

Forum:[Hack Forums](#)

Thread: [Bypassing chromes xss audit](#)

vorticalbox - June 12, 2017, 12:16 am

I have found a website with a xss but if using any chrome based browser the xss detection kicks in and blocks the attack.

Any one have any tips how to by pass it? Firefox,ie etc. Work fine.

Lor?d - June 12, 2017, 12:16 am

Not using Chrome seems like a good start.

vorticalbox - June 12, 2017, 12:41 am

(Jun 12, 2017 12:16 AM)That One Random Wrote: [\[CITE\]](#) Not using Chrome seems like a good start. Yeah that's one idea but I cant know what the user will be using and this want to maximise victims.

?Criminal - June 12, 2017, 1:03 am

(Jun 12, 2017 12:41 AM)vorticalbox Wrote: [\[CITE\]](#) Yeah that's one idea but I cant know what the user will be using and this want to maximise victims.

<https://hackforums.net/showthread.php?tid=5472183>

can do something like this to maximize targets^ with a little SE you can force them to use another browser like firefox for example which if it detects their on the correct browser will redirect them to the payload.

vorticalbox - June 12, 2017, 1:41 am

(Jun 12, 2017 01:03 AM)?Criminal Wrote: [\[CITE\]](#) can do something like this to maximize targets^ with a little SE you can force them to use another browser like firefox for example which if it detects their on the correct browser will redirect them to the payload.

Thanks for the idea didn't think of that :)

?Criminal - June 12, 2017, 2:13 am

(Jun 12, 2017 01:41 AM)vorticalbox Wrote: [\[CITE\]](#) Thanks for the idea didn't think of that :) in hacking the skys the limit.

pop.pop.ret - June 12, 2017, 4:50 am

It's currently possible to bypass Chrome's XSS filter and various CSP configurations via an SWF assuming that your victim has flash enabled. PM me for more info.

Or alternatively you could just go find a universal bypass for chrome :) not too difficult.

Also, depending on what context the reflection to source is (for example whether its inline, tag-based or w/e) can massively effect how easy it is to come up with a bypass. If its inline injection e.g. its being reflected as an attribute within a hidden input tag or something then I can give you a working bypass for this too.

Just gimme the context, show me the reflection point and how its landing in the source.. and maybe I can help.