

Forum:[Hack Forums](#)

Thread: [Upload Shell Trough Permanent XSS ?](#)

PedroDJavier - January 5, 2015, 6:49 am

Hi guys. There is any way to upload a shell into a webpage that cointains twice xss permanent vulnerabilities?

A friend used one trough, web redirection, and shell was into the metadata or something ?

But, there should be a easier way, shouldn't it?
Thanks in advance

CRResearch - January 5, 2015, 7:01 am

Not sure about the answer to this question but you might wanna look over your grammar in this post and future ones :) - Just to help us understand what you're asking.

PedroDJavier - January 5, 2015, 7:05 am

? sorry, im not native english, so its a bit difficult to express for me.
Thanks in advance!

PD: What i want is upload a shell trough a cross site scripting permanent vulnerability

WillHackForPizza - January 5, 2015, 8:36 am

You can't shell through persistant XSS (unless you can write PHP to a file and view parsed PHP back but thats really rare) - most of the time you want to work with BeeF

<http://www.thesecurityblogger.com/cool-tool-beef-browser-exploitation-framework-on-backtrack-5/>

Or you can always redirect to something more fun ;)

Peace

TheWholeWorldExplodes - January 5, 2015, 2:18 pm

depending on the website you have found it on you could use this
<https://github.com/Prochainezo/xss2shell>

Frosteh - January 5, 2015, 4:50 pm

A thread came up about this the other day.

The short answer is not directly, no. XSS makes use of Javascript which runs in the users browser and doesn't have access to modify anything server side.

However if an admin with elevated privileges visits the page with XSS you can use XSS to steal his session cookies (assuming HTTP only cookies isn't enabled) and once authed against the website you may have access to an admin area or a CMS that has upload capability.

If you're familiar with the CMS, AND it's vulnerable to file upload, AND an admin who is authed visits your page then you could theoretically do this in one shot and have the Javascript upload the shell for you, and people have done that for specific CMS's with known vulnerabilities.

So the long answer is yes, it's possible but only in very specific circumstances, generally speaking you'd use it as part of a larger attack.