الفصل الثالث و العشرين
ثغرة ال HTTP Splitting

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

ثغرة ال HTTP Splitting

- بعض المواقع الإلكترونية تلجأ الى جزء من مدخلات المستخدم لتستخدمها في الـ" HTTP Response Headers" أكثر الأمثلة وضوحا على هذه الثغرة هي المواقع التي تتيح للمستخدم إختيار الصفحة التي يريد أن يتم "تحويله" اليها بإستخدام أحد وسائل الإدخال .

- سوف أقوم بشرح "Scenario" كامل لعملية إختبار إختراق موقع إفتراضي لتكون الصورة واضحة للجميع , وسوف نطلق على الموقع fakewebsite.fake

- في البداية نبحث داخل الموقع عن Form يسمح للمستخدم الإدخال ويقوم الموقع من بعدها التحويل الى الصفحة التي طلبها المستخدم.

ثغرة ال HTTP Splitting (تكمله...)

- لنقم على سبيل المثال بإرسال طلب للسيرفر بأننا نريد الذهاب لصفحة /sales-100 فسوف يكون الرد كالآتي :

```
HTTP/1.1 302 Moved Temporarily
Location : http://fakewebsite.fake/100-sales
[other http headers]
```

- نلاحظ أن مدخلنا الذي قمنا بإدخاله /sales-100 تم التعامل معه في أحد الـ" HTTP Response Headers
- قد يتسائل أحد الأشخاص , ما هو الخطر الذي يكمن وراء هذه الثغرة ؟

ثغرة ال HTTP Splitting (تكمله...)

- يستطيع المخترق بوساطة هذه الثغرة أن يكوّن أكثر من ردّين من السيرفر , ماذا أعني بهذا الكلام ؟ بالرجوع للأعلى , قمنا بطلب الصفحة/sales-100 تم الرد برد واحد يقوم بالتحويل لصفحة معينة . بإستخدام هذه الثغرة يقوم المخترق بإرسال طلب وتشكيل ردّين مختلفين لصفحتين مختلفتين !
- أعلم أن الكلام معقد وغير مفهوم للبعض , ولكن أفضل طريقة للفهم هي بالأمثلة .
- لو قمنا مثلا بتعديل الصفحة المراد اليها , كالآتي :

```
HTTP/1.1 302 Moved Temporarily
Location : http://fakewebsite.fake/sales-
100%0d%0aHTTP/1.1%20200%20OK%0d%0aContent-
Type:%20text/html%0d%0a%0d%0aContent-
<Length:%2035%0d%0a%0d%0a<html>hacked</html
[other http headers]
```

ثغرة ال HTTP Splitting (تكمله...)

- ما الذي قمنا بفعله ؟
  - قمنا بإرسال طلب للسيرفر بأنه نريد إستعراض الصفحة

```
sales-100%0d%0a%0d%0aHTTP/1.1%20200%20OK%0d%0aContent-“
                                Type:%20text/html%0d%0aContent-
                  ”<Length:%2035%0d%0a%0d%0a<html>hacked</html
```

- ولكن هذا المدخل يحتوي على Response عند طلب صفحة معينة داخل الموقع. ماذا يحصل؟
- تم تشفير الصفحة المراد تحويلها من خلال URL Encode لكي يتم التعامل معه على أنه مدخل واحد.

ثغرة ال HTTP Splitting (تكمله...)

- عند فك تشفيره نجده كالآتي :

```
sales-100

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 35

<html>hacked</html>
```

- لنعد تشكيل الرد الأصلي كامل بدون تشفير لنرى ماذا حصل :

```
HTTP/1.1 302 Moved Temporarily
Location : sales-100

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 35

<html>hacked</html>
```

ثغرة ال HTTP Splitting (تكمله...)

- نجد أنه هناك ردّين ! , الأول للتحويل الى صفحة /sales-100 والأخر هو رد غير مرتبط بطلب معين و يحوي على أكواد HTML لو قام مختبر الإختراق بالتحويل الى الصفحة الرئيسية بشكل سريع سيتم مقابلة الطلب "تحويل الى الصفحة الرئيسية" بالرد الثاني "محتوى الصفحة الذي سوف يظهر .

تم بحمد الله انتهاء الفصل الثالث و العشرين