

Forum:[Hack Forums](#)

Thread: [~\[XSS Tutorial\]~ Xss tutorial for beginners ~\[Scripts | Step by Step | Pictures\]~](#)

~[DogiD]~ - October 2, 2012, 3:32 am

[Htmlspecialchars\(\) Tutotrial for beginners](#)

What is XSS?

XSS is website vulnerability, which allows you modify website source code.

Only if vulnerability is persistent/stored, it can modify permanently website source code.

There is 3 type of xss vulnerability; non-persistent, persistent and DOM Based.

Non-persistent

The non-persistent (or reflected) cross-site scripting vulnerability is by far the most common type.

These holes show up when the data provided by a web client, most commonly in HTTP query parameters or in HTML form submissions,

is used immediately by server-side scripts to generate a page of results for that user, without properly sanitizing the request.

Persistent

The persistent (or stored) XSS vulnerability is a more devastating variant of a cross-site scripting

flaw: it occurs when the data provided by the attacker is saved by the server,

and then permanently displayed on "normal" pages returned to other users in the course of regular browsing, without proper HTML escaping.

A classic example of this is with online message boards where users are allowed to post HTML formatted messages for other users to read.

DOM Based XSS

DOM Based XSS (or as it is called in some texts, "type-0 XSS") is an XSS attack wherein the attack payload is executed as a result of modifying the DOM "environment" in the victim's browser used by the original client side script, so that the client side code runs in an "unexpected" manner. That is, the page itself (the HTTP response that is) does not change, but the client side code contained in the page executes differently due to the malicious modifications that have occurred in the DOM environment.

Source: [Wikipedia.org](#) and [Owasp.org](#)

Example 1# (EASY ~ Non-persistent)

1. Whenever i personally want start find xss vulnerability (and also the most easiest way found it), is to check if website have the search bar.

Site what i use has search bar, so let's write ">" in search bar and click "search".

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

2. After the page load, i can right away see that something isn't right at bottom of the page. Let's take a look site source code.

Other tricks is that you write ">xss", then you search "xss" from the source code. That way you can easily see if the target HTMLEncode characters or not!

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

Look like we broke the page * oops

Also seems like website let me search everything, even HTML code like ">. If website has protection against XSS, the HTML code would look something like this .. ">.

Spoiler ([Click to View](#))

3. Let's popup alert box in website.

Write this code to search bar and click search.

Spoiler ([Click to View](#))

When page is loaded, we should get a popup alert box.

Spoiler ([Click to View](#))

Now you know how basically XSS work. You manipulate website source code.

But I can tell you, it's not always that easy to find XSS vulnerability.

Example 2# (MEDIUM ~ Non-persistent)

Even if I say this is medium difficulty, it will still be easy, if you know what you are doing.

Let's start example 2#

1. I still use same site, but now we not use search bar. Let's take a look page URL, `./section.php?ID=18&Lang=En&Nav=Section`

Try change URL little bit,

Spoiler ([Click to View](#))

2. Let's see if page is now different,

Spoiler ([Click to View](#))

3. Now we can again popup alert box, but now write your name/nickname in the alert box,

Spoiler ([Click to View](#))

Here is other way to write your name in alert box:

Spoiler ([Click to View](#))

XSS usage

- [Cookie Stealing](#).

- [XSS Worm](#).

- [Beef Project](#). (XSS Tunnel)

There are also other possibilities, really you just have to think out of the box. But I will list here a few things to get you started. [JDB](#), [Exploit kit](#) iframe, [CSFR](#) think out of the box.

XSS scripts / bypass / Other

We use just the basic alert popup script, but there is a lot of more scripts to popup alert box.

Here I list of scripts/bypass/other,

- [HackBar add-ons](#) (Firefox add-ons)

- https://owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

- <https://wiremask.eu/articles/>
- <https://hackforums.net/showthread.php?tid=2008347>

PS. I hope this tutorial help you to get start xss. If i miss something or you dont understand, then PM ME and i will help & fix it :]
I will update this if i see something what i need to fix.

~ DogiD
WOOF! *

nawtblood - October 2, 2012, 10:47 am

EPIC!, Thx for the tutorial!
This really helped me!

Mr.Phoenix - October 2, 2012, 10:58 am

Making xss tutorial with demo is really superb dude :)
keep it up man :-)

cms_star - October 2, 2012, 11:22 am

Wow man . Nice guide . Very helpful superb
Keep it up.

legends. - October 2, 2012, 11:25 am

Nice tutorial for beginners :)

Regards Roxxor

-Loading- - October 2, 2012, 11:56 am

Thanks for this tutorial, really should help me.

Beowolf - October 2, 2012, 1:46 pm

very good tutorial for newbies!!DogiD

lol...even sqli vulnerablity
inuitcircumpolar.com/section.php?ID='18&Lang=En&Nav=Section

hannah187 - October 2, 2012, 4:33 pm

HI and thanks..
Under Example 1 section 3 is this code still working?
<script>alert(1)</script>

I could not get it to open a pop-up box though..

(Oct 2, 2012 01:46 PM)Beowolf Wrote: [\[CITE\]](#) very good tutorial for newbies!!DogiD

lol...even sqli vulnerablity
inuitcircumpolar.com/section.php?ID='18&Lang=En&Nav=Section
indeed..epic SQLI and good find..I wonder if we can get all the tables..

~[DogiD]~ - October 3, 2012, 3:27 am

(Oct 2, 2012 04:33 PM)hannah187 Wrote: [\[CITE\]](#) HI and thanks..

Under Example 1 section 3 is this code still working?

Yes, It's still working.

If you use tor browser or Firefox, disable NoScript add-ons or other xss block add-ons.

~ DogiD ?

hannah187 - October 3, 2012, 3:54 pm

(Oct 3, 2012 03:27 AM)~[DogiD]~ Wrote: [\[CITE\]](#) Yes, It's still working.
If you use tor browser or Firefox, disable NoScript add-ons or other xss block add-ons.

~ DogiD ?

Thanks it's working in Firefox.. for some reason it did not work in Chromiun browser. Sorry for the trouble and thanks a lot for this tut.

thedudor - November 14, 2012, 10:55 pm

Thanks excellent tutorial i finally got it working

Nakamoto. - November 14, 2012, 11:07 pm

this is a great tutorial good job and thanks.

VoidEx. - November 14, 2012, 11:17 pm

Good tutorial from great member. Well done :)

ScRipT_kld.Die - November 15, 2012, 4:52 am

what a nice thread thank you very much

Kainaan - November 15, 2012, 6:03 am

Awesome tutorial man. Appreciate you taking the time to help people out. If anyone is interested in learning more about how the background code works check out my sig :)

darkheero - November 18, 2012, 12:16 pm

nice tutorial i will try this one soon, i have to look for a better free web hosting first

boyics - November 18, 2012, 1:01 pm

Wow man . Nice guide . Very helpful superb
Keep it up.

thedudor - November 18, 2012, 9:35 pm

(Oct 3, 2012 03:54 PM)hannah187 Wrote: [\[CITE\]](#) Thanks it's working in Firefox.. for some reason it did not work in Chromiun browser. Sorry for the trouble and thanks a lot for this tut.
No, i noticed it does not work with chrome either. it has to be script tweaked...

????? - November 21, 2012, 12:01 pm

Very Nice thread..well explained
Above all sweet one :)

proudweird - November 21, 2012, 2:13 pm

Thx for the tutorial!
This really helped me!

Guest007 - November 21, 2012, 6:08 pm

Nice TUT dude. Thanks 4 that. Keep up the good work, mate.

Ripperpt - November 28, 2012, 2:30 am

Tks m8, now i understande how to find the Vul in code :D

Ps3k0dz - December 4, 2012, 10:54 am

hey Great TuT, well i'll try it later thank's for sharing

zungdsl - December 4, 2012, 12:55 pm

thanks for the tut, really helped me get started ;)

Hacker 4949 - December 5, 2012, 4:40 am

This is really amazing tutorial thanks for helping me.

SIM-111414 - December 5, 2012, 5:08 am

Awesome tut bro.

Thanks for sharing it.

Nice and very well explained. :)

Mumble - December 5, 2012, 8:06 am

Very nice and well written tutorial mate! Very useful for beginners like me, lol.

DreamVII - December 5, 2012, 1:24 pm

Nice tutorial, I appreciate this very much, thanks! :)

DevilChild - December 5, 2012, 5:31 pm

Great tut man, thanks! I learned a lot. :)

alexlandonflicksss - December 24, 2012, 7:22 pm

Thanks a lot for this TUT... Merry christmas...:-)

bUgmAny - December 29, 2012, 5:47 am

Thanks a lot...That's very useful to me...

yhuyhu - January 1, 2013, 5:33 am

threat is awesome and it is right for beginner.

GeoEcon - January 1, 2013, 7:17 pm

Thanks dude...

Nice Tutorial....!!!

creativesnipr - January 13, 2013, 6:50 am

thanks....very good tut with live practical..nice work..

Szakalaka - January 15, 2013, 12:14 pm

one question to cookie grabber, it steals all of the cookies or only one from the site where the script is hidden in url?

AnonRobot - January 15, 2013, 1:05 pm

hey your tut looks very good but the images are not working for me idk why can you help i use chrome and i also tried opera

androdax - January 31, 2013, 5:26 am

(Yea, this thread is a few days old.. found it from the search bar^^)

Great tutorial, so a XSS is just modifying the search script (or the script from another input)?

One question - is there any way to 'crawl' XSS's with Google Dorks or something, like SQLi?

Anyway, thx for this epic tut. :P

Van1la - January 31, 2013, 5:42 am

Thanks for this great tutorial.
Tried and 100% working.

chipp_zanuff - March 28, 2013, 2:34 pm

btw, i tried to the site you gave (<http://inuitcircumpolar.com>), and it doesn't work... how to find a xss-vulnerable site? did you just search for "search" or "login" page, like search.html?

HSM4EVER - April 2, 2013, 1:16 pm

google dorks my friend, google dorks.

vanitywax85 - April 3, 2013, 11:01 pm

thanks man! its very useful. its good to learn the basics.

cyber uryuu - April 4, 2013, 10:00 am

thanks for the tutorial and have a good day

Toasties - April 12, 2013, 10:26 pm

very very good tut, i highly recommend it

Hacker 4949 - April 13, 2013, 10:15 am

Thank u i got bunch of links redirected
Thank a lot.

KaranMohadkar - April 13, 2013, 12:54 pm

THANK YOU VERY MUCH WORKED :) HELPED ME A LOT !

gajraisinghethicalhacker - April 15, 2013, 11:23 pm

can anybody help me in solving xss challenge by yamgata <http://xss-quiz.int21h.jp>

DeleteMeYouWont - April 15, 2013, 11:27 pm

i will be book marking this thanks bro i will learn about it all tmrw thanks for the time and everything

repoh31 - April 16, 2013, 12:28 am

Thank you so much with tutortial
Cheers.

milessoftrials - April 16, 2013, 12:30 am

thank you, cleared up a lot of points for me!

ConfidentialEU - July 26, 2013, 8:03 am

A high quality, well explained tutorial which I'm sure will help out many members.

Djengo - July 26, 2013, 9:18 am

awesome tutorial.
Thank you very much

CYB3RB0X - July 26, 2013, 11:41 am

Awesome tutorial man it was great :DDD!!

herrdeutschland - July 26, 2013, 3:08 pm

very nice tutorial dude ,keep the good work

Colonel Panic - August 1, 2013, 3:59 pm

Excellent tut really helped me understand.

Hackerz93 - August 1, 2013, 5:52 pm

Thanks you for the tutorial ;) hihihihihhi

nephelim - August 3, 2013, 3:40 am

very good job to keep it up tutorial

Luteil - August 13, 2013, 8:56 am

This is a great help for one like me, I'm slowly learning trick of the trade, and I thank you for assisting

Alcapxwn - August 14, 2013, 3:44 pm

Thank's you for your sharing ! NicoTine.

H34T0N - December 10, 2013, 8:28 pm

nice & awesome tutorial, thanks, noscript sucks

133720 - December 10, 2013, 11:43 pm

I love this xss tut.

It help me a lot.

Thanks you.

~[DogiD]~ - December 11, 2013, 2:45 am

(Dec 11, 2013 12:43 AM)133720 Wrote: [\[CITE\]](#) I love this xss tut.

It help me a lot.

Thanks you.

Thank you :)

I'm glad my tutorial help <3

P.S: Tutorial is now updated ;)

~ DogiD

* WOOF! *

Gee4rce - July 26, 2018, 4:46 pm

Nice write up!

Recomended to anyone who is looking to start into XSS.

Cheers, Gee.

~[DogiD]~ - July 27, 2018, 3:58 am

(Jul 26, 2018 04:46 PM)Gee4rce Wrote: [\[CITE\]](#) Nice write up!

Recomended to anyone who is looking to start into XSS.

Cheers, Gee.

Thank you <3 :3

I'm planing to rewrite my tutorial, covering lot more deeper in to the xss.

~ DogiD

lapolis - July 28, 2018, 2:08 am

Thanks for the knowledge! I have something to try today! :)

Aznmig0s - August 3, 2018, 7:12 pm

Nice tutorial for beginners :)

Thank you !

Hackxxxgod001 - January 4, 2019, 9:22 pm

Thanks bro for this... really an introduction

SecureOp - January 5, 2019, 4:40 am

Really enjoy seeing tutorials such as these, keep up the work man.

Hetepheres - January 5, 2019, 5:02 am

Very nice and detailed thread!

goldyroger - January 7, 2019, 4:18 pm

thank you for sharing this tut

momoclo - January 26, 2019, 3:29 pm

threat is awesome and it is right for beginner.

hacker1 - February 17, 2019, 2:16 pm

owasp cheat sheet is something worth reading couple of times ? ?

k1llph1ll - June 14, 2019, 10:49 pm

You can base64 your alert boxes to test if you can bypass av

SwitchOff - September 4, 2020, 10:11 pm

(Feb 17, 2019 03:16 PM)hacker1 Wrote: [CITE](#) owasp cheat sheet is something worth reading couple of times ? ?

"Turn on your Fan please?"

mocxlb0r - November 1, 2022, 3:49 am

Xss is very nice lol this is xss then it nice

SIM-5382664 - July 2, 2023, 9:34 am

thanks man appreciate it