

Forum:[Hack Forums](#)

Thread: [\[TuT\] - SQLi to XSS - \[TuT\]](#)

zer0pwn - January 5, 2012, 4:35 pm

[\[TuT\] - SQLi to XSS - \[TuT\]](#)

Hello all of Hack Forums, I decided to post another tutorial on XSS. This tutorial will be involving SQLi aswell though. I will teach you how to get XSS, out of ANY SQLi vulnerable site. This method is very useful for sites that don't have any useful information stored. You can use this method to get the administrator's cookie quite easily

Starting Off

So first of all, we need an SQLi vulnerable site. Just use a google dork like "inurl:event.php?id=". Once you've found a vulnerable site, SQL inject it like you would with ANY site. Now at the part where it displays the vulnerable columns, we will inject our XSS. Now, this is almost impossible for the admin to tell whether you're trying to steal his cookie or not. Usually you will do something like this:

Code `http://www.site.com/news.php?id=1337 UNION SELECT 1,2,3,4,5--+--`

Then it will display our vulnerable column. So, on the vulnerable column, we will add our own little comment. Now, of course the site won't allow any plain-text. We have to use Hex, which is a huge help in this case. So we will encrypt our XSS Vector into Hex. I suggest you do this at:

Code `http://www.swingnote.com/tools/texttohex.php`

Once you've encrypted it, put it in the place of your vulnerable column. But we can't just put the hex there, we have to let the server know that we want our Hex to be decoded on it's way to the page. So we will use "0x" So basically, put "0xHEXHERE". Now hit enter.

Now you should have an alert.

NOTE: It will block the quotes, so you have to do `<script>alert(/XSS/)</script>`

Although, it shouldn't be a problem for our cookie logger.

That's pretty much it, I hope you guys liked it and will find it useful. If you have any questions or need any help just PM me and I'll get back to you ::)

One more thing, I'd like to thank Zer0Freak for helping me use this method (Because I didn't know how to use comments in SQL -facepalm-). Thanks Zer0Freak!

Zhen. - January 5, 2012, 4:38 pm

Nice tutorial bro

Keep it up

Very useful for XSS

IHateMyOldUsername - January 5, 2012, 4:38 pm

You have to many Tutorials they are filling up my bookmarks.

But nice work very HQ tut.

BeggFoMercy - January 5, 2012, 4:38 pm

Nice tut mates keep up the good work
helped me alot Xd

Ichi - January 5, 2012, 4:47 pm

Once again, another good tutorial. Keep it up man

zer0pwn - January 5, 2012, 4:50 pm

Here's an example:

http://ogra.org.pk/cats_disp.php?cat=-172%20/*!UNION*/%20/*!SELECT*/%201,2,3,4,5,0x3c7363726970743e616c6572742831293c2f7363726970743e%20,7,8--+-

Come on guys, this is a useful method for cookie stealing! Haha, ?

Hooded Robin - January 5, 2012, 9:54 pm

Here is another example of XFS, compliments of Rutgers EDU:

Code <https://www.camden.rutgers.edu/security-bb/page.php?id=-2> UNION SELECT
1,0x3c7363726970743e616c657274282758535327293c2f7363726970743e,3,4,5--
Enjoy!