

بسمه تعالی



کز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

آسیب پذیری جدید پیام رسان واتس اپ و دسترسی به فایل های موجود در سیستم کاربر

گزارش آسیب پذیری



یک محقق امنیتی جزییات فنی از آسیب پذیری های چندگانه با حساسیت بالا را در پیام رسان واتس اپ منتشر کرد که با بهره برداری از آنها امنیت میلیون ها کاربر به خطر خواهد افتاد و یک مهاجم از راه دور می تواند با ارسال یک پیام مخرب به قربانی در برنامه واتس اپ فایل های موجود در سیستم ویندوزی یا mac کاربر را سرقت کند. این آسیب پذیری با شناسه CVE-2019-18426 که توسط محقق PerimeterX به نام Gal Weizman کشف شده است، در نسخه وب واتس اپ واقع شده است.

۱ درباره ی این آسیب پذیری

این آسیب پذیری نشان می دهد در نسخه وب واتس اپ یک آسیب پذیری خطرناک از نوع open-redirect وجود دارد که می تواند با ارسال یک پیام مخرب به حملات cross-site scripting ختم شود.

در نتیجه اگر پیام مخرب توسط قربانی در نسخه وب واتس اپ در مرورگر باز شود امکان اجرای کد از راه دور در context برنامه وجود دارد؛ اگر پیام در برنامه نسخه desktop باز شود نیز کد مخرب در گیرنده ی سیستم و در context برنامه اجرا می شود. علاوه بر این به دلیل اشتباه در تنظیم (misconfigure) محتوای سیاست های امنیتی دامین نسخه وب واتس اپ، امکان بارگذاری payload های XSS با استفاده از iframe از یک وب سایت دیگر در اینترنت که تحت کنترل مهاجم است، وجود دارد. به گفته ی این محقق اگر قوانین CSP بهتر تنظیم شده بودند، قدرت عمل XSS کاهش پیدا می کرد. با دور زدن قوانین CPS مهاجم می تواند اطلاعات بالارزشی از قربانی سرقت کند و payload های XSS را به راحتی بارگذاری کند.

The screenshot shows a web browser window with the URL `csp-evaluator.withgoogle.com`. The page title is "Content Security Policy". There are two links: "Sample unsafe policy" and "Sample safe policy".

The main content is a code editor showing a CSP configuration:

```

default-src 'self' data: blob: *;
script-src *.facebook.com *.fbcdn.net *.facebook.net *.google-analytics.com *.virtualsearch.com *.google.com 127.0.0.1:*
*.spotilocal.com:* 'unsafe-inline' 'unsafe-eval' blob: data: 'self' https://ajax.googleapis.com
https://api.search.live.net https://maps.googleapis.com https://www.youtube.com https://s.ytimg.com;
style-src data: blob: 'unsafe-inline' * 'self' https://fonts.googleapis.com;
connect-src *.facebook.com facebook.com *.fbcdn.net *.facebook.net *.spotilocal.com:* wss://*.facebook.com:*
https://fb.scanandcleanlocal.com:* attachment.fbsbx.com ws://localhost:* blob: *.cdninstagram.com 'self'
chrome-extension://boadgeojelhgndaghljhdicfkmllpafd chrome-extension://dliochdbjfkdbacpmh1cpmeaejdimm
https://*.whatsapp.net https://www.facebook.com https://*.giphy.com https://*.tenor.co
https://crashlogs.whatsapp.net/wa_clb_data https://crashlogs.whatsapp.net/wa_fl_upload_check
https://www.bingapis.com/api/v6/images/search https://*.google-analytics.com wss://*.web.whatsapp.com
wss://web.whatsapp.com https://dyn.web.whatsapp.com;
font-src data: 'self' https://fonts.googleapis.com https://fonts.gstatic.com;
img-src * data: blob;
media-src 'self' https://*.whatsapp.net https://*.giphy.com https://*.tenor.co https://*.cdninstagram.com
  
```

Below the code editor, there is a dropdown menu set to "CSP Version 3 (nonce based + backward compatibility checks)" and a "CHECK CSP" button.

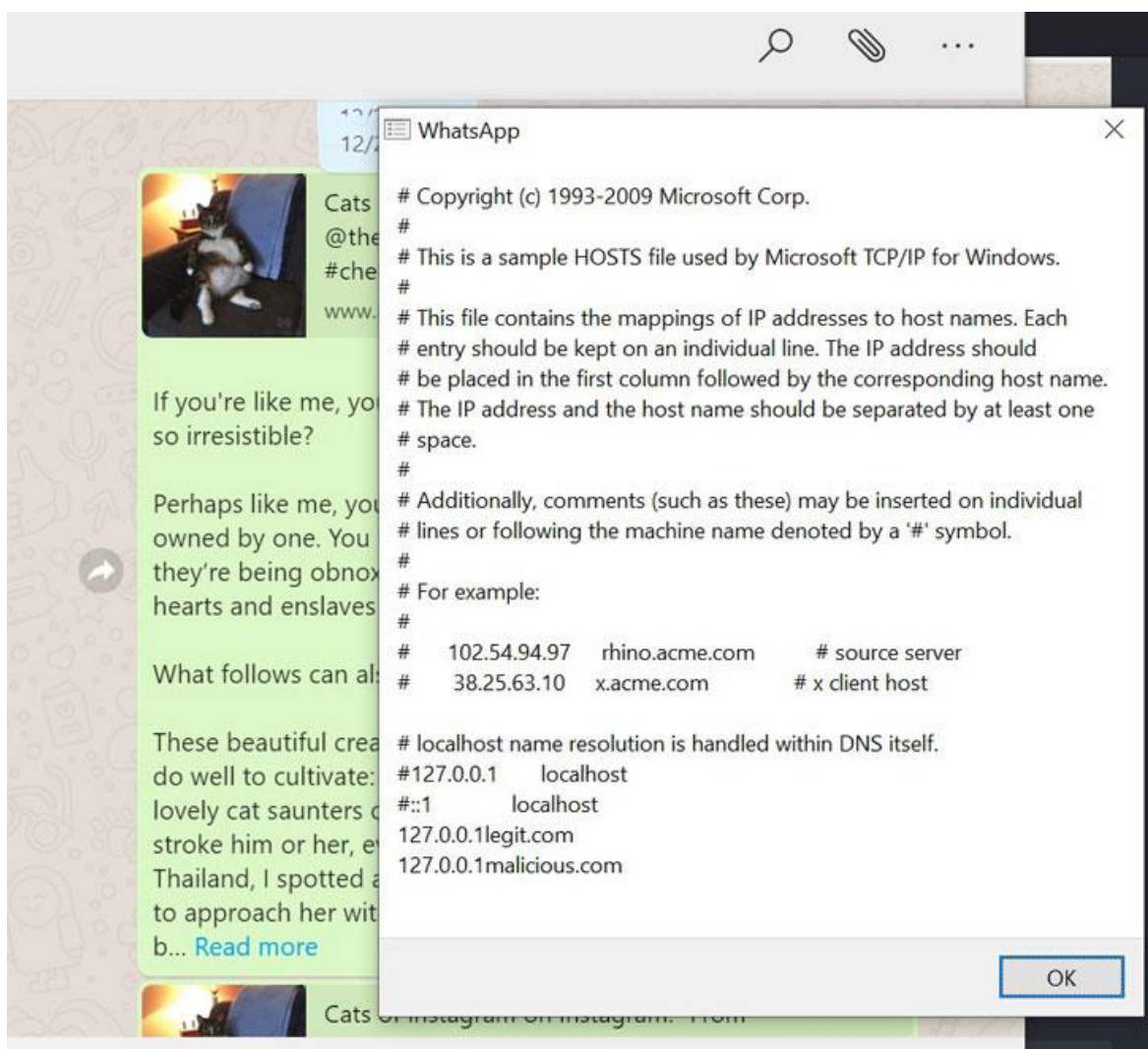
The evaluation results are shown below the button:

Evaluated CSP as seen by a browser supporting CSP Version 3 [expand/collapse all](#)

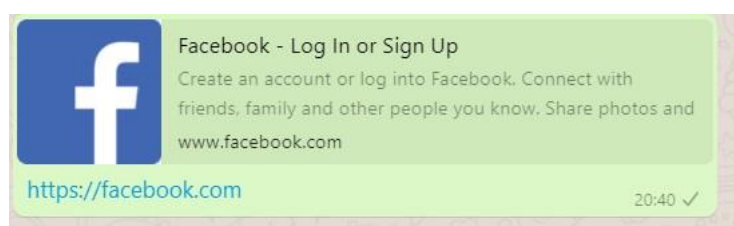
- ❌ **default-src**
- ❌ **script-src** Host whitelists can frequently be bypassed. Consider using 'strict-dynamic' in combination with CSP nonces or hashes.
- ✅ **style-src**
- ✅ **connect-src**
- ✅ **font-src**
- ✅ **img-src**
- ✅ **media-src**
- ✅ **child-src**
- ✅ **frame-src**
- ❌ **object-src [missing]** Can you restrict object-src to 'none'?

شکل شماره ۱: اشتباه در تنظیم (misconfigure) محتوای سیاست‌های امنیتی دامین نسخه وب واتس‌آپ

همان‌طور که در تصویر زیر مشاهده می‌شود، حمله‌ی دسترسی به فایل، بوسیله‌ی واتس‌آپ اثبات می‌شود. فایل زیر در آدرس `C:\Windows\System32\drivers\etc\hosts` در سیستم قربانی دریافت شده است.

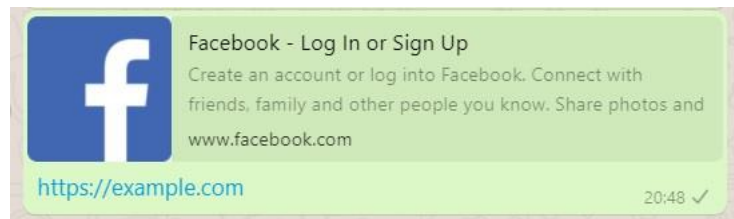


با استفاده از پیام‌هایی که مطابق شکل زیر، preview banner دارند امکان بهره‌برداری از رخنه امنیتی -open redirect فراهم می‌شود.



شکل شماره ۲: پیامی که preview banner دارد

با توجه به شکل زیر Banner پیام، سایت facebook را نشان می‌دهد درحالی‌که لینکی که کاربر به آن هدایت می‌شود آدرس <https://example.com> است.



مطابق شکل زیر مهاجم می‌تواند یک قدم فراتر رفته و علاوه بر ظاهر banner ظاهر لینک را به گونه‌ای تغییر دهد که شبیه آدرس سایت facebook باشد ولی به کاربر را به وبسایت دیگری هدایت کند. این موضوع می‌تواند کاربر را فریب داده و منجر به حملات فیشینگ شود.



۲ محافظت از سیستم خود در برابر آسیب پذیری

نسخه‌های قبل از 0.3.9309 در ویندوز و نسخه‌های قبل از iPhone 2.20.10 تحت تاثیر این آسیب‌پذیری هستند. این آسیب‌پذیری سال پیش توسط Weizman به facebook گزارش شد و وصله امنیتی آن در نسخه‌های بعدی منتشر شد. در نتیجه پیشنهاد می‌شود اگر از نسخه‌های آسیب‌پذیر استفاده می‌کنید هر چه سریع‌تر به روز رسانی آن اقدام کنید.

۳ منابع

[۱] <https://www.facebook.com/security/advisories/cve-2019-18426>

[۲] <https://www.perimeterx.com/tech-blog/2020/whatsapp-fs-read-vuln-disclosure/>

[۳] <https://thehackernews.com/2020/02/hack-whatsapp-web.html>

