الفصل العاشر
ثغرات ال Redirection

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

ثغرات ال Redirection

- نستعرض فى هذا الفصل شرح مفصل لثغرات التحويل (ثغرات اعادة التوجيه) وهما ثغرتان:
- الأولى : Server-side HTTP Redirection
- الثانية : Open Redirect
- اولا:Server-side HTTP Redirection
- ببساطة هى ثغرة تقوم بتحويلك من رابط الى رابط اخر داخل التطبيق او ربما رابط خارجى. تظهر هذه الثغرة عندما يتم ادخال قيم معينة فى تطبيق الويب ثم يقوم السيرفر بمعالجة هذه القيم واضافتها الى الرابط الأصلى وبالتالى توجيه التطبيق لهذه القيمة

ثغرات ال Redirection (تكمله...)

- مثال: موقع يوفر عدة ثيمات مختلفة ليظهر بها وعندما تختار ثيم معين يقوم السيرفر بمعالجة طلبك مثل الصورة التالية:

```
POST /home HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: isecur1ty.com
Content-Length: 65

view=default&theme=isecur1ty.com/themes/theme1
```

- واضح من الصورة ان الموقع ياخذ طلبك ويدمجه فى بارمتر يسمى theme ثم يعرض اختيارك فى المتصفح وهو الثيم الأول

ثغرات ال Redirection (تكمله...)

- سبب الثغرة فى الأساس هو ان السيرفر لا يقوم بالتحقق من مدخلات المستخدم حيث يستطيع المستخدم تغيير قيم البارامتر theme بدون اى حظرعلى القيم اى ان هذه الثغرة تعتبر بروكسى -وسيط- بين المهاجم وبين السيرفر. حيث يستطيع المهاجم التحويل الى روابط اخرى وعرض صفحات بها اكواد خبيثة والإتصال بخدمات اخرى على السيرفر وربما الدخول الى صفحات حساسة داخل الموقع والدخول الى الشبكة الداخلية لموقع الشركة واحيانا تساعد الثغرة فى تخطى الجدار النارى والحصول على صلاحيات اكبر فى تصفح الموقع .
- لإكتشاف هذه الثغرة يجب عليك البحث عن كل البارمترز الى تقوم بالتحويل من صفحة الى صفحة اخرى .ابحث عن البارمترز التى تحتوى على روابط او على IP كالتالى

theme=isecur1ty.com/themes/theme1

theme=192.168.1.1

ثغرات ال Redirection (تكمله...)

- اجمع كل البارمترز من هذا النوع لنبدا فى عملية الإستغلال:
- سنقوم بالتعديل على قيمة البارمتر theme=isecur1ty.com/files ونرى استجابة السيرفر للطلب .اذا تم توجيهك لهذا المسار الجديد فالموقع مصاب .بالتأكيد تسطيع استبدال قيمة البارمتر بأى رابط سواء داخل الموقع او رابط خارجى وسيتم توجيهك الى الرابط الجديد وبالتالى تستطيع الدخول الى كثير من صفحات الموقع بدون اى صلاحيات .
- مثال1: استغلال متقدم لثغرة Server-side HTTP Redirection
- سنحاول الإتصال بخدمة ftp من خلال هذه الثغرة .كما تعلمون خدمة ftp تعمل على بورت 21 وسنرى استجابة السيرفر للطلب لاحظ الصورة التالية

ثغرات ال Redirection (تكمله...)

```
POST /home HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: isecur1ty.com
Content-Length: 65

view=default&theme=isecur1ty.com:21
```

يستخدم هذا الإستغلال فى banner grabbing او ربما الدخول مباشرة الى الخدمة.
فتكون نتيجة الإستغلال غالبا على هذا الشكل -عرفنا البرنامج المثبت على بورت 21 واصداره وعرفنا نظام التشغيل المستخدم- وبالتالى توجيه هجمات اخرى ضده

```
HTTP/1.1 200 OK
Connection: close
220 ProFTPD 1.2.4 Server(Debian)
```

ثغرات ال Redirection (تكمله...)

- مثال2: استغلال متقدم لثغرة Server-side HTTP Redirection
- سنحاول الدخول الى الشبكة الداخلية للموقع واكتشاف الأجهزة المختلفة داخل هذه الشبكة وعمل فحص للبورتات المفتوحة على هذه الأجهزة واكتشاف الثغرات بها

```
POST /home HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: isecur1ty.com
Content-Length: 65

view=default&theme=192.168.0.1:21
```

نستبدل 192.168.0.1 بجموعة من IP ونستبدل 21 بقائمة من اشهر البورتات
يمكن تنفيذ هذا الهجوم من خلال برمجة سكربت خاص "لعشاق البرمجة" او من الممكن الإعتماد على اداة burp intruder احد اداوت burp suite

ثغرات ال Redirection (تكمله...)

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Compa

1 × | 2 × | ...

Target | Positions | Payloads | Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack typ

Attack type: Cluster bomb

```
POST /home HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: isecurity.com
Content-Length: 65
view=default&loc=§192.168.0.1§:§22§
```

ثغرات ال Redirection (تكمله...)

- مثال3: استغلال متقدم لثغرة Server-side HTTP Redirection
- سندمج هذه الثغرة مع ثغرة xss ونقوم بإستغلال مزدوج
- عند فحص الموقع اكتشفنا ثغرة اخرى من نوع xss فى search.php?s=
- لاحظ الإستغلال فى الصورة التالية

```
POST /home HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: isecurlty.com
Content-Length: 65

view=default&loc=isecurlty.com/search.php?s=<script>alert("hacked")</script>
```

ثغرات ال Redirection (تكمله...)

- قمنا بإستخدام بايلود يعرض كلمة hacked يمكنك استخدام بايلود اخر يناسب احتياجاتك .
- اذن استخدمنا ثغرة التحويل وقمنا بالتحويل الى صفحة اخرى مصابة بثغرة xss وذلك يقوى من الثغرتين ويزيد من مساحة الإختراق فى الموقع.

ثغرات ال Redirection (تكمله...)

- ثانيا:Open Redirect
- ببساطة هى ثغرة تقوم بالتحويل الى صفحات او روابط اخرى ولكنها اقل خطورة تستخدم بشكل رئيسى فى هجمات phishing الصفحات المزورة" حيث بقوم بتحويل الضحية من الموقع الأصلى الى صفحة مزورة لسرقة البيانات وتعتبر اكثر قوة واقناعا من هجمات phishing التقليدية لأن التحويل يتم على الموقع الأصلى بدون اى مشاكل فيعطى الضحية الكثير من الثقة والراحة .
- تظهر هذه الثغرة عندما يقبل تطبيق الويب مدخلات اى بارمتر ويقوم بتنفيذه بدون التحقق من قيمة المدخلات

http://www.isecur1ty.com?redirect=http://www.isecur1ty.org

ثغرات ال Redirection (تكمله...)

- فى المثال السابق هناك بارمتر يسمى redirect يقوم بالتحويل من isecur1ty.com الى isecur1ty.org لكن ماذا اذا قمنا بالتعديل على قيمة البارمتر واسندنا له قيمة جديدة :

http://www.isecur1ty.com?redirect=http://www.phishing.com

- بالطبع سيتم تحويلك الى الرابط الجديد اذا كان الموقع مصاب "لا يتحقق من القيم".
- لإكتشاف الثغرة عليك فحص كل البارمترز الى تقوم بالتحويل الى روابط اخرى وقم بالتعديل على هذه الروابط ولاحظ استجابة الموقع :هل قام بالتحويل ام صد هذا الهجوم ؟
- عملية التحويل يمكن اكتشافها فى الموقع بعدة طرق:
- مباشرة من البارمترز
- او من خلال رسائل التحويل التالية فى HTTP Headers

```
HTTP/1.1 302 Object moved
Location: http://www.isecur1ty.com
```

```
HTTP/1.1 200 OK
Refresh: 0; url=http://www.isecur1ty.com
```

ثغرات ال Redirection (تكمله...)

```
$redirect = $_GET['url'];
 header("Location: " . $redirect);
```

- اكتشاف الثغرة فى اكواد php
- هذا كود بسيط يقوم بالتحويل الى url المسند الى المتغير redirect
- يعتبر هذا الكود مصاب بثغرة Open Redirect لعدم وجود اى وسيلة للتحقق من قيمة المتغير redirect وعدم وجود اى فلترة للمدخلات وتكون النتيجة كالأتى:

```
<strong> http://www.isecur1ty.com/vuln.php?<span style="color: #993300;">url</span>=<span style="color:
#808000;">http://www.hacked.com
</span></strong>
```

- قمنا بالتحويل الى موقع اخر hacked.com وهو موقع المهاجم مثلا !!!

ثغرات ال Redirection (تكمله...)

```
var redirect = location.hash.substring(1);
if (redirect)
   window.location='http://'+decodeURIComponent(redirect);
```

- اكتشاف الثغرة فى اكواد javascript
- كود جافا سكريبت يقوم بعملية التحويل لكن واضح انه لا يوجد اى نوع من انواع التحقق لقيمة المتغير redirect اذن فالموقع مصاب بالثغرة وتكون النتيجة هى الأتى:

```
<strong>http://www.isecur1ty.com/<span style="color: #ff0000;">?#</span>www.hacked.com</strong>
```

- قمنا بالتحويل الى موقع اخر hacked.com وهو موقع المهاجم مثلا !!!
- ولكن ماذا اذا كان الموقع يقوم بعملية تحقق من القيم المدخلة ؟!! سيتوجب علينا التلاعب بالرابط قليلا ومحاولة تخطى الفلترة او كود التحقق من خلال تشفير الرابط url encoding سنستعرض الأن بعض هذه الطرق المتقدمة .

ثغرات ال Redirection (تكمله...)

- مثال1: استغلال متقدم لثغرة Open Redirect
- احظ الإستغلال التالى :استغلال عادى ولكن عندما قمنا به لم تنجح عملية التحويل

http://www.isecur1ty.com/vuln.php?url=http://www.hacked.com

- سنستخدم بعض الحيل لتخطى هذه الفلترة :
- 1/اضافة null byte (%00 or 0x00) قبل الرابط احيانا تخدع WAF وتتخطى الفلترة
- 2/ تشفير كل الرابط url encoding

http://www.isecur1ty.com/vuln.php?url=%68%74%74%70%3a%2f%2f%77%77%77%2e%68%61%63%6b%65%64%2e%63%6f%6d

ثغرات ال Redirection (تكمله...)

- 3/تشفير http://

```
http://www.isecur1ty.com/vuln.php?url=http://www.hacked.com
http://www.isecur1ty.com/vuln.php?url=%68%74%74%70%3a%2f%2fwww.hacked.com
```

- 4/التلاعب فى حالة الحروف مثلا نحول http الى HtTp وهكذا

http://www.isecur1ty.com/vuln.php?url=HtTp://www.hacked.com

- 5/التكرار

http://www.isecur1ty.com/vuln.php?url=http://http://www.hacked.com

ثغرات ال Redirection (تكمله...)

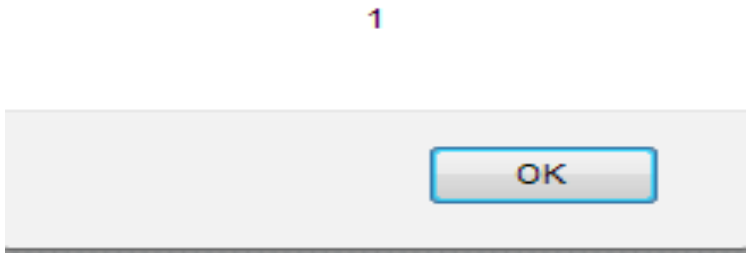
- مثال2: استغلال متقدم لثغرة Open Redirect
- عندما فحصنا الموقع من ثغرات xss لم نكتشف اى ثغرة فالموقع محمى جيدا من ثغرات xss لذا قررنا محاولة استخدام ثغرة Open Redirect لإكتشاف واستغلال ثغرة xss
- هذا استغلال ثغرة التحويل كما تعلمنا: http://www.isecur1ty.com/vuln.php?url=http://www.hacked.com
- محاولة اكتشاف ثغرة xss: http://www.isecur1ty.com/vuln.php?url=<script>alert(1);</script>
- لكن لا جديد فالموقع محمى جيدا من ثغرات xss فما الحل ؟
- سنقوم بتشفير البايلود base64 ليصبح بالشكل التالى PHNjcmlwdD5hbGVydCgxKTs8L3NjcmlwdD4=
- سندمج التشفيرة فى الرابط بهذا الشكل http://www.isecur1ty.com/vuln.php?url=data:text/html; base64,PHNjcmlwdD5hbGVydCgxKTs8L3NjcmlwdD4=

ثغرات ال Redirection (تكمله...)

- والأن سنقوم بنشفير من نوع url encoding ليصبح البايلود النهائى :

http://www.isecur1ty.com/vuln.php?
url=%64%61%74%61%3a%74%65%78%74%2f%68%74%6d%6c%3b%62%61
%73%65%36%34%2c%50%48%4e%6a%63%6d%6c%77%64%44%35%68%62
%47%56%79%64%43%67%78%4b%54%73%38%4c%33%4e%6a%63%6d%6c
%77%64%44%34%3d

- وتصبح النتيجة كالأتى :



- ثغرة xss تعمل 100% فى موقع محمى من xss عن طريق ثغرة open redirect

ثغرات ال Redirection (تكمله...)

- ننتقل الأن الى طرق الحماية من هذه الثغرة :
- يفضل اولا عدم استخدام عملية التحويل او اعادة التوجيه فى موقعك قدر الإمكان
- اضافة فلترة قوية على قيم المدخلات
- منع كل meta characters الغير مستخدمة
- كل عمليات التحويل تكون الى روابط داخلية فى موقعك وعدم السماح بإستخدام روابط خارجية

تم بحمد الله انتهاء الفصل العاشر