

Forum:[Hack Forums](#)

Thread: [Bypassing XSS filters?](#)

Abducted - November 10, 2016, 2:19 pm

Hey, could anyone help me bypassing some browser XSS filters? If you think you might do it leave a post so I can shoot you a PM!

Cheers,
Abducted ?

libc - November 10, 2016, 2:25 pm

Find which characters the web application filters and construct a payload that doesn't contain them. Try the OWASP cheat sheet.

Abducted - November 10, 2016, 2:26 pm

(Nov 10, 2016 03:25 PM)libc Wrote: [\[CITE\]](#) Find which characters the web application filters and construct a payload that doesn't contain them. Try the OWASP cheat sheet.

I was talking about browser XSS filters.

Sorry gonna update OP.

Straight Grizzly - November 10, 2016, 6:23 pm

(Nov 10, 2016 03:26 PM)Abducted Wrote: [\[CITE\]](#) I was talking about browser XSS filters.

Sorry gonna update OP.

It depends on the browser entirely. When testing a web application, I test for XSS manually through Firefox because their filters seem to be the worst. You would still follow the same methodology that Libc has presented nonetheless

Abducted - November 10, 2016, 8:21 pm

(Nov 10, 2016 07:23 PM)Straight Grizzly Wrote: [\[CITE\]](#) It depends on the browser entirely. When testing a web application, I test for XSS manually through Firefox because their filters seem to be the worst. You would still follow the same methodology that Libc has presented nonetheless

I need to get Chrome filters bypassed somehow. Thanks for the advice though!

LittleBobbyTables - November 10, 2016, 8:24 pm

(Nov 10, 2016 09:21 PM)Abducted Wrote: [\[CITE\]](#) I need to get Chrome filters bypassed somehow. Thanks for the advice though!

Is this a personal test? If so, don't use Chrome.

Outside of that, what are you breaking out of?

Straight Grizzly - November 11, 2016, 8:18 am

(Nov 10, 2016 09:21 PM)Abducted Wrote: [\[CITE\]](#) I need to get Chrome filters bypassed somehow. Thanks for the advice though!

Google will provide a wealth of information for you. Knowing what version you need to bypass will help as well.

Fladrif - November 11, 2016, 10:18 am

Have a look at "OWASP Xenotix XSS Exploit Framework" - its a great tool which emulates each of the major browsers, so you can see if your XSS would work on what browser, then start to home in

on how to bypass Webkit/Chrome.

But I agree it is a bit of trial and error working out which characters are being filtered. @brutellogic on Twitter is a great resource.

HiddenEyE - November 11, 2016, 8:44 pm

OP shot me a PM, i can help you on this.
chrome has never been my challenge so far.

?Anubis - November 13, 2016, 11:57 am

Depends on the filters, if for example the filter replace "<" with "\<", you could change your input to "\<" and after the filter applied, it would be "\\<", wich would work.