور دسترسی به تعدادی پایگاه داده نمونه ایجاد گردد. وجود چنین حساب‌هایی در کاربردهای واقعی (و غیر آموزشی) توجیه امنیتی ندارد و لازم است چنین حساب‌هایی به طور کامل از اراکل حذف گردند.

در ادامه امن‌سازی حساب‌های کاربری با گذرواژه‌های پیش‌فرض و امن‌سازی حساب‌های کاربری نمونه مورد بحث و بررسی قرار می گیرند. همچنین پیکربندی امن فایل‌های ذخیره داده و فایل‌های رویدادنگاری نیز توضیح داده می‌شوند.

۱ – ۱ امن‌سازی حساب‌های کاربری با گذرواژه‌های پیش‌فرض

در زمان نصب اراکل، بسته به نحوه نصب و انتخاب گزینه‌های مختلف، تعدادی حساب کاربری به طور خودکار ایجاد می‌شود که برای اجرای گام‌های مختلف نصب و نیز مدیریت سیستم نصب شده مورد استفاده قرار می‌گیرند. گذرواژه‌های بسیاری از این حساب‌ها به طور خودکار و با مقادیر پیش‌فرض مقداردهی می‌شوند و گذرواژه‌های تعداد اندکی نیز از کاربر نصب کننده دریافت می‌گردد. اگرچه اکثر حساب‌های کاربری ایجاد شده در زمان نصب، بلافاصله با پایان نصب اراکل، به طور خودکار غیرفعال و قفل می‌شوند، ممکن است در آینده به هر دلیلی فعال و باز گردند. در نتیجه، با توجه به این‌که حساب‌های کاربری مذکور معمولا مجوزهای پر قدرتی دارند، آگاهی از گذرواژه‌های پیش‌فرض‌شان ممکن است منجر به سوء استفاده از آن‌ها گردد. به منظور مقاوم‌سازی اراکل در برابر این تهدید، لازم است گذرواژه‌های پیش‌فرض حساب‌های کاربری تعویض شوند.

تهدید/توجیه امنیتی:

از آنجایی که گذرواژه‌های پیش‌فرض برای مهاجمین نیز شناخته شده است، در صورت عدم تغییر آن ها، هر مهاجمی که به پایگاه‌داده دسترسی پیدا کند، می‌تواند با نام کاربری و گذرواژه پیش فرض احراز اصالت شود.

اطلاع از وضعیت فعلی:

برای یافتن نام‌های کاربری با گذرواژه پیش فرض می‌توان از دستور زیر استفاده کرد.

```
SELECT USERNAME
FROM DBA_USERS_WITH_DEFPWD
WHERE USERNAME NOT LIKE '%XS$NULL%';
```

با اجرای دستور فوق، لیستی از نام های کاربری که گذرواژه پیش فرض آن ها تغییر داده نشده است، به نمایش در می‌آید.

مقاوم سازی:

با استفاده از روش های زیر می‌توان گذرواژه نام‌های کاربری را تغییر داد:

- برای هر یک از نام‌های کاربری نمایش داده شده در لیست کاربران با گذرواژه‌های پیش فرض دستور زیر برای تغییر گذرواژه اجرا شود.

```
PASSWORD <username>
```

- با استفاده از اسکریپت زیر می‌توان گذرواژه‌ای را به صورت تصادفی ایجاد و به هر کاربر که گذرواژه پیش فرض دارد، اختصاص داد.

```
begin
for r_user in
(select username from dba_users_with_defpwd where username not
like '%XS$NULL%')
loop
DBMS_OUTPUT.PUT_LINE('Password for user '||r_user.username||'
will be changed.');
execute immediate 'alter user "'||r_user.username||'" identified
by "'||DBMS_RANDOM.string('a',16)||'"account lock password expire';
end loop;
end;
```

در این بخش، ۲۷ حساب کاربری که در زمان نصب اراکل ایجاد می‌شوند و ممکن است دارای گذرواژه پیش‌فرض باشند، معرفی می‌گردند و نحوه تغییر گذرواژه‌شان بیان می‌شود.

۱-۱-۱ حساب کاربری APEX_040000

حساب کاربری APEX_040000 مالک بیشتر اشیائی است که در زمان نصب Oracle Database Application Express (ODAE) ایجاد می‌شوند.

تهدید/توجیه امنیتی:

ممکن است در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری APEX_040000 منتسب گردد. اطلاع از این گذرواژه می‌تواند منجر به دسترسی غیر مجاز به اشیاء تحت مالکیت APEX_040000 شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این حساب کاربری از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name = 'APEX_040000' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_to_raw('oracle') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM sys.user$ WHERE name = 'APEX_040000' AND password='EE7785338B8FFE3D';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "APEX_040000" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۲ حساب کاربری APPQOSSYS

حساب کاربری APPQOSSYS مالک تمامی اشیاء مرتبط با کیفیت خدمات (Quality of Service) است.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری APPQOSSYS منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به دسترسی غیر مجاز به اشیاء تحت مالکیت APPQOSSYS شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این حساب کاربری از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'APPQOSSYS' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('appqossys') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'APPQOSSYS';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "APPQOSSYS" IDENTIFIED BY "<new password phrase>";
```

۳-۱-۱ حساب کاربری CTXSYS

حساب کاربری CTXSYS مدیر Oracle Text است.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری CTXSYS منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این حساب کاربری از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1، defaultpwd2 و یا defaultpwd3 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'CTXSYS' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('ctxsys') || hextoraw(substr(spare4,43,20)), 3)))
union
```

```
SELECT 'defaultpwd2' AS defaultpassword FROM sys.user$ WHERE name =
'CTXSYS' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('change_on_install') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd3' FROM dba_users_with_defpwd WHERE username =
'CTXSYS';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "CTXSYS" IDENTIFIED BY "<new password phrase>";
```

۴-۱-۱ حساب کاربری DBSNMP

حساب کاربری DBSNMP توسط واسط وبی مدیریت اراکل (Oracle Enterprise Manager) برای مدیریت و نظارت بر عملکرد اراکل مورد استفاده قرار می‌گیرد.

تهدید/توجیه امنیتی:

بسته به نحوه نصب اراکل، ممکن است گذرواژه پیش‌فرضی به حساب کاربری DBSNMP منتسب گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری (مثلا بازیابی مقدار درهم‌سازی شده گذرواژه سایر کاربران، hashed password) شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این حساب کاربری از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'DBSNMP' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('dbsnmp') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'DBSNMP';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "DBSNMP" IDENTIFIED BY "<new password phrase>";
```

۵-۱-۱ حساب کاربری DIP

حساب کاربری DIP در اجرای عملیات مرتبط با Oracle Internet Directory و نیز Oracle Label Security مورد استفاده قرار می‌گیرد.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری DIP منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این حساب کاربری از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'DIP' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('dip') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'DIP';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "DIP" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۶ حساب کاربری EXFSYS

حساب کاربری EXFSYS برای دسترسی به شمای EXFSYS مورد استفاده قرار می‌گیرد. این شمای[1] فرآیند بکارگیری Rules Manager و Expression Filter را تسهیل می‌کند و به کاربران اجازه ایجاد قواعد PL/SQL پیچیده را می‌دهد.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری EXFSYS منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود.

اطلاع از وضعیت فعلی:

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'EXFSYS' AND

substr(spare4,3,40) =

rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('exfsys') || hextoraw(substr(spare4,43,20)), 3)))

union

SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'EXFSYS';
```

چنانچه با اجرای پرسمان فوق، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "EXFSYS" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۷ حساب کاربری MDDATA

حساب کاربری MDDATA مالک شمای MDDATA است که برای ذخیره و بازیابی اطلاعات جغرافیایی و مکان‌یابی (مشابه GPS) استفاده می‌شود.

تهدید/توجیه امنیتی:

[1] Scheme

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری MDDATA منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود. به عنوان نمونه، مهاجم قادر است با دسترسی به مجوزهای این حساب، یک بدافزار را به عنوان یک فرایند کاری در سیستم نصب کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامت از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 و یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name = 'MDDATA' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_to_raw('mddata') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username = 'MDDATA';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "MDDATA" IDENTIFIED BY "<new password phrase>";
```

۸-۱-۱ حساب کاربری MDSYS

حساب کاربری MDSYS در عملیات مرتبط با Oracle Multimedia Locator که ذخیره و بازیابی داده‌های صوتی و تصویری را تسهیل می‌کند، استفاده می‌شود.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری MDSYS منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود. به عنوان مثال، مهاجم با دسترسی به مجوزهای این حساب کاربری می‌تواند یک بدافزار را در قالب افزونه صوتی/تصویری (AV plugin) در سیستم نصب کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از دستور زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1، defaultpwd2 یا defaultpwd3 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'MDSYS' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('sys') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' AS defaultpassword FROM sys.user$ WHERE name =
'MDSYS' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('mdsys') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd3' FROM dba_users_with_defpwd WHERE username =
'MDSYS';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "MDSYS" IDENTIFIED BY "<new password phrase>";
```

۹-۱-۱ حساب کاربری LBACSYS

حساب کاربری LBACSYS مدیر Oracle Label Security (OLS) است.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری LBACSYS منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری و اخلال در OLS شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از دستور زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'LBACSYS' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('lbacsys') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'LBACSYS';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "LBACSYS" IDENTIFIED BY "<new password phrase>";
```

۱۰-۱-۱ حساب کاربری OLAPSYS

حساب کاربری OLAPSYS مالک کاتالوگ online analytical processing (OLAP) است.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری OLAPSYS منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری و نصب بدافزار در سیستم شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'OLAPSYS'AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('manager') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'OLAPSYS';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "OLAPSYS" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۱۱ حساب کاربری ORACLE_OCM

حساب کاربری ORACLE_OCM توسط مدیر پیکربندی[2] استفاده می‌شود.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری ORACLE_OCM منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'ORACLE_OCM' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('oracle_ocm') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'ORACLE_OCM';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "ORACLE_OCM" IDENTIFIED BY "<new password phrase>";
```

[2] Configuration Manager

۱-۱-۱۲ حساب کاربری ORDDATA

حساب کاربری ORDDATA مالک اشیاء مرتبط با Oracle Multimedia DICOM است. استاندارد DICOM[3] برای تصویربرداری پزشکی ارائه شده است و ذخیره، مدیریت و بازیابی فرمت DICOM را توصیف می‌کند.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری ORDDATA منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'ORDDATA' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('orddata') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'ORDDATA';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "ORDDATA" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۱۳ حساب کاربری ORDPLUGINS

حساب کاربری ORDPLUGINS برای مدیریت افزونه‌هایی است که در فرآیند ذخیره و بازیابی داده‌های صوتی و تصویری (مانند داده‌های پزشکی/بیمارستانی با فرمت DICOM) به کار می‌آیند.

---

[3] Digital Imaging AND Communications in Medicine

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری ORDPLUGINS منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری و نصب بدافزار در قالب یک افزونه صوتی- تصویری در سیستم شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'ORDPLUGINS' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('ordplugins') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'ORDPLUGINS';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "ORDPLUGINS" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۱۴ حساب کاربری ORDSYS

حساب کاربری ORDSYS مدیر Oracle Multimedia است.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری ORDSYS منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری و نصب بدافزار در قالب افزونه صوتی-تصویری در سیستم شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'ORDSYS' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('ordsys') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'ORDSYS';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "ORDSYS" IDENTIFIED BY "<new password phrase>";
```

۱۵-۱-۱ حساب کاربری OUTLN

حساب کاربری OUTLN برای جلوگیری از اعمال یک سری تغییرات که تاثیر مخربی بر روی کارایی پایگاه داده دارند به کار می‌آید.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری OUTLN منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'OUTLN' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('outln') || hextoraw(substr(spare4,43,20)), 3)))
union
```

```
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'OUTLN';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "OUTLN" IDENTIFIED BY "<new password phrase>";
```

۱۶-۱-۱ حساب کاربری OWBSYS_AUDIT

حساب کاربری OWBSYS_AUDIT برای دسترسی به جداول رویدادنگاری مرتبط با Warehouse Builder مورد استفاده قرار می‌گیرد.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری OWBSYS_AUDIT منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری و اعمال تغییر در جداول رویدادنگاری شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'OWBSYS_AUDIT' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('owbsys_audit') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'OWBSYS_AUDIT';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "OWBSYS_AUDIT" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۱۷ حساب کاربری OWBSYS

حساب کاربری OWBSYS مدیر Oracle Warehouse Builder است.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری OWBSYS منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name = 'OWBSYS' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_to_raw('owbsys') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username = 'OWBSYS';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "OWBSYS" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۱۸ حساب کاربری SI_INFORMTN_SCHEMA

حساب کاربری SI_INFORMTN_SCHEMA برای مدیریت و ذخیره‌سازی افزونه‌های به کار می‌رود که توسط اراکل و یا سایر شرکت‌ها ارائه شده‌اند.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری SI_INFORMTN_SCHEMA منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری و نصب بدافزار در قالب یک افزونه در سیستم شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'SI_INFORMTN_SCHEMA' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('si_informtn_schema') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'SI_INFORMTN_SCHEMA';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "SI_INFORMTN_SCHEMA" IDENTIFIED BY "<new passwordphrase>";
```

۱۹-۱-۱ حساب کاربری SPATIAL_CSW_ADMIN_USR

حساب کاربری SPATIAL_CSW_ADMIN_USR مالک CSW[4] است.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری SPATIAL_CSW_ADMIN_USR منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری و نصب بدافزار در سیستم شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

[4] Catalog Services for the Web

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'SPATIAL_CSW_ADMIN_USR' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('spatial_csw_admin_usr') || hextoraw(substr(spare4,43,20)),
3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'SPATIAL_CSW_ADMIN_USR';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "SPATIAL_CSW_ADMIN_USR" IDENTIFIED BY "<new password
phrase>";
```

۲۰-۱-۱ حساب کاربری SPATIAL_WFS_ADMIN_USR

حساب کاربری SPATIAL_WFS_ADMIN_USR مالک[5] WFS است.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری SPATIAL_WFS_ADMIN_USR منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری و نصب بدافزار در سیستم شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'SPATIAL_WFS_ADMIN_USR' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
```

[5] Web Feature Service

```
o_raw('spatial_wfs_admin_usr')    ||    hextoraw(substr(spare4,43,20)),
3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'SPATIAL_WFS_ADMIN_USR';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "SPATIAL_WFS_ADMIN_USR" IDENTIFIED BY "<new password
phrase>";
```

۱-۱-۲۱ حساب کاربری SYS

حساب کاربری SYS پرقدرت ترین کاربری است که در زمان نصب اراکل ایجاد می‌شود.

تهدید/توجیه امنیتی:

در زمان نصب نسخه‌های قدیمی اراکل، گذرواژه‌های پیش‌فرضی به حساب کاربری SYS منتسب می‌شد. با توجه به این‌که تعدادی از کاربران اراکل بر حسب عادت همچنان از همان گذرواژه‌ها استفاده می‌کنند (و مثلا در زمان نصب یک نسخه جدید اراکل نیز یک گذرواژه قدیمی را انتخاب می‌کنند)، اطلاع از این گذرواژه‌ها می‌تواند منجر به سوء استفاده از مجوزهای بیشمار این حساب کاربری قدرتمند شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1، defaultpwd2، defaultpwd3، یا defaultpwd4 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض قدیمی است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'SYS' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('manager') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' AS defaultpassword FROM sys.user$ WHERE name =
'SYS' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('change_on_install') || hextoraw(substr(spare4,43,20)), 3)))
union
```

```
SELECT 'defaultpwd3' AS defaultpassword FROM sys.user$ WHERE name =
'SYS' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('d_syspw') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd4' FROM dba_users_with_defpwd WHERE username =
'SYS';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "SYS" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۲۲ حساب کاربری SYSTEM

حساب کاربری SYSTEM یکی از حساب‌هایی است که برای مدیریت اراکل و در زمان نصب آن ایجاد می‌شود.

تهدید/توجیه امنیتی:

در زمان نصب نسخه‌های قدیمی اراکل، گذرواژه‌های پیش‌فرضی به حساب کاربری SYSTEM منتسب می‌شد. با توجه به این‌که تعدادی از کاربران اراکل، بر حسب عادت، همچنان از همان گذرواژه‌ها استفاده می‌کنند (و مثلا در زمان نصب یک نسخه جدید اراکل نیز یک گذرواژه قدیمی را انتخاب می‌کنند)، اطلاع از این گذرواژه‌ها می‌تواند منجر به سوء استفاده از مجوزهای مدیریتی این حساب کاربری شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1، defaultpwd2 یا defaultpwd3 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'SYSTEM' AND
substr(spare4,3,40)                                              =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('manager') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' AS defaultpassword FROM sys.user$ WHERE name =
'SYSTEM' AND
```

```
substr(spare4,3,40)                                                    =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('d_systpw') || hextoraw(substr(spare4,43,20)), 3)))

union

SELECT 'defaultpwd3' FROM dba_users_with_defpwd WHERE username =
'SYSTEM';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "SYSTEM" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۲۳ حساب کاربری WK_TEST

حساب کاربری WK_TEST برای دسترسی به Oracle Ultra Search استفاده می‌شود.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری WK_TEST منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'WK_TEST' AND

substr(spare4,3,40) =

rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('wk_test') || hextoraw(substr(spare4,43,20)), 3)))

union

SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'WK_TEST';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "WK_TEST" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۲۴ حساب کاربری WKPROXY

حساب کاربری WKPROXY برای دسترسی به Oracle 9i Application Ultra Search استفاده می‌شود.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری WKPROXY منتسب می‌گردد. اطلاع از این گـذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1، defaultpwd2 یا defaultpwd3 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'WKPROXY' AND
substr(spare4,3,40)                                                =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('change_on_install') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' AS defaultpassword FROM sys.user$ WHERE name =
'WKPROXY' AND
substr(spare4,3,40)                                                =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('wkproxy') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd3' FROM dba_users_with_defpwd WHERE username =
'WKPROXY';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "WKPROXY" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۲۵ حساب کاربری WKSYS

حساب کاربری WKSYS مدیر Oracle Ultra Search است.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری WKSYS منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'WKSYS' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('wksys') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'WKSYS';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "WKSYS" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۲۶ حساب کاربری WMSYS

حساب کاربری WMSYS برای مدیریت Workspace Manager به کار می‌رود.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری WMSYS منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1 یا defaultpwd2 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'WMSYS' AND
substr(spare4,3,40) =
```

```
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('wmsys') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' FROM dba_users_with_defpwd WHERE username =
'WMSYS';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "WMSYS" IDENTIFIED BY "<new password phrase>";
```

۱-۱-۲۷ حساب کاربری XDB

حساب کاربری XDB برای ذخیره و بازیابی داده‌های XML استفاده می‌شود.

تهدید/توجیه امنیتی:

در زمان نصب، گذرواژه پیش‌فرضی به حساب کاربری XDB منتسب می‌گردد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، defaultpwd1، defaultpwd2 یا defaultpwd3 به عنوان پاسخ تولید شود، این حساب کاربری دارای گذرواژه پیش‌فرض است.

```
SELECT 'defaultpwd1' AS defaultpassword FROM sys.user$ WHERE name =
'XDB' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('xdb') || hextoraw(substr(spare4,43,20)), 3)))
union
SELECT 'defaultpwd2' AS defaultpassword FROM sys.user$ WHERE name =
'XDB' AND
substr(spare4,3,40) =
rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cast_t
o_raw('change_on_install') || hextoraw(substr(spare4,43,20)), 3)))
union
```

```
SELECT 'defaultpwd3' FROM dba_users_with_defpwd WHERE username =
'XDB';
```

مقاوم‌سازی:

با اجرای دستور زیر، گذرواژه به مقدار جدید تغییر می‌یابد.

```
ALTER USER "XDB" IDENTIFIED BY "<new password phrase>";
```

۲ – ۱ امن‌سازی حساب‌های کاربری نمونه

در زمان نصب اراکل، بسته به نحوه انتخاب گزینه‌های مختلف، ممکن است تعدادی حساب کاربری نمونه به منظور دسترسی به تعدادی پایگاه داده نمونه ایجاد گردد. وجود چنین حساب‌هایی در کاربردهای واقعی (و غیر آموزشی) توجیه امنیتی ندارد و لازم است چنین حساب‌هایی به طور کامل از اراکل حذف گردند.

تهدید/توجیه امنیتی

کاربران، دیدها، رویه ها و توابع پیش فرض در محیط های عملیاتی می‌توانند مورد سوء استفاده قرار بگیرند.

اطلاع از وضعیت فعلی

برای بررسی وجود کاربران نمونه می توان از دستور زیر استفاده کرد.

```
SELECT USERNAME
FROM ALL_USERS
WHERE USERNAME IN ('BI','HR','IX','OE','PM','SCOTT','SH');
```

مقاوم سازی

ابتدا می توان با دستور زیر شماهای نمونه را از سیستم حذف کرد:

```
$ORACLE_HOME/demo/schema/drop_sch.sql
```

اسکریپت فوق تمامی حساب های کاربری نمونه به غیر از SCOTT را حذف می کند. بنابراین، پس از آن با دستور زیر حساب کاربری SCOTT را نیز به همراه تمامی اشیاء وابسته به آن می توان حذف کرد.

```
DROP USER SCOTT CASCADE;
```

توجه به این نکته حائز اهمیت است که پیش از اجرای اسکریپت حذف شماها و حساب های کاربری نمونه باید این اطمینان حاصل شود که این حساب های کاربری، نام های کاربری مجاز در محیط عملیاتی نیستند.

در ادامه، هفت حساب کاربری نمونه که در زمان نصب اراکل ایجاد می‌شوند و تنها کاربرد آموزشی دارند، معرفی می‌گردند و نحوه حذف‌شان از سیستم بیان می‌شود.

۱-۲-۱ حساب کاربری نمونه BI

حساب کاربری نمونه BI مالک شمای نمونه BI[6] است.

تهدید/توجیه امنیتی:

حساب کاربری نمونه BI که ممکن است در زمان نصب ایجاد شود، یک گذرواژه پیش‌فرض دارد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود. همچنین احتمال دارد که این حساب کاربری به طریقی مجوز دسترسی به سایر داده‌های مهم موجود در پایگاه داده را به دست بیاورد که در آن صورت، خسارت ناشی از وجود چنین حساب کاربری نمونه و در واقع بی‌استفاده‌ای افزایش می‌یابد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، رکوردی برگردانده شود، این حساب کاربری نمونه در اراکل وجود دارد.

```
SELECT username FROM all_users WHERE username = 'BI';
```

مقاوم‌سازی:

با اجرای دستور زیر، این حساب کاربری نمونه و تمامی اشیاء وابسته به آن حذف می‌شوند.

```
DROP USER "BI" CASCADE;
```

۱-۲-۲ حساب کاربری نمونه HR

حساب کاربری نمونه HR مالک شمای نمونه HR[7] است.

تهدید/توجیه امنیتی:

حساب کاربری نمونه HR که ممکن است در زمان نصب ایجاد شود، یک گذرواژه پیش‌فرض دارد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود. همچنین احتمال دارد که

---

[6] Business Intelligence
[7] Human Resources

این حساب کاربری به طریقی مجوز دسترسی به سایر داده‌های مهم موجود در پایگاه داده را به دست بیاورد که در آن صورت، خسارت ناشی از وجود چنین حساب کاربری نمونه و در واقع بی‌استفاده‌ای افزایش می‌یابد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، رکوردی برگردانده شود، این حساب کاربری نمونه در اراکل وجود دارد.

```
SELECT username FROM all_users WHERE username = 'HR';
```

مقاوم‌سازی:

با اجرای دستور زیر، این حساب کاربری نمونه و تمامی اشیاء وابسته به آن حذف می‌شوند.

```
DROP USER "HR" CASCADE;
```

۳-۲-۱ حساب کاربری نمونه IX

حساب کاربری نمونه IX مالک شمای نمونه[8] IX است.

تهدید/توجیه امنیتی:

حساب کاربری نمونه IX که ممکن است در زمان نصب ایجاد شود، یک گذرواژه پیش‌فرض دارد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود. همچنین احتمال دارد که این حساب کاربری به طریقی مجوز دسترسی به سایر داده‌های مهم موجود در پایگاه داده را به دست بیاورد که در آن صورت، خسارت ناشی از وجود چنین حساب کاربری نمونه و در واقع بی‌استفاده‌ای افزایش می‌یابد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، رکوردی برگردانده شود، این حساب کاربری نمونه در اراکل وجود دارد.

```
SELECT username FROM all_users WHERE username = 'IX';
```

مقاوم‌سازی:

با اجرای دستور زیر، این حساب کاربری نمونه و تمامی اشیاء وابسته به آن حذف می‌شوند.

[8] Information eXchange

```
DROP USER "IX" CASCADE;
```

۱-۲-۴ حساب کاربری نمونه OE

حساب کاربری نمونه OE مالک شمای نمونه[9]OE است.

تهدید/توجیه امنیتی:

حساب کاربری نمونه OE که ممکن است در زمان نصب ایجاد شود، یک گذرواژه پیش‌فرض دارد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود. همچنین احتمال دارد که این حساب کاربری به طریقی مجوز دسترسی به سایر داده‌های مهم موجود در پایگاه داده را به دست بیاورد که در آن صورت، خسارت ناشی از وجود چنین حساب کاربری نمونه و در واقع بی‌استفاده‌ای افزایش می‌یابد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، رکوردی برگردانده شود، این حساب کاربری نمونه در اراکل وجود دارد.

```
SELECT username FROM all_users WHERE username = 'OE';
```

مقاوم‌سازی:

با اجرای دستور زیر، این حساب کاربری نمونه و تمامی اشیاء وابسته به آن حذف می‌شوند.

```
DROP USER "OE" CASCADE;
```

۱-۲-۵ حساب کاربری نمونه PM

حساب کاربری نمونه PM مالک شمای نمونه[1]PM است.

تهدید/توجیه امنیتی:

حساب کاربری نمونه PM که ممکن است در زمان نصب ایجاد شود، یک گذرواژه پیش‌فرض دارد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود. همچنین احتمال دارد که

[9] Order Entry
[1] Product Media [0]

این حساب کاربری به طریقی مجوز دسترسی به سایر داده‌های مهم موجود در پایگاه داده را به دست بیاورد که در آن صورت، خسارت ناشی از وجود چنین حساب کاربری نمونه و در واقع بی‌استفاده‌ای افزایش می‌یابد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، رکوردی برگردانده شود، این حساب کاربری نمونه در اراکل وجود دارد.

```
SELECT username FROM all_users WHERE username = 'PM';
```

مقاوم‌سازی:

با اجرای دستور زیر، این حساب کاربری نمونه و تمامی اشیاء وابسته به آن حذف می‌شوند.

```
DROP USER "PM" CASCADE;
```

۶-۲-۱ حساب کاربری نمونه SCOTT

حساب کاربری نمونه SCOTT در بسیاری از مثال‌های موجود در مستندات اراکل مورد استفاده قرار می‌گیرد.

تهدید/توجیه امنیتی:

حساب کاربری نمونه SCOTT که ممکن است در زمان نصب ایجاد شود، یک گذرواژه پیش‌فرض دارد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود. همچنین احتمال دارد که این حساب کاربری به طریقی مجوز دسترسی به سایر داده‌های مهم موجود در پایگاه داده را به دست بیاورد که در آن صورت، خسارت ناشی از وجود چنین حساب کاربری نمونه و در واقع بی‌استفاده‌ای افزایش می‌یابد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، رکوردی برگردانده شود، این حساب کاربری نمونه در اراکل وجود دارد.

```
SELECT username FROM all_users WHERE username = 'SCOTT';
```

مقاوم‌سازی:

با اجرای دستور زیر، این حساب کاربری نمونه و تمامی اشیاء وابسته به آن حذف می‌شوند.

```
DROP USER "SCOTT" CASCADE;
```

۱-۲-۷ حساب کاربری نمونه SH

حساب کاربری نمونه SH مالک شمای نمونهٔ SH[1] است.

تهدید/توجیه امنیتی:

حساب کاربری نمونه SH که ممکن است در زمان نصب ایجاد شود، یک گذرواژه پیش‌فرض دارد. اطلاع از این گذرواژه می‌تواند منجر به سوء استفاده از مجوزهای این حساب کاربری شود. همچنین احتمال دارد که این حساب کاربری به طریقی مجوز دسترسی به سایر داده‌های مهم موجود در پایگاه داده را به دست بیاورد که در آن صورت، خسارت ناشی از وجود چنین حساب کاربری نمونه و در واقع بی‌استفاده‌ای افزایش می‌یابد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، رکوردی برگردانده شود، این حساب کاربری نمونه در اراکل وجود دارد.

```
SELECT username FROM all_users WHERE username = 'SH';
```

مقاوم‌سازی:

با اجرای دستور زیر، این حساب کاربری نمونه و تمامی اشیاء وابسته به آن حذف می‌شوند.

```
DROP USER "SH" CASCADE;
```

۱-۳ پیکربندی فایل‌های ذخیره داده

در پایگاه داده اراکل، می‌توان مسیر ذخیره‌سازی داده‌های اصلی (مانند جداول و غیره) را با استفاده از دستور زیر به دست آورد:

```
SELECT name FROM v$datafile;
```

دید v$datafile شامل اطلاعاتی در مورد هر یک از فایل‌های داده مربوط به فضای جدول[1] در اراکل است. هر فضای جدول در پایگاه داده اراکل شامل یک یا چندین فایل داده است.

---

1 Sales History
1 Tablespace

تهدید/توجیه امنیتی:

برخلاف فایل‌های دیگر، مدیر پایگاه داده نباید مالک فایل‌های داده باشد. مالکیت فایل‌ها باید متعلق به کاربری بدون هرگونه حقوق ممتاز (مثلا کاربری با نام oracle) باشد؛ زیرا این کاربر اجازه انجام هیچ عملیاتی داخل سیستم لینوکس را ندارد. همچنین علاوه بر مدیر، هیچ‌کس دیگری نیز حق خواندن، تغییر یا اجرای فایل‌های داده را نباید داشته باشد. درنتیجه تمامی حقوق روی این فایل‌ها را از همه گرفته و مجوزهای مربوطه را تنها به کاربر oracle می‌دهیم.

اطلاع از وضعیت فعلی:

با استفاده از دستور زیر می‌توان حقوق دسترسی مربوط به فایل‌های داده را مشاهده نمود:

```
ls -lh <datafile path>
```

حقوق دسترسی، مالک و گروه کاربری مالکیت فایل‌های داده به صورت زیر می‌باشند:

```
rw-r----- oracle oinstall
```

مقاوم‌سازی:

دستورات زیر به ترتیب مالکیت، گروه کاربری مالکیت و حقوق دسترسی به فایل‌های داده را به صورت امن تعیین می‌نماید.

```
sudo  su
chown oracle <datafile>
chgrp oinstall <datafile>
chmod 640 <datafile>
```

۴ – ۱ پیکربندی فایل‌های رویدادنگاری

مهمترین ساختار در اراکل که می‌توان از آن برای عملیات بازیابی[3]استفاده کرد، redo log است. Redo log شامل دو یا چندین فایل است که تمامی تغییراتی که در پایگاه داده رخ می‌دهد را ذخیره می‌کند.

در پایگاه داده اراکل، می‌توان مسیر فایل‌های redo log را با استفاده از دستور زیر به دست آورد:

```
SELECT member FROM v$logfile;
```

[1] Recovery [3]

تهدید/توجیه امنیتی:

هیچ کاربری به جز oracle نباید حق خواندن یا نوشتن روی فایل‌های رویدادنگاری را داشته باشد. رعایت این مورد امنیتی از نشت اطلاعات این فایل‌ها جلوگیری می‌کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی مجوزهای مربوط به فایل‌های redo log، از دستور زیر استفاده می‌شود:

```
ls -lh <redolog file path>
```

حقوق دسترسی، مالک و گروه کاربری مالکیت فایل‌های رویدادنگاری به صورت زیر می‌باشند:

```
rw-r----- oracle oinstall
```

مقاوم‌سازی:

دستورات زیر به ترتیب مالکیت، گروه کاربری مالکیت و حقوق دسترسی به فایل‌های رویدادنگاری را به صورت امن مشخص می‌نمایند:

```
sudo  su
chown oracle <redolog>
chgrp oinstall <redolog>
chmod 640 <redolog>
```

۵-۱ جمع‌بندی

در این فصل به تشریح پارامترهای امنیتی محیط اجرای سمپاد که به طور مستقیم بر عملکرد آن تاثیرگذار است، پرداختیم. در این راستا، امن‌سازی حساب‌های کاربری با گذرواژه‌های پیش‌فرض، امن‌سازی حساب‌های کاربری نمونه، پیکربندی امن فایل‌های ذخیره داده و فایل‌های رویدادنگاری مورد بحث و بررسی قرار گرفت. مدیر سامانه به منظور بررسی پارامترهای مقاوم‌سازی و تهیه گزارش در این زمینه می‌تواند از چک لیست زیر استفاده نماید.

	عنوان	تنظیم صحیح	
		بله	خیر
۱	**ایمن سازی محیط اجرا**		
۱-۱	**امن‌سازی حساب‌های کاربری با گذرواژه‌های پیش‌فرض**		
۱-۱-۱	حساب کاربری APEX_040000	☐	☐

۱-۱-۲	حساب کاربری APPQOSSYS	☐	☐
۱-۱-۳	حساب کاربری CTXSYS	☐	☐
۱-۱-۴	حساب کاربری DBSNMP	☐	☐
۱-۱-۵	حساب کاربری DIP	☐	☐
۱-۱-۶	حساب کاربری EXFSYS	☐	☐
۱-۱-۷	حساب کاربری MDDATA	☐	☐
۱-۱-۸	حساب کاربری MDSYS	☐	☐
۱-۱-۹	حساب کاربری LBACSYS	☐	☐
۱-۱-۱۰	حساب کاربری OLAPSYS	☐	☐
۱-۱-۱۱	حساب کاربری ORACLE_OCM	☐	☐
۱-۱-۱۲	حساب کاربری ORDDATA	☐	☐
۱-۱-۱۳	حساب کاربری ORDPLUGINS	☐	☐
۱-۱-۱۴	حساب کاربری ORDSYS	☐	☐
۱-۱-۱۵	حساب کاربری OUTLN	☐	☐
۱-۱-۱۶	حساب کاربری OWBSYS_AUDIT	☐	☐
۱-۱-۱۷	حساب کاربری OWBSYS	☐	☐
۱-۱-۱۸	حساب کاربری SI_INFORMTN_SCHEMA	☐	☐
۱-۱-۱۹	حساب کاربری SPATIAL_CSW_ADMIN_USR	☐	☐
۱-۱-۲۰	حساب کاربری SPATIAL_WFS_ADMIN_USR	☐	☐
۱-۱-۲۱	حساب کاربری SYS	☐	☐
۱-۱-۲۲	حساب کاربری SYSTEM	☐	☐
۱-۱-۲۳	حساب کاربری WK_TEST	☐	☐
۱-۱-۲۴	حساب کاربری WKPROXY	☐	☐
۱-۱-۲۵	حساب کاربری WKSYS	☐	☐
۱-۱-۲۶	حساب کاربری WMSYS	☐	☐
۱-۱-۲۷	حساب کاربری XDB	☐	☐

۱-۲	امن‌سازی حساب‌های کاربری نمونه		
۱-۲-۱	حساب کاربری نمونه BI	☐	☐
۱-۲-۲	حساب کاربری نمونه HR	☐	☐
۱-۲-۳	حساب کاربری نمونه IX	☐	☐
۱-۲-۴	حساب کاربری نمونه OE	☐	☐
۱-۲-۵	حساب کاربری نمونه PM	☐	☐
۱-۲-۶	حساب کاربری نمونه SCOTT	☐	☐
۱-۲-۷	حساب کاربری نمونه SH	☐	☐
۱-۳	پیکربندی فایل‌های ذخیره داده	☐	☐
۱-۴	پیکربندی فایل‌های رویدادنگاری	☐	☐

۲ پیکربندی امن پایگاه‌داده

عملیات یک نمونه[۴]از پایگاه داده اراکل توسط پارامترهای متعددی تنظیم می شوند. این پارامترها در فایل‌های پیکربندی مشخصی تنظیم می‌گردند. تغییر این پارامترها می‌تواند مشکلاتی را به همراه داشته باشد. از جمله این مشکلات می‌توان به منع ارائه سرویس و سرقت اطلاعات اشاره کرد. بنابراین تنظیم پارامترها باید با دقت انجام شود. در این فصل، امنیت پارامترهای مختلف مربوط به پیکربندی اراکل مورد بررسی قرار می‌گیرد.

۲ – ۱ تنظیمات شبکه‌ای

تنظیمات مربوط به Listener که در فایل پیکربندی listener.ora قرار دارد، در این بخش مورد بررسی قرار می‌گیرد.

[1] Instance [4]

۲-۱-۱ پارامتر SECURE_CONTROL_<listener_name>

این پارامتر مشخص می‌کند که چه نوع پروتکل ارتباطی برای برقراری ارتباط با سرور به منظور اجرای کارهای مدیریتی مورد قبول است. مقادیر قابل قبول و امن برای این پارامتر، tcps (TCP/IP with SSL) و ipc هستند.

تهدید/توجیه امنیتی:

اجرای دستورات مدیریتی باید بر روی کانالی کاملا امن و غیر قابل شنود صورت گیرد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از دستور زیر استفاده می‌کنیم. در این دستور، $ORACLE_HOME مسیر نصب اراکل را نشان می‌دهد. با مشاهده خروجی می‌توان شناسایی کرد که پارامتر SECURE_CONTROL_<listener_name> چه مقداری دارد. اگر نتیجه‌ای به خروجی ارسال نگردد، یعنی تمامی پروتکل‌ها قابل قبول هستند.

```
grep -i SECURE_CONTROL $ORACLE_HOME/network/admin/listener.ora
```

مقاوم‌سازی:

برای مقاوم‌سازی این پارامتر از تمهید زیر استفاده می‌شود.

```
# add either of the following lines to listener.ora
SECURE_CONTROL_<listener_name>=tcps
SECURE_CONTROL_<listener_name>=ipc
```

۲-۱-۲ تنظیمات EXTPROC

پیکربندی مناسب Oracle Extproc اجازه اجرای رویه‌ها از درون کتابخانه‌های مشترک سیستم عامل را فراهم می‌کند. چنین کتابخانه‌هایی امکان اجرای هر دستوری در سطح سیستم عامل را دارند.

تهدید/توجیه امنیتی:

با توجه به امکان سوء استفاده مهاجم از Oracle Extproc، این امکان باید غیر فعال باشد. بدین ترتیب ریسک اجرای کتابخانه‌های سیستم عامل از درون نمونه اراکل کاهش می‌یابد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از دستور زیر استفاده می‌کنیم. چنانچه این دستور سطری را به عنوان خروجی برگرداند یعنی امکان استفاده از EXTPROC وجود دارد.

```
grep -i EXTPROC $ORACLE_HOME/network/admin/listener.ora
```

مقاوم‌سازی:

برای مقاوم‌سازی این پارامتر از تمهید زیر استفاده می‌شود.

```
# remove the lines configuring EXTPROC from listener.ora
```

۲-۱-۳ پارامتر ADMIN_RESTRICTIONS_<listener_name>

چنانچه این پارامتر مقدار ON داشته باشد، امکان تغییر پویای پارامترهای listener (با استفاده از دستور set در محیط lsnrctl) وجود ندارد و لازمه هر گونه تغییری، ویرایش فایل listener.ora است.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از امکان تغییر تنظیمات listener به طور پویا می‌تواند سیستم را دچار مشکل کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از دستور زیر استفاده می‌کنیم. با اجرای این دستور، مقدار فعلی پارامتر ADMIN_RESTRICTIONS_<listener_name> نمایش داده می‌شود. اگر دستور فوق خروجی نداشته باشد، مقدار این پارامتر، مقدار پیش‌فرض و برابر با OFF است.

```
grep -i ADMIN_RESTRICTIONS $ORACLE_HOME/network/admin/listener.ora
```

مقاوم‌سازی:

برای مقاوم‌سازی این پارامتر از تمهید زیر استفاده می‌شود.

```
# add the following line to listener.ora
ADMIN_RESTRICTIONS_<listener_name>=ON
```

۲-۱-۴ شماره پورت

به طور پیش‌فرض، اراکل از پورت ۱۵۲۱ برای listener استفاده می‌کند.

تهدید/توجیه امنیتی:

لازم است از شماره پورت دیگری استفاده گردد تا توانایی مهاجمان در شناسایی مشخصات سرور و حمله به آن کاهش یابد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از دستور زیر استفاده می‌کنیم. با بررسی خروجی این دستور می‌توان تعیین کرد که از پورت پیش‌فرض ۱۵۲۱ استفاده می‌شود یا خیر.

```
grep 1521 $ORACLE_HOME/network/admin/listener.ora
```

مقاوم‌سازی:

برای مقاوم‌سازی این پارامتر از تمهید زیر استفاده می‌شود.

```
#configure the listener to listen on a port other than 1521
```

۲-۱-۵ پارامتر SECURE_ REGISTER_<listener_name>

این پارامتر مشخص می‌کند که درخواست‌های registration با پیروی از چه پروتکل‌هایی پذیرفته می‌شوند. مقادیر قابل قبول و امن برای این پارامتر، tcps (TCP/IP with SSL) و ipc هستند.

تهدید/توجیه امنیتی:

اجرای درخواست‌های registration باید بر روی ارتباطی کاملا امن و غیر قابل شنود صورت بگیرد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از دستور زیر استفاده می‌کنیم. با مشاهده خروجی می‌توان شناسایی کرد که پارامتر SECURE_REGISTER_<listener_name> چه مقداری دارد. اگر این دستور خروجی نداشته باشد، یعنی تمامی پروتکل‌ها قابل قبول هستند.

```
grep -i SECURE_REGISTER $ORACLE_HOME/network/admin/listener.ora
```

مقاوم‌سازی:

برای مقاوم‌سازی این پارامتر از تمهید زیر استفاده می‌شود.

```
# add either of the following lines to listener.ora
SECURE_REGISTER_<listener_name>=tcps
SECURE_ REGISTER _<listener_name>=ipc
```

۲-۲ تنظیمات عمومی

در این بخش، ملاحظات امنیتی مربوط به پارامترهای عمومی پیکربندی اراکل بیان می‌گردد.

۲-۲-۱ پارامتر AUDIT_SYS_OPERATIONS

چنانچه مقدار این پارامتر TRUE باشد کلیه دستوراتی که یک کاربر با مجوز SYSOPER یا SYSDBA اجرا می‌کند، در فایل‌های سیستم عامل ثبت و رویدادنگاری می‌شوند.

تهدید/توجیه امنیتی:

چنانچه مهاجم به مجوزهای SYSOPER یا SYSDBA دسترسی داشته باشد، محدوده وسیعی از عملیات مخرب را می‌تواند انجام دهد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از دستور زیر استفاده می‌کنیم. چنانچه با اجرای این دستور، مقدار TRUE برگردانده شود، کلیه دستوراتی که یک کاربر با مجوز SYSOPER یا SYSDBA اجرا می‌کند، ثبت و رویدادنگاری می‌شوند.

```
SELECT UPPER(VALUE)FROM V$PARAMETER WHERE UPPER(NAME) =
'AUDIT_SYS_OPERATIONS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه دستوراتی که یک کاربر با مجوز SYSOPER یا SYSDBA اجرا می‌کند، ثبت و رویدادنگاری می‌شوند.

```
ALTER SYSTEM SET AUDIT_SYS_OPERATIONS = TRUE SCOPE = SPFILE;
```

۲-۲-۲ پارامتر AUDIT_TRAIL

این پارامتر چگونگی اجرای رویدادنگاری را نشان می‌دهد. مقادیر ممکن عبارتند از:

NONE: رویدادنگاری غیرفعال است.

OS: رویدادنگاری در فایل‌های تحت مدیریت سیستم‌عامل انجام می‌شود.

DB: رویدادنگاری در جدول $SYS.AUD در درون پایگاه داده انجام می‌شود (البته تعدادی از وقایع که در حالت غیر فعال بودن پایگاه داده رخ می‌دهند، تنها در فایل‌های تحت مدیریت سیستم‌عامل ثبت می‌شوند).

DB, EXTENDED: همان DB به همراه ثبت دستوارت SQL ای که باعث فعال شدن رویدادنگاری شده‌اند.

XML: رویدادنگاری در فایل‌های XML تحت مدیریت سیستم عامل انجام می‌شود.

XML, EXTENDED: همان XML به همراه ثبت دستوارت SQL ای که باعث فعال شدن رویدادنگاری شده‌اند.

تهدید/توجیه امنیتی:

فعال‌سازی ویژگی‌های پایه و اصلی ممیزی در یک نمونه از پایگاه داده اوراکل، امکان جمع آوری داده برای رفع مشکلات احتمالی را فراهم می‌سازد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از دستور زیر استفاده می‌کنیم. چنانچه با اجرای این دستور، مقدار NONE برگردانده شود، رویدادنگاری در سیستم غیر فعال است.

```
SELECT UPPER(VALUE)FROM V$PARAMETER WHERE UPPER(NAME) =
'AUDIT_TRAIL';
```

مقاوم‌سازی:

با اجرای هر کدام از دستورات زیر، رویدادنگاری فعال می‌شود.

```
ALTER SYSTEM SET AUDIT_TRAIL = DB,EXTENDED SCOPE = SPFILE;
--or
ALTER SYSTEM SET AUDIT_TRAIL = OS SCOPE = SPFILE;
--or
ALTER SYSTEM SET AUDIT_TRAIL = XML,EXTENDED SCOPE = SPFILE;
--or
ALTER SYSTEM SET AUDIT_TRAIL = DB SCOPE = SPFILE;
--or
ALTER SYSTEM SET AUDIT_TRAIL = XML SCOPE = SPFILE;
```

۳-۲-۲ پارامتر GLOBAL_NAMES

چنانچه مقدار این پارامتر TRUE باشد می‌بایست یک DATABASE LINK همنام با پایگاه داده که به آن متصل می‌شود، موجود باشد.

تهدید/توجیه امنیتی:

چنانچه مقدار این پارامتر TRUE باشد، شانس مهاجم برای سوء استفاده از امکان DATABASE LINK کاهش می‌یابد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مقدار TRUE برگردانده شود می‌بایست یک DATABASE LINK همنام با پایگاه داده که به آن متصل می‌شود موجود باشد.

```
SELECT UPPER(VALUE)FROM V$PARAMETER WHERE UPPER(NAME) =
'GLOBAL_NAMES';
```

مقاوم‌سازی:

با اجرای دستور زیر می‌بایست یک DATABASE LINK همنام با پایگاه داده‌ای که به آن متصل می‌شود موجود باشد.

```
ALTER SYSTEM SET GLOBAL_NAMES = TRUE SCOPE = SPFILE;
```

۲-۲-۴ پارامتر LOCAL_LISTENER

این پارامتر یک Network Name را مشخص می‌کند که به آدرس یک یا تعدادی Oracle Net listener بر روی سرور میزبان پایگاه داده (local) نگاشت می‌شود.

تهدید/توجیه امنیتی:

با توجه به حمله TNS poisoning که در صورت فعال بودن پروتکل TCP/IP در زمان registration رخ می‌دهد، لازم است تنها از پروتکل IPC به این منظور استفاده گردد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مشخص شود که امکان استفاده از پروتکل TCP/IP وجود دارد، می بایست از پروتکل IPC به جای TCP/IP استفاده گردد.

```
SELECT VALUE FROM V$PARAMETER WHERE UPPER(NAME) = 'LOCAL_LISTENER';
```

مقاوم‌سازی:

با اجرای دستور زیر، از پروتکل IPC استفاده می‌شود.

```
ALTER SYSTEM SET
```

```
LOCAL_LISTENER='(DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=REGISTER)))'
SCOPE = BOTH;
```

۲-۲-۵ پارامتر O7_DICTIONARY_ACCESSIBILITY

معمولا برای تسهیل در مدیریت اشیاء، مجوزهای ANY به یک سری از مدیران برنامه‌های کاربردی اعطا می‌شود. مثلا ممکن است مجوز DROP ANY TABLE به یک کاربر اعطا شود. چنین مجوز قدرتمندی می‌تواند عواقبی در پی داشته باشد. برای جلوگیری از چنین خطراتی، کافی است پارامتر O7_DICTIONARY_ACCESSIBILITY مقدار FALSE داشته باشد که در آن صورت مجوزهای ANY مانند DROP ANY TABLE برای اجرای عملیات روی جداول سیستمی قابل استفاده نیستند.

تهدید/توجیه امنیتی:

در صورتی که دسترسی به شمای SYS محدود نباشد، می‌تواند منجر به دسترسی‌های غیرمجاز به ساختارهای اطلاعاتی حساس گردد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مقدار FALSE برگردانده شود، مجوز ANY برای انجام عملیات بر روی جداول سیستمی کافی نیست.

```
SELECT UPPER(VALUE)FROM V$PARAMETER WHERE UPPER(NAME) =
'O7_DICTIONARY_ACCESSIBILITY';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز ANY برای انجام عملیات بر روی جداول سیستمی کفایت نمی‌کند.

```
ALTER SYSTEM SET O7_DICTIONARY_ACCESSIBILITY = FALSE SCOPE = SPFILE;
```

۲-۲-۶ پارامتر OS_ROLES

چنانچه مقدار این پارامتر TRUE باشد مدیریت نقش‌ها به طور کلی بر عهده سیستم عامل قرار می‌گیرد. و اگر این پارامتر FALSE باشد، خود پایگاه داده مسئول مدیریت نقش‌ها است.

تهدید/توجیه امنیتی:

با توجه به اینکه ممکن است سیستم عامل در اختیار مهاجم باشد، باید مدیریت نقش‌ها در سطح خود پایگاه‌داده انجام شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مقدار FALSE برگردانده شود، پایگاه داده مسوول مدیریت نقش‌ها است.

```
SELECT UPPER(VALUE)FROM V$PARAMETER WHERE UPPER(NAME) = 'OS_ROLES';
```

مقاوم‌سازی:

با اجرای دستور زیر، پایگاه داده و نه سیستم‌عامل مسئول مدیریت نقش‌ها می‌شود.

```
ALTER SYSTEM SET OS_ROLES = FALSE SCOPE = SPFILE;
```

۲-۲-۷ پارامتر REMOTE_LISTENER

این پارامتر یک Network Name را مشخص می‌کند که به آدرس یک یا تعدادی Oracle Net listener بر روی ماشینی مجزا از سرور میزبان پایگاه داده (یک ماشین remote) نگاشت می‌شود.

تهدید/توجیه امنیتی:

چنانچه استفاده از remote listener امکان پذیر باشد، مهاجم امکان شنود یا اعمال تغییر در ارتباطات را به راحتی به دست می‌آورد. در نتیجه بهتر است این امکان غیر فعال گردد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، سطری برگردانده نشود، امکان remote listener غیرفعال است.

```
SELECT UPPER(VALUE)FROM V$PARAMETER WHERE UPPER(NAME) =
'REMOTE_LISTENER';
```

مقاوم‌سازی:

با اجرای دستور زیر، امکان remote listener غیرفعال می‌شود.

```
ALTER SYSTEM SET REMOTE_LISTENER = '' SCOPE = SPFILE;
```

۲-۲-۸ پارامتر REMOTE_LOGIN_PASSWORDFILE

چنانچه مقدار این پارامتر NONE باشد مدیران پایگاه‌داده برای انجام یک سری از فعالیت‌های مدیریتی باید توسط سیستم عامل احراز اصالت شوند. در غیر این صورت، یک سری اطلاعات مربوط به احراز اصالت در فایل گذرواژه ذخیره می‌شود.

تهدید/توجیه امنیتی:

مهاجم با شناسایی و سوء استفاده از فایل گذرواژه قادر است فرایند احراز اصالت را دچـار اخـتلال کنـد و در نتیجه توصیه می‌شود این پارامتر دارای مقدار NONE باشد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مقدار NONE برگردانده شود، استفاده از فایل گذرواژه غیر فعال است.

```
SELECT UPPER(VALUE)FROM V$PARAMETER WHERE UPPER(NAME) =
'REMOTE_LOGIN_PASSWORDFILE';
```

مقاوم‌سازی:

با اجرای دستور زیر، استفاده از فایل گذرواژه غیر فعال می‌شود.

```
ALTER SYSTEM SET REMOTE_LOGIN_PASSWORDFILE = 'NONE' SCOPE = SPFILE;
```

۹-۲-۲ پارامتر REMOTE_OS_AUTHENT

چنانچه مقدار این پارامتر TRUE باشد یک کاربر راه دور[۵] پس از تصدیق اصـالت در سیسـتم عامـل خـودش می‌تواند در پایگاه داده فعالیت کند.

تهدید/توجیه امنیتی:

با توجه به عدم اطمینان به امن بودن رایانه کاربر راه دور، این امکان باید غیر فعال باشد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مقدار FALSE برگردانده شود، این امکان غیر فعال است.

```
SELECT UPPER(VALUE)FROM V$PARAMETER WHERE UPPER(NAME) =
'REMOTE_OS_AUTHENT';
```

مقاوم‌سازی:

با اجرای دستور زیر، این امکان غیر فعال می‌شود.

---

[1] Remote [5]

```
ALTER SYSTEM SET REMOTE_OS_AUTHENT = FALSE SCOPE = SPFILE;
```

۲-۲-۱۰ پارامتر REMOTE_OS_ROLES

چنانچه مقدار این پارامتر TRUE باشد نقش‌های تحت مدیریت سیستم عامل رایانه کاربر راه دور، توسط پایگاه داده به رسمیت شناخته می‌شوند.

تهدید/توجیه امنیتی:

با توجه به عدم اطمینان به امن بودن رایانه کاربر راه دور، این امکان باید غیر فعال باشد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مقدار FALSE برگردانده شود، این امکان غیر فعال است.

```
SELECT UPPER(VALUE)FROM V$PARAMETER WHERE UPPER(NAME) =
'REMOTE_OS_ROLES';
```

مقاوم‌سازی:

با اجرای دستور زیر، این امکان غیر فعال می‌شود.

```
ALTER SYSTEM SET REMOTE_OS_ROLES = FALSE SCOPE = SPFILE;
```

۲-۲-۱۱ پارامتر UTL_FILE_DIR

این پارامتر، مسیرهایی را مشخص می‌کند که کاربران پایگاه داده می‌توانند با استفاده از بسته‌ها[1]ایی همچون UTL_FILE به آن مسیرها دسترسی پیدا کنند و عملیات خواندن/نوشتن/حذف/تغییر فایلی را انجام دهند.

تهدید/توجیه امنیتی:

اگر این پارامتر مقدار معتبر داشته باشد، مهاجم با سوء استفاده از آن قادر است در سطح سیستم فایل خرابکاری کند.

اطلاع از وضعیت فعلی:

[1] Package

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، null برگردانده شود، هیچ مسیری برای UTL_FILE_DIR وجود ندارد.

```
SELECT VALUE  FROM V$PARAMETER WHERE UPPER(NAME)='UTL_FILE_DIR';
```

مقاوم‌سازی:

با اجرای دستور زیر، UTL_FILE_DIR هیچ مسیری را معین نمی‌کند.

```
ALTER SYSTEM SET UTIL_FILE_DIR = '' SCOPE = SPFILE;
```

۲-۲-۱۲ پارامتر SEC_CASE_SENSITIVE_LOGON

چنانچه مقدار این پارامتر TRUE باشد، گذرواژه حساس به حروف[۱] خواهد بود.

تهدید/توجیه امنیتی:

در صورتی که گذرواژه نسبت به حروف حساس باشد، نه تنها کاراکترهایی که برای گذرواژه می توان انتخاب کرد بیشتر خواهند بود، بلکه حمله های brute force نیز دشوارتر می شوند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مقدار TRUE برگردانده شود، گذرواژه حساس به حروف است.

```
SELECT UPPER(VALUE)FROM V$PARAMETER WHERE UPPER(NAME) =
'SEC_CASE_SENSITIVE_LOGON';
```

مقاوم‌سازی:

با اجرای دستور زیر، این پارامتر مقدار مناسب را خواهد گرفت.

```
ALTER SYSTEM SET SEC_CASE_SENSITIVE_LOGON = TRUE SCOPE = SPFILE;
```

---

[1] Case Sensitive [7]

۲-۲-۱۳ پارامتر SEC_MAX_FAILED_LOGIN_ATTEMPTS

این پارامتر تعداد دفعاتی را مشخص می‌کند که یک کاربر می‌تواند به طور متوالی برای ورود به پایگاه داده تلاش کند پیش از آن که سرور اتصال را قطع نماید. مقادیر ممکن برای این پارامتر UNLIMITED (به معنای نامحدود)، یک و اعداد بزرگتر از یک است.

تهدید/توجیه امنیتی:

چنانچه مقدار این پارامتر نامحدود باشد، یک مهاجم امکان اجرای حمله Brute Force و منع سرویس[۱۸] را به دست می‌آورد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مقدار UNLIMITED برگردانده شود، هیچ محدودیت در این مورد وجود ندارد.

```
SELECT UPPER(VALUE)FROM V$PARAMETER WHERE UPPER(NAME) =
'SEC_MAX_FAILED_LOGIN_ATTEMPTS';
```

مقاوم‌سازی:

با اجرای دستور زیر، مقدار این پارامتر عدد ۳ تعیین می‌شود.

```
ALTER SYSTEM SET SEC_MAX_FAILED_LOGIN_ATTEMPTS = 3 SCOPE = SPFILE;
```

۲-۲-۱۴ پارامتر SEC_PROTOCOL_ERROR_FURTHER_ACTION

این پارامتر عکس العمل پردازه سرور را در برابر دریافت یک بسته معیوب از کلاینت مشخص می‌کند که می‌تواند به صورت‌های زیر باشد:

- CONTINIUE: پردازه سرور با اجرای خود و پاسخگویی به سایر درخواست‌های کاربر ادامه می‌دهد. در این وضعیت، سرور در معرض حمله منع سرویس قرار دارد (مثلا TCP SYN Flood).
- (DELAY,integer): پردازه سرور به اندازه integer ثانیه در پاسخگویی به سایر درخواست‌های کاربر وقفه ایجاد می‌کند.
- (DROP,integer): پردازه سرور پس از دریافت integer بسته معیوب، اتصال را قطع می‌کند.

---

[1] Denial of Service Attack [8]

تهدید/توجیه امنیتی:

دریافت بسته‌های معیوب از جانب کلاینت می‌تواند نشان‌دهنده حملات مبتنی بر بسته[9]همچون TCP SYN Flood یا Smurf باشد. این حملات منجر به منع سرویس می‌شوند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مقدار CONTINIUE برگردانده شود، سرور عکس العمل مناسبی در برابر دریافت بسته‌های معیوب از خود نشان نمی‌دهد.

```
SELECT UPPER(VALUE)FROM V$PARAMETER WHERE UPPER(NAME) =
'SEC_PROTOCOL_ERROR_FURTHER_ACTION';
```

مقاوم‌سازی:

با اجرای دستور زیر، با دریافت سه بسته معیوب، ارتباط میان سرور و کاربر قطع می‌شود.

```
ALTER SYSTEM SET SEC_PROTOCOL_ERROR_FURTHER_ACTION = 'DROP,3' SCOPE =
SPFILE;
```

۱۵-۲-۲ پارامتر SEC_PROTOCOL_ERROR_TRACE_ACTION

این پارامتر نحوه ثبت رویداد دریافت یک بسته معیوب از یک کاربر را مشخص می‌کند که می‌تواند به صورت‌های زیر باشد.

- NONE: این رویداد ثبت نمی‌شود.
- TRACE: یک فایل ردگیری ایجاد می‌شود و جزئیات مربوط به رخداد این مساله در آن ثبت می‌شود تا در آینده قابل پیگیری باشد.
- LOG: یک پیام هشدار با حداقل اطلاعات در مورد این رویداد تولید و در فایل‌های ثبت سرور درج می‌شود.
- ALERT: یک پیام هشدار تولید و به مدیر سیستم ارسال می‌شود.

تهدید/توجیه امنیتی:

---

[1] Packet-based Attack [9]

با ثبت رویدادهای مربوط به دریافت بسته‌های معیوب می‌توان برای رفع مشکل و احتمالا شناسایی عامل عمدی رخداد آن اقدام کرد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، چنانچه با اجرای پرس و جوی فوق، مقدار NONE برگردانده شود، رویداد بسته معیوب ثبت نمی‌شود.

```
SELECT UPPER(VALUE) FROM V$PARAMETER WHERE UPPER(NAME) =
'SEC_PROTOCOL_ERROR_TRACE_ACTION';
```

مقاوم‌سازی:

با اجرای دستور زیر، رویداد بسته معیوب به صورت LOG ثبت می‌شود.

```
ALTER SYSTEM SET SEC_PROTOCOL_ERROR_TRACE_ACTION = LOG SCOPE =
SPFILE;
```

۱۶-۲-۲ پارامتر SEC_RETURN_SERVER_RELEASE_BANNER

چنانچه مقدار این پارامتر TRUE باشد اطلاعات کاملی در مورد نرم‌افزار پایگاه‌داده و نسخه نصب شده آن به کاربر متقاضی ارسال می‌شود.

تهدید/توجیه امنیتی:

مهاجم با دسترسی به این اطلاعات و آگاهی از کاستی‌های امنیتی نسخه‌های مختلف اراکل، قادر است امنیت سیستم را به خطر بیاندازد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مقدار FALSE برگردانده شود، یک سری اطلاعات کلی و نه نسخه دقیق نرم‌افزار نصب شده به کاربر برگردانده می‌شود.

```
SELECT UPPER(VALUE) FROM V$PARAMETER WHERE UPPER(NAME) =
'SEC_RETURN_SERVER_RELEASE_BANNER';
```

مقاوم‌سازی:

با اجرای دستور زیر، این پارامتر مقدار FALSE می‌گیرد.

```
ALTER SYSTEM SET SEC_RETURN_SERVER_RELEASE_BANNER = FALSE SCOPE =
SPFILE;
```

۲-۲-۱۷ پارامتر SQL92_SECURITY

چنانچه مقدار این پارامتر FALSE باشد این امکان وجود دارد که یک کاربر پرسمان UPDATE یا DELETE روی یک جدول اجرا کند و پرسمانش دارای where clause غیر تهی باشد، ولی کاربر روی آن جدول مجوز SELECT نداشته باشد.

تهدید/توجیه امنیتی:

یک کاربر بدون مجوز SELECT می‌تواند مقادیر ذخیره شده در یک ستون را با به کارگیری آن ستون در عبارات UPDATE و DELETE استنتاج کند. این تنظیم، تنها به کاربرانی که مجوز SELECT دارند، اجازه اجرای عباراتی همچون UPDATE و DELETE که با استفاده از آن‌ها می‌توان مقادیر ذخیره شده را استنتاج کرد، می‌دهد و بدین ترتیب جلوی افشای اطلاعات به صورت غیرعمدی را می‌گیرد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مقدار TRUE برگردانده شود، لازمه اجرای دستورات UPDATE و DELETE با where clause غیر تهی، دسترسی به مجوز SELECT است.

```
SELECT UPPER(VALUE)FROM V$PARAMETER WHERE UPPER(NAME) =
'SQL92_SECURITY';
```

مقاوم‌سازی:

با اجرای دستور زیر، برای اجرای دستورات UPDATE و DELETE با where clause غیر تهی، نیاز به دسترسی به مجوز SELECT است.

```
ALTER SYSTEM SET SQL92_SECURITY = TRUE SCOPE = SPFILE;
```

۲-۲-۱۸ پارامتر _trace_files_public

چنانچه مقدار این پارامتر TRUE باشد فایل ردگیری سیستم توسط همگان قابل خواندن است. لازم به ذکر است که مجوز خواندن در سطح سیستم عامل به همگان اعطا شده است.

تهدید/توجیه امنیتی:

با توجه به اینکه ممکن است فایل ردگیری حاوی اطلاعات حساس و محرمانه باشد، نباید توسط همگان قابل خواندن باشد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مقدار TRUE برگردانده شود، فایل ردگیری سیستم توسط همگان قابل خواندن است.

```
SELECT VALUE FROM V$PARAMETER WHERE LOWER(NAME) =
'_trace_files_public';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز خواند فایل ردگیری از همگان لغو می‌گردد.

```
ALTER SYSTEM SET "_trace_files_public" = FALSE SCOPE = SPFILE;
```

۱۹-۲-۲ پارامتر RESOURCE_LIMIT

این پارامتر تعیین می‌کند که آیا محدودیت منابع در پروفایل‌های پایگاه داده اعمال می‌شود یا خیر.

تهدید/توجیه امنیتی:

در صورتی که مقدار این پارامتر FALSE باشد، هیچ یک از محدودیت‌های منابع سیستم که در پروفایل‌های پایگاه داده تنظیم شده‌اند، اعمال نخواهند شد. مقدار این پارامتر باید TRUE باشد تا جلوی کاربران برای اجرای عملیاتی که منابع زیادی از سیستم را مصرف می‌کند، گرفته شود. با اعمال محدودیت‌های منابع می‌توان مطمئن شد که کاربران نشست‌های طولانی مدت با پایگاه داده برقرار نمی‌کنند [۲].

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی این پارامتر از پرسمان زیر استفاده می‌شود. چنانچه با اجرای این پرسمان، مقدار TRUE برگردانده شود، محدودیت های تنظیم شده در پروفایل های پایگاه داده اعمال می شوند.

```
SELECT UPPER(VALUE)
FROM V$PARAMETER
WHERE UPPER(NAME)='RESOURCE_LIMIT';
```

مقاوم‌سازی:

با اجرای دستور زیر، محدودیت‌های تنظیم شده در پروفایل‌های پایگاه‌داده اعمال می‌شوند.

```
ALTER SYSTEM SET RESOURCE_LIMIT = TRUE SCOPE = SPFILE;
```

۲-۳ بسته‌های تکمیلی اراکل Oracle Patches

معمولا پس از ارایه هر نسخه اصلی اراکل، تعدادی بسته‌های تکمیلی (نسخه فرعی) به منظور رفع مشکلات شناسایی شده امنیتی و عملکردی نسخه اصلی توسط شرکت اراکل ارایه می‌شود. توصیه می‌شود همواره آخرین بسته‌های تکمیلی ارائه شده موجود، بر روی نسخه نصب شده از پایگاه داده اراکل اعمال گردد.

تهدید/توجیه امنیتی:

در زمان ارایه بسته‌های تکمیلی جدید، مشکلات امنیتی نسخه‌های قبلی اراکل که با نصب آن بسته‌های تکمیلی برطرف می‌شوند، به طور علنی در اختیار عموم قرار می‌گیرد. در نتیجه یک مهاجم، با مطلع شدن از این مشکلات امنیتی، قادر است امنیت نسخه‌های نصب شده قدیمی اراکل (که افزونه بر روی آنها اعمال نشده است) را تهدید کند.

اطلاع از وضعیت فعلی:

دید dba_registry_history حاوی اطلاعات مربوط به نسخه نصب شده اراکل و بسته‌های تکمیلی اعمال شده بر روی آن است.

```
SELECT * FROM dba_registry_history;
```

همچنین با استفاده از دستور زیر می‌توان نسبت به نصب آخرین نسخه بسته‌های تکمیلی اراکل اطمینان حاصل کرد.

```
opatch lsinventory | grep -e "^.*<latest_patch_version_numer>\s*.*$"
```

مقاوم‌سازی:

با ورود به پیوند زیر، می‌توان آخرین بسته‌های تکمیلی مربوط به پایگاه‌داده اراکل را دانلود و نصب کرد.

```
--Download the appropriate patch and apply it to the installed
version.
--          http://www.oracle.com/technetwork/topics/security/alerts-
086861.html
```

۲-۴ جمع‌بندی

در این فصل به تشریح برخی از مهم‌ترین پارامترهای امنیتی مربوط به پیکربندی سمپاد قبل از بکارگیری عملیاتی آن پرداختیم. در این راستا، تنظیمات شبکه‌ای، تنظیمات عمومی و بسته‌های تکمیلی اراکل مورد بحث و بررسی قرار گرفت. مدیر سامانه به منظور بررسی پارامترهای مقاوم‌سازی و تهیه گزارش در این زمینه می‌تواند از چک لیست زیر استفاده نماید.

	عنوان	تنظیم صحیح	
		بله	خیر
۲	**پیکربندی امن پایگاه‌داده**		
	تنظیمات شبکه‌ای		
۲-۱	پارامتر <SECURE_CONTROL_<listener_name>	☐	☐
۲-۲	تنظیمات EXTPROC	☐	☐
۲-۳	پارامتر <ADMIN_RESTRICTIONS_<listener_name>	☐	☐
۲-۴	شماره پورت	☐	☐
۲-۵	پارامتر <SECURE_ REGISTER_<listener_name>	☐	☐
	تنظیمات عمومی		
۲-۶	پارامتر AUDIT_SYS_OPERATIONS	☐	☐
۲-۷	پارامتر AUDIT_TRAIL	☐	☐
۲-۸	پارامتر GLOBAL_NAMES	☐	☐
۲-۹	پارامتر LOCAL_LISTENER	☐	☐
۲-۱۰	پارامتر O7_DICTIONARY_ACCESSIBILITY	☐	☐
۲-۱۱	پارامتر OS_ROLES	☐	☐
۲-۱۲	پارامتر REMOTE_LISTENER	☐	☐
۲-۱۳	پارامتر REMOTE_LOGIN_PASSWORDFILE	☐	☐
۲-۱۴	پارامتر REMOTE_OS_AUTHENT	☐	☐
۲-۱۵	پارامتر REMOTE_OS_ROLES	☐	☐
۲-۱۶	پارامتر UTL_FILE_DIR	☐	☐
۲-۱۷	پارامتر SEC_CASE_SENSITIVE_LOGON	☐	☐
۲-۱۸	پارامتر SEC_MAX_FAILED_LOGIN_ATTEMPTS	☐	☐
۲-۱۹	پارامتر SEC_PROTOCOL_ERROR_FURTHER_ACTION	☐	☐
۲-۲۰	پارامتر SEC_PROTOCOL_ERROR_TRACE_ACTION	☐	☐

۲-۲۱	پارامتر SEC_RETURN_SERVER_RELEASE_BANNER	☐	☐
۲-۲۲	پارامتر SQL92_SECURITY	☐	☐
۲-۲۳	پارامتر _trace_files_public	☐	☐
۲-۲۴	پارامتر RESOURCE_LIMIT	☐	☐
سایر تنظیمات			
۲-۲۵	نصب بسته‌های تکمیلی اراکل	☐	☐

۳ امن سازی اتصال به پایگاه‌داده

در اراکل مفهومی به نام پروفایل ایجاد شده است که با استفاده از آن می‌توان یک سری سیاست‌های امنیتی را در مورد اتصال و ورود کاربران به پایگاه داده اعمال کرد. به طور پیش‌فرض، هر حساب کاربری که ایجاد می‌شود، سیاست‌های مشخص شده در پروفایل پیش‌فرض (با عنوان DEFAULT) بر روی آن حساب کاربری اعمال می‌شوند. در این بخش، پارامترهای مختلف موجود در این پروفایل و مقادیر آن معرفی می‌شود. همچنین یک سری مقادیر پیشنهاد می‌شود که در صورت استفاده از آن‌ها، یک سطح حداقلی از امنیت در مورد اتصال و ورود کاربران به اراکل برآورده می‌گردد. چنانچه در داخل سیستم پروفایل‌های دیگری نیز تعریف شده است و مورد استفاده قرار می‌گیرد، باید مقادیر پارامترهای مختلف در آن پروفایل‌ها نیز وارسی و در صورت نیاز اصلاح گردند.

۳-۱ پارامتر FAILED_LOGIN_ATTEMPTS

این پارامتر تعداد دفعات متوالی تلاش ناموفق یک کاربر برای ورود به اراکل قبل از اینکه حساب کاربری‌اش قفل و غیرفعال گردد را نشان می‌دهد.

تهدید/توجیه امنیتی:

تلاش متوالی و ناموفق برای ورود به سیستم می‌تواند نشانه تلاش یک مهاجم برای حدس زدن گذرواژه یک کاربر مجاز باشد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از دستور زیر استفاده می‌شود.

```
SELECT LIMIT FROM DBA_PROFILES WHERE PROFILE = 'DEFAULT' AND
RESOURCE_NAME = 'FAILED_LOGIN_ATTEMPTS';
```

در صورتی که پرسمان زیر خروجی داشته باشد، مقدار مناسبی برای پارامتر مذکور تنظیم نشده است.

```
SELECT PROFILE, RESOURCE_NAME, LIMIT
FROM DBA_PROFILES
WHERE RESOURCE_NAME='FAILED_LOGIN_ATTEMPTS'
AND
(LIMIT = 'DEFAULT'
OR LIMIT = 'UNLIMITED'
OR LIMIT > 5);
```

مقاوم‌سازی:

با اجرای دستور زیر، پارامتر FAILED_LOGIN_ATTEMPTS با عدد ۵ مقداردهی می‌شود.

```
ALTER PROFILE DEFAULT LIMIT FAILED_LOGIN_ATTEMPTS 5;
```

لازم به ذکر است اینگونه مقداردهی ممکن است منجر به رخداد حمله منع سرویس بر روی اراکل گردد. از آنجاییکه در چنین شرایطی، مهاجم با ارسال ۵ رشته دلخواه به عنوان گذرواژه برای هر حساب کاربری می‌تواند آن حساب کاربری را غیر فعال کند. چنانچه رخداد چنین حمله‌ای محتمل باشد، بهتر است این پارامتر با مقدار UNLIMITED مقداردهی گردد.

```
ALTER PROFILE DEFAULT LIMIT FAILED_LOGIN_ATTEMPTS UNLIMITED;
```

در حقیقت دو دستور فوق، بنابر نیاز برای هر یک از پروفایل‌ها می‌تواند به صورت زیر اجرا می شود.

```
ALTER PROFILE <profile_name> LIMIT FAILED_LOGIN_ATTEMPTS 5;
```

۳-۲ پارامتر PASSWORD_LOCK_TIME

این پارامتر تعداد روزهایی را نشان می‌دهد که بعد از قفل و غیر فعال شدن یک حساب کاربری (در اثر رسیدن به محدودیت FAILED_LOGIN_ATTEMPTS) باید سپری شود تا حساب کاربری مجددا باز و فعال شود.

تهدید/توجیه امنیتی:

اگر پس از قفل شدن یک حساب کاربری (در اثر وارد کردن اشتباهی گذرواژه در تعداد دفعات زیاد)، راهی برای فعال شدن مجدد حساب به صورت خودکار (و پس از سپری شدن یک زمان مشخص) وجود نداشته باشد، میزان موفقیت حمله منع سرویس بر روی اراکل افزایش می‌یابد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از دستور زیر استفاده می‌شود.

```
SELECT LIMIT FROM DBA_PROFILES WHERE PROFILE = 'DEFAULT' AND
RESOURCE_NAME = 'PASSWORD_LOCK_TIME';
```

همچنین، در صورتی که دستور زیر خروجی داشته باشد، پروفایل های لیست شده دارای مقدار مناسب برای این پارامتر نیستند.

```
SELECT PROFILE, RESOURCE_NAME, LIMIT
FROM DBA_PROFILES
WHERE RESOURCE_NAME='PASSWORD_LOCK_TIME'
```

```
AND
(LIMIT = 'DEFAULT'
OR LIMIT = 'UNLIMITED'
OR LIMIT < 1);
```

مقاوم‌سازی:

با اجرای دستور زیر، طول دوره زمانی قفل ماندن یک حساب کاربری، یک روز تعیین می‌گردد.

```
ALTER PROFILE DEFAULT LIMIT PASSWORD_LOCK_TIME 1;
```

با استفاده از دستور زیر برای تمامی پروفایل هایی که مقدار مناسبی برای این پارامتر ندارند، طول دوره زمانی قفل ماندن یک حساب کاربری، یک روز تعیین می‌گردد.

```
ALTER PROFILE <profile_name> LIMIT PASSWORD_LOCK_TIME 1;
```

۳-۳ پارامتر PASSWORD_LIFE_TIME

این پارامتر تعداد روزهایی را نشان می‌دهد که کاربر قادر است از یک گذرواژه استفاده کند. با سپری شدن این بازه زمانی، لازم است گذرواژه جدیدی انتخاب گردد.

تهدید/توجیه امنیتی:

اگر گذرواژه برای مدت زمان طولانی ثابت باشد، شانس مهاجم برای شناسایی آن از طریق اجرای حمله Brute Force افزایش می‌یابد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از دستور زیر استفاده می‌شود.

```
SELECT LIMIT FROM DBA_PROFILES WHERE PROFILE = 'DEFAULT' AND
RESOURCE_NAME = 'PASSWORD_LIFE_TIME';
```

در صورتی که دستور زیر لیستی از پروفایل ها را به نمایش درآورد، پروفایل‌های لیست شده دارای مقدار مناسبی برای این پارامتر نیستند.

```
SELECT PROFILE, RESOURCE_NAME, LIMIT
FROM DBA_PROFILES
WHERE RESOURCE_NAME='PASSWORD_LIFE_TIME'
AND
(LIMIT = 'DEFAULT'
```

```
OR LIMIT = 'UNLIMITED'
OR LIMIT > 90);
```

مقاوم‌سازی:

با اجرای دستور زیر، مقدار این پارامتر ۹۰ روز تعیین می‌گردد.

```
ALTER PROFILE DEFAULT LIMIT PASSWORD_LIFE_TIME 90;
```

دستور زیر برای تمامی پروفایل هایی که مقدار مناسبی برای این پارامتر ندارند، باید اجرا می شود.

```
ALTER PROFILE <profile_name> LIMIT PASSWORD_LIFE_TIME 90;
```

۳-۴ پارامتر PASSWORD_REUSE_MAX

این پارامتر، تعداد گذرواژه‌های متمایزی را نشان می‌دهد که باید توسط یک کاربر انتخاب شوند تا او بتواند از یک گذرواژه قدیمی دوباره استفاده کند.

تهدید/توجیه امنیتی:

معمولا کاربران تمایل دارند از یک یا تعدادی گذرواژه ثابت استفاده کنند و حتی در صورت دریافت تقاضا برای تعویض گذرواژه نیز همچنان گذرواژه‌های قبلی خود را انتخاب می‌کنند. استفاده مجدد از گذرواژه‌های قدیمی در طول مدت زمان کوتاه خطر موفقیت در حملات Brute Force و مهندسی اجتماعی[۲] را افزایش می دهد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از دستور زیر استفاده می‌شود.

```
SELECT LIMIT FROM DBA_PROFILES WHERE PROFILE = 'DEFAULT' AND
RESOURCE_NAME = 'PASSWORD_REUSE_MAX';
```

در صورتی که دستور زیر لیستی از پروفایل ها را به نمایش درآورد، پروفایل‌های لیست شده دارای مقدار مناسبی برای این پارامتر نیستند.

```
SELECT PROFILE, RESOURCE_NAME, LIMIT
FROM DBA_PROFILES
```

[2] Social Engineering

```
WHERE RESOURCE_NAME='PASSWORD_REUSE_MAX'
AND
(LIMIT = 'DEFAULT'
OR LIMIT = 'UNLIMITED'
OR LIMIT < 20);
```

مقاوم‌سازی:

با اجرای دستور فوق، این پارامتر با عدد ۲۰ مقداردهی می‌شود.

```
ALTER PROFILE DEFAULT LIMIT PASSWORD_REUSE_MAX 20;
```

با استفاده از دستور زیر، تمامی پروفایل‌هایی که مقدار مناسبی برای این پارامتر ندارند، باید مقدار ۲۰ برای آنها تعیین گردد.

```
ALTER PROFILE <profile_name> LIMIT PASSWORD_REUSE_MAX 20;
```

۳-۵ پارامتر PASSWORD_REUSE_TIME

این پارامتر، تعداد روزهایی را نشان می‌دهد که باید سپری تا یک کاربر بتواند از یک گذرواژه قدیمی دوباره استفاده نماید.

تهدید/توجیه امنیتی:

معمولا کاربران تمایل دارند از یک یا تعدادی گذرواژه ثابت استفاده کنند و حتی در صورت دریافت تقاضا برای تعویض گذرواژه نیز همچنان گذرواژه‌های قبلی خود را انتخاب می‌کنند. استفاده مجدد از گذرواژه‌های قدیمی در طول مدت زمان کوتاه خطر موفقیت در حملات Brute Force را افزایش می‌دهد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود.

```
SELECT LIMIT FROM DBA_PROFILES WHERE PROFILE = 'DEFAULT' AND
RESOURCE_NAME = 'PASSWORD_REUSE_TIME';
```

در صورتی که دستور زیر لیستی از پروفایل‌ها را به نمایش درآورد، پروفایل‌های لیست شده دارای مقدار مناسبی برای این پارامتر نیستند.

```
SELECT PROFILE, RESOURCE_NAME, LIMIT
FROM DBA_PROFILES
WHERE RESOURCE_NAME='PASSWORD_REUSE_TIME'
```

```
AND
(LIMIT = 'DEFAULT'
OR LIMIT = 'UNLIMITED'
OR LIMIT < 365);
```

مقاوم‌سازی:

با اجرای دستور زیر، این پارامتر با عدد ۳۶۵ مقداردهی می‌شود.

```
ALTER PROFILE DEFAULT PASSWORD_REUSE_TIME 365;
```

دستور فوق می‌بایست برای تمامی پروفایل هایی که مقدار مناسبی برای این پارامتر ندارند، اجرا شود.

```
ALTER PROFILE <profile_name> LIMIT PASSWORD_REUSE_TIME 365;
```

۳-۶ پارامتر PASSWORD_GRACE_TIME

این پارامتر تعداد روزهایی را نشان می‌دهد که پس از منقضی شدن اعتبار یک گذرواژه، همچنان کاربر قادر است با استفاده از گذرواژه منقضی شده وارد سیستم گردد و در این فرصت، گذرواژه جدیدی برای خود انتخاب کند.

تهدید/توجیه امنیتی:

با مقداردهی مناسب این پارامتر، می‌توان از سوء استفاده از گذرواژه‌های منقضی شده جلوگیری کرد و همچنین فرصتی به کاربران مجاز داد تا گذرواژه خود را عوض کنند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از دستور زیر استفاده می‌شود.

```
SELECT LIMIT FROM DBA_PROFILES WHERE PROFILE = 'DEFAULT' AND
RESOURCE_NAME = 'PASSWORD_GRACE_TIME';
```

در صورتی که دستور زیر لیستی از پروفایل‌ها را به نمایش درآورد، پروفایل‌های لیست شده دارای مقدار مناسبی برای این پارامتر نیستند.

```
SELECT PROFILE, RESOURCE_NAME, LIMIT
FROM DBA_PROFILES
WHERE RESOURCE_NAME='PASSWORD_GRACE_TIME'
AND
(LIMIT = 'DEFAULT'
```

```
OR LIMIT = 'UNLIMITED'
OR LIMIT > 5);
```

مقاوم‌سازی:

با اجرای دستور زیر، مقدار این پارامتر پنج روز تعیین می‌گردد.

```
ALTER PROFILE DEFAULT LIMIT PASSWORD_GRACE_TIME 5;
```

دستور فوق می‌بایست برای تمامی پروفایل‌هایی که مقدار مناسبی برای این پارامتر ندارند، اجرا شود.

```
ALTER PROFILE <profile_name> LIMIT PASSWORD_GRACE_TIME 5;
```

۳-۷ پارامتر AUTHENTICATION_TYPE

چنانچه نوع احراز اصالت یک کاربر، خارجی باشد، یعنی احراز اصالت بر عهده سیستم‌عامل راه دور[1] است و عملا اراکل بدون نیاز به گذرواژه کاربر به او اجازه ورود به سیستم را می‌دهد.

تهدید/توجیه امنیتی:

چنانچه سیستم‌عامل راه دور در اختیار مهاجم قرار گیرد، مهاجم می‌تواند از کلیه مجوزهایش سوء استفاده کند بدون اینکه لازم باشد گذرواژه‌ای را به دست آورد.

اطلاع از وضعیت فعلی:

با استفاده از پرسمان زیر، لیست کاربرانی که احراز اصالت خارجی برایشان فعال شده است، نشان داده می‌شود.

```
SELECT USERNAME FROM DBA_USERS WHERE AUTHENTICATION_TYPE =
'EXTERNAL';
```

مقاوم‌سازی:

با اجرای دستور زیر برای کلیه کاربرانی که احراز اصالت خارجی برایشان فعال شده است، دریافت گذرواژه از آن‌ها الزامی می‌شود.

```
ALTER USER <username> IDENTIFIED BY <password>;
```

---

[1] Remote [2]

۳-۸ پارامتر PASSWORD_VERIFY_FUNCTION

این پارامتر تابعی را مشخص می‌کند که باید روی گذرواژه انتخاب شده توسط کاربر اجرا شود و میزان پیچیدگی گذرواژه را تعیین نماید.

تهدید/توجیه امنیتی:

معمولا کاربران گذرواژه‌های ساده انتخاب می‌کنند که به راحتی قابل حدس است. با اعمال یک تابع وارسی‌کننده می‌توان کاربر را مجبور کرد که حداقلی از پیچیدگی را در گذرواژه خود لحاظ کند. مثلا گذرواژه ترکیبی از حروف الفبایی بزرگ و کوچک، اعداد و کاراکترهای غیر الفبایی باشد و حداقل طول گذرواژه ۸ کاراکتر باشد.

اطلاع از وضعیت فعلی:

خروجی حاصل از پرسمان زیر نشان می‌دهد که آیا تابعی برای وارسی پیچیدگی گذرواژه‌ها در پروفایل پیش‌فرض تعریف شده است یا خیر. چنانچه این تابع موجود باشد، نام آن به عنوان خروجی تولید می‌شد.

```
SELECT LIMIT FROM DBA_PROFILES WHERE PROFILE = 'DEFAULT' AND
RESOURCE_NAME = 'PASSWORD_VERIFY_FUNCTION';
```

در صورتی که دستور زیر لیستی از پروفایل ها را به نمایش درآورد، پروفایل‌های لیست شده دارای تابعی برای وارسی پیچیدگی گذرواژه‌ها نیستند.

```
SELECT PROFILE, RESOURCE_NAME, LIMIT
FROM DBA_PROFILES
WHERE RESOURCE_NAME='PASSWORD_VERIFY_FUNCTION'
AND (LIMIT = 'DEFAULT' OR LIMIT = 'NULL');
```

مقاوم‌سازی:

با اجرای دستور زیر، تابع verify_function_12c که باید از قبل تعریف شده باشد، به عنوان پارامتر PASSWORD_VERIFY_FUNCTION تعیین می‌شود.

```
--Create a custom password verification function, say
verify_function_12c, which fulfills the password requirements of the
organization.
ALTER PROFILE DEFAULT LIMIT PASSWORD_VERIFY_FUNCTION
verify_function_12c;
```

۳-۹ پارامتر SESSIONS_PER_USER

این پارامتر حداکثر تعداد نشست‌هایی را نشان می‌دهد که یک کاربر قادر است به طور همزمان باز کند.

تهدید/توجیه امنیتی:

با تعیین مقدار معین و کوچکی برای این پارامتر، می‌توان از هدر رفتن منابع سیستمی در اثر بازکردن بی‌رویه نشست توسط یک کاربر مجاز و یا رخداد حمله منع سرویس توسط یک مهاجم که تنها به تعداد محدودی حساب کاربری دسترسی دارد جلوگیری کرد.

اطلاع از وضعیت فعلی:

خروجی حاصل از پرسمان زیر، مقدار فعلی این پارامتر را نشان می‌دهد.

```
SELECT LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME = 'SESSIONS_PER_USER' AND PROFILE = 'DEFAULT';
```

در صورتی که دستور زیر لیستی از پروفایل ها را به نمایش درآورد، پروفایل های لیست شده دارای مقدار مناسبی برای این پارامتر نیستند.

```
SELECT PROFILE, RESOURCE_NAME, LIMIT
FROM DBA_PROFILES
WHERE RESOURCE_NAME='SESSIONS_PER_USER'
AND
(LIMIT = 'DEFAULT'
OR LIMIT = 'UNLIMITED'
OR LIMIT > 10);
```

مقاوم‌سازی:

با اجرای دستورات زیر، این پارامتر با عدد ۱۰ مقداردهی می‌شود.

```
ALTER PROFILE DEFAULT LIMIT SESSIONS_PER_USER 10;
--To enable this setting it is necessary to enable the RESOURCE_LIMIT , that is,
ALTER SYSTEM SET RESOURCE_LIMIT = TRUE SCOPE=spfile;
```

دستور فوق می‌بایست برای تمامی پروفایل‌هایی که مقدار مناسبی برای این پارامتر ندارند، اجرا شود.

```
ALTER PROFILE <profile_name> LIMIT SESSIONS_PER_USER 10;
```

۳-۱۰ هیچ کاربری به پروفایل DEFAULT تخصیص داده نشود

به صورت پیش فرض هنگام ایجاد کاربر پایگاه داده، کاربر به پروفایل DEFAULT تخصیص داده می‌شود، مگرآنکه پروفایل دیگری تعیین شود. هیچ کاربری نباید به پروفایل DEFAULT تخصیص داده شود.

تهدید/توجیه امنیتی

پروفایل DEFAULT با تغییرات و بروزرسانی‌های پایگاه داده اراکل تغییر می‌کند. این پروفایل دارای تنظیمات بدون محدودیت است که اغلب برای کاربر SYS مناسب است. این تنظیمات بدون محدودیت نباید به کاربران عادی اختصاص داده شوند.

اطلاع از وضعیت فعلی

در صورتی که دستور زیر خروجی نداشته باشد، بدین معناست کاربران غیرضروری به پروفایل DEFAULT تخصیص داده نشده‌اند. کاربرانی که در لیست خروجی دستور زیر قرار می‌گیرند، به پروفایل DEFAULT تخصیص داده شده‌اند و باید پروفایل آن‌ها تغییر کند.

```
SELECT USERNAME
FROM DBA_USERS
WHERE PROFILE='DEFAULT'
AND ACCOUNT_STATUS='OPEN'
AND USERNAME NOT IN
('ANONYMOUS', 'CTXSYS', 'DBSNMP', 'EXFSYS', 'LBACSYS',
'MDSYS', 'MGMT_VIEW','OLAPSYS','OWBSYS', 'ORDPLUGINS',
'ORDSYS', 'OUTLN', 'SI_INFORMTN_SCHEMA','SYS',
'SYSMAN', 'SYSTEM', 'TSMSYS', 'WK_TEST', 'WKSYS',
'WKPROXY', 'WMSYS', 'XDB', 'CISSCAN');
```

مقاوم‌سازی

با استفاده از دستور زیر می‌توان پروفایل نامناسب هر کاربر را تغییر داد.

```
ALTER USER <username> PROFILE <appropriate_profile>;
```

۳-۱۱ جمع‌بندی

در این فصل به تشریح تنظیمات مربوط به امن‌سازی اتصال به سمپاد پرداختیم. در این راستا، برخی از پارامترهای مرتبط و توجه به این نکته که هیچ کاربری به پروفایل Default تخصیص داده نشود، مورد بحث و بررسی قرار گرفت. مدیر سامانه به منظور بررسی پارامترهای مقاوم‌سازی و تهیه گزارش در این زمینه می‌تواند از چک لیست زیر استفاده نماید.

عنوان	تنظیم صحیح	
	بله	خیر

۳	**امن‌سازی اتصال به پایگاه‌داده**		
۳-۱	پارامتر FAILED_LOGIN_ATTEMPTS	☐	☐
۳-۲	پارامتر PASSWORD_LOCK_TIME	☐	☐
۳-۳	پارامتر PASSWORD_LIFE_TIME	☐	☐
۳-۴	پارامتر PASSWORD_REUSE_MAX	☐	☐
۳-۵	پارامتر PASSWORD_REUSE_TIME	☐	☐
۳-۶	پارامتر PASSWORD_GRACE_TIME	☐	☐
۳-۷	پارامتر AUTHENTICATION_TYPE	☐	☐
۳-۸	پارامتر PASSWORD_VERIFY_FUNCTION	☐	☐
۳-۹	پارامتر SESSIONS_PER_USER	☐	☐
۳-۱۰	هیچ کاربری به پروفایل DEFAULT تخصیص داده نشود	☐	☐

۴ کنترل دسترسی و مجازشماری

طبق اصل اعطای حداقل مجوزها به عنوان یک اصل کلی امنیتی، هر کاربر باید تنها مجوزهایی را دارا باشد که واقعا برای اجرای مسوولیت‌های روزمره‌اش به آن مجوزها نیاز دارد. در این بخش، مجوزهایی که معمولا به همگان اعطا می‌شوند در حالی که نیازی به اعطای آن‌ها نیست معرفی می‌شوند و نحوه لغو چنین مجوزهایی نیز بیان می‌گردد.

۴ – ۱ مجوزهای عمومی پیش‌فرض

با نصب اراکل، مجوز اجرای توابع موجود در تعداد زیادی از بسته‌ها[2] به همه کاربران داده می‌شود. چنانچه در اجرای عملیات عادی سیستم نیازی به این مجوزها نباشد، لازم است این مجوزها لغو گردند.

۴-۱-۱ بسته DBMS_ADVISOR

از بسته DBMS_ADVISOR به منظور نوشتن در فایل‌هایی استفاده می‌شود که بر روی همان سروری قرار دارند که اراکل بر روی آن نصب شده است.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته DBMS_ADVISOR قادر است فایل‌های سیستمی موجود بر روی سرور میزبان اراکل را تخریب کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE
FROM DBA_TAB_PRIVS
WHERE GRANTEE='PUBLIC'
AND PRIVILEGE='EXECUTE'
AND TABLE_NAME='DBMS_ADVISOR';
```

مقاوم‌سازی:

---

[2] Package [2]

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_ADVISOR FROM PUBLIC;
```

۴-۱-۲ بسته DBMS_CRYPTO

بسته DBMS_CRYPTO واسطی فراهم می‌کند که با استفاده از آن می‌توان عملیات رمزنگاری و رمزگشایی را بر روی داده‌های ذخیره شده در اراکل اجرا کرد.

تهدید/توجیه امنیتی:

سوء استفاده از این بسته ممکن است منجر به تخریب داده‌های ذخیره شده در پایگاه داده گردد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE
TABLE_NAME = 'DBMS_CRYPTO'
AND GRANTEE = 'PUBLIC'
AND PRIVILEGE='EXECUTE';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_CRYPTO FROM PUBLIC;
```

۴-۱-۳ بسته DBMS_JAVA

از بسته DBMS_JAVA برای دسترسی به یک سری امکانات اراکل با زبان برنامه نویسی جاوا استفاده می‌شود. این بسته امکان اجرای کلاس‌های جاوا را دارد.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته DBMS_JAVA قادر است دستوراتی را در سطح سیستم عامل میزبان اراکل اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE
FROM DBA_TAB_PRIVS
WHERE GRANTEE='PUBLIC'
AND PRIVILEGE='EXECUTE'
AND TABLE_NAME='DBMS_JAVA';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_JAVA FROM PUBLIC;
```

۴-۱-۴ بسته DBMS_JAVA_TEST

بسته DBMS_JAVA_TEST امکان تست کردن رویه‌های نوشته شده به زبان جاوا در اراکل را فراهم می‌کند. این بسته امکان اجرای کلاس‌های جاوا را دارد.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته DBMS_JAVA_TEST قادر است دستوراتی را در سطح سیستم عامل میزبان اراکل اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE
FROM DBA_TAB_PRIVS
WHERE GRANTEE='PUBLIC'
AND PRIVILEGE='EXECUTE'
AND TABLE_NAME='DBMS_JAVA_TEST';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_JAVA_TEST FROM PUBLIC;
```

۴-۱-۵ بسته DBMS_JOB

از بسته DBMS_JOB برای زمان‌بندی و مدیریت کارهای ارسال شده به job queue استفاده می‌شود. در نسخه‌های اخیر اراکل، بسته DBMS_SCHEDULER به عنوان جایگزین این بسته ارائه شده است و ارائه DBMS_JOB تنها به منظور پشتیبانی از برنامه‌های توسعه یافته قدیمی است.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته DBMS_JOB قادر است فعالیت job queue را مختل کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_JOB';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_JOB FROM PUBLIC;
```

۴-۱-۶ بسته DBMS_LDAP

از بسته DBMS_LDAP به منظور دسترسی به یک LDAP Server استفاده می‌شود.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از بسته DBMS_LDAP قادر است اطلاعاتی را از داخل پایگاه داده از طریق تولید پیام‌های خطای خاص و یا ارسال درخواست‌های DNS، به بیرون از سرور میزبان اراکل ارسال کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE
FROM DBA_TAB_PRIVS
WHERE GRANTEE='PUBLIC'
```

```
AND PRIVILEGE='EXECUTE'
AND TABLE_NAME='DBMS_LDAP';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_LDAP FROM PUBLIC;
```

۴-۱-۷ بسته DBMS_LOB

از بسته DBMS_LOB به منظور نوشتن و خواندن large object هایی همچون BLOB، CLOB، NCLOB، BFILE، و LOB های موقتی استفاده می‌شود.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته DBMS_LOB قادر است داده‌های مربوط به large object ها را بر روی سرور میزبان اراکل تخریب کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_LOB';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_LOB FROM PUBLIC;
```

۴-۱-۸ بسته DBMS_OBFUSCATION_TOOLKIT

بسته DBMS_OBFUSCATION_TOOLKIT امکان اجرای رمزنگاری بر روی داده‌های ذخیره شده در اراکل با استفاده از الگوریتم‌های DES و Triple DES را فراهم می‌کند. در نسخه‌های اخیر اراکل، بسته DBMS_CRYPTO به عنوان جایگزین این بسته ارائه شده است و ارائه DBMS_OBFUSCATION_TOOLKIT تنها به منظور پشتیبانی از برنامه‌های توسعه یافته قدیمی است.

تهدید/توجیه امنیتی:

سوء استفاده از این بسته ممکن است منجر به تخریب داده‌های ذخیره شده در پایگاه داده گردد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_OBFUSCATION_TOOLKIT';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_OBFUSCATION_TOOLKIT FROM PUBLIC;
```

۴-۱-۹ بسته DBMS_RANDOM

از بسته DBMS_RANDOM به منظور تولید عددهای تصادفی در کاربردهای غیر مرتبط با رمزنگاری استفاده می‌شود.

تهدید/توجیه امنیتی:

استفاده بی‌مورد مهاجم از این بسته ممکن است در روند کاری سیستم اخلال ایجاد کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_RANDOM';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_RANDOM FROM PUBLIC;
```

۴-۱-۱۰ بسته DBMS_SCHEDULER

از بسته DBMS_SCHEDULER به منظور زمان‌بندی و مدیریت کارهای مرتبط با پایگاه داده و سیستم‌عامل استفاده می‌شود.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته DBMS_SCHEDULER قادر است کارهای دلخواه خود را در سطح پایگاه داده و سیستم عامل انجام دهد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC'
AND PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_SCHEDULER';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_SCHEDULER FROM PUBLIC;
```

۱۱-۱-۴ بسته DBMS_SQL

از بسته DBMS_SQL به منظور اجرای دستورات SQL پویا[2] استفاده می‌شود.

تهدید/توجیه امنیتی:

در استفاده از امکانات فراهم شده توسط بسته DBMS_SQL، اگر وارسی ورودی‌ها به درستی صورت نگیرد، ممکن است به نشت مجوز[3] منجر شود.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_SQL';
```

مقاوم‌سازی:

---

[2] Dynamic SQL Statements
[3] Privilege Escalation

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_SQL FROM PUBLIC;
```

۴-۱-۱۲ بسته DBMS_XMLGEN

بسته DBMS_XMLGEN یک پرسمان دلخواه SQL را به عنوان ورودی دریافت می‌کند، آن را به قالب XML تبدیل می‌کند و حاصل را در قالب CLOB بر می‌گرداند.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته DBMS_XMLGEN قادر است تمامی فضای پایگاه داده‌ها را برای دسترسی به اطلاعات حساسی همچون شماره حساب[۲۵] جستجو کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_XMLGEN';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_XMLGEN FROM PUBLIC;
```

۴-۱-۱۳ بسته DBMS_XMLQUERY

بسته DBMS_XMLQUERY یک پرسمان دلخواه SQL را به عنوان ورودی دریافت می‌کند، آن را به قالب XML تبدیل می‌کند و حاصل را بر می‌گرداند. عملکرد این بسته مشابه عملکرد بسته DBMS_XMLGEN است.

تهدید/توجیه امنیتی:

---

[2] Credit Card Number [5]

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته DBMS_XMLQUERY قادر است تمامی فضای پایگاه داده‌ها را برای دسترسی به اطلاعات حساسی همچون شماره حساب جستجو کند. کاربران مخرب ممکن است بتوانند از این بسته به عنوان تابع تزریق کمکی[۶] در یک حمله تزریق SQL[۷] استفاده کنند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_XMLQUERY';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_XMLQUERY FROM PUBLIC;
```

۴-۱-۱۴ بسته UTL_FILE

از بسته UTL_FILE به منظور خواندن و نوشتن در فایل‌هایی استفاده می‌شود که بر روی همان سروری قرار دارند که اراکل بر روی آن نصب شده است.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته UTL_FILE قادر است فایل‌های سیستمی موجود بر روی سرور میزبان اراکل را تخریب کند و یا فایل‌های حاوی داده‌های محرمانه تحت مدیریت پایگاه داده را به سرقت ببرد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='UTL_FILE';
```

---

[2] Auxiliary Inject Function
[2] SQL Injection Attack
[6]
[7]

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON UTL_FILE FROM PUBLIC;
```

۴-۱-۱۵ بسته UTL_INADDR

بسته UTL_INADDR واسطی فراهم می‌کند که با استفاده از آن می‌توان نام میزبان[۲۸] آدرس IP رایانه‌های محلی[۲۹] راه دور[۳۰] بازیابی کرد.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته UTL_INADDR قادر است حمله تزریق SQL را برای پایگاه‌داده اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='UTL_INADDR';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON UTL_INADDR FROM PUBLIC;
```

۴-۱-۱۶ بسته UTL_TCP

بسته UTL_TCP به منظور برقراری ارتباط با سرورهای خارجی با استفاده از پروتکل TCP/IP به کار می‌آید.

تهدید/توجیه امنیتی:

---

2 Host Name
2 Local
3 Remote
8
9
0

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته UTL_TCP قادر است در ارتباطات میان سرور میزبان اراکل با سرورهای خارجی اخلال ایجاد کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='UTL_TCP';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON UTL_TCP FROM PUBLIC;
```

۱۷-۱-۴ بسته UTL_MAIL

از بسته UTL_MAIL به منظور ارسال ایمیل از سروری که اراکل بر روی آن نصب شده است، استفاده می‌شود.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته UTL_MAIL قادر است ایمیل‌های بی‌ارزش[۳۱] تولید کند و با استفاده از توان پردازشی سرور میزبان اراکل، حمله منع سرویس را اجرا کند (مثلا تمامی ترافیک شبکه ارتباطی را هدر دهد).

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='UTL_MAIL';
```

---

[3] Junk [1]

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON UTL_MAIL FROM PUBLIC;
```

۴-۱-۱۸ بسته UTL_SMTP

از بسته UTL_ SMTP به منظور ارسال ایمیل از سروری که اراکل بر روی آن نصب شده است، استفاده می‌شود.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته UTL_SMTP قادر است ایمیل‌های بی‌ارزش تولید کند و با استفاده از توان پردازشی سرور میزبان اراکل، حمله منع از سرویس را اجرا کند (مثلا تمامی ترافیک شبکه ارتباطی را هدر دهد).

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='UTL_SMTP';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON UTL_SMTP FROM PUBLIC;
```

۴-۱-۱۹ بسته UTL_DBWS

از بسته UTL_DBWS به منظور دسترسی به وب سرویس استفاده می‌شود. در حقیقت از این بسته برای خواندن و نوشتن فایل‌ها از برنامه‌های کاربردی تحت وب بر روی سروری که اراکل بر روی آن نصب است، استفاده می شود.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته UTL_DBWS قادر است در ارتباطات میان پایگاه داده اراکل و وب سرویس‌های مورد نیاز آن اختلال ایجاد کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='UTL_DBWS';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON UTL_DBWS FROM 'PUBLIC';
```

۴-۱-۲۰ بسته UTL_ORAMTS

از بسته UTL_ORAMTS به منظور ارسال درخواست‌های HTTP استفاده می‌شود.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته UTL_ORAMTS قادر است اطلاعات محرمانه را از سرور اراکل به خارج ارسال کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='UTL_ORAMTS';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON UTL_ORAMTS FROM PUBLIC;
```

۴-۱-۲۱ بسته UTL_HTTP

از بسته UTL_HTTP به منظور ارسال درخواست‌های HTTP استفاده می‌شود.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته UTL_HTTP قادر است اطلاعات محرمانه را از سرور اراکل به خارج ارسال کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='UTL_HTTP';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON UTL_HTTP FROM PUBLIC;
```

۴-۱-۲۲ نوع شیء HTTPURITYPE

از نوع شیء HTTPURITYPE به منظور ارسال درخواست‌های HTTP استفاده می‌شود.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط HTTPURITYPE قادر است اطلاعات محرمانه را از سرور اراکل به خارج ارسال کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='HTTPURITYPE';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON HTTPURITYPE FROM PUBLIC;
```

۴-۱-۲۳ بسته DBMS_XMLSTORE

بسته DBMS_XMLSTORE قابلیت های XML را فراهم می‌کند. این بسته نام یک جـدول و XML را بـه عنوان ورودی دریافت کرده و عملیات DML را بر روی جدول انجام می‌دهد.

تهدید/توجیه امنیتی:

کاربران مخرب ممکن است بتوانند از این بسته به عنوان تابع تزریق کمکی در یک حمله تزریق SQL استفاده کنند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT GRANTEE FROM DBA_TAB_PRIVS WHERE TABLE_NAME = 'DBMS_XMLSTORE'
AND GRANTEE = 'PUBLIC' AND PRIVILEGE = 'EXECUTE';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_XMLSTORE FROM PUBLIC;
```

۴-۱-۲۴ بسته DBMS_XMLSAVE

بسته DBMS_XMLSAVE قابلیت های XML را فراهم می‌کند. این بسته نـام یـک جـدول و XML را بـه عنوان ورودی دریافت کرده و سپس آن را در جدول درج کرده و یا بروزرسانی می‌کند.

تهدید/توجیه امنیتی:

کاربران مخرب ممکن است بتوانند از این بسته به عنوان تابع تزریق کمکی در یک حمله تزریق SQL استفاده کنند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT GRANTEE FROM DBA_TAB_PRIVS WHERE TABLE_NAME = 'DBMS_XMLSAVE'
AND GRANTEE = 'PUBLIC' AND PRIVILEGE = 'EXECUTE';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_XMLSAVE FROM PUBLIC;
```

۴-۱-۲۵ بسته DBMS_REDACT

بسته DBMS_REDACT یک رابط به Oracle Data Redaction فراهم می‌کند و این امکان را می‌دهد که در صورتی که پرسمانی از جانب کاربر یا برنامه کاربردی با مجوز محدود اجرا شد، داده های بازگشتی تغییر داده شوند.[۳۲]

تهدید/توجیه امنیتی:

کاربران مخرب ممکن است بتوانند از این بسته به عنوان تابع تزریق کمکی در یک حمله تزریق SQL استفاده کنند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT GRANTEE
FROM DBA_TAB_PRIVS
WHERE TABLE_NAME = 'DBMS_REDACT'
AND GRANTEE = 'PUBLIC'
AND PRIVILEGE = 'EXECUTE';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_REDACT FROM PUBLIC;
```

---

[3] Mask [2]

۴-۲ مجوزهای عمومی غیر پیش‌فرض

در طول عمر فعالیت یک پایگاه داده اراکل، معمولا مجوز اجرای توابع موجود در تعداد زیادی از بسته‌ها بی‌دلیل توسط مدیران پایگاه داده به همه کاربران داده می‌شود. چنانچه در اجرای عملیات عادی سیستم نیازی به این مجوزها نباشد، لازم است لغو گردند.

۴-۲-۱ بسته DBMS_SYS_SQL

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته DBMS_SYS_SQL قادر است کدهای خود را با مجوزهای کاربری دیگر اجرا کند بدون اینکه لازم باشد احراز اصالت گردد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_SYS_SQL';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_SYS_SQL FROM PUBLIC;
```

۴-۲-۲ بسته DBMS_BACKUP_RESTORE

از بسته DBMS_BACKUP_RESTORE به منظور اجرای دستورات RMAN در داخل کد PL/SQL استفاده می‌شود.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته DBMS_BACKUP_RESTORE قادر است مجوز دسترسی به فایل‌های تحت مدیریت سیستم عامل میزبان اراکل را به دست آورد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_BACKUP_RESTORE';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_BACKUP_RESTORE FROM PUBLIC;
```

۴-۲-۳ بسته DBMS_AQADM_SYSCALLS

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط این بسته قادر است یک دستور SQL را با مجوزهای کاربر SYS (مدیر اصلی پایگاه داده اراکل) اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_AQADM_SYSCALLS';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_AQADM_SYSCALLS FROM PUBLIC;
```

۴-۲-۴ بسته DBMS_REPACT_SQL_UTL

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط این بسته قادر است یک دستور SQL را با مجوزهای کاربر SYS (مدیر اصلی پایگاه داده اراکل) اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_REPCAT_SQL_UTL';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_REPACT_SQL_UTL FROM PUBLIC;
```

۴-۲-۵ بسته INITJVMAUX

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط این بسته قادر است یک دستور SQL را با مجوزهای کاربر SYS (مدیر اصلی پایگاه داده اراکل) اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='INITJVMAUX';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON INITJVMAUX FROM PUBLIC;
```

۴-۲-۶ بسته DBMS_STREAMS_ADM_UTL

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط این بسته قادر است یک دستور SQL را با مجوزهای کاربر SYS (مدیر اصلی پایگاه داده اراکل) اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE'AND TABLE_NAME='DBMS_STREAMS_ADM_UTL';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_STREAMS_ADM_UTL FROM PUBLIC;
```

۴-۲-۷ بسته DBMS_AQADM_SYS

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط این بسته قادر است یک دستور SQL را با مجوزهای کاربر SYS (مدیر اصلی پایگاه داده اراکل) اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_AQADM_SYS';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_AQADM_SYS FROM PUBLIC;
```

۴-۲-۸ بسته DBMS_STREAMS_RPC

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط این بسته قادر است یک دستور SQL را با مجوزهای کاربر SYS (مدیر اصلی پایگاه داده اراکل) اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_STREAMS_RPC';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_STREAMS_RPC FROM PUBLIC;
```

۴-۲-۹ بسته DBMS_PRVTAQIM

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط این بسته قادر است یک دستور SQL را با مجوزهای کاربر SYS (مدیر اصلی پایگاه داده اراکل) اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_PRVTAQIM';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_PRVTAQIM FROM PUBLIC;
```

۴-۲-۱۰ بسته LTADM

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط این بسته قادر است یک دستور SQL را با مجوزهای کاربر SYS (مدیر اصلی پایگاه داده اراکل) اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='LTADM';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON LTADM FROM PUBLIC;
```

۴-۲-۱۱ بسته WWV_DBMS_SQL

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط این بسته قادر است یک دستور SQL را با مجوزهای کاربر Application Express (APEX) اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='WWV_DBMS_SQL';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON WWV_DBMS_SQL FROM PUBLIC;
```

۴-۲-۱۲ بسته WWV_EXECUTE_IMMEDIATE

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط این بسته قادر است یک دستور SQL را با مجوزهای کاربر Application Express (APEX) اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='WWV_EXECUTE_IMMEDIATE';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON WWV_EXECUTE_IMMEDIATE FROM PUBLIC;
```

۴-۲-۱۳ بسته DBMS_IJOB

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط این بسته قادر است یک دستور SQL را با مجوزهای هر کاربر دلخواه دیگری اجرا کند.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_IJOB';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_IJOB FROM PUBLIC;
```

۴-۲-۱۴ بسته DBMS_FILE_TRANSFER

از بسته DBMS_FILE_TRANSFER به منظور ارسال فایل از یک سرور اراکل به یک سرور دیگر اراکل استفاده می‌شود.

تهدید/توجیه امنیتی:

یک مهاجم با استفاده از امکانات فراهم شده توسط بسته DBMS_FILE_TRANSFER قادر است فایل‌های موجود بر روی سرور اراکل را به سرقت ببرد.

اطلاع از وضعیت فعلی:

برای اطلاع از وضعیت فعلی پارامتر مذکور از پرسمان زیر استفاده می‌شود. چنانچه خروجی حاصل از این پرسمان، مقدار EXECUTE را برگرداند، یعنی مجوز اجرای توابع این بسته به همگان داده شده است.

```
SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND
PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_FILE_TRANSFER';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز همگانی اجرای این بسته لغو می‌شود.

```
REVOKE EXECUTE ON DBMS_FILE_TRANSFER FROM PUBLIC;
```

۴-۳ مجوزهای سیستمی

تعدادی از مجوزهای سیستمی تنها برای انجام کارهای مدیریتی و توسط مدیران پایگاه داده مورد استفاده قرار می‌گیرند. چنین مجوزهایی نباید در اختیار سایر کاربران عادی قرار گیرد.

۴-۳-۱ مجوز SELECT ANY DICTIONARY

این مجوز به کاربر اجازه دسترسی به اشیاء شمای SYS را می‌دهد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند کلیه اشیاء شمای SYS را بخواند. مثلا، مقدار درهم‌سازی شده گذرواژه[3]تمامی کاربران در شمای SYS قرار دارد و به این ترتیب فاش می‌شود.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نیازی به این مجوز ندارند در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='SELECT
ANY DICTIONARY' AND GRANTEE NOT IN ('DBA','DBSNMP','OEM_MONITOR',
'OLAPSYS','ORACLE_OCM','SYSMAN','WMSYS','SYSBACKUP','SYSDG');
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز کاربر grantee که از پرسمان قبلی بدست آمده است، لغو می‌شود.

```
REVOKE SELECT ANY DICTIONARY FROM <grantee>;
```

۴-۳-۲ مجوز SELECT_ANY_TABLE

این مجوز به کاربر اجازه دسترسی به کلیه جداول به جز جداول شمای SYS را می‌دهد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند به اطلاعات محرمانه موجود در جداول مختلف دسترسی پیدا کند.

اطلاع از وضعیت فعلی:

---

[3] Hashed Password [3]

با اجرای پرسمان زیر، نام کاربرانی که نیازی به این مجوز ندارند در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='SELECT
ANY TABLE' AND GRANTEE NOT IN ('DBA', 'MDSYS', 'SYS',
'IMP_FULL_DATABASE','EXP_FULL_DATABASE','DATAPUMP_IMP_FULL_DATABASE',
'WMSYS', 'SYSTEM','OLAP_DBA', 'DV_REALM_OWNER');
```

مقاوم‌سازی:

با اجرای پرسمان زیر، مجوز کاربر grantee که از پرسمان قبلی بدست آمده است، لغو می‌شود.

```
REVOKE SELECT ANY TABLE FROM <grantee>;
```

۴-۳-۳ مجوز AUDIT SYSTEM

این مجوز به کاربر اجازه مدیریت رویدادنگاری را می‌دهد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند مانع از ثبت رویدادهای مربوط بـه فعالیت‌هـای مخـرب خـود در سیستم شود.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نیازی به این مجوز ندارند در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='AUDIT
SYSTEM' AND GRANTEE NOT IN ('DBA', 'DATAPUMP_IMP_FULL_DATABASE',
'IMP_FULL_DATABASE', 'SYS', 'AUDIT_ADMIN');
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز کاربر grantee که از پرسمان قبلی بدست آمده است، لغو می‌شود.

```
REVOKE AUDIT SYSTEM FROM <grantee>;
```

۴-۳-۴ مجوز EXEMPT ACCESS POLICY

این مجوز به کاربر اجازه دسترسی به کلیه سطرهای جداول بدون توجه به برچسب امنیتی آن‌ها را می‌دهد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند سطرهایی که مجاز به مشاهده آن‌ها نیست را ببینـد و داده‌هـا را تغییر دهد.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نیازی به این مجوز ندارند در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='EXEMPT
ACCESS POLICY';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز کاربر grantee که از پرسمان قبلی بدست آمده است، لغو می‌شود.

```
REVOKE EXEMPT ACCESS POLICY FROM <grantee>;
```

۴-۳-۵ مجوز BECOME USER

این مجوز به کاربر اجازه دسترسی به مجوزهای کاربران دیگر را می‌دهد. در حقیقت کاربر می‌تواند مجوزهای سایر کاربران را به ارث ببرد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند خود را به کاربر قدرتمندتری در سیستم تبدیل کند.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نیازی به این مجوز ندارند در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='BECOME
USER' AND GRANTEE NOT IN ('DBA','SYS','IMP_FULL_DATABASE');
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز کاربر grantee که از پرسمان قبلی بدست آمده است، لغو می‌شود.

```
REVOKE BECOME USER FROM <grantee>;
```

۴-۳-۶ مجوز CREATE PROCEDURE

این مجوز به کاربر اجازه ساختن یک رویه ذخیره شده[3] می‌دهد.

---

[3] Stored Procedure [4]

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند رویه‌های ذخیره‌شده‌ای ایجاد کند که وی را در انجام فعالیت‌های مخربش یاری کنند.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نیازی به این مجوز ندارند در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='CREATE
PROCEDURE' AND GRANTEE NOT IN ( 'DBA', 'DBSNMP', 'MDSYS', 'OLAPSYS',
'OWB$CLIENT',               'OWBSYS',       'RECOVERY_CATALOG_OWNER',
'SPATIAL_CSW_ADMIN_USR',        'SPATIAL_WFS_ADMIN_USR',        'SYS',
'APEX_030200',  'APEX_040000',  'APEX_040100',  'APEX_040200',  'DVF',
'RESOURCE',      'DV_REALM_RESOURCE','APEX_GRANTS_FOR_NEW_USERS_ROLE',
'APEX_050000', 'MGMT_VIEW', 'SYSMAN_MDS', 'SYSMAN_OPSS', 'SYSMAN_RO',
'SYSMAN_STB');
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز کاربر grantee که از پرسمان قبلی بدست آمده است، لغو می‌شود.

```
REVOKE CREATE PROCEDURE FROM <grantee>;
```

۴-۳-۷ مجوز ALTER SYSTEM

این مجوز به کاربر اجازه اعمال تغییرات در پارامترهای سیستمی و عملیات در حال اجرای اراکل را می‌دهد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند هر گونه تغییر دلخواهی در پارامترهای سیستمی اعمال نماید.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نیازی به این مجوز ندارند در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='ALTER
SYSTEM'   AND   GRANTEE   NOT   IN   ('SYS','SYSTEM',   'APEX_030200',
'APEX_040000', 'APEX_040100', 'APEX_040200', 'DBA', 'EM_EXPRESS_ALL',
'SYSBACKUP',      'GSMADMIN_ROLE',      'GSM_INTERNAL',      'SYSDG',
'GSMADMIN_INTERNAL');
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز کاربر grantee که از پرسمان قبلی بدست آمده است، لغو می‌شود.

```
REVOKE ALTER SYSTEM FROM <grantee>;
```

۴-۳-۸ مجوزهای CREATE ANY LIBRARY

این مجوز به کاربر اجازه ساختن اشیاء مرتبط با کتابخانه‌های مشترک[۳۵] می‌دهد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند جامعیت[۳۶] کتابخانه‌های مشترک را نقض کند.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نیازی به این مجوزها ندارند در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='CREATE
ANY LIBRARY' AND GRANTEE NOT IN ('SYS', 'SYSTEM', 'DBA',
'IMP_FULL_DATABASE');
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوزهای کاربر grantee که از پرسمان قبلی بدست آمده است، لغو می‌شود.

```
REVOKE CREATE ANY LIBRARY FROM <grantee>;
```

۴-۳-۹ مجوز CREATE LIBRARY

این مجوز به کاربر اجازه ساختن اشیاء مرتبط با کتابخانه‌های مشترک[۳۷] می‌دهد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند جامعیت[۳۸] کتابخانه‌های مشترک را نقض کند.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نیازی به این مجوزها ندارند در ستون GRANTEE برگردانده می‌شود.

---

3 Shared Library 5
3 Integrity 6
3 Shared Library 7
3 Integrity 8

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='CREATE
LIBRARY' AND GRANTEE NOT IN ('SYS', 'SYSTEM', 'DBA', 'MDSYS',
'SPATIAL_WFS_ADMIN_USR', 'SPATIAL_CSW_ADMIN_USR', 'DVSYS',
'GSMADMIN_INTERNAL' ,'XDB');
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوزهای کاربر grantee که از پرسمان قبلی بدست آمده است، لغو می‌شود.

```
REVOKE CREATE LIBRARY FROM <grantee>;
```

۴-۳-۱۰ مجوز GRANT ANY OBJECT PRIVILEGE

این مجوز به کاربر اجازه اعطای مجوز به دیگران برای هر شیئی را می‌دهد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند باعث فاش شدن یا تخریب داده‌های حساس گردد.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نیازی به این مجوز ندارند در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='GRANT
ANY OBJECT PRIVILEGE' AND GRANTEE NOT IN
('DBA','SYS','IMP_FULL_DATABASE', 'DATAPUMP_IMP_FULL_DATABASE',
'EM_EXPRESS_ALL', 'DV_REALM_OWNER');
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز کاربر grantee که از پرسمان قبلی بدست آمده است، لغو می‌شود.

```
REVOKE GRANT ANY OBJECT PRIVILEGE FROM <grantee>;
```

۴-۳-۱۱ مجوز GRANT ANY ROLE

این مجوز به کاربر اجازه می‌دهد که هر نقشی را به هر کاربری اختصاص دهد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند باعث فاش شدن و یا تخریب داده‌های حساس گردد.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نیازی به این مجوز ندارند در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='GRANT
ANY ROLE' AND GRANTEE NOT IN ('DBA', 'SYS',
'DATAPUMP_IMP_FULL_DATABASE', 'IMP_FULL_DATABASE',
'SPATIAL_WFS_ADMIN_USR', 'SPATIAL_CSW_ADMIN_USR','GSMADMIN_INTERNAL',
'DV_REALM_OWNER', 'EM_EXPRESS_ALL', 'DV_OWNER');
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز کاربر grantee که از پرسمان قبلی بدست آمده است، لغو می‌شود.

```
REVOKE GRANT ANY ROLE FROM <grantee>;
```

۴-۳-۱۲ مجوز GRANT ANY PRIVILEGE

این مجوز به کاربر اجازه اعطای هر مجوز به هر موجودیت را می‌دهد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند باعث فاش شدن و یا تخریب داده‌های حساس گردد.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نیازی به این مجوز ندارند در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='GRANT
ANY PRIVILEGE' AND GRANTEE NOT IN ('DBA','SYS','IMP_FULL_DATABASE',
'DATAPUMP_IMP_FULL_DATABASE', 'DV_REALM_OWNER','EM_EXPRESS_ALL');
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز کاربر grantee که از پرسمان قبلی بدست آمده است، لغو می‌شود.

```
REVOKE GRANT ANY PRIVILEGE FROM <grantee>;
```

۴ – ۴ ارث‌بری مجوز از نقش‌های قدرتمند

تعدادی از نقش‌های قدرتمند در اراکل تعریف شده‌اند که ارث‌بری مجوز از آن‌ها باید به صورت بسیار محدود و تنها برای کاربران خاص (مثلا مدیران پایگاه داده) مجاز باشد. در این بخش، این نقش‌ها معرفی می‌شوند.

۴-۴-۱ نقش DELETE_CATALOG_ROLE

این نقش، مجوز حذف رکوردها از جدول رویدادنگاری سیستمی را دارد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند باعث تخریب رویدادهای ثبت شده و یا مانع از ثبت رویدادهای مربوط به فعالیت‌های مخرب خود در سیستم شود.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نباید از این نقش به ارث ببرند، در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE
granted_role='DELETE_CATALOG_ROLE' AND GRANTEE NOT IN ('DBA','SYS');
```

مقاوم‌سازی:

با اجرای دستور زیر، ارث بری کاربر grantee از این نقش، لغو می‌شود.

```
REVOKE DELETE_CATALOG_ROLE FROM <grantee>;
```

۴-۴-۲ نقش SELECT_CATALOG_ROLE

این نقش، مجوز خواندن از کلیه جداول سیستمی واقع در شمای SYS را دارد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند کلیه اطلاعات سیستمی را به سرقت ببرد.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نباید از این نقش به ارث ببرند در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE
granted_role='SELECT_CATALOG_ROLE' AND grantee not in ('DBA', 'SYS',
'IMP_FULL_DATABASE', 'EXP_FULL_DATABASE', 'OEM_MONITOR', 'SYSBACKUP',
'EM_EXPRESS_BASIC', 'SYSMAN');
```

مقاوم‌سازی:

با اجرای دستور زیر، ارث‌بری کاربر grantee از این نقش، لغو می‌شود.

```
REVOKE SELECT_CATALOG_ROLE FROM <grantee>;
```

۴-۴-۳ نقش EXECUTE_CATALOG_ROLE

این نقش، مجوز اجرای بسیاری از بسته‌ها و رویه‌های ذخیره شده‌ی موجود در شمای SYS را دارد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند توابع متنوع موجود در بسته‌های شمای SYS را فراخوانی کند.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نباید از این نقش به ارث ببرند، در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE
granted_role='EXECUTE_CATALOG_ROLE' AND grantee not in ('DBA', 'SYS',
'IMP_FULL_DATABASE', 'EXP_FULL_DATABASE');
```

مقاوم‌سازی:

با اجرای دستور زیر، ارث بری کاربر grantee از این نقش، لغو می‌شود.

```
REVOKE EXECUTE_CATALOG_ROLE FROM <grantee>;
```

۴-۴-۴ نقش DBA

نقش DBA، بسیاری از مجوزهای لازم برای مدیریت پایگاه داده اراکل را دارد و در حقیقت، نقش مدیریتی پیش فرض در پایگاه داده است.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند با مجوزهای مدیر پایگاه داده به اجرای فعالیت‌های تخریبی خود بپردازد.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نباید از این نقش به ارث ببرند، در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE
GRANTED_ROLE='DBA' AND GRANTEE NOT IN ('SYS','SYSTEM');
```

مقاوم‌سازی:

با اجرای دستور زیر، ارث بری کاربر grantee از این نقش، لغو می‌شود.

```
REVOKE DBA FROM <grantee>;
```

۴-۵ مجوز دسترسی به جداول و دیدهای سیستمی

دسترسی به جداول و دیدهای سیستمی تنها باید برای کاربرانی امکان‌پذیر باشد که برای انجام فعالیت‌های روزمره خود به آن جداول و دیدها نیاز دارند. در ادامه جداول و دیدهای سیستمی حساس و مجوزهای کاربران بر روی آن‌ها مورد بررسی قرار می‌گیرد.

۴-۵-۱ جدول SYS.AUD$

این جدول، یکی از مکان‌هایی است که رویدادنگاری در آن انجام می‌شود.

تهدید/توجیه امنیتی:

مهاجم با دسترسی به این جدول می‌تواند باعث تخریب رویدادهای ثبت شده و یا مانع از ثبت رویدادهای مربوط به فعالیت‌های مخرب خود در سیستم شود.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نباید هیچ‌گونه مجوزی روی این جدول داشته باشند، در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='AUD$'
AND GRANTEE NOT IN ('DELETE_CATALOG_ROLE');
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه مجوزهای کاربر grantee که از پرسمان بالا به دست آمده است، برای این جدول، لغو می‌شود.

```
REVOKE ALL ON AUD$ FROM <grantee>;
```

۴-۵-۲ جدول SYS.USER_HISTORY$

این جدول، تاریخچه‌ای از تغییرات گذرواژه‌های کاربران را در خود نگه می‌دارد. مثلا چنانچه پارامتر PASSWORD_REUSE_TIME برای پروفایل یک کاربر مقداری غیر از UNLIMITED داشته باشد، برای وارسی برآورده شدن این محدودیت، به جدول USER_HISTORY$ مراجعه می‌شود.

تهدید/توجیه امنیتی:

مهاجم با دسترسی به این جدول می‌تواند سیاست‌های امنیتی سیستم را در مورد نحوه انتخاب و تعویض گذرواژه نقض کند.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نباید هیچ‌گونه مجوزی روی این جدول داشته باشند، در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='USER_HISTORY$' AND OWNER = 'SYS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه مجوزهای کاربر grantee که از پرسمان بالا به دست آمده است، برای این جدول لغو می‌شود.

```
REVOKE ALL ON USER_HISTORY$ FROM <grantee>;
```

۳-۵-۴ جدول SYS.LINK$

این جدول، اطلاعات مربوط به گذرواژه کاربران و data table link را ذخیره می‌کند.

تهدید/توجیه امنیتی: مهاجم با دسترسی به این جدول می‌تواند گذرواژه کاربران را به سرقت ببرد و یا در لینک‌های[۳۹] پایگاه داده اختلال ایجاد کند.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نباید هیچ‌گونه مجوزی روی این جدول داشته باشند، در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='LINK$'
AND GRANTEE NOT IN ('DV_SECANALYST') AND OWNER='SYS';
```

مقاوم‌سازی:

[۳۹] لینک پایگاه داده روشی برای دسترسی از یک سرور به سرور دیگر است. هر لینک یک شیء در پایگاه داده است که به شما امکان دسترسی به اشیای پایگاه داده دیگر را می‌دهد.

با اجرای دستور زیر، کلیه مجوزهای کاربر grantee که از پرسمان بالا به دست آمده است، برای این جدول، لغو می‌شود.

```
REVOKE ALL ON LINK$ FROM <grantee>;
```

۴-۵-۴ جدول SYS.USER$

این جدول، حاوی اطلاعات مربوط به حساب کاربری و نیز گذرواژه درهم‌سازی شده فعلی کاربران است.

تهدید/توجیه امنیتی:

مهاجم با دسترسی به این جدول می‌تواند گذرواژه درهم‌سازی شده کاربران را به سرقت ببرد.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نباید هیچ‌گونه مجوزی روی این جدول داشته باشند، در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE  FROM DBA_TAB_PRIVS WHERE TABLE_NAME = 'USER$' AND OWNER='SYS' AND GRANTEE NOT IN ('CTXSYS', 'XDB', 'APEX_030200', 'SYSMAN','APEX_040000', 'APEX_040100', 'APEX_040200', 'DV_SECANALYST', 'DVSYS', 'ORACLE_OCM');
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه مجوزهای کاربر grantee که از پرسمان بالا به دست آمده است، برای این جدول، لغو می‌شود.

```
REVOKE ALL ON SYS.USER$ FROM <grantee>;
```

۴-۵-۵ دیدهای مدیریتی DBA_%

مجموعه‌ی دیدهای مدیریتی که با عبارت DBA_ شروع می‌شوند، اطلاعات سودمندی را برای مدیران سیستم فراهم می‌کنند.

تهدید/توجیه امنیتی:

دسترسی به این دیدها توسط مهاجم می‌تواند منجر به فاش شدن اطلاعات مدیریتی گردد.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نباید هیچ‌گونه مجوزی روی دیدهای مدیریتی داشته باشند، در ستون GRANTEE برگردانده می‌شود.

```
SELECT grantee||'.'||table_name FROM DBA_TAB_PRIVS WHERE TABLE_NAME
LIKE 'DBA_%' AND GRANTEE NOT IN ('DBA', 'AUDIT_ADMIN',
'AUDIT_VIEWER', 'CAPTURE_ADMIN', 'DVSYS', 'SYSDG', 'DV_SECANALYST',
'SYSKM', 'DV_MONITOR', 'ORACLE_OCM', 'DV_ACCTMGR',
'GSMADMIN_INTERNAL', 'XDB', 'SYS', 'APPQOSSYS',
'AQ_ADMINISTRATOR_ROLE', 'CTXSYS', 'EXFSYS', 'MDSYS',
'OLAP_XS_ADMIN', 'OLAPSYS', 'ORDSYS', 'OWB$CLIENT', 'OWBSYS',
'SELECT_CATALOG_ROLE', 'WM_ADMIN_ROLE','WMSYS','XDBADMIN','LBACSYS',
'ADM_PARALLEL_EXECUTE_TASK', 'CISSCANROLE') AND NOT REGEXP_LIKE
(grantee, '^APEX_0[3-9][0-9][0-9][0-9][0-9]$');
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه مجوزهای کاربر grantee که از پرسمان بالا به دست آمده است، برای یک دید مدیریتی، لغو می‌شود.

```
REVOKE ALL ON <DBA_view> FROM <grantee>;
```

۴-۵-۶ جدول SCHEDULER$_CREDENTIAL

این جدول، حاوی اطلاعات credential مربوط به زمان‌بند پایگاه داده است.

تهدید/توجیه امنیتی:

دسترسی به این جدول توسط مهاجم می‌تواند منجر به فاش شدن اطلاعات حساس موجود در آن گردد.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نباید هیچ‌گونه مجوزی روی این جدول داشته باشند، در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='SCHEDULER$_CREDENTIAL' AND OWNER='SYS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه مجوزهای کاربر grantee که از پرسمان بالا به دست آمده است، برای این جدول لغو می‌شود.

```
REVOKE ALL ON SYS.SCHEDULER$_CREDENTIAL FROM <grantee>;
```

۴-۵-۷ جدول SYS.USER$MIG

این جدول در زمان مهاجرت از یک نسخه اراکل به نسخه دیگر ایجاد می‌شود و حاوی گذرواژه درهم‌سازی شده کاربران قبل از مهاجرت است.

تهدید/توجیه امنیتی:

چنانچه پس از پایان فرآیند مهاجرت، این جدول حذف نگردد، مهاجم با دسترسی به آن می‌تواند گذرواژه درهم‌سازی شده کاربران را بدست بیاورد.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر رکوردی را برگرداند نشانه وجود این جدول در پایگاه داده است.

```
SELECT OWNER, TABLE_NAME FROM ALL_TABLES WHERE OWNER='SYS' AND
TABLE_NAME='USER$MIG';
```

مقاوم‌سازی:

با اجرای دستور زیر، این جدول حذف می‌گردد.

```
DROP TABLE sys.user$mig;
```

۴-۶ مجوزهای خاص

در این بخش، سایر مجوزهایی که اعطای آن‌ها می‌تواند خطرات امنیتی به دنبال داشته باشد و در دسته‌بندی‌های قبلی این فصل قرار نمی‌گیرند، مورد بررسی قرار گرفته‌اند.

۴-۶-۱ مجوزهای ANY

واژه ANY در یک مجوز، نشان دهنده محدوده وسیعی از عملیاتی است که کاربر با دریافت آن مجوز قادر است آنها را انجام دهد. مثلا کاربری که مجوز EXECUTE ANY PROCEDURE را دارد، می‌تواند هر رویه ذخیره‌شده‌ای را اجرا کند.

تهدید/توجیه امنیتی:

اعطای مجوزهای ANY به کاربران معمولا بیش از نیاز آن‌ها است و ممکن است منجر به سوء استفاده از مجوزها گردد.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نباید مجوزهای ANY داشته باشند، در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE LIKE
'%ANY%' AND GRANTEE NOT IN ('AQ_ADMINISTRATOR_ROLE', 'DBA', 'DBSNMP',
'EXFSYS',                    'EXP_FULL_DATABASE','IMP_FULL_DATABASE',
'DATAPUMP_IMP_FULL_DATABASE', 'JAVADEBUGPRIV','MDSYS', 'OEM_MONITOR',
'OLAPSYS','OLAP_DBA','ORACLE_OCM','OWB$CLIENT','OWBSYS','SCHEDULER_AD
MIN','SPATIAL_CSW_ADMIN_USR','SPATIAL_WFS_ADMIN_USR','SYS','SYSMAN','
SYSTEM','WMSYS',    'APEX_030200',    'APEX_040000',    'APEX_040100',
'APEX_040200',  'LBACSYS',  'SYSBACKUP',  'CTXSYS',  'OUTLN',  'DVSYS',
'ORDPLUGINS',          'ORDSYS',          'RECOVERY_CATALOG_OWNER_VPD',
'GSMADMIN_INTERNAL',    'XDB','SYSDG',    'AUDIT_ADMIN',    'DV_OWNER',
'DV_REALM_OWNER',      'EM_EXPRESS_ALL',      'RECOVERY_CATALOG_OWNER',
'APEX_050000', 'SYSMAN_STB', 'SYSMAN_TYPES');
```

مقاوم‌سازی:

با اجرای دستور زیر، یک مجوز ANY کاربر grantee که از پرسمان فوق به دست آمده‌اند، لغو می‌گردد.

```
REVOKE <ANY Privilege> FROM <grantee>;
```

۲-۶-۴ مجوز با گزینه WITH_ADMIN

چنانچه در زمان اعطای یک مجوز به یک کاربر از عبارت WITH ADMIN استفاده گردد، کاربر دارای آن مجوز قادر است مجوز خود را به دیگران اعطا کند.

تهدید/توجیه امنیتی:

این گزینه می‌تواند منجر به انتشار غیر قابل کنترل مجوزهای حساس گردد.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام کاربرانی که نباید مجوز با گزینه WITH_ADMIN داشته باشند، در ستون GRANTEE برگردانده می‌شود.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE ADMIN_OPTION='YES'
AND    GRANTEE    not    in    ('AQ_ADMINISTRATOR_ROLE','DBA','OWBSYS',
'SCHEDULER_ADMIN','SYS','SYSTEM','WMSYS',        'DVSYS',    'SYSKM',
'DV_ACCTMGR')  AND  NOT  REGEXP_LIKE(grantee,'^APEX_0[3-9][0-9][0-9][0-
9][0-9]$');
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز privilege از کاربر grantee که از پرسمان فوق به دست آمده است، لغو می‌گردد.

```
REVOKE <privilege> FROM <grantee>;
```

۴-۶-۳ مجوزهای مربوط به proxy user

در اراکل این امکان وجود دارد که یک مجوز به طور مستقیم به یک proxy user اعطا گردد.

تهدید/توجیه امنیتی:

تنها مجوز مورد نیاز برای یک proxy user، امکان متصل شدن به پایگاه داده است. در نتیجه اعطای سایر مجوزها به غیر از مجوز CONNECT به این کاربر، بی‌مورد است.

اطلاع از وضعیت فعلی:

با اجرای پرسمان زیر، نام proxy user ها و مجوزهای غیر مجازشان در ستون‌های GRANTEE و PRIVILEGE برگردانده می‌شود.

```
SELECT GRANTEE,GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTEE IN (SELECT PROXY FROM DBA_PROXIES) AND GRANTED_ROLE NOT IN ('CONNECT')
UNION
SELECT GRANTEE,PRIVILEGE FROM DBA_SYS_PRIVS WHERE GRANTEE IN (SELECT PROXY FROM DBA_PROXIES) AND PRIVILEGE NOT IN ('CREATE SESSION')
UNION
SELECT GRANTEE,PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE IN (SELECT PROXY FROM DBA_PROXIES);
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز privilege از کاربر proxy_user که از پرسمان فوق به دست آمده است، لغو می‌گردد.

```
REVOKE <privilege> FROM <proxy_user>;
```

۴-۶-۴ مجوز EXECUTE ANY PROCEDURE کاربر OUTLN

مجوز EXECUTE ANY PROCEDURE به طور پیش‌فرض به کاربر OUTLN اعطا می‌شود.

تهدید/توجیه امنیتی:

کاربر OUTLN نیازی به این مجوز ندارد و در صورت داشتن این مجوز می‌تواند خطرات امنیتی به دنبال داشته باشد.

اطلاع از وضعیت فعلی:

اگـر پرسـمان زیـر، سـطری برگردانـد بـدین معناسـت کـه کـاربر OUTLN مجـوز EXECUTE ANY PROCEDURE را دارد.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='EXECUTE
ANY PROCEDURE' AND GRANTEE='OUTLN';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز EXECUTE ANY PROCEDURE کاربر OUTLN لغو می‌گردد.

```
REVOKE EXECUTE ANY PROCEDURE FROM OUTLN;
```

۴-۶-۵ مجوز EXECUTE ANY PROCEDURE کاربر DBSNMP

مجوز EXECUTE ANY PROCEDURE به طور پیش‌فرض به کاربر DBSNMP اعطا می‌شود.

تهدید/توجیه امنیتی:

کاربر DBSNMP نیازی به این مجوز ندارد و در صورت داشتن این مجوز می‌تواند خطرات امنیتی بـه دنبـال داشته باشد.

اطلاع از وضعیت فعلی:

اگـر پرسـمان زیـر، سـطری برگردانـد بـدین معناسـت کـه کـاربر DBSNMP مجـوز EXECUTE ANY PROCEDURE را دارد.

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='EXECUTE
ANY PROCEDURE' AND GRANTEE='DBSNMP';
```

مقاوم‌سازی:

با اجرای دستور زیر، مجوز EXECUTE ANY PROCEDURE کاربر DBSNMP لغو می‌گردد.

```
REVOKE EXECUTE ANY PROCEDURE FROM DBSNMP;
```

۴-۷ جمع‌بندی

در این فصل به تشریح برخی از مهم‌ترین پارامترهـای امنیتـی مربـوط بـه کنتـرل دسترسـی و مجازشـماری پرداختیم. در این راستا، تنظیمات مربوط به مجوزهای عمومی پیش‌فرض، مجوزهای عمومی غیر پیش‌فـرض، مجوزهای سیستمی، ارث‌بری مجوز از نقش های قدرتمند، مجوز دسترسی به جداول و دیدهای سیسـتمی و برخی مجوزهای خاص مورد بحث و بررسی قرار گرفت. مدیر سامانه به منظور بررسی پارامترهای مقاوم‌سازی و تهیه گزارش در این زمینه می‌تواند از چک لیست زیر استفاده نماید.

عنوان		تنظیم صحیح	
		بله	خیر
۴	کنترل دسترسی و مجازشماری		
	مجوزهای عمومی پیش‌فرض		
۴-۱	بسته DBMS_ADVISOR	☐	☐
۴-۲	بسته DBMS_CRYPTO	☐	☐
۴-۳	بسته DBMS_JAVA	☐	☐
۴-۴	بسته DBMS_JAVA_TEST	☐	☐
۴-۵	بسته DBMS_JOB	☐	☐
۴-۶	بسته DBMS_LDAP	☐	☐
۴-۷	بسته DBMS_LOB	☐	☐
۴-۸	بسته DBMS_OBFUSCATION_TOOLKIT	☐	☐
۴-۹	بسته DBMS_RANDOM	☐	☐
۴-۱۰	بسته DBMS_SCHEDULER	☐	☐
۴-۱۱	بسته DBMS_SQL	☐	☐
۴-۱۲	بسته DBMS_XMLGEN	☐	☐
۴-۱۳	بسته DBMS_XMLQUERY	☐	☐
۴-۱۴	بسته UTL_FILE	☐	☐
۴-۱۵	بسته UTL_INADDR	☐	☐
۴-۱۶	بسته UTL_TCP	☐	☐
۴-۱۷	بسته UTL_MAIL	☐	☐
۴-۱۸	بسته UTL_SMTP	☐	☐
۴-۱۹	بسته UTL_DBWS	☐	☐
۴-۲۰	بسته UTL_ORAMTS	☐	☐
۴-۲۱	بسته UTL_HTTP	☐	☐

۴-۲۲	نوع شیء HTTPURITYPE	☐	☐
۴-۲۳	بسته DBMS_XMLSTORE	☐	☐
۴-۲۴	بسته DBMS_XMLSAVE	☐	☐
۴-۲۵	بسته DBMS_REDACT	☐	☐
	مجوزهای عمومی غیر پیش‌فرض		
۴-۲۶	بسته DBMS_SYS_SQL	☐	☐
۴-۲۷	بسته DBMS_BACKUP_RESTORE	☐	☐
۴-۲۸	بسته DBMS_AQADM_SYSCALLS	☐	☐
۴-۲۹	بسته DBMS_REPACT_SQL_UTL	☐	☐
۴-۳۰	بسته INITJVMAUX	☐	☐
۴-۳۱	بسته DBMS_STREAMS_ADM_UTL	☐	☐
۴-۳۲	بسته DBMS_AQADM_SYS	☐	☐
۴-۳۳	بسته DBMS_STREAMS_RPC	☐	☐
۴-۳۴	بسته DBMS_PRVTAQIM	☐	☐
۴-۳۵	بسته LTADM	☐	☐
۴-۳۶	بسته WWV_DBMS_SQL	☐	☐
۴-۳۷	بسته WWV_EXECUTE_IMMEDIATE	☐	☐
۴-۳۸	بسته DBMS_IJOB	☐	☐
۴-۳۹	بسته DBMS_FILE_TRANSFER	☐	☐
	مجوزهای سیستمی		
۴-۴۰	مجوز SELECT ANY DICTIONARY	☐	☐
۴-۴۱	مجوز SELECT_ANY_TABLE	☐	☐
۴-۴۲	مجوز AUDIT SYSTEM	☐	☐
۴-۴۳	مجوز EXEMPT ACCESS POLICY	☐	☐
۴-۴۴	مجوز BECOME USER	☐	☐
۴-۴۵	مجوز CREATE PROCEDURE	☐	☐

۴-۴۶	مجوز ALTER SYSTEM	☐	☐
۴-۴۷	مجوزهای CREATE ANY LIBRARY	☐	☐
۴-۴۸	مجوز CREATE LIBRARY	☐	☐
۴-۴۹	مجوز GRANT ANY OBJECT PRIVILEGE	☐	☐
۴-۵۰	مجوز GRANT ANY ROLE	☐	☐
۴-۵۱	مجوز GRANT ANY PRIVILEGE	☐	☐
	ارث‌بری مجوز از نقش‌های قدرتمند		
۴-۵۲	نقش DELETE_CATALOG_ROLE	☐	☐
۴-۵۳	نقش SELECT_CATALOG_ROLE	☐	☐
۴-۵۴	نقش EXECUTE_CATALOG_ROLE	☐	☐
۴-۵۵	نقش DBA	☐	☐
	مجوز دسترسی به جداول و دیدهای سیستمی		
۴-۵۶	جدول SYS.AUD$	☐	☐
۴-۵۷	جدول SYS.USER_HISTORY$	☐	☐
۴-۵۸	جدول SYS.LINK$	☐	☐
۴-۵۹	جدول SYS.USER$	☐	☐
۴-۶۰	دیدهای مدیریتی DBA_%	☐	☐
۴-۶۱	جدول SCHEDULER$_CREDENTIAL	☐	☐
۴-۶۲	جدول SYS.USER$MIG	☐	☐
	مجوزهای خاص		
۴-۶۳	مجوزهای ANY	☐	☐
۴-۶۴	مجوز با گزینه WITH_ADMIN	☐	☐
۴-۶۵	مجوزهای مربوط به proxy user	☐	☐
۴-۶۶	مجوز EXECUTE ANY PROCEDURE کاربر OUTLN	☐	☐
۴-۶۷	مجوز EXECUTE ANY PROCEDURE کاربر DBSNMP	☐	☐

۵ تنظیمات رویدادنگاری

ثبت وقایع سیستم و بازبینی آن‌ها در صورت رخداد مشکلات فنی یا امنیتی یکی از نیازمندی‌های اصلی در پایگاه‌داده است. با توجه به این‌که انواع وقایعی که در سیستم رخ می‌دهند از درجه اهمیت متفاوتی برخوردارند و ثبت کلیه وقایع (بدون توجه به ارزش هر یک) می‌تواند منجر به کاهش کارایی سرور یا هدر رفتن فضای دیسک گردد، بنابراین لازم است یک زیرمجموعه از وقایع مهم شناسایی و رویدادنگاری در مورد آن وقایع همواره انجام شود. در مورد رویدادنگاری سایر وقایع، بسته به توانمندی‌های پردازشی و ذخیره‌سازی سرور، می‌توان تصمیم‌گیری کرد. در این قصل تعدادی از وقایع مهم که ثبت آن‌ها از ارزش امنیتی بالایی برخوردار است، معرفی می‌شوند.

۵ – ۱ رویدادنگاری سنتی

در صورتی که ممیزی به روش سنتی[4] بر پایگاه داده پیاده سازی شود، پیشنهادات این بخش برای رویدادنگاری باید مورد توجه قرار گیرند.

۵-۱-۱ USER

با استفاده از شیء USER حساب های کاربری ایجاد می‌شوند که می‌توانند با پایگاه داده با توجه به نقش‌ها و مجوزهایی که به آن‌ها تخصیص داده شده است در تعامل باشند. همچنین شیء USER می‌تواند مالک اشیای پایگاه‌داده باشد. با فعال‌سازی ممیزی بر روی شیء USER، از کلیه فعالیت‌های ایجاد، حذف، تغییر یک کاربر و هچنین تغییر گذرواژه کاربر، ممیزی تهیه می‌شود.

تهدید/توجیه امنیتی:

هر نوع تلاش غیرمجاز برای ایجاد، حذف و تغییر یک کاربر به صورت موفقیت آمیز یا ناموفق از اهمیت بالایی برخوردار است.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر، سطری برگرداند بدین معناست که کلیه وقایع مربوط به ایجاد، تغییر یا حذف یک کاربر، رویدادنگاری و ثبت می‌شود.

---

4 Traditional Auditing

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='USER' AND USER_NAME IS NULL AND PROXY_NAME IS NULL AND
SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه وقایع مربوط به ایجاد، تغییر یا حذف یک کاربر (اجرای هر کدام از دستورات CREATE USER، ALTER USER و DROP USER) رویدادنگاری و ثبت می‌شود.

```
AUDIT USER;
```

۵-۱-۲ ROLE

با استفاده از نقش، مدیریت کنترل دسترسی تسهیل می‌شود. زیرا هر نقش دارای یک مجموعه از مجوزهاست که برای اجرای عملیات کاربرانی که آن نقش را بر عهده دارند به کار می‌آید.

تهدید/توجیه امنیتی:

هر گونه تغییر در مشخصات نقش‌های موجود در پایگاه داده‌ها (مثلا ایجاد نقش، تغییر مجوزها، حذف نقش) باید با نظارت مدیران پایگاه‌داده انجام شود.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر، سطری برگرداند بدین معناست که کلیه وقایع مربوط به ایجاد، تغییر یا حذف یک نقش، رویدادنگاری و ثبت می‌شود.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='ROLE' AND USER_NAME IS NULL AND PROXY_NAME IS NULL AND
SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه وقایع مربوط به ایجاد، تغییر یا حذف یک نقش (اجرای هر کدام از دستورات CREATE ROLE، ALTER ROLE و DROP ROLE) رویدادنگاری و ثبت می‌شود.

```
AUDIT ROLE;
```

۵-۱-۳ SYSTEM GRANT

به دستورات اعطای مجوز GRANT یا لغو مجوز REVOKE که با مجوزها و نقش‌های سیستمی سر و کار دارند به طور کلی دستورات SYSTEM GRANT گفته می‌شود.

تهدید/توجیه امنیتی:

با توجه به قابلیت‌های زیادی که یک کاربر با استفاده از مجوزها و نقش‌های سیستمی به دست می‌آورد، لازم است هر گونه تغییر در اعطا یا لغو چنین مجوزها و نقش‌هایی ثبت شود.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر، سطری برگرداند بدین معناست که کلیه دستورات مربوط به اعطا یا لغو مجوزها و نقش‌های سیستمی، رویدادنگاری و ثبت می‌شود.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='SYSTEM GRANT' AND USER_NAME IS NULL AND PROXY_NAME IS
NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه دستورات مربوط به اعطا یا لغو مجوزها و نقش‌های سیستمی (اجرای دستورات GRANT system_privileges_and_roles و REVOKE system_privileges_and_roles) رویدادنگاری و ثبت می‌شود.

```
AUDIT SYSTEM GRANT;
```

۵-۱-۴ PROFILE

با استفاده از شی PROFILE می‌توان مجموعه‌ای از محدودیت‌های منابع را تعریف و به یک کاربر تخصیص داد، بدین ترتیب کاربر نمی‌تواند از منابع محدود شده فراتر رود.

تهدید/توجیه امنیتی:

با توجه به اینکه پروفایل‌ها بخشی از زیرساخت امنیتی پایگاه‌داده به حساب می‌آیند، ایجاد، تغییر و حذف آن‌ها از اهمیت بالایی برخوردار است و باید رویدادنگاری و ثبت شوند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر، سطری برگرداند بدین معناست که کلیه دستورات مربوط به ایجاد، حذف و تغییر پروفایل رویدادنگاری و ثبت می‌شود.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='PROFILE' AND USER_NAME IS NULL AND PROXY_NAME IS NULL
AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه وقایع مربوط به ایجاد، تغییر یا حذف یک پروفایل (اجرای هر کدام از دستورات CREATE PROFILE، ALTER PROFILE و DROP PROFILE) رویدادنگاری و ثبت می‌شود.

```
AUDIT PROFILE;
```

۵-۱-۵ DATABASE LINK

یک DATABASE LINK در واقع یک شمای در پایگاه داده است که امکان دسترسی به اشیائی که در یک پایگاه داده دیگر قرار دارند را فراهم می‌کند.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از یک DATABASE LINK یا تغییر در مشخصات DATABASE LINKهای موجود قادر است به سرقت اطلاعات و یا تخریب آن‌ها اقدام نماید. بنابراین رویدادنگاری از فعالیت های مرتبط با ایجاد و حذف یک DATABASE LINK از اهمیت بالایی برخوردار است.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر، سطری برگرداند بدین معناست که کلیه وقایع مربوط به ایجاد، تغییر، یا حذف یک DATABASE LINK رویدادنگاری و ثبت می‌شود.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='DATABASE LINK' AND USER_NAME IS NULL AND PROXY_NAME IS
NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه وقایع مربوط به ایجاد، تغییر، یا حذف یک DATABASE LINK (اجرای دستورات CREATE DATABASE LINK، ALTER DATABASE LINK و DROP DATABASE LINK) رویدادنگاری و ثبت می‌شود.

```
AUDIT DATABASE LINK;
```

۵-۱-۶ PUBLIC DATABASE LINK

یک PUBLIC DATABASE LINK در واقع یک شمای در پایگاه‌داده است که امکان دسترسی به اشیائی که در یک پایگاه داده دیگر قرار دارند را برای همه کاربران فراهم می‌کند.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از یک PUBLIC DATABASE LINK یا تغییر در مشخصات PUBLIC DATABASE LINKهای موجود قادر است به سرقت اطلاعات و یا تخریب آن‌ها اقدام نماید. بنابراین

رویدادنگاری از فعالیت های مرتبط با ایجاد، تغییر و حذف یک PUBLIC DATABASE LINK از اهمیت بالایی برخوردار است.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر، سطری برگرداند بدین معناست که کلیه وقایع مربوط به ایجاد، تغییر یا حذف یک PUBLIC DATABASE LINK رویدادنگاری و ثبت می‌شود.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='PUBLIC DATABASE LINK' AND USER_NAME IS NULL AND
PROXY_NAME IS NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY
ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه وقایع مربوط به ایجاد، تغییر یا حذف یک PUBLIC DATABASE LINK (اجرای دستورات CREATE PUBLIC DATABASE LINK، ALTER PUBLIC DATABASE LINK و DROP PUBLIC DATABASE LINK) رویدادنگاری و ثبت می‌شود.

```
AUDIT PUBLIC DATABASE LINK;
```

۷-۱-۵ PUBLIC SYNONYM

یک PUBLIC SYNONYM یک نام معادل است که برای یکی از اشیاء موجود در پایگاه داده (مثلا جدول، دید یا رویه ذخیره‌شده) ایجاد می‌شود. PUBLIC SYNONYM توسط تمامی کاربرانی که مجوز دسترسی به شیء مورد نظر با نام اصلی را دارند، قابل استفاده است.

تهدید/توجیه امنیتی:

دسترسی به اشیاء با استفاده از نام‌های مختلف می‌تواند در زمان جمع‌آوری شواهد مربوط به یک رویداد امنیتی به کار آید.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه وقایع مربوط به ایجاد و حذف یک PUBLIC SYNONYM رویدادنگاری و ثبت می‌شود.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='PUBLIC SYNONYM' AND USER_NAME IS NULL AND PROXY_NAME IS
NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه وقایع مربوط به ایجاد و حذف یک PUBLIC SYNONYM (اجرای دستورات CREATE PUBLIC SYNONYM و DROP PUBLIC SYNONYM) رویدادنگاری و ثبت می‌شود.

```
AUDIT PUBLIC SYNONYM;
```

۵-۱-۸ SYNONYM

یک SYNONYM یک نام معادل است که برای یکی از اشیاء موجود در پایگاه داده (مثلا جدول، دید یا رویه ذخیره‌شده) ایجاد می‌شود.

تهدید/توجیه امنیتی:

دسترسی به اشیاء با استفاده از نام‌های مختلف می‌تواند در زمان جمع‌آوری شواهد مربوط به یک رویداد امنیتی به کار آید.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه وقایع مربوط به ایجاد و حذف یک SYNONYM رویدادنگاری و ثبت می‌شود.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='SYNONYM' AND USER_NAME IS NULL AND PROXY_NAME IS NULL
AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه وقایع مربوط به ایجاد و حذف یک SYNONYM (اجرای دستورات CREATE SYNONYM و DROP SYNONYM) رویدادنگاری و ثبت می‌شود.

```
AUDIT SYNONYM;
```

۵-۱-۹ DIRECTORY

شیء DIRECTORY در واقع یک نام مستعار برای یک دایرکتوری بر روی فایل سیستم سرور است.

تهدید/توجیه امنیتی:

رویدادنگاری فعالیت های مرتبط با شیء DIRECTORY همچون ایجاد و حذف آن برای یافتن فعالیت‌های غیرمجاز مورد نیاز است.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه وقایع مربوط به ایجاد و حذف یک DIRECTORY رویدادنگاری و ثبت می‌شود.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='DIRECTORY' AND USER_NAME IS NULL AND PROXY_NAME IS NULL
AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه وقایع مربوط به ایجاد و حذف یک DIRECTORY (اجرای دستورات CREATE DIRECTORY و DROP DIRECTORY) رویدادنگاری و ثبت می‌شود.

```
AUDIT DIRECTORY;
```

۵-۱-۱۰ SELECT ANY DICTIONARY

یک کاربر با استفاده از مجوز SELECT ANY DICTIONARY قادر است تمامی اشیای شماها را مشاهده نماید.

تهدید/توجیه امنیتی:

اطلاعات محرمانه زیادی مانند گذرواژه درهم‌سازی شده کاربران در جداول سیستمی ذخیره می‌شوند. مهاجم با دسترسی به این مجوز قادر است چنین اطلاعاتی را به سرقت ببرد.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه دستوراتی که برای اجرای خود از مجوز SELECT ANY DICTIONARY استفاده می‌کنند، رویدادنگاری و ثبت می‌شوند.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='SELECT ANY DICTIONARY' AND USER_NAME IS NULL AND
PROXY_NAME IS NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY
ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه دستوراتی که برای اجرای خود از مجوز SELECT ANY DICTIONARY استفاده می‌کنند، رویدادنگاری و ثبت می‌شوند.

```
AUDIT SELECT ANY DICTIONARY;
```

۵-۱-۱۱ GRANT ANY OBJECT PRIVILEGE

یک کاربر با مجوز GRANT ANY OBJECT PRIVILEGE قادر است هر مجوزی را برای هر کدام از اشیائی که به آنها دسترسی دارد به دیگران اعطا یا از آنها بگیرد.

تهدید/توجیه امنیتی:

سوء استفاده از مجوز GRANT ANY OBJECT PRIVILEGE می‌تواند منجر به انتشار کنترل نشده مجوزهای مهم شود.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه دستورات اعطا یا لغو مجوزی که برای اجرای خود از مجوز GRANT ANY OBJECT PRIVILEGE استفاده می‌کنند، رویدادنگاری و ثبت می‌شوند.

```
SELECT PRIVILEGE, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE
PRIVILEGE='GRANT ANY OBJECT PRIVILEGE' AND USER_NAME IS NULL AND
PROXY_NAME IS NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY
ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه دستورات اعطا یا لغو مجوزی که برای اجرای خود از مجوز GRANT ANY OBJECT PRIVILEGE استفاده می‌کنند، رویدادنگاری و ثبت می‌شوند.

```
AUDIT GRANT ANY OBJECT PRIVILEGE;
```

۵-۱-۱۲ GRANT ANY PRIVILEGE

یک کاربر با مجوز GRANT ANY PRIVILEGE قادر است هر گونه مجوزی را (شامل مجوزهای سیستمی) اعطا یا لغو کند.

تهدید/توجیه امنیتی:

سوء استفاده از مجوز GRANT ANY PRIVILEGE می‌تواند منجر به انتشار کنترل نشده مجوزهای مهم شود.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه دستورات اعطا یا لغو مجوزی که برای اجرای خود از مجوز GRANT ANY PRIVILEGE استفاده می‌کنند، رویدادنگاری و ثبت می‌شوند.

```
SELECT PRIVILEGE, SUCCESS, FAILURE
FROM DBA_PRIV_AUDIT_OPTS
```

```
WHERE PRIVILEGE='GRANT ANY PRIVILEGE'
AND USER_NAME IS NULL
AND PROXY_NAME IS NULL
AND SUCCESS = 'BY ACCESS'
AND FAILURE = 'BY ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه دستورات اعطا یا لغو مجوزی که برای اجرای خود از مجوز GRANT ANY PRIVILEGE استفاده می‌کنند، رویدادنگاری و ثبت می‌شوند.

```
AUDIT GRANT ANY PRIVILEGE;
```

۵-۱-۱۳ DROP ANY PROCEDURE

یک کاربر برای برای حذف یک رویه ذخیره شده در شمای یک کاربر دیگر به مجوز DROP ANY PROCEDURE نیاز دارد.

تهدید/توجیه امنیتی:

بازبینی وقایع مرتبط با حذف رویه‌های ذخیره شده، در زمان جمع‌آوری شواهد مربوط به یک رویداد امنیتی به کار می‌آید.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه دستورات حذف یک رویه ذخیره‌شده که برای اجرای خود از مجوز DROP ANY PROCEDURE استفاده می‌کنند، رویدادنگاری و ثبت می‌شوند.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='DROP ANY PROCEDURE' AND USER_NAME IS NULL AND
PROXY_NAME IS NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY
ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه دستورات حذف یک رویه ذخیره‌شده که برای اجرای خود از مجوز DROP ANY PROCEDURE استفاده می‌کنند، رویدادنگاری و ثبت می‌شوند.

```
AUDIT DROP ANY PROCEDURE;
```

۵-۱-۱۴ SYS.AUD$

این جدول حاوی اطلاعات رویدادنگاری است.

تهدید/توجیه امنیتی:

با توجه به ثبت رویدادهای سیستم در این جدول، هرگونه دسترسی به آن یا تغییر آن باید ثبت شود.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه وقایع مربوط به دسترسی به این جدول، رویدادنگاری و ثبت می‌شود.

```
SELECT * FROM DBA_OBJ_AUDIT_OPTS WHERE OBJECT_NAME='AUD$' AND
ALT='A/A' AND AUD='A/A' AND COM='A/A' AND DEL='A/A' AND GRA='A/A' AND
IND='A/A' AND INS='A/A' AND LOC='A/A' AND REN='A/A' AND SEL='A/A' AND
UPD='A/A' AND FBK='A/A';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه وقایع مربوط به دسترسی به این جدول (SELECT, UPDATE, DELETE) رویدادنگاری و ثبت می‌شود.

```
AUDIT ALL ON SYS.AUD$ BY ACCESS;
```

۵-۱-۱۵ PROCEDURE

یک PROCEDURE نامی کلی است که به اشیائی همچون رویه ذخیره شده، تابع، کتابخانه مشترک و بسته اطلاق می‌شود.

تهدید/توجیه امنیتی:

بازبینی وقایع مرتبط با PROCEDUREها در زمان جمع‌آوری شواهد مربوط به یک رویداد امنیتی به کار می‌آید.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه دستورات ایجاد و حذف یک PROCEDURE در شمای کاربر اجرا کننده دستور، رویدادنگاری و ثبت می‌شوند.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='PROCEDURE' AND USER_NAME IS NULL AND PROXY_NAME IS NULL
AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه دستورات ایجاد و حذف یک PROCEDURE (دستورات CREATE FUNCTION، CREATE LIBRARY، CREATE PACKAGE، CREATE PACKAGE BODY،

DROP و DROP PACKAGE ،DROP LIBRARY ،DROP FUNCTION ،CREATE PROCEDURE PROCEDURE) در شمای کاربر اجرا کننده دستور، رویدادنگاری و ثبت می‌شوند.

```
AUDIT PROCEDURE;
```

۵-۱-۱۶ ALTER SYSTEM

کاربری که مجوز ALTER SYSTEM را دارد قادر است تنظیمات پایگاه‌داده از جمله تنظیمات امنیتی و رویدادنگاری را تغییر دهد.

تهدید/توجیه امنیتی:

مهاجم در صورت دسترسی به این مجوز قادر است پایگاه‌داده را تخریب کند و یا تنظیمات امنیتی و کارایی آن را مطابق میل خود تغییر دهد.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه دستورات ALTER SYSTEM رویدادنگاری و ثبت می‌شود.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='ALTER SYSTEM' AND USER_NAME IS NULL AND PROXY_NAME IS
NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه دستورات ALTER SYSTEM رویدادنگاری و ثبت می‌شود.

```
AUDIT ALTER SYSTEM;
```

۵-۱-۱۷ TRIGGER

با استفاده از TRIGGER می‌توان اعمال DML را تغییر داد یا در صورت اجرای برخی از اعمال شروع کننده توسط کاربر، اعمال دیگری اجرا شوند.

تهدید/توجیه امنیتی:

تریگر در یک شمای می‌تواند برای افزایش مجوزها، ارسال داده‌ها و سایر اعمال ناخواسته به کار گرفته شود. بنابراین تلاش برای ایجاد، تغییر و حذف تریگر در شمای دیگر از اهمیت بالایی برخوردار است.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه دستورات مربوط به ایجاد، تغییر و حذف TRIGGER (CREATE TRIGGER، DROP TRIGGER و ALTER TRIGGER) رویدادنگاری و ثبت می‌شود.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='TRIGGER' AND USER_NAME IS NULL AND PROXY_NAME IS NULL
AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه دستورات مربوط به ایجاد، تغییر و حذف TRIGGER رویدادنگاری و ثبت می‌شود.

```
AUDIT TRIGGER;
```

۵-۱-۱۸ CREATE SESSION

ایجاد نشست، پیش‌نیاز ورود هر کاربر به پایگاه داده اراکل است. با فعال‌سازی این گزینه رویدادنگاری، تمامی تلاش‌ها برای اتصال به پایگاه داده، قطع اتصال نشست و خروج از پایگاه داده به صورت موفقیت آمیز یا ناموفق، ثبت می‌شوند.

تهدید/توجیه امنیتی:

ثبت ورود و خروج کاربران به پایگاه‌داده می‌تواند در شناسایی وقایع امنیتی موثر باشد.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه وقایع مربوط به ورود و خروج تمامی کاربران رویدادنگاری و ثبت می‌شود.

```
SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE
AUDIT_OPTION='CREATE SESSION' AND USER_NAME IS NULL AND PROXY_NAME IS
NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه وقایع مربوط به ورود و خروج تمامی کاربران رویدادنگاری و ثبت می‌شود.

```
AUDIT CREATE SESSION;
```

۵-۲ ممیزی یکپارچه

در صورتی که ممیزی یکپارچه پیاده سازی شود، موارد پیشنهاد شده در این بخش می‌بایست رعایت گردد.

۵-۲-۱ CREATE USER

این دستور یک حساب کاربری جدید ایجاد می‌کند.

تهدید/توجیه امنیتی:

حساب‌های کاربری موجود در پایگاه داده باید محدود و توسط مدیران پایگاه داده کاملا شناخته شده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که ایجاد یک حساب کاربری جدید رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'CREATE USER' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، ایجاد یک حساب کاربری جدید (اجرای دستور CREATE USER) رویدادنگاری و ثبت می‌شود. می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به ایجاد کاربر تغییر داد. در صورتی که خط مشی‌ای با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS CREATE USER;
```

۵-۲-۲ ALTER USER

این دستور مشخصات مربوط به یک حساب کاربری موجود را تغییر می‌دهد.

تهدید/توجیه امنیتی:

حساب‌های کاربری موجود در پایگاه داده باید محدود و مشخصاتشان توسط مدیران پایگاه داده‌ها کاملا شناخته شده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان فوق سطری برگرداند بدین معناست که تغییر مشخصات هر حساب کاربری رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'ALTER USER' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، تغییر مشخصات هر حساب کاربری (اجرای دستور ALTER USER) رویدادنگاری و ثبت می‌شود. می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به ویرایش کاربر تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS ALTER USER;
```

۳-۲-۵ DROP USER

این دستور یک حساب کاربری را حذف می‌کند.

تهدید/توجیه امنیتی:

حساب‌های کاربری موجود در پایگاه داده باید تحت مدیریت کامل مدیران پایگاه داده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که حذف هر حساب کاربری رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'DROP USER' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، حذف هر حساب کاربری (اجرای دستور DROP USER) رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به حذف کاربر تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
```

```
ADD ACTIONS DROP USER;
```

۵-۲-۴ CREATE ROLE

این دستور یک نقش جدید ایجاد می‌کند.

تهدید/توجیه امنیتی:

نقش‌های موجود در پایگاه‌داده باید محدود و توسط مدیران پایگاه داده کاملا شناخته شده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که ایجاد یک نقش جدید، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'CREATE ROLE' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، ایجاد یک نقش جدید (اجرای دستور CREATE ROLE) رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به ایجاد نقش، تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS CREATE ROLE;
```

۵-۲-۵ ALTER ROLE

این دستور مشخصات مربوط به یک نقش موجود را تغییر می‌دهد.

تهدید/توجیه امنیتی:

نقش‌های موجود در پایگاه داده باید محدود و مشخصاتشان توسط مدیران پایگاه داده کاملا شناخته شده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که تغییر مشخصات هر نقش رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'ALTER ROLE' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، تغییر مشخصات هر نقش (اجرای دستور ALTER ROLE) رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط بـه ویـرایش نقش، تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS ALTER ROLE;
```

۶-۲-۵ DROP ROLE

این دستور یک نقش را حذف می‌کند.

تهدید/توجیه امنیتی:

نقش‌های موجود در پایگاه داده باید تحت مدیریت کامل مدیران پایگاه داده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که حذف هر نقش، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'DROP ROLE' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، حذف هر نقش (اجرای دستور DROP ROLE) رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به حذف نقش، تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجـود نـدارد، بـا دسـتور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS DROP ROLE;
```

۵-۲-۷ GRANT

این دستور برای اعطای مجوزها به کابران و نقش‌های پایگاه‌داده اراکل به کار می‌آید.

تهدید/توجیه امنیتی:

مجوزهای اعطا شده به کاربران و نقش‌های موجود در پایگاه داده باید تحت مدیریت کامل مدیران پایگاه داده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که اعطای مجوز به کاربران و نقش‌ها، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'GRANT' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، اعطای مجوزها (اجرای دستور GRANT) رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط اعطای مجوزها به کاربران و نقش‌ها، تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS GRANT;
```

۵-۲-۸ REVOKE

این دستور برای لغو مجوزهای کابران و نقش‌های پایگاه‌داده اراکل به کار می‌آید.

تهدید/توجیه امنیتی:

لغو مجوزهای از پیش اعطا شده به کاربران و نقش‌های موجود در پایگاه‌داده باید تحت مدیریت کامل مدیران پایگاه داده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که لغو مجوز کاربران و نقش‌ها رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'REVOKE' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، لغو مجوزها (اجرای دستور REVOKE) رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به لغو مجوزهای کاربران و نقش‌ها، تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS REVOKE;
```

۵-۲-۹ CREATE PROFILE

پروفایل‌های پایگاه داده اراکل برای اعمال محدودیت‌های استفاده از منابع و اجرای خط‌مشی‌های رمزعبور همچون قوانین پیچیدگی رمزعبور و محدودیت‌های استفاده مجدد از رمزهای عبور پیشین، استفاده می‌شود. با فعال‌سازی تهیه ممیزی از عبارت‌های CREATE PROFILE، تمامی عبارت‌های CREATE PROFILE اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

یک مهاجم با ایجاد یک پروفایل جعلی می‌تواند سیاست‌های امنیتی را نقض کند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که ایجاد یک پروفایل، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'CREATE PROFILE' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، ایجاد یک پروفایل (اجرای دستور CREATE PROFILE) رویدادنگاری و ثبت می‌شود. می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به ایجاد پروفایل، تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS CREATE PROFILE;
```

۵-۲-۱۰ ALTER PROFILE

با فعال‌سازی تهیه ممیزی از عبارت‌های ALTER PROFILE، تمامی عبارت‌های ALTER PROFILE اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

یک مهاجم با ایجاد تغییر در یک پروفایل می‌تواند سیاست‌های امنیتی را نقض کند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که تغییر یک پروفایل، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'ALTER PROFILE' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، تغییر یک پروفایل (اجرای دستور ALTER PROFILE) رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به ویرایش پروفایل تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS ALTER PROFILE;
```

۵-۲-۱۱ DROP PROFILE

با فعال‌سازی تهیه ممیزی از عبارت‌های DROP PROFILE، تمامی عبارت‌های DROP PROFILE اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

یک مهاجم با حذف یک پروفایل می‌تواند سیاست‌های امنیتی را نقض کند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که حذف یک پروفایل، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'DROP PROFILE' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، حذف یک پروفایل (اجرای دستور DROP PROFILE) رویدادنگاری و ثبت می‌شود.

لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به حذف پروفایل تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS DROP PROFILE;
```

۵-۲-۱۲ CREATE DATABASE LINK

لینک‌های پایگاه داده اراکل، برای برقراری ارتباط از یک پایگاه داده به پایگاه داده دیگر به کار برده می‌شوند. پس از برقراری ارتباط، ارتباط ایجاد شده بدون نیاز به تصدیق اصالت در دسترس است. با فعال‌سازی تهیه ممیزی از اعمال CREATE DATABASE LINK، کلیه عبارات CREATE DATABASE LINK و CREATE PUBLIC DATABASE LINK اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

لینک‌های پایگاه‌داده و تلاش برای ایجاد آن‌ها باید تحت مدیریت کامل مدیران پایگاه‌داده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که ایجاد یک لینک، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
```

```
'CREATE DATABASE LINK' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION'
AND ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، ایجاد یک لینک (اجرای دستور CREATE DATABASE LINK) رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به ایجاد لینک تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS CREATE DATABASE LINK;
```

۱۳-۲-۵ ALTER DATABASE LINK

با فعال‌سازی تهیه ممیزی از اعمال ALTER DATABASE LINK، کلیه عبارات ALTER DATABASE LINK و ALTER PUBLIC DATABASE LINK اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

لینک‌های پایگاه داده و تلاش برای تغییر آن‌ها باید تحت مدیریت کامل مدیران پایگاه داده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که تغییر یک لینک، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'ALTER DATABASE LINK' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION'
AND ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، تغییر یک لینک (اجرای دستور ALTER DATABASE LINK) رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به ویرایش لینک تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
```

```
ADD ACTIONS ALTER DATABASE LINK;
```

۵-۲-۱۴ DROP DATABASE LINK

با فعال‌سازی تهیه ممیزی از اعمال DROP DATABASE LINK، کلیه عبارات DROP DATABASE LINK و DROP PUBLIC DATABASE LINK اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

لینک‌های پایگاه‌داده و تلاش برای حذف آن‌ها باید تحت مدیریت کامل مدیران پایگاه داده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که حذف یک لینک، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'DROP DATABASE LINK' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION'
AND ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، حذف یک لینک (اجرای دستور DROP DATABASE LINK) رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به حذف لینک تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS DROP DATABASE LINK;
```

۵-۲-۱۵ CREATE SYNONYM

در پایگاه داده اراکل از SYNONYM برای ایجاد نام دیگری برای شی‌ای از پایگاه‌داده همچون جدول، دید یا رویه استفاده می‌شود. با فعال‌سازی تهیه ممیزی از اعمال CREATE SYNONYM، کلیه عبارات CREATE SYNONYM و CREATE PUBLIC SYNONYM اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

SYNONYMهای پایگاه‌داده و تلاش برای ایجاد آن‌ها باید تحت مدیریت کامل مدیران پایگاه داده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که ایجاد یک SYNONYM، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'CREATE SYNONYM' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، ایجاد یک SYNONYM (اجرای دستور CREATE SYNONYM) رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به ایجاد SYNONYM تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS CREATE SYNONYM;
```

۱۶-۲-۵ ALTER SYNONYM

با فعال‌سازی تهیه ممیزی از اعمال ALTER SYNONYM، کلیه عبارات ALTER SYNONYM و ALTER PUBLIC SYNONYM اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

SYNONYM های پایگاه داده و تلاش برای تغییر آن ها باید تحت مدیریت کامل مدیران پایگاه داده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که تغییر یک SYNONYM، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'ALTER SYNONYM' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، تغییر یک SYNONYM (اجرای دستور ALTER SYNONYM) رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به ویرایش SYNONYM تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS ALTER SYNONYM;
```

۵-۲-۱۷ DROP SYNONYM

با فعال‌سازی تهیه ممیزی از اعمال DROP SYNONYM، کلیه عبارات DROP SYNONYM و DROP PUBLIC SYNONYM اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

SYNONYM های پایگاه‌داده و تلاش برای حذف آن‌ها باید تحت مدیریت کامل مدیران پایگاه داده باشند.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که حذف یک SYNONYM، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'DROP SYNONYM' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، حذف یک SYNONYM (اجرای دستور DROP SYNONYM) رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به حذف SYNONYM تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS DROP SYNONYM;
```

۵-۲-۱۸ مجوز SELECT ANY DICTIONARY

این مجوز به کاربر اجازه دسترسی به اشیاء شمای SYS را می‌دهد.

تهدید/توجیه امنیتی:

مهاجم با سوء استفاده از این مجوز می‌تواند کلیه اشیاء شمای SYS را بخواند. به عنوان مثال، مقدار درهم‌سازی شده گذرواژه تمامی کاربران در شمای SYS قرار دارد که به این ترتیب فاش می‌شود.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که هر تلاشی برای دسترسی به اشیای شمای SYS، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'SELECT ANY DICTIONARY' AND AUD.AUDIT_OPTION_TYPE = 'SYSTEM
PRIVILEGE' AND ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES'
AND ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، هر تلاشی برای دسترسی به اشیای شمای SYS، رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به مجوز SELECT ANY DICTIONARY تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD PRIVILEGES SELECT ANY DICTIONARY;
```

۱۹-۲-۵ دید UNIFIED_AUDIT_TRAIL

دید UNIFIED_AUDIT_TRAIL رکوردهای رویدادنگاری که توسط پایگاه داده تولید شده‌اند را ثبت می‌نماید.

تهدید/توجیه امنیتی:

تمامی تلاش‌ها برای دسترسی به دید UNIFIED_AUDIT_TRAIL از اهمیت بالایی برخوردار است و باید تحت مدیریت کامل مدیران پایگاه داده باشد.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که هر تلاشی برای دسترسی به دید UNIFIED_AUDIT_TRAIL، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'ALL' AND AUD.AUDIT_OPTION_TYPE = 'OBJECT ACTION' AND
AUD.OBJECT_SCHEMA = 'SYS' AND AUD.OBJECT_NAME = 'UNIFIED_AUDIT_TRAIL'
AND ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، هر تلاشی برای دسترسی به دید UNIFIED_AUDIT_TRAIL رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به دسترسی به دید UNIFIED_AUDIT_TRAIL تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS
ALL on SYS.UNIFIED_AUDIT_TRAIL;
```

۵-۲-۲۰ CREATE PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY

رویه‌های ذخیره شده، توابع، بسته‌ها و بدنه‌ی بسته‌ها[1]در پایگاه داده ذخیره می‌شوند و برای انجام وظایف مختلف در پایگاه داده به کار می‌روند. با فعال‌سازی این نوع ممیزی، تمامی عبارات CREATE PROCEDURE، CREATE FUNCTION، CREATE PACKAGE و CREATE PACKAGE BODY اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

رویه های ذخیره شده، توابع، بسته ها و بدنه‌ی بسته ها و تلاش برای ایجاد آن ها باید تحت مدیریت کامل مدیران پایگاه داده باشد.

اطلاع از وضعیت فعلی:

---

[4] Package bodies [1]

اگر پرسمان زیر سطری برگرداند بدین معناست که هر تلاشی برای ایجاد رویه‌های ذخیره شده، توابع، بسته‌ها و بدنه‌ی بسته‌ها، رویدادنگاری و ثبت می‌شود.

```
SELECT * FROM AUDIT_UNIFIED_ENABLED_POLICIES ENABLED WHERE
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS' AND
EXISTS ( SELECT 'x' FROM AUDIT_UNIFIED_POLICIES AUD WHERE
AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'CREATE
PROCEDURE' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION') AND EXISTS
( SELECT 'x' FROM AUDIT_UNIFIED_POLICIES AUD WHERE AUD.POLICY_NAME =
ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'CREATE FUNCTION' AND
AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION') AND EXISTS ( SELECT 'x'
FROM AUDIT_UNIFIED_POLICIES AUD WHERE AUD.POLICY_NAME =
ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'CREATE PACKAGE' AND
AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION') AND EXISTS ( SELECT 'x'
FROM AUDIT_UNIFIED_POLICIES AUD WHERE AUD.POLICY_NAME =
ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'CREATE PACKAGE BODY' AND
AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION');
```

مقاوم‌سازی:

با اجرای دستور زیر، هر تلاشی برای ایجاد رویه‌های ذخیره شده، توابع، بسته‌ها و بدنه‌ی بسته‌ها، رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به ایجاد رویه‌های ذخیره شده، توابع، بسته‌ها و بدنه‌ی بسته‌ها تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY ADD ACTIONS CREATE
PROCEDURE, CREATE FUNCTION, CREATE PACKAGE, CREATE PACKAGE BODY;
```

۵-۲-۲۱ ALTER PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY

با فعال‌سازی این نوع ممیزی، تمامی عبارات ALTER PROCEDURE، ALTER FUNCTION، ALTER PACKAGE و ALTER PACKAGE BODY اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

رویه های ذخیره شده، توابع، بسته‌ها و بدنه‌ی بسته‌ها و تلاش برای تغییر آن‌ها باید تحت مدیریت کامل مدیران پایگاه داده باشد.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که هر تلاشی برای تغییر رویه‌های ذخیره شده، توابع، بسته‌ها و بدنه‌ی بسته‌ها، رویدادنگاری و ثبت می‌شود.

```
SELECT * FROM AUDIT_UNIFIED_ENABLED_POLICIES ENABLED WHERE
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS' AND
EXISTS ( SELECT 'x' FROM AUDIT_UNIFIED_POLICIES AUD WHERE
AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'ALTER
PROCEDURE' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION') AND EXISTS
( SELECT 'x' FROM AUDIT_UNIFIED_POLICIES AUD WHERE AUD.POLICY_NAME =
ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'ALTER FUNCTION' AND
AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION') AND EXISTS ( SELECT 'x'
FROM AUDIT_UNIFIED_POLICIES AUD WHERE AUD.POLICY_NAME =
ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'ALTER PACKAGE' AND
AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION') AND EXISTS ( SELECT 'x'
FROM AUDIT_UNIFIED_POLICIES AUD WHERE AUD.POLICY_NAME =
ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'ALTER PACKAGE BODY' AND
AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION');
```

مقاوم‌سازی:

با اجرای دستور زیر، هر تلاشی برای تغییر رویه‌های ذخیره شده، توابع، بسته‌ها و بدنه‌ی بسته‌ها، رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به تغییر رویه‌های ذخیره شده، توابع، بسته‌ها و بدنه‌ی بسته‌ها تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS
ALTER PROCEDURE,
ALTER FUNCTION,
ALTER PACKAGE,
ALTER PACKAGE BODY;
```

۵-۲-۲۲ DROP PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY

با فعال‌سازی این نوع ممیزی، تمامی عبارات DROP PROCEDURE، DROP FUNCTION، DROP PACKAGE و DROP PACKAGE BODY اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

رویه‌های ذخیره شده، توابع، بسته‌ها و بدنه‌ی بسته‌ها و تلاش برای حذف آن ها باید تحت مدیریت کامل مدیران پایگاه داده باشد.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که هر تلاشی برای حذف رویه‌های ذخیره شده، توابع، بسته‌ها و بدنه‌ی بسته‌ها، رویدادنگاری و ثبت می‌شود.

```
SELECT * FROM AUDIT_UNIFIED_ENABLED_POLICIES ENABLED WHERE
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS' AND
EXISTS ( SELECT 'x' FROM AUDIT_UNIFIED_POLICIES AUD WHERE
AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'DROP
PROCEDURE' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION') AND EXISTS
( SELECT 'x' FROM AUDIT_UNIFIED_POLICIES AUD WHERE AUD.POLICY_NAME =
ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'DROP FUNCTION' AND
AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION') AND EXISTS ( SELECT 'x'
FROM AUDIT_UNIFIED_POLICIES AUD WHERE AUD.POLICY_NAME =
ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'DROP PACKAGE' AND
AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION') AND EXISTS ( SELECT 'x'
FROM AUDIT_UNIFIED_POLICIES AUD WHERE AUD.POLICY_NAME =
ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'DROP PACKAGE BODY' AND
AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION');
```

مقاوم‌سازی:

با اجرای دستور زیر، هر تلاشی برای حذف رویه‌های ذخیره شده، توابع، بسته‌ها و بدنه‌ی بسته‌ها، رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به حذف رویه‌های ذخیره شده، توابع، بسته‌ها و بدنه‌ی بسته‌ها تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD
ACTIONS
DROP PROCEDURE,
DROP FUNCTION,
DROP PACKAGE,
DROP PACKAGE BODY;
```

۵-۲-۲۳ ALTER SYSTEM

مجوز ALTER SYSTEM به کاربر این امکان را می‌دهد که تنظیمات اراکل که بر روی امنیت، کارایی و عملکرد عادی پایگاه داده تأثیرگذار است را تغییر دهند.

تهدید/توجیه امنیتی:

تلاش‌ها برای اجرای عبارت‌های ALTER SYSTEM باید تحت مدیریت کامل مدیران پایگاه‌داده باشد.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که هر تلاشی برای اجرای عبارت ALTER SYSTEM، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'ALTER SYSTEM' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، هر تلاشی برای اجرای عبارت ALTER SYSTEM رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به تلاش برای اجرای عبارت ALTER SYSTEM تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS
ALTER SYSTEM;
```

۵-۲-۲۴ CREATE TRIGGER

هنگامی که شرایط از پیش تعریف شده‌ای بر روی اشیای پایگاه داده به وقوع انجامد، رهانا به صورت خودکار اجرا می شود. با فعال‌سازی تهیه ممیزی از اعمال CREATE TRIGGER، کلیه عبارات CREATE TRIGGER اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

بازبینی وقایع مرتبط با ایجاد رهاناها در زمان جمع‌آوری شواهد مربوط به یک رویداد امنیتی به کار می‌آید.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه دستورات ایجاد یک رهانا، رویدادنگاری و ثبت می‌شود.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
```

```
'CREATE TRIGGER' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه دستورات ایجاد یک رهانا رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به ایجاد رهانا تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS
CREATE TRIGGER;
```

۵-۲-۲۵ ALTER TRIGGER

با فعال‌سازی تهیه ممیزی از اعمال ALTER TRIGGER، کلیه عبارات ALTER TRIGGER اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

بازبینی وقایع مرتبط با تغییر رهاناها در زمان جمع‌آوری شواهد مربوط به یک رویداد امنیتی، به کار می‌آید.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه دستورات تغییر یک رهانا رویدادنگاری و ثبت می‌شوند.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'ALTER TRIGGER' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه دستورات تغییر یک رهانا رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به ویرایش رهانا تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS
ALTER TRIGGER;
```

۵-۲-۲۶ DROP TRIGGER

با فعال‌سازی تهیه ممیزی از اعمال DROP TRIGGER، کلیه عبارات DROP TRIGGER اجرا شده به صورت موفقیت‌آمیز یا ناموفق ثبت می‌شوند.

تهدید/توجیه امنیتی:

بازبینی وقایع مرتبط با حذف رهاناها در زمان جمع‌آوری شواهد مربوط به یک رویداد امنیتی به کار می‌آید.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که کلیه دستورات حذف یک رهانا، رویدادنگاری و ثبت می‌شوند.

```
SELECT AUD.POLICY_NAME, AUD.AUDIT_OPTION, AUD.AUDIT_OPTION_TYPE FROM
AUDIT_UNIFIED_POLICIES AUD, AUDIT_UNIFIED_ENABLED_POLICIES ENABLED
WHERE AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION =
'DROP TRIGGER' AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION' AND
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS';
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه دستورات حذف یک رهانا رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به حذف رهانا تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS
DROP TRIGGER;
```

۵-۲-۲۷ LOGON و LOGOFF

کاربران پایگاه‌داده برای انجام کارهای مختلف وارد پایگاه داده می‌شوند.

تهدید/توجیه امنیتی:

فعال‌سازی رویدادنگاری از عملیات ورود به پایگاه داده و خروج از آن برای جرم شناسی وقایع مخرب اهمیت بسزایی دارد.

اطلاع از وضعیت فعلی:

اگر پرسمان زیر سطری برگرداند بدین معناست که ورود و خروج کاربران از پایگاه‌داده، رویدادنگاری و ثبت می‌شود.

```
SELECT * FROM AUDIT_UNIFIED_ENABLED_POLICIES ENABLED WHERE
ENABLED.SUCCESS = 'YES' AND ENABLED.FAILURE = 'YES' AND
ENABLED.ENABLED_OPT = 'BY' AND ENABLED.USER_NAME = 'ALL USERS' AND
EXISTS ( SELECT 'x' FROM AUDIT_UNIFIED_POLICIES AUD WHERE
AUD.POLICY_NAME = ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'LOGON'
AND AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION') AND EXISTS ( SELECT
'x' FROM AUDIT_UNIFIED_POLICIES AUD WHERE AUD.POLICY_NAME =
ENABLED.POLICY_NAME AND AUD.AUDIT_OPTION = 'LOGOFF' AND
AUD.AUDIT_OPTION_TYPE = 'STANDARD ACTION');
```

مقاوم‌سازی:

با اجرای دستور زیر، کلیه‌ی ورودها و خروج‌های کاربران از پایگاه‌داده رویدادنگاری و ثبت می‌شود. لازم به ذکر است که می‌توان یک خط مشی از پیش تعریف شده را برای ثبت رویدادهای مربوط به ورود و خروج کاربران از پایگاه داده تغییر داد. در صورتی که خط مشی با نام CIS_UNIFIED_AUDIT_POLICY وجود ندارد، با دستور CREATE AUDIT POLICY می‌توان آن را ایجاد کرد.

```
ALTER AUDIT POLICY CIS_UNIFIED_AUDIT_POLICY
ADD ACTIONS
LOGON,
LOGOFF;
```

۳-۵ جمع‌بندی

در این فصل به تشریح برخی از مهم‌ترین پارامترهای امنیتی مربوط به پیکربندی تنظیمات رویدادنگاری پرداختیم. در این راستا، تنظیمات مربوط به رویدادنگاری سنتی و ممیزی یکپارچه مورد بحث و بررسی قرار گرفت. مدیر سامانه به منظور بررسی پارامترهای مقاوم‌سازی و تهیه گزارش در این زمینه می‌تواند از چک لیست زیر استفاده نماید.

عنوان	تنظیم صحیح

٪	ع	
		۵ تنظیمات رویدادنگاری
		رویدادنگاری سنتی
☐	☐	USER ۵-۱
☐	☐	ROLE ۵-۲
☐	☐	SYSTEM GRANT ۵-۳
☐	☐	PROFILE ۵-۴
☐	☐	DATABASE LINK ۵-۵
☐	☐	PUBLIC DATABASE LINK ۵-۶
☐	☐	PUBLIC SYNONYM ۵-۷
☐	☐	SYNONYM ۵-۸
☐	☐	DIRECTORY ۵-۹
☐	☐	SELECT ANY DICTIONARY ۵-۱۰
☐	☐	GRANT ANY OBJECT PRIVILEGE ۵-۱۱
☐	☐	GRANT ANY PRIVILEGE ۵-۱۲
☐	☐	DROP ANY PROCEDURE ۵-۱۳
☐	☐	SYS.AUD$ ۵-۱۴
☐	☐	PROCEDURE ۵-۱۵
☐	☐	ALTER SYSTEM ۵-۱۶
☐	☐	TRIGGER ۵-۱۷
☐	☐	CREATE SESSION ۵-۱۸
		ممیزی یکپارچه
☐	☐	CREATE USER ۵-۱۹
☐	☐	ALTER USER ۵-۲۰
☐	☐	DROP USER ۵-۲۱

☐	☐	CREATE ROLE	۵-۲۲
☐	☐	ALTER ROLE	۵-۲۳
☐	☐	DROP ROLE	۵-۲۴
☐	☐	GRANT	۵-۲۵
☐	☐	REVOKE	۵-۲۶
☐	☐	CREATE PROFILE	۵-۲۷
☐	☐	ALTER PROFILE	۵-۲۸
☐	☐	DROP PROFILE	۵-۲۹
☐	☐	CREATE DATABASE LINK	۵-۳۰
☐	☐	ALTER DATABASE LINK	۵-۳۱
☐	☐	DROP DATABASE LINK	۵-۳۲
☐	☐	CREATE SYNONYM	۵-۳۳
☐	☐	ALTER SYNONYM	۵-۳۴
☐	☐	DROP SYNONYM	۵-۳۵
☐	☐	SELECT ANY DICTIONARY	۵-۳۶
☐	☐	UNIFIED_AUDIT_TRAIL	۵-۳۷
☐	☐	CREATE PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY	۵-۳۸
☐	☐	ALTER PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY	۵-۳۹
☐	☐	DROP PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY	۵-۴۰
☐	☐	ALTER SYSTEM	۵-۴۱
☐	☐	CREATE TRIGGER	۵-۴۲
☐	☐	ALTER TRIGGER	۵-۴۳
☐	☐	DROP TRIGGER	۵-۴۴
☐	☐	LOGON و LOGOFF	۵-۴۵

۶ راهنمای ابزار مقاوم‌سازی

این پروژه دارای سه فایل اجرایی است که در ادامه به بررسی هر یک می‌پردازیم.

۶-۱ فایل start.sh

این فایل، تنها فایلی است که کاربر باید آن را اجرا نماید. برای اجرای این فایل باید یا با استفاده از نام کاربری oracle و با دستور sudo su – oracle وارد شده و این اسکریپت اجرا شود یا با استفاده از دستور زیر اسکریپت اجرا شده و سایر اسکریپت‌ها در محل دایرکتوری /home/oracle قرار داشته باشند.

```
su -  -c "<path>/start.sh" oracle
```

برای آنکه فرآیند تست پایگاه‌داده و امن‌سازی آن صورت گیرد، ابتدا لازم است از وجود Oracle روی سیستم اطمینان حاصل گردد. در صورتی که Oracle روی سیستم نصب بوده، متغیرهای محیطی ORACLE_HOME و ORACLE_SID اگر تا به حال تنظیم نشده باشند، تنظیم می شوند و سپس اسکریپت script.sh اجرا می‌شود. در اثر اجرای این فایل، دو پوشه حاوی نتایج آزمایش و نتایج مورد انتظار ایجاد می‌شوند. حال در این اسکریپت قصد داریم این دو پوشه را با هم مقایسه کنیم تا مغایرت‌های سیستم با موارد امنیتی مورد انتظار مشخص شوند. نتایج این آزمایش در فایل first_test_result ثبت می‌شود. نمونه‌ای از خروجی این برنامه در شکل (۱) نشان داده شده است.

```
     "ORACLE RESULT"                                    "EXPECTED RESULT"

<------1-1-Default Passwords for Default Users ------>      <------1-1-Default Passwords for Default Users ------>
LBACSYS REMOTE_SCHEDULER_AGENT WMSYS APPQOSSYS OJVMSYS GSMCAT | NONE


<------1-2-Sample Users and Data ------>                    <------1-2-Sample Users and Data ------>
NONE                                                       NONE


<------2-1-1-SECURE_CONTROL Parameter ------>               <------2-1-1-SECURE_CONTROL Parameter ------>
NONE                                                     | SECURE_CONTROL_listener = (TCPS,IPC)
                                                         > OR
                                                         > SECURE_CONTROL_listener = TCPS
                                                         > OR
                                                         > SECURE_CONTROL_listener = IPC


<------2-1-2-EXTPROC Configuration ------>               | <------2-1-2-EXTPROC Configuratio ------>
  (sid_name=extproc)                                     | NONE
  (program=extproc)                                      <


<------2-1-3-ADMIN_RESTRICTIONS Parameter ------>          <------2-1-3-ADMIN_RESTRICTIONS Parameter ------>
NONE                                                     | ADMIN_RESTRICTIONS_listener = ON
```

شکل ۱: محتوای فایل first_test_result

ستون سمت چپ نشان دهنده تنظیمات فعلی و ستون سمت راست نشان دهنده تنظیمات مورد انتظار است. پس از اجرای این اسکریپت، در صورت تمایل کاربر، اسکریپت repair اجرا می‌شود. سپس هر مورد امنیتی که

در آن نتیجه مورد انتظار و نتیجه حاصل از تست مغایر باشند، با موافقت کاربر امن‌سازی شده و در آخر نیز تست دوباره‌ای روی سیستم انجام می‌شود. نتیجه تست دوم در فایل second_test_result ذخیره خواهد شد.

توجه به این نکته حائز اهمیت است که تنظیمات مربوط به شنونده‌ها[4] تنها برای شنونده‌هایی بررسی و بهبود می‌یابد که در زمان اجرای اسکریپت در وضعیت در حال اجرا قرار داشته باشند.

در کل فرآیند امن سازی پایگاه‌داده اراکل، تنها امن‌سازی سه مورد به طور خودکار انجام نشده و اعمال تنظیمات باید توسط کاربر انجام شوند. این سه مورد عبارتند از:

- نصب آخرین بسته‌های تکمیلی برای پایگاه داده اراکل: بسته های تکمیلی باید توسط کاربر از سایت‌های مناسب بارگیری و سپس نصب شوند.
- تنظیمات مربوط به EXTPROC
- تنظیمات مربوط به پارامتر SECURE_CONTROL

مورد دوم و سوم یعنی تنظیمات مربوط به EXTPROC و SECURE_CONTROL در فایل listener.ora انجام می‌شوند. با توجه به وابسته بودن تنظیمات مختلف به تنظیمات مذکور، دستی انجام شدن آن‌ها از خطاهای احتمالی حاصل از خودکار تغییر دادن فایل listener.or جلوگیری می‌کند. در صورت عدم اعمال تنظیمات مناسب یا به درستی تمامی تنظیمات مربوط به EXTPROC حذف نمی‌شوند و یا تنظیمات مربوط به پارامتر SECURE_CONTROL باعث عدم اجرای شنونده می‌شوند. بنابراین تنظیمات این دو پارامتر باید با دقت در فایل listener.ora اعمال شوند.

4 Listener 2

```
|      "ORACLE RESULT"                                    "EXPECTED RESULT"

<------1-1-Default Passwords for Default Users ------>      <------1-1-Default Passwords for Default Users ------>
NONE                                                       NONE



<------1-2-Sample Users and Data ------>                   <------1-2-Sample Users and Data ------>
NONE                                                       NONE



<------2-1-1-SECURE_CONTROL Parameter ------>              <------2-1-1-SECURE_CONTROL Parameter ------>
NONE                                                     | SECURE_CONTROL_LISTENER = (TCPS,IPC)
                                                         > OR
                                                         > SECURE_CONTROL_LISTENER = TCPS
                                                         > OR
                                                         > SECURE_CONTROL_LISTENER = IPC



<------2-1-2-EXTPROC Configuration ------>               | <------2-1-2-EXTPROC Configuratio ------>
  (sid_name=extproc)                                     | NONE
  (program=extproc)                                      <



<------2-1-3-ADMIN_RESTRICTIONS Parameter ------>           <------2-1-3-ADMIN_RESTRICTIONS Parameter ------>
ADMIN_RESTRICTIONS_listener = ON                         | ADMIN_RESTRICTIONS_LISTENER = ON
```

شکل ۲: محتوای فایل second_file_result

۶-۲ فایل script.sh

در این فایل دو متغیر با نام‌های result_path و expected_path تعریف شده است. این دو متغیر به پوشه‌هایی اشاره می‌کنند که در آن‌ها به ترتیب نتایج هر آزمایش و نتیجه مورد انتظار آن آزمایش، ساخته می‌شود. در اینجا لازم است بنا به نیازمندی سیستم و نکات گفته شده حین توضیح هر مورد، نتایج مورد انتظار برای هر مورد امنیتی تنظیم شود. این کد توسط برنامه start.sh اجرا می‌شود.

۶-۳ فایل repair.sh

فایل آخر مربوط به تغییر تنظیمات سیستم می‌باشد. در صورتی که تنظیمات به درستی انجام شده باشد، انتظار می‌رود که مورد امنیتی در ستون دوم وجود نداشته باشد و تنها چند پیشنهاد برای امنیت بیشتر در آن باقی بماند. در شکل (۲) می‌توان نمونه ای از فایل second_test-result را پس از اعمال تغییرات مشاهده نمود.

۷ جمع‌بندی

در این مستند به بررسی موارد امنیتی مربوط به مقاوم‌سازی اراکل پرداخته شد. تنظیمات مربوط به مقاوم‌سازی اراکل در پنج بخش مختلف دسته بندی شدند. در بخش اول، امن‌سازی محیط اجرا، بخش دوم نصب و پیکربندی امن پایگاه‌داده، بخش سوم امن‌سازی اتصال به پایگاه‌داده، بخش چهارم تنظیمات کنترل دسترسی و مجازشماری و بخش پنجم تنظیمات رویداد نگاری بررسی شدند. در مورد هر پارامتر، کاربرد، ارزش امنیتی و نحوه آگاهی از مقدار کنونی آن پارامتر و چگونگی مقداردهی امن آن توضیحاتی داده شد. در پایان نیز نحوه اجرای اسکریپت‌ها و خروجی‌های سیستم بیان شدند. خلاصه‌ای از گزارش ارائه شده به صورت یک چک لیست در ادامه آورده شده است.

	عنوان	تنظیم صحیح	
		ع.	بله
۱	**ایمن سازی محیط اجرا**		
۱-۱	**امن‌سازی حساب‌های کاربری با گذرواژه‌های پیش‌فرض**		
۱-۱-۱	حساب کاربری APEX_040000	☐	☐
۱-۱-۲	حساب کاربری APPQOSSYS	☐	☐
۱-۱-۳	حساب کاربری CTXSYS	☐	☐
۱-۱-۴	حساب کاربری DBSNMP	☐	☐
۱-۱-۵	حساب کاربری DIP	☐	☐
۱-۱-۶	حساب کاربری EXFSYS	☐	☐
۱-۱-۷	حساب کاربری MDDATA	☐	☐
۱-۱-۸	حساب کاربری MDSYS	☐	☐
۱-۱-۹	حساب کاربری LBACSYS	☐	☐
۱-۱-۱۰	حساب کاربری OLAPSYS	☐	☐
۱-۱-۱۱	حساب کاربری ORACLE_OCM	☐	☐

۱-۱-۱۲	حساب کاربری ORDDATA	☐	☐
۱-۱-۱۳	حساب کاربری ORDPLUGINS	☐	☐
۱-۱-۱۴	حساب کاربری ORDSYS	☐	☐
۱-۱-۱۵	حساب کاربری OUTLN	☐	☐
۱-۱-۱۶	حساب کاربری OWBSYS_AUDIT	☐	☐
۱-۱-۱۷	حساب کاربری OWBSYS	☐	☐
۱-۱-۱۸	حساب کاربری SI_INFORMTN_SCHEMA	☐	☐
۱-۱-۱۹	حساب کاربری SPATIAL_CSW_ADMIN_USR	☐	☐
۱-۱-۲۰	حساب کاربری SPATIAL_WFS_ADMIN_USR	☐	☐
۱-۱-۲۱	حساب کاربری SYS	☐	☐
۱-۱-۲۲	حساب کاربری SYSTEM	☐	☐
۱-۱-۲۳	حساب کاربری WK_TEST	☐	☐
۱-۱-۲۴	حساب کاربری WKPROXY	☐	☐
۱-۱-۲۵	حساب کاربری WKSYS	☐	☐
۱-۱-۲۶	حساب کاربری WMSYS	☐	☐
۱-۱-	حساب کاربری XDB	☐	☐

۲۷			
۱-۲	**امن‌سازی حساب‌های کاربری نمونه**		
۱-۲-۱	حساب کاربری نمونه BI	☐	☐
۱-۲-۲	حساب کاربری نمونه HR	☐	☐
۱-۲-۳	حساب کاربری نمونه IX	☐	☐
۱-۲-۴	حساب کاربری نمونه OE	☐	☐
۱-۲-۵	حساب کاربری نمونه PM	☐	☐
۱-۲-۶	حساب کاربری نمونه SCOTT	☐	☐
۱-۲-۷	حساب کاربری نمونه SH	☐	☐
۱-۳	پیکربندی فایل‌های ذخیره داده	☐	☐
۱-۴	پیکربندی فایل‌های رویدادنگاری	☐	☐
۲	**پیکربندی امن پایگاه‌داده**		
	تنظیمات شبکه‌ای		
۲-۱	پارامتر <SECURE_CONTROL_<listener_name>	☐	☐
۲-۲	تنظیمات EXTPROC	☐	☐
۲-۳	پارامتر <ADMIN_RESTRICTIONS_<listener_name>	☐	☐
۲-۴	شماره پورت	☐	☐
۲-۵	پارامتر <SECURE_ REGISTER_<listener_name>	☐	☐
	تنظیمات عمومی		
۲-۶	پارامتر AUDIT_SYS_OPERATIONS	☐	☐
۲-۷	پارامتر AUDIT_TRAIL	☐	☐
۲-۸	پارامتر GLOBAL_NAMES	☐	☐
۲-۹	پارامتر LOCAL_LISTENER	☐	☐
۲-۱۰	پارامتر O7_DICTIONARY_ACCESSIBILITY	☐	☐
۲-۱۱	پارامتر OS_ROLES	☐	☐

۲-۱۲	پارامتر REMOTE_LISTENER	☐	☐
۲-۱۳	پارامتر REMOTE_LOGIN_PASSWORDFILE	☐	☐
۲-۱۴	پارامتر REMOTE_OS_AUTHENT	☐	☐
۲-۱۵	پارامتر REMOTE_OS_ROLES	☐	☐
۲-۱۶	پارامتر UTL_FILE_DIR	☐	☐
۲-۱۷	پارامتر SEC_CASE_SENSITIVE_LOGON	☐	☐
۲-۱۸	پارامتر SEC_MAX_FAILED_LOGIN_ATTEMPTS	☐	☐
۲-۱۹	پارامتر SEC_PROTOCOL_ERROR_FURTHER_ACTION	☐	☐
۲-۲۰	پارامتر SEC_PROTOCOL_ERROR_TRACE_ACTION	☐	☐
۲-۲۱	پارامتر SEC_RETURN_SERVER_RELEASE_BANNER	☐	☐
۲-۲۲	پارامتر SQL92_SECURITY	☐	☐
۲-۲۳	پارامتر _trace_files_public	☐	☐
۲-۲۴	پارامتر RESOURCE_LIMIT	☐	☐
	سایر تنظیمات		
۲-۲۵	نصب بسته‌های تکمیلی اراکل	☐	☐
۳	**امن‌سازی اتصال به پایگاه‌داده**		
۳-۱	پارامتر FAILED_LOGIN_ATTEMPTS	☐	☐
۳-۲	پارامتر PASSWORD_LOCK_TIME	☐	☐
۳-۳	پارامتر PASSWORD_LIFE_TIME	☐	☐
۳-۴	پارامتر PASSWORD_REUSE_MAX	☐	☐
۳-۵	پارامتر PASSWORD_REUSE_TIME	☐	☐
۳-۶	پارامتر PASSWORD_GRACE_TIME	☐	☐
۳-۷	پارامتر AUTHENTICATION_TYPE	☐	☐
۳-۸	پارامتر PASSWORD_VERIFY_FUNCTION	☐	☐
۳-۹	پارامتر SESSIONS_PER_USER	☐	☐
۳-۱۰	هیچ کاربری به پروفایل DEFAULT تخصیص داده نشود	☐	☐

۴	کنترل دسترسی و مجازشماری		
	مجوزهای عمومی پیش‌فرض		
۴-۱	بسته DBMS_ADVISOR	☐	☐
۴-۲	بسته DBMS_CRYPTO	☐	☐
۴-۳	بسته DBMS_JAVA	☐	☐
۴-۴	بسته DBMS_JAVA_TEST	☐	☐
۴-۵	بسته DBMS_JOB	☐	☐
۴-۶	بسته DBMS_LDAP	☐	☐
۴-۷	بسته DBMS_LOB	☐	☐
۴-۸	بسته DBMS_OBFUSCATION_TOOLKIT	☐	☐
۴-۹	بسته DBMS_RANDOM	☐	☐
۴-۱۰	بسته DBMS_SCHEDULER	☐	☐
۴-۱۱	بسته DBMS_SQL	☐	☐
۴-۱۲	بسته DBMS_XMLGEN	☐	☐
۴-۱۳	بسته DBMS_XMLQUERY	☐	☐
۴-۱۴	بسته UTL_FILE	☐	☐
۴-۱۵	بسته UTL_INADDR	☐	☐
۴-۱۶	بسته UTL_TCP	☐	☐
۴-۱۷	بسته UTL_MAIL	☐	☐
۴-۱۸	بسته UTL_SMTP	☐	☐
۴-۱۹	بسته UTL_DBWS	☐	☐
۴-۲۰	بسته UTL_ORAMTS	☐	☐
۴-۲۱	بسته UTL_HTTP	☐	☐
۴-۲۲	نوع شیء HTTPURITYPE	☐	☐
۴-۲۳	بسته DBMS_XMLSTORE	☐	☐
۴-۲۴	بسته DBMS_XMLSAVE	☐	☐

۴-۲۵	بسته DBMS_REDACT	☐	☐
مجوزهای عمومی غیر پیش‌فرض			
۴-۲۶	بسته DBMS_SYS_SQL	☐	☐
۴-۲۷	بسته DBMS_BACKUP_RESTORE	☐	☐
۴-۲۸	بسته DBMS_AQADM_SYSCALLS	☐	☐
۴-۲۹	بسته DBMS_REPACT_SQL_UTL	☐	☐
۴-۳۰	بسته INITJVMAUX	☐	☐
۴-۳۱	بسته DBMS_STREAMS_ADM_UTL	☐	☐
۴-۳۲	بسته DBMS_AQADM_SYS	☐	☐
۴-۳۳	بسته DBMS_STREAMS_RPC	☐	☐
۴-۳۴	بسته DBMS_PRVTAQIM	☐	☐
۴-۳۵	بسته LTADM	☐	☐
۴-۳۶	بسته WWV_DBMS_SQL	☐	☐
۴-۳۷	بسته WWV_EXECUTE_IMMEDIATE	☐	☐
۴-۳۸	بسته DBMS_IJOB	☐	☐
۴-۳۹	بسته DBMS_FILE_TRANSFER	☐	☐
مجوزهای سیستمی			
۴-۴۰	مجوز SELECT ANY DICTIONARY	☐	☐
۴-۴۱	مجوز SELECT_ANY_TABLE	☐	☐
۴-۴۲	مجوز AUDIT SYSTEM	☐	☐
۴-۴۳	مجوز EXEMPT ACCESS POLICY	☐	☐
۴-۴۴	مجوز BECOME USER	☐	☐
۴-۴۵	مجوز CREATE PROCEDURE	☐	☐
۴-۴۶	مجوز ALTER SYSTEM	☐	☐
۴-۴۷	مجوزهای CREATE ANY LIBRARY	☐	☐
۴-۴۸	مجوز CREATE LIBRARY	☐	☐

۴-۴۹	مجوز GRANT ANY OBJECT PRIVILEGE	☐	☐
۴-۵۰	مجوز GRANT ANY ROLE	☐	☐
۴-۵۱	مجوز GRANT ANY PRIVILEGE	☐	☐
	ارث‌بری مجوز از نقش‌های قدرتمند		
۴-۵۲	نقش DELETE_CATALOG_ROLE	☐	☐
۴-۵۳	نقش SELECT_CATALOG_ROLE	☐	☐
۴-۵۴	نقش EXECUTE_CATALOG_ROLE	☐	☐
۴-۵۵	نقش DBA	☐	☐
	مجوز دسترسی به جداول و دیدهای سیستمی		
۴-۵۶	جدول SYS.AUD$	☐	☐
۴-۵۷	جدول SYS.USER_HISTORY$	☐	☐
۴-۵۸	جدول SYS.LINK$	☐	☐
۴-۵۹	جدول SYS.USER$	☐	☐
۴-۶۰	دیدهای مدیریتی DBA_%	☐	☐
۴-۶۱	جدول SCHEDULER$_CREDENTIAL	☐	☐
۴-۶۲	جدول SYS.USER$MIG	☐	☐
	مجوزهای خاص		
۴-۶۳	مجوزهای ANY	☐	☐
۴-۶۴	مجوز با گزینه WITH_ADMIN	☐	☐
۴-۶۵	مجوزهای مربوط به proxy user	☐	☐
۴-۶۶	مجوز EXECUTE ANY PROCEDURE کاربر OUTLN	☐	☐
۴-۶۷	مجوز EXECUTE ANY PROCEDURE کاربر DBSNMP	☐	☐
۵	**تنظیمات رویدادنگاری**		
	رویدادنگاری سنتی		
۵-۱	USER	☐	☐

☐	☐	ROLE	۵-۲
☐	☐	SYSTEM GRANT	۵-۳
☐	☐	PROFILE	۵-۴
☐	☐	DATABASE LINK	۵-۵
☐	☐	PUBLIC DATABASE LINK	۵-۶
☐	☐	PUBLIC SYNONYM	۵-۷
☐	☐	SYNONYM	۵-۸
☐	☐	DIRECTORY	۵-۹
☐	☐	SELECT ANY DICTIONARY	۵-۱۰
☐	☐	GRANT ANY OBJECT PRIVILEGE	۵-۱۱
☐	☐	GRANT ANY PRIVILEGE	۵-۱۲
☐	☐	DROP ANY PROCEDURE	۵-۱۳
☐	☐	SYS.AUD$	۵-۱۴
☐	☐	PROCEDURE	۵-۱۵
☐	☐	ALTER SYSTEM	۵-۱۶
☐	☐	TRIGGER	۵-۱۷
☐	☐	CREATE SESSION	۵-۱۸
ممیزی یکپارچه			
☐	☐	CREATE USER	۵-۱۹
☐	☐	ALTER USER	۵-۲۰
☐	☐	DROP USER	۵-۲۱
☐	☐	CREATE ROLE	۵-۲۲
☐	☐	ALTER ROLE	۵-۲۳
☐	☐	DROP ROLE	۵-۲۴
☐	☐	GRANT	۵-۲۵
☐	☐	REVOKE	۵-۲۶

۵-۲۷	CREATE PROFILE	☐	☐
۵-۲۸	ALTER PROFILE	☐	☐
۵-۲۹	DROP PROFILE	☐	☐
۵-۳۰	CREATE DATABASE LINK	☐	☐
۵-۳۱	ALTER DATABASE LINK	☐	☐
۵-۳۲	DROP DATABASE LINK	☐	☐
۵-۳۳	CREATE SYNONYM	☐	☐
۵-۳۴	ALTER SYNONYM	☐	☐
۵-۳۵	DROP SYNONYM	☐	☐
۵-۳۶	مجوز SELECT ANY DICTIONARY	☐	☐
۵-۳۷	دید UNIFIED_AUDIT_TRAIL	☐	☐
۵-۳۸	CREATE PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY	☐	☐
۵-۳۹	ALTER PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY	☐	☐
۵-۴۰	DROP PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY	☐	☐
۵-۴۱	ALTER SYSTEM	☐	☐
۵-۴۲	CREATE TRIGGER	☐	☐
۵-۴۳	ALTER TRIGGER	☐	☐
۵-۴۴	DROP TRIGGER	☐	☐
۵-۴۵	LOGON و LOGOFF	☐	☐

۸ مراجع

[1] https://www.cisecurity.org/

[2] http://www.dba-oracle.com/t_resource_profiles.htm