

Forum:[Hack Forums](#)

Thread: [Cookie stealing with XSS on Google Chrome](#)

Hakuna Matata - January 26, 2015, 8:16 am

I need your help peeps.

I'm trying to figure out how to steal cookies using XSS on Google Chrome. It works fine on Firefox, as the browser doesn't have any kind of XSS protection but Google Chrome does.

When trying to inject some code into the site, this happens.

Probably because this is an old method of doing it.
Help me pls. Is it even possible on Chrome?

-Acid - January 26, 2015, 8:29 am

Chrome has its own XSS filters...refer here and try again

PHP Code

<?php

<http://www.frameloss.org/2011/11/01/using-google-chrome-for-security-testing/>

Hakuna Matata - January 26, 2015, 9:35 am

(Jan 26, 2015 09:29 AM)-Acid Wrote: [\[CITE\]](#) Chrome has its own XSS filters...refer here and try again

PHP Code

<?php

<http://www.frameloss.org/2011/11/01/using-google-chrome-for-security-testing/>

How about you actually read the thread, post whore.

?Criminal - January 26, 2015, 9:40 am

Cookie Stealing in 2015 is pretty much dead any site worth it's salt has the httponly flag set and xss can do more then just steal cookies refer to xss2shell for an example on how powerful xss is and thats just on wordpress imagine if you thought of your own payload, you can do anything in the victims browser that javascript has access to including the DOM.

EDIT: looks like a wordpress site in that case xss2shell will help you out possibly.As for bypassing chromes filters the SVG html5 element used to not be blacklisted but im not sure what methods people use nowadays.

Frosteh - January 26, 2015, 10:47 am

You're going up against chromes XSS filter which is no small task.

Firefox doesn't have any XSS prevention which makes it ideal for testing, IE has some but it's quite easily broken, often as little as a double URL encode will bypass it. However chromes is quite extensive.

Some large sites do set httponly flags but I don't think it's that common among sites in general (when looking at it from a pure numbers stand point), and in general you can just make Javascript do whatever you want in the users browser, rather than trying to steal the cookie and do it for them,

you'll still pass all the authentication. So in that regards XSS still has a lot of uses.

Regarding the original question, I'm not completely sure what's best to bypass chromes anti-xss filter, certainly you can't get away with <script> tags in the URL, however the more obscure XSS attack vectors can sometimes get through, there's a massive list here https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

Hakuna Matata - January 26, 2015, 12:37 pm

(Jan 26, 2015 11:47 AM)Frosteh Wrote: [\[CITE\]](#) You're going up against chromes XSS filter which is no small task.

Firefox doesn't have any XSS prevention which makes it ideal for testing, IE has some but it's quite easily broken, often as little as a double URL encode will bypass it. However chromes is quite extensive.

Some large sites do set httponly flags but I don't think it's that common among sites in general (when looking at it from a pure numbers stand point), and in general you can just make Javascript do whatever you want in the users browser, rather than trying to steal the cookie and do it for them, you'll still pass all the authentication. So in that regards XSS still has a lot of uses.

Regarding the original question, I'm not completely sure what's best to bypass chromes anti-xss filter, certainly you can't get away with <script> tags in the URL, however the more obscure XSS attack vectors can sometimes get through, there's a massive list here https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

Great information, thank you.

The site doesn't use httponly, as it's a rather small site :].

Misha the unfortunate - January 27, 2015, 8:10 am

(Jan 26, 2015 01:37 PM)Hakuna Matata Wrote: [\[CITE\]](#) Great information, thank you.

The site doesn't use httponly, as it's a rather small site :].

Gonna do some testing and report back OP.

If I don't report back in max 2 days, pm me cus i've probably forgotten.

 works on Chrome upto 38, but only works on Chrome.

<iframe srcdoc="" /> works on Chrome upto 35, Firefox upto 28 and Opera upto 15. This would be your best bet.

?Criminal - January 29, 2015, 7:14 am

(Jan 27, 2015 09:10 AM)Misha the unfortunate Wrote: [\[CITE\]](#) Gonna do some testing and report back OP.

If I don't report back in max 2 days, pm me cus i've probably forgotten.

 works on Chrome upto 38, but only works on Chrome.

<iframe srcdoc="" /> works on Chrome upto 35, Firefox upto 28 and Opera upto 15. This would be your best bet.

current version is 40 and chrome auto updates so how would this help OP when chrome practically updates the filter every update.

Misha the unfortunate - January 29, 2015, 7:32 am

(Jan 29, 2015 08:14 AM)maybeBlue Wrote: [\[CITE\]](#) current version is 40 and chrome auto updates so how would this help OP when chrome practically updates the filter every update.I didn't know

Chrome autoupdates, sorry.