

Forum:[Hack Forums](#)

Thread: [\[Question\] Sellfy Hack XSS](#)

SIM-2988035 - February 28, 2016, 10:19 am

Hello Hackforums,

If I post this thread today, it's to ask a question. I recently saw that a few people managed to hack the website sellfy.com using simple Cross Site Scripting.

I'm very interested in knowing how these people might of performed this hack. Is there a kind soul that could explain to me what is Cross Site Scripting and tell me what tools/tutorials and whatever else I need to know to make a XSS on this website.

Thank you ! And any answer, video, picture, link or anything regarding my question would help !

SlimJimTheHunter - February 28, 2016, 10:37 am

XSS is when unsanitized input is passed to a page and so becomes part of the makeup of the page in some form. This input is usually retrieved by POST or GET forms utilised by the webpage such as a search bar. An attacker will look to utilise XSS when characters such as " > / < are allowed, however there are many complex ways of performing XSS called vectors. The end result is to be able to input an attackers own code to perform a multitude of actions, the most common of which is stealing a legitimate site members or admin's cookies which can then be used to hijack his session and gain access without actually needing a password. There are two types of XSS, stored which is when code is indefinitely placed into a code for multiple users to see and potentially access, reflected however is when the injected code is only available at the time of the request and so a generated link must be sent to a victim. To learn more just search XSS using the search bar

SIM-2988035 - February 28, 2016, 1:09 pm

Thanks a lot SlimJimTheHunter !! A friend of mine also sent me a youtube playlist with videos that explain XSS, I haven't watched them yet but if other people have the same question as me and want to check it out, here is the link: w w w .
[youtube.com/playlist?list=PL1A2CSdiySGIRec2pvDMkYNi3iRO89Zot](https://www.youtube.com/playlist?list=PL1A2CSdiySGIRec2pvDMkYNi3iRO89Zot)

Gee4rce - February 28, 2016, 2:27 pm

Here in this Forum we have also a lot of tutorials which cover XSS (besides other techniques), for a good XSS Tut, click here and scroll down to XSS, choose the first one (by MaXone) and read it:

<https://hackforums.net/showthread.php?tid=2008347&highlight=Megathread>

If you read and dont understand something, then you can ask back here of course, or even pm me for specific questions.

Cheers, Gee.

SIM-2988035 - February 29, 2016, 12:24 am

(Feb 28, 2016 03:27 PM)Gee4rce Wrote: [\[CITE\]](#) Here in this Forum we have also a lot of tutorials which cover XSS (besides other techniques), for a good XSS Tut, click here and scroll down to XSS, choose the first one (by MaXone) and read it:

If you read and dont understand something, then you can ask back here of course, or even pm me for specific questions.

Cheers, Gee.Wow that's a lot of tutorials !! Thanks a lot man I'm sure it will be very helpfull <3

Gee4rce - March 1, 2016, 1:54 am

(Feb 29, 2016 01:24 AM)adhyft Wrote: [\[CITE\]](#) Wow that's a lot of tutorials !! Thanks a lot man I'm sure it will be very helpfull <3

No problems, i am glad you recognise the value of that collection. ?

Cheers, Gee.

CrackPotShot - March 1, 2016, 2:06 pm

(Feb 28, 2016 03:27 PM)Gee4rce Wrote: [\[CITE\]](#) Here in this Forum we have also a lot of tutorials which cover XSS (besides other techniques), for a good XSS Tut, click here and scroll down to XSS, choose the first one (by MaXone) and read it:

If you read and dont understand something, then you can ask back here of course, or even pm me for specific questions.

Cheers, Gee.yo so may tutorials ???

Gee4rce - March 1, 2016, 2:12 pm

Yes, it's one of HF's biggest, i also learned from a lot of the listed ones.

Bookmark it guys ?

SIM-2988035 - March 2, 2016, 4:33 am

Yup I did ;-)) and btw if I can exploit a sql vulnerability can I upload a shell ?

Gee4rce - March 2, 2016, 11:23 pm

This depends,

if the user that runs the SQL Server has writing permissions you could shell the server via INTO_OUTFILE method.

Chances go up if you are allowed to use queries like INSERT, UPDATE, etc. where you can write into the DB.

Another thing would be LOAD_FILE, you can include local files and depending on server configuration you

could eventually combine that with logfile poisoning.

So to answer your question; in general yes, but not in all cases and it strongly depends on how the server is configured.

Cheers, Gee.

SIM-2988035 - March 3, 2016, 2:46 am

Humm.. I'll check that out more in detail. Thank you !!