

Forum:[Hack Forums](#)

Thread: [\[TuT\] - File Upload to Persistent XSS - \[TuT\]](#)

zer0pwn - January 3, 2012, 6:59 pm

[TuT] - File Upload to Persistent XSS - [TuT]

Hi guys, I made a tutorial sort of like this this morning. Except it's with HTML Forms to persistent XSS. In this tutorial, I'll be explaining how you can get persistent XSS from a simple file upload. You can do it with any file extension too (preferably an image file (.png, .jpg)). This is sort of the same method as in my other tutorial, we will need Tamper Data again.

So first of all, let's find a vulnerable page. I'm not sure if this method is public or not (I'm sure it is, because it's not a bad idea, except I haven't seen it around). I actually tested this method on an XSS challenge made by a friend of mine (ring0_).

Once you've found a vulnerable site (It'll be hard to tell if it's vulnerable or not though.) open select your file. I will choose a file "TrollFaic.png". I actually have that file on my PC, and I do use it for this LOL. Now, open tamper data, and start tampering. Once you find the right request to edit, edit it. Change the file name to ".png". If a broken image pops up instead of an alert, use this vector: ".png". That should do it.

As long as the file stays there, it should keep shooting up alert boxes. If you have any questions, requests, or comments, just PM me and I'll get back to you as soon as I can!

Thanks for reading this tutorial!

FastFive - January 3, 2012, 7:29 pm

good tutorial... going to try this soon.

1n54n3 - January 3, 2012, 8:36 pm

Good tutorial mate.

Trying to do this one too.

Ichi - January 3, 2012, 9:12 pm

Once again, great tut bro. Keep em coming

rAtoN - January 3, 2012, 9:23 pm

Can you put images and a example of a shell lol

.Satan - January 3, 2012, 9:59 pm

Do you have a website to use as an example?

zer0pwn - January 3, 2012, 10:07 pm

<http://onlinescan.avast.com/>

Try that for now :D

.Satan - January 3, 2012, 10:21 pm

Couldnt find the thing to edit within the time before the scanner said file to big :(

also

<http://vscan.novirusthanks.org/analysis/68582323963312c8d7fd766d026e603f/aW1nLXNyYy1qYWxlcuQteHNzLXBuZw==/> didnt work, would hex bypassing work?

zer0pwn - January 3, 2012, 10:33 pm

It might, I'll try it.

That's a good idea :)

bluebknight - January 5, 2012, 2:16 pm

You can also upload the file first and then use the rename function to rename to something like the OP posted.

My mediafire XSS worked like that.

Girby2K11 - January 5, 2012, 3:31 pm

Nice tutorial, clearly explained. Well done.

IHateMyOldUsername - January 5, 2012, 3:33 pm

Thanks for posting this it helped alot!

BeggFoMercy - January 5, 2012, 4:03 pm

Really great and hard work mate keep it up <3

rand0 - January 5, 2012, 5:02 pm

Heheh :) This makes a lot of sense, working off of the old IMG xss vector. Nicely done. I never thought of this.

Ashutosh.panda - July 6, 2012, 10:33 am

can you plz detailly expalin how to open a image file and edit it to test xss

looping - March 9, 2013, 12:31 am

hey anyone have tried this and have a working sitee? post heree nice tut!

vehla - March 9, 2013, 1:10 am

Mozilla sucks nowadays with XSS. Chrome shows and Mozilla don't. lol

#Skyline - March 9, 2013, 2:18 am

Nice tutorial. Will help a lot of users out. Good work.

MaXoNe - March 9, 2013, 7:45 am

Use linux it allow <> in filenames.

White_Star - April 20, 2013, 10:28 pm

graet tutorial bud :D

//35 characters

whitehatreborn - April 21, 2013, 6:26 am

Is there anyway to stop the alert box from apearing again?..

1337Orb - November 11, 2015, 7:48 am

Great tut, never found any xss persistent but ive found dom-based and reflected

