الفصل الثاني عشر
ثغرة ال SSRF

المؤلف
د.م/ أحمد هاشم الفقي
استشارى أمن المعلومات و التحول الرقمي
Ahmed.Hashem.ElFiky@outlook.com

ثغرة ال SSRF

- سوف نتكلم عن SSRF حيث يتم إعتبار SSRF عبارة عن أحد أنواع الهجمات وليس ثغرة بحد ذاتها لكن سنشرحها كثغرة لسهولة الفهم هي إختصار لـ (Sever Side Request Forgery) وتظهر حينما يكون المهاجم له القدرة في إرسال طلب بأستخدام السيرفر المصاب .
- عادة يتم أستخدام SSRF في الهجوم على الشبكة الداخلية لسيرفر ما والتي تكون محمية بجدار ناري للعامة لكن لنفس السرفر يسمح بدخول حزم المعلومات (سيتم استغلالها في SSRF) ويمكن ايضاً معرفة الخدمات المتوفرة على السيرفر والتنصت الى واجهة الاسترجاع او ما يرد به السيرفر على الطلب .

ثغرة ال SSRF (تكمله...)

- كيف يتم ذلك ؟
- لو فرضنا مثلا انه لدينا موقع يقوم بجلب البيانات من ال localhost الخاص به فرضاً سيكون الطلب كالاتي :

```
1 GET http://www.target.com/proxy.php?curl=http://www.target.com/min.css
```

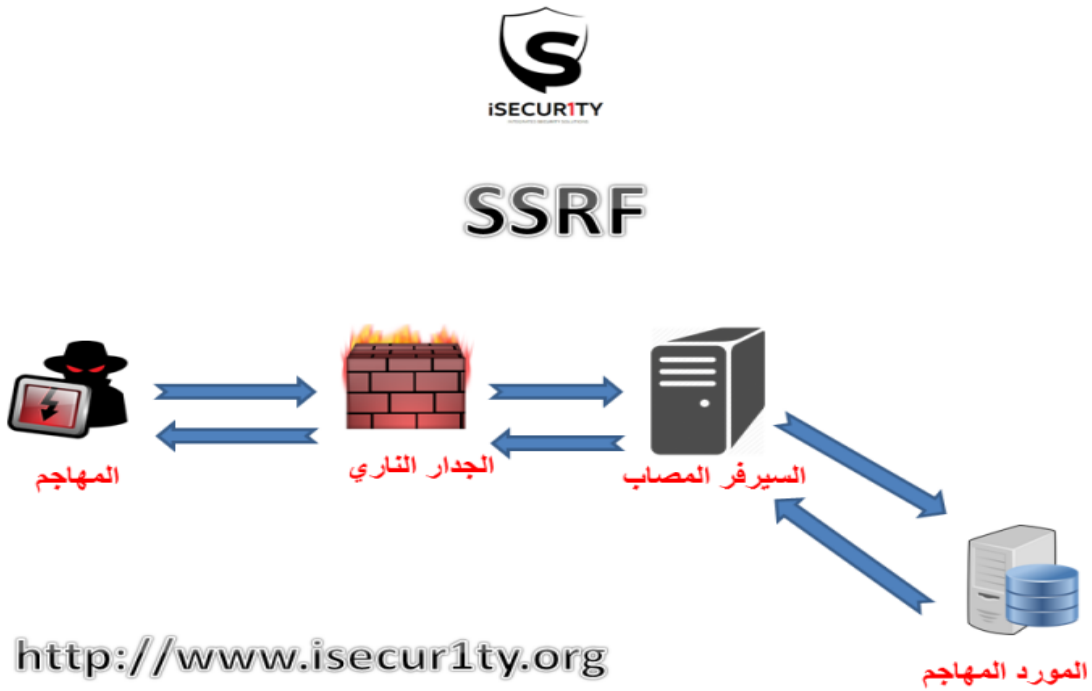
- الان لنعمل تحقق ونغير الوجهة الى localhost ونضع منفذ معين في حالة ان المنفذ يعمل سيرجع 200 ok واذا كان لا يعمل سيرد اي كود من اكواد الاخطاء 500 404 الخ ... اكثرها سوف يكون 304 في حالة عدم العمل .

ثغرة ال SSRF (تكمله...)

- فائدة ثغرات SSRF
  - البحث ومهاجمة الشبكة الداخلية للسيرفر .
  - عد و مهاجمة الخدمات التي تعمل على تلك الاستضافات .
  - استغلال خدمات المصادقة المستندة إلى المضيف (سيتم شرحها في اجزاء اخرى) .
  - تخطي SOP للمتصفحات وجلب محتوى خارجي .
- بالاعتماد على السيرفر المصاب هناك العديد من الاحتمالات القابلة للاستغلال مثلا لو كان السيرفر يستخدم cURL التي تدعم الاتصال باكثر من برتكول غير HTTPS و HTTP .فلو كان السيرفر المصاب يعمل بي cURL يمكن ايضاً استخدام (dict://) لارسال بيانات معينة وطلب معين لاي ايبي وعلى اي منفذ .
- يمكن استخدام (dict://locahost:11211/stat) سيجعل السيرفر يتصل ب localhost عن طريق المنفذ 11211 بارسال stat كبيانات .

ثغرة ال SSRF (تكمله...)

- معلومة مهمة جداً منفذ 11211 هو المنفذ الافتراضي ل Memcached والتي لها دور في تحسين وتسريع قواعد البيانات وتكون غير قابلة للدخول من الشبكة العنكبوتية . ولكن باستخدام SSRF يمكن الدخول لها وتفصح المعلومات وارسال طلبات كبيرة لها قد يسبب في عمل هجوم DoS على السيرفر نفسه.



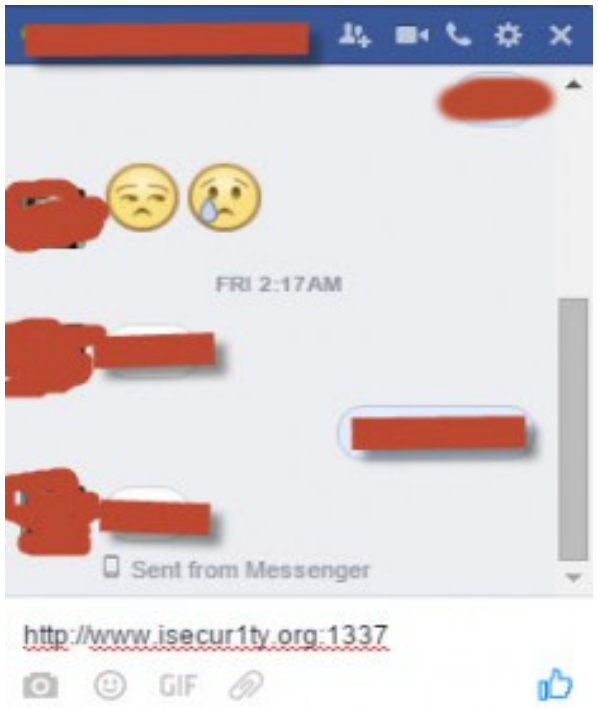
ثغرة ال SSRF (تكمله...)

- المورد المُهاجم قد يكون :
  - ملف مشترك بين السيرفرات الداخلية
  - قواعد البيانات
  - عميل
- وغيره .. ونقصد بمهاجمة منها فحص وكشف وتحديد بعض الخدمات وليس اختراق مباشر حيث يُمكن إستخدام SSRF لعمل DoS على سيرفرات داخلية او خارجية باستخدام قدرة السيرفر كما يتم استخدام SSRF لفحص البورتات للمهاجم باسم السيرفر او بعنوان السيرفر نفسه لكي لا يتم تحديد الايبي للمهاجم.

ثغرة ال SSRF (تكمله...)

- إستخدام SSRF السليم :
- يكون الاستخدام السليم حين يتم السيطرة على الوجهة الخاصة بالحزمة ونوعها ، مثلاً شركة فيس بوك تستعمل SSRF للتاكد من ان الرابط سليم وموجود حتى تتجنب التصيد وغيره.
- ولو وضعنا في فيسبوك ماسنجر الرابط (http://www.isecur1ty.org:80) سوف يظهر محتوى الموقع والبنر الخاص به كما بالصورة التالية :

ثغرة ال SSRF (تكمله...)

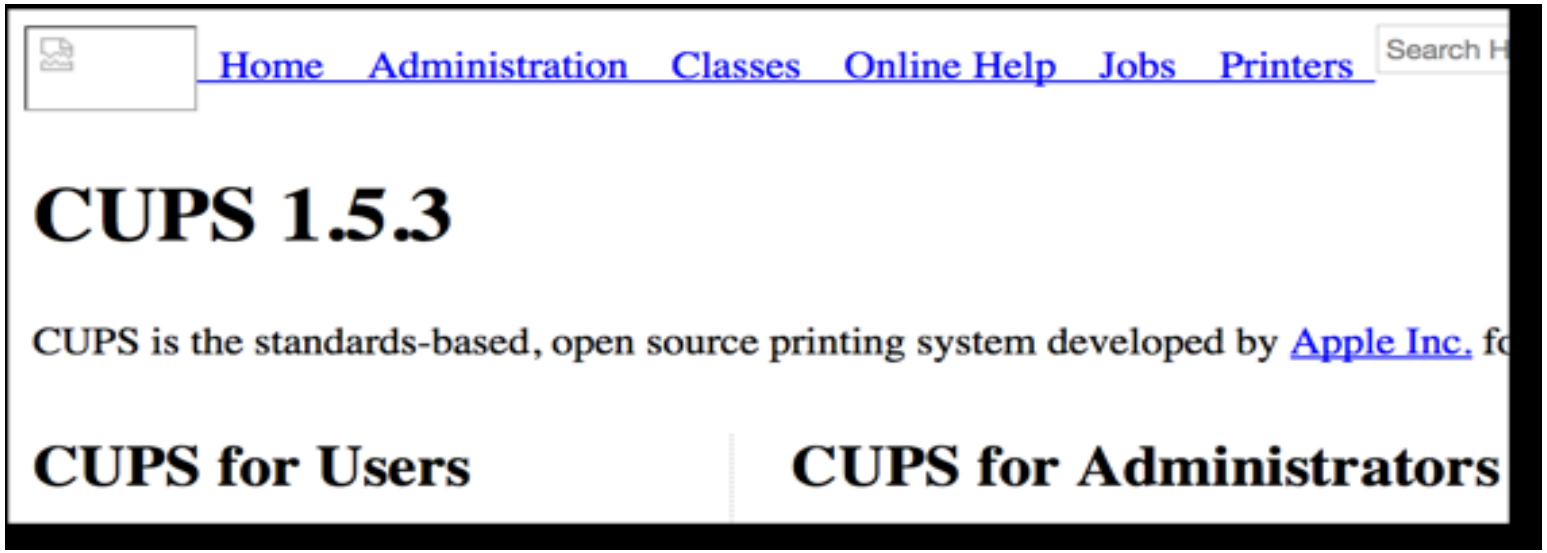


- لان المنفذ 80 مفتوح ولكن ماذا لو وضعنا منفذ مغلق ؟
- لم يظهر بنر الموقع دليل على ان المنفذ مغلق وتم الفحص عن طريق سيرفر فيس بوك
- مثال أخر
- لو فرضنا وجود موقع مصاب نقوم بعمل اتصال لل localhost عن طريق منفذ 631

http://target/proxy.php?csurl=http://localhost:631

ثغرة ال SSRF (تكمله...)

- منفذ 631 يستخدم لل CUPS HTTP والتي تستعمل "للطابعات" وعند الذهاب للرابط ظهرت لنا الصحفة التالية :



ثغرة ال SSRF (تكمله...)

- يمكن عمل brute force على المنافذ المفتوحة ايضاً في ال localhost بنفس الطريقة.
- أسماء اخرى
  - Cross Site Port Attack

تم بحمد الله انتهاء الفصل الثاني عشر