

Forum:[Hack Forums](#)

Thread: [Question on XSS + Javascript | \[??\] XSS javascript capabilities \[??\]](#)

?asp3r - September 22, 2012, 2:57 pm

So I've XSS'd a site "non-persistent" but I'm able to use XSSShell.

Im almost 100% sure that you can use the javascript function to force a download + execution of a file.

What all is needed? Do i have to XSS in a link to a JDB?
or can i use the javascript: command to bypass that?

Any help would be fine.

Thanks.

Anli - September 22, 2012, 2:59 pm

yes you can use javascript, so if you want to execute file you need to get browser vulnerability this is only one way to execute file with browser using javascript :))

if you have more question PM or post here

?asp3r - September 22, 2012, 5:05 pm

still open for any help. anli + me didnt really get all that much done

No?????? - September 22, 2012, 8:24 pm

You can make someone download a file, but not execute it. That being said, it could be done if you have an exploit for their browser or an installed plugin.

?asp3r - September 23, 2012, 11:39 am

(Sep 22, 2012 08:24 PM)??Yes Wrote: [\[CITE\]](#) You can make someone download a file, but not execute it. That being said, it could be done if you have an exploit for their browser or an installed plugin.

can you have it load a 1x1 iframe that has a direct link to a page with only a jdb.

would the run java popup come outside the iframe?

?asp3r - September 23, 2012, 12:07 pm

(Sep 23, 2012 12:02 PM)Th3PonyWizard Wrote: [\[CITE\]](#) No.

-snip-

okay. so <https://hackforums.net/showthread.php?tid=341603> doesnt work?

And i know its not javascript but why cant i do that with a non persistent link? and send that link to some1 who thinks they are running a game?

Th3PonyWizard - September 23, 2012, 12:12 pm

(Sep 23, 2012 12:07 PM)14942744 Wrote: [\[CITE\]](#) okay. so <https://hackforums.net/showthread.php?tid=341603> doesnt work?

And i know its not javascript but why cant i do that with a non persistant link? and send that link to some1 who thinks they are running a game?Um, you can in fact do it with a non-pers link. Yeah, the pop-up will appear.

MajorFail - September 23, 2012, 12:12 pm

You could use the exploit in Java7, or the new one in IE, as far as I know they are silent driveby's so there will not be any popups.

?asp3r - September 23, 2012, 12:18 pm

(Sep 23, 2012 12:12 PM)Th3PonyWizard Wrote: [\[CITE\]](#) Um, you can in fact do it with a non-pers link. Yeah, the pop-up will appear.

so why then, when ppl xss, they just try and steal cookies, instead of taking out the whole computer?