بسمه تعالی

آسیب‌پذیری جدید پیام‌رسان واتس اپ و دسترسی به فایل‌های موجود در سیستم کاربر

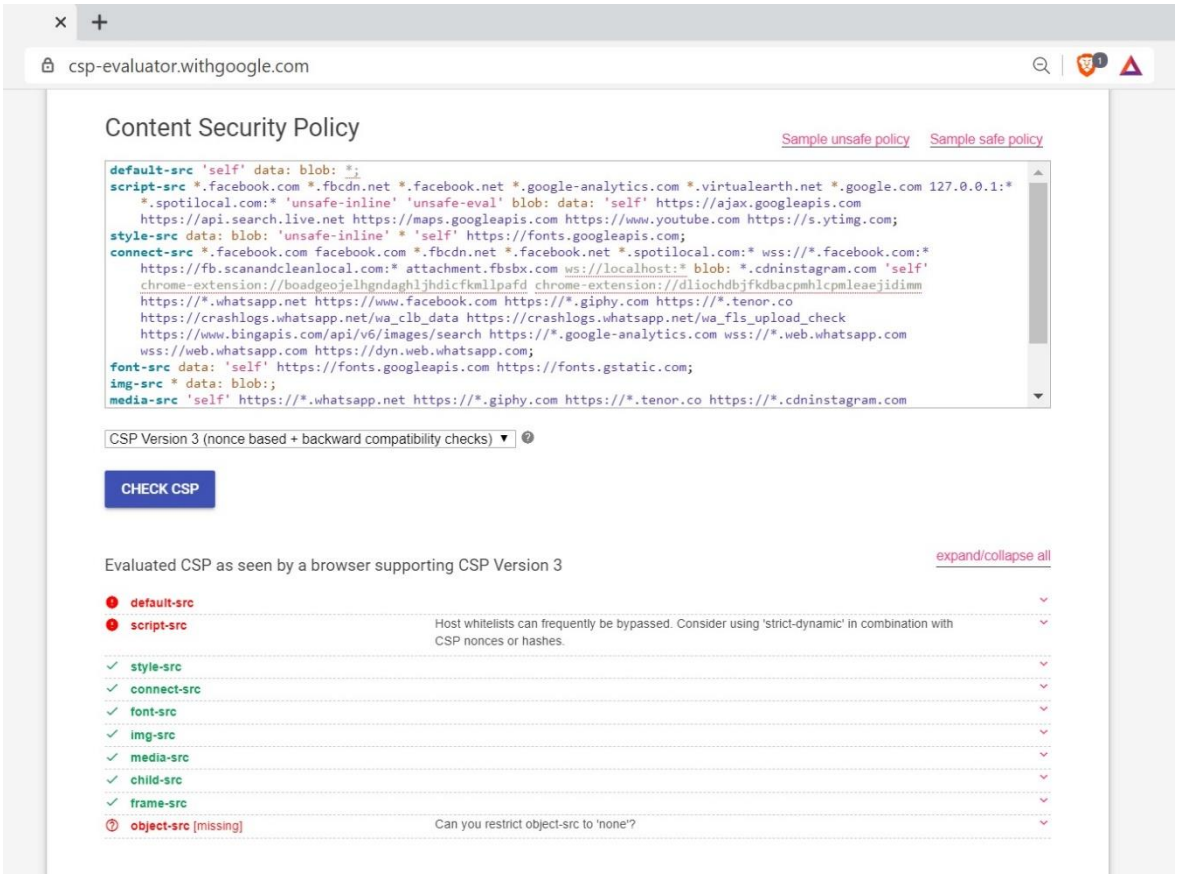
گزارش آسیب‌پذیری

یک محقق امنیتی جزییات فنی از آسیب‌پذیری‌های چندگانه با حساسیت بالا را در پیام‌رسان واتس‌اپ منتشر کرد که با بهره‌برداری از آنها امنیت میلیون‌ها کاربر به خطر خواهد افتاد و یک مهاجم از راه دور می‌تواند با ارسال یک پیام مخرب به قربانی در برنامه واتس‌اپ فایل‌های موجود در سیستم ویندوزی یا mac کاربر را سرقت کند.این آسیبب پذیری با شناسه CVE-2019-18426 که توسط محقق PerimeterX به نام Gal Weizman کشف شده است، در نسخه وب واتس‌اپ واقع شده است.

۱ درباره‌ی این آسیب‌پذیری

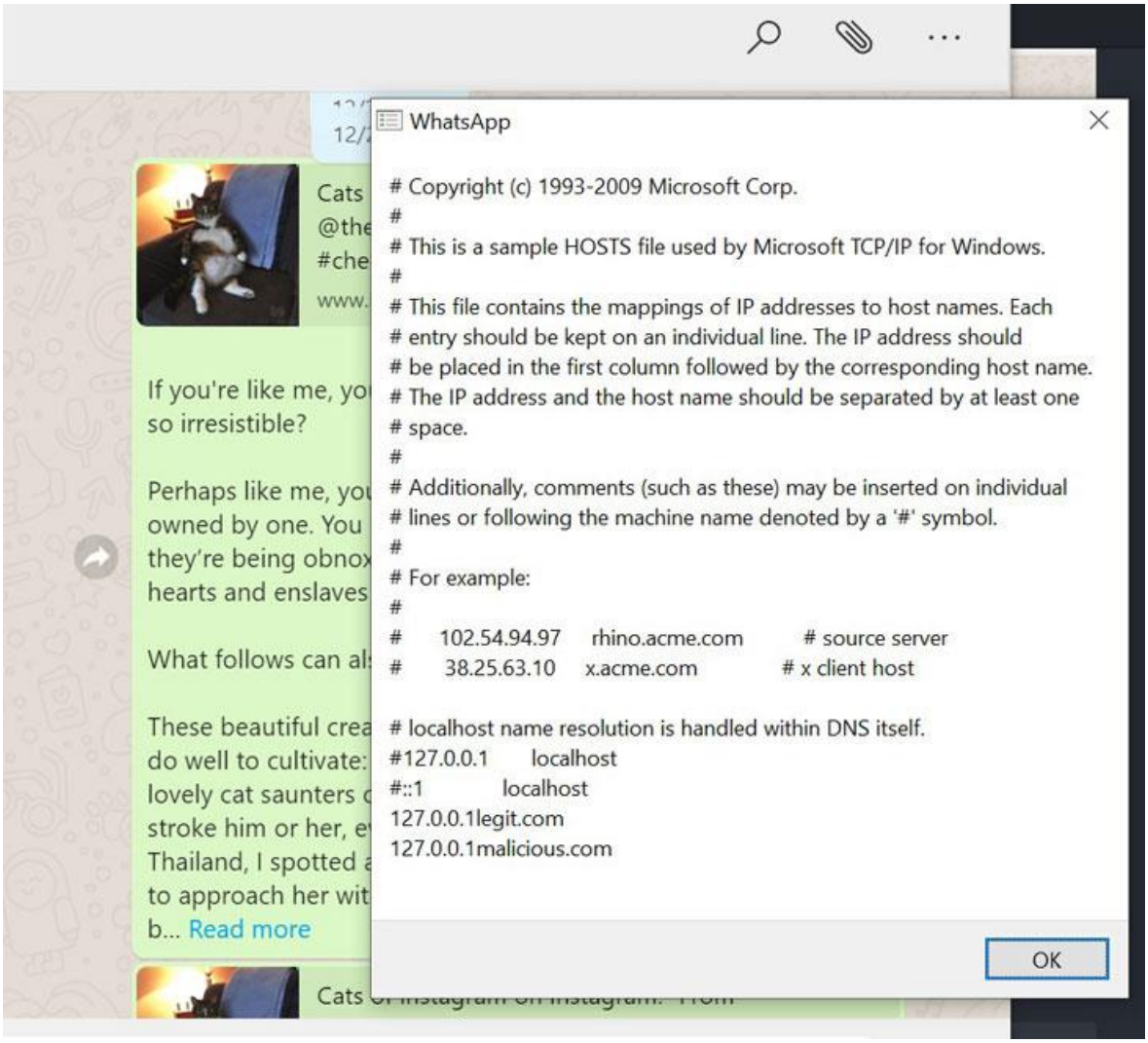
این آسیب‌پذیری نشان می‌دهد در نسخه وب واتس‌اپ یک آسیب‌پذیری خطرناک از نوع open-redirect وجود دارد که می‌تواند با ارسال یک پیام مخرب به حملات cross-site scripting ختم شود.

درنتیجه اگر پیام مخرب توسط قربانی در نسخه وب واتس‌اپ 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 گیرنده‌ی سیستم و در context برنامه اجرا می‌شود. علاوه بر این به دلیل اشتباه در تنظیم (misconfigure) محتوای سیاست‌های امنیتی دامین نسخه وب واتس‌اپ، امکان بارگذاری payloadهای XSS با استفاده از iframe از یک وب سایت دیگر در اینترنت که تحت کنترل مهاجم است، وجود دارد. به گفته‌ی این محقق اگر قوانین CSP بهتر تنظیم شده بودند، قدرت عمل XSS کاهش پیدا می‌کرد. با دور زدن قوانین CPS مهاجم می‌تواند اطلاعات باارزشی از قربانی سرقت کند و payloadهای XSS را به راحتی بارگذاری کند.

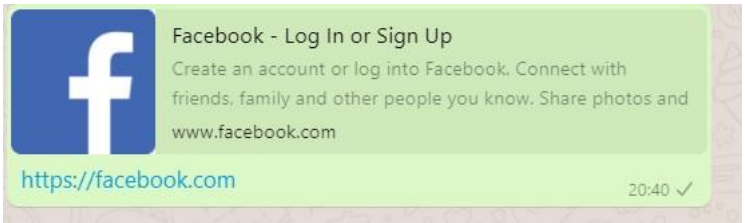


شکل شماره ۱: اشتباه در تنظیم (misconfigure) محتوای سیاست‌های امنیتی دامین نسخه وب واتس‌اپ

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

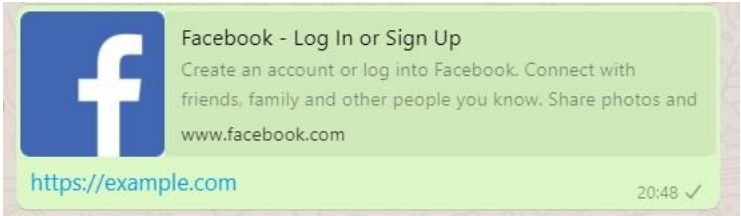


با استفاده از پیام‌هایی که مطابق شکل زیر، preview banner دارند امکان بهره‌برداری از رخنه امنیتی open-redirect فراهم می‌شود.

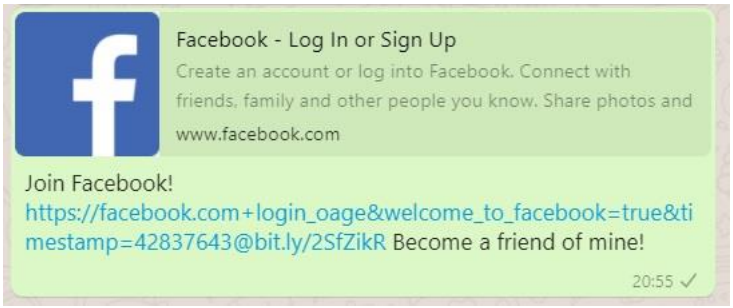


شکل شماره ۲: پیامی که preview banner دارد

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. درنتیجه پیشنهاد می‌شود اگر از نسخه‌های آسیب‌پذیر استفاده می‌کنید هر چه سریع‌تر به 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