SECURITYWORLD

# XSS Write-ups 01

# Cross Site Scripting (XSS) Reflected in one of the subdomains of “General Motors”(Bugbounty)

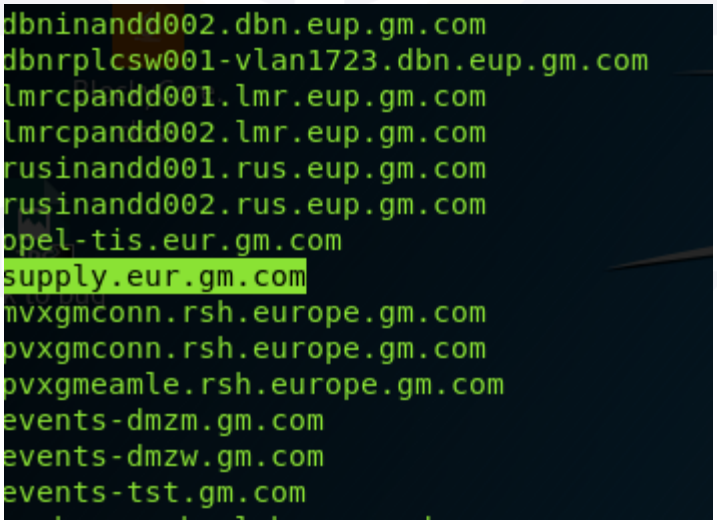
## شناسایی آسیب‌پذیری XSS از نوع Reflected در یکی از زیردامنه‌های شرکت جنرال موتورز

در این پست قصد داریم تا به نحوه شناسایی و اکسپلویت آسیب‌پذیری XSS یا Cross Site Scripting از نوع Reflected در یکی از زیر دامنه‌های General Motors بپردازیم.

اولین نکته ای که باید به آن توجه کنیم این است که شرکت جنرال موتورز دارای برنامه Bug Bounty در سایت Hackerone می‌باشد. که این موضوع به تست نفوذگران اجازه می‌دهد تا آدرس‌های موجود در Scope این شرکت را بررسی نموده و در صورت وجود آسیب‌پذیری آن را گزارش نمایند. به یاد داشته باشید در صورتی که این شرکت برنامه باگ بانتی نداشته باشد، برای تست آسیب‌پذیری ممکن است دچار مشکل شویم و باید حتما آن‌ها را از فرآیند تست و شناسایی آسیب‌پذیری آگاه کنیم.

همچنین توجه داشته باشید که تعلق داشتن به برنامه‌های باگ بانتی به این معنی است که احتمال یافتن آسیب‌پذیری در آن‌ها بسیار کاهش می‌یابد. به همین دلیل بهتر است در زیردامنه‌های آن‌ها اقدام به جست و جو و شناسایی آسیب‌پذیری نمایید.

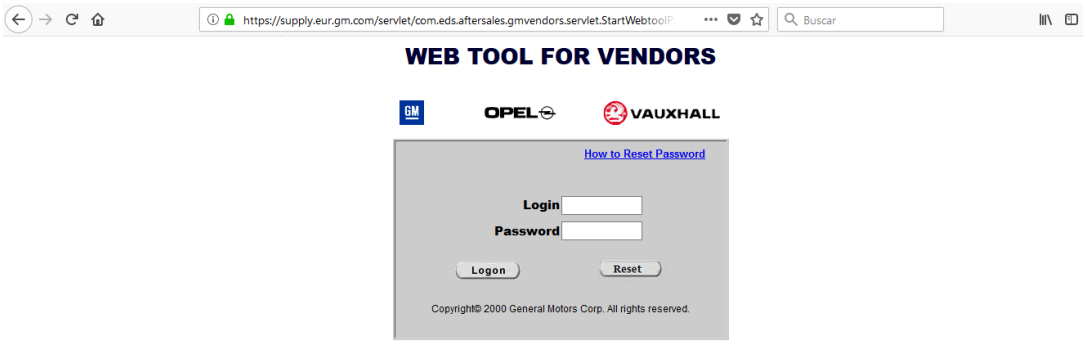
در این مورد تست نفوذگر از برنامه Sublist3r برای شناسایی زیردامنه‌های سایت جنرال موتورز استفاده نموده است. تصویر زیر نمایانگر برخی از زیردامنه‌های سایت جنرال موتورز می‌باشد:



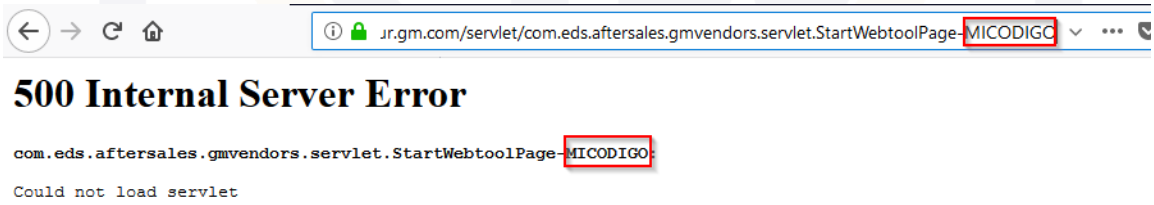

شما می‌توانید ابزار Sublist3r را از لینک زیر دانلود نمایید:

https://github.com/aboul3la/Sublist3r

پس از هفته‌ها جست و جو، تست نفوذگر بر روی یکی از زیر دامنه‌ها به آدرس supply.eur.gm.com متمرکز می‌شود. این وب سایت به دلیل اینکه کمی قدیمی به نظر می‌رسید، توجه تست نفوذگر را به خود جلب می‌کند:



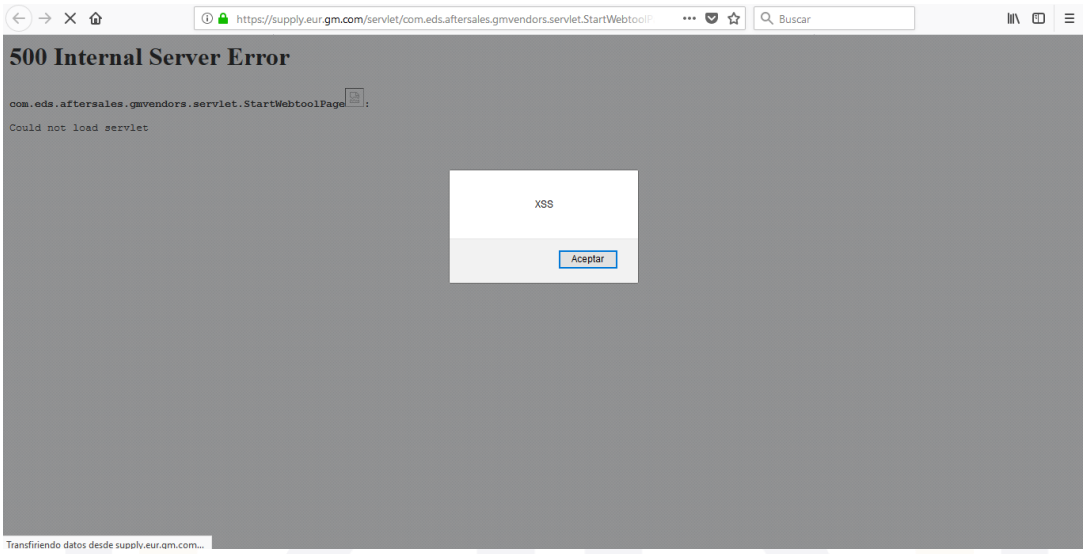

پس از انجام تست‌های متعدد مانند User Enumeration، Directory Listing ، SQL Injection و آسیب‌پذیری‌های دیگر، تست نفوذگر متوجه می‌شود که هنگام بروز مشکل و نمایش پیام خطا، کنترل خطا به درستی صورت نمی‌پذیرد و تمام متن موجود در URL در پیام خطای ایجاد شده نمایش داده می‌شود:




تست نفوذگر با توجه به وجود پیام خطا و عدم فیلتر نمودن صحیح ورودی‌ها در این صفحه، اقدام به تزریق کد اسکریپت می‌نماید. در انتها وی دو PoC یا Proof of Concept را برای سایت Hackerone ارسال می‌نماید که به صورت زیر می‌باشد:

[POC 1] Payload: <img%20src=a%20onerror=alert(“XSS”)>

[POC 2] Payload: <img onerror=javascript:window.location.replace(‘http:www.google.com’) src=”x”>




این آسیب‌پذیری می‌تواند به نفوذگر اجازه دهد تا کاربر قانونی سایت را به یک سایت مخرب هدایت نموده و یک حمله فیشینگ را صورت دهد و یا اقدام به سرقت کوکی‌های کاربران سایت نماید.

متاسفانه پاداشی برای این آسیب‌پذیری از طرف شرکت جنرال موتورز در نظر گرفته نشد (برابر صفر) که این اتفاق اغلب در برنامه‌های باگ بانتی رخ می‌دهد.

**منبع:**

https://securitytrooper.com/en/cross-site-scripting-xss-reflected-in-one-of-the-subdomains-of-general-motorsbugbounty