

Forum:[Hack Forums](#)

Thread: [Test your javascript skills | XSS challenge](#)

redlightrouter - December 4, 2016, 7:27 am

Hello all,

I made a little XSS challenge that's pretty advanced, not the hardest but also not the easiest. I am very curious who of you can really think like a hacker and bypass this challenge I made. This is the url:

Quote:<http://xsschallenge.coolpage.biz/> I know alot of you guys will find the solution, but don't post it here ;).

Good luck :)

Spoiler ([Click to View](#))

EDIT: I am hosting it on a different site than yesterday, that's why I double posted. Sorry for that.

Faith Connors - December 4, 2016, 1:55 pm

Damn it, got a solution but now my browser's XSS auditor pops up telling me it won't parse the request :P

Oh well, back to the drawing board.

redlightrouter - December 6, 2016, 8:25 am

(Dec 4, 2016 02:55 PM)Faith Connors Wrote: ([CITE](#)) Damn it, got a solution but now my browser's XSS auditor pops up telling me it won't parse the request :P

Oh well, back to the drawing board.

Haha nice, keep it going.

Hint:

Spoiler ([Click to View](#))

The app filters words like: alert, prompt and confirm. If there only was a way to split words and execute those splitted words all at once..

j1nx0 - December 6, 2016, 8:49 am

<https://imgur.com/a/SytoA>

nice challenge tho

FormerlyS - December 6, 2016, 9:19 am

Thanks for the challenge

SIMON - December 6, 2016, 9:52 am

lol I can't figure it out :(but again I don't have much experience in cross-site scripting :P

redlightrouter - December 6, 2016, 11:38 am

(Dec 6, 2016 10:19 AM)FormerlyS Wrote: [\[CITE\]](#)

Thanks for the challenge

Nice and thanks! Can you send me the vector you used in a PM? I am kinda curious how someone else would do this :)

(Dec 6, 2016 09:49 AM)j1nx0 Wrote: [\[CITE\]](#) <https://imgur.com/a/SytoA>

nice challenge tho

Nice and you also thanks! Can you also hit me a PM with your vector.

semendaemon - December 6, 2016, 11:48 am

I cheated the shit out of this one. The alert hints it away ;)

redlightrouter - December 6, 2016, 1:28 pm

Yeah, my noob ass forgot to filter out prompt (lol). For everyone that did it with a vector like '... onerror=prompt(1)/>' try it again ^^

semendaemon - December 6, 2016, 1:46 pm

(Dec 6, 2016 02:28 PM)redlightrouter Wrote: [\[CITE\]](#) Yeah, my noob ass forgot to filter out prompt (lol). For everyone that did it with a vector like '... onerror=prompt(1)/>' try it again ^^Will do, also filter out console.log while you're at it :p

SIMON - December 6, 2016, 1:58 pm

Lol 2 hours later and i have still not completed it ;(

redlightrouter - December 6, 2016, 2:41 pm

(Dec 6, 2016 02:58 PM)Siimon. Wrote: [\[CITE\]](#) Lol 2 hours later and i have still not completed it ;(

Another hint and a pretty much a spoiler:

Spoiler ([Click to View](#))

Imagine a guard on an airport that doesn't want H2o to be smuggled. The only thing he is checking for is H2o. So people with h2 can pass, people with o can pass, but once someone with H2o tries to get on the plane he gets denied. So if there's someone smart enough to think 'hey, let me bring h2 and o, and once I arrive in Columbia then I will make it H2o.' You pretty much get the same result, right?

This is the final hint since this is also a pretty big spoiler.

Succes ?

Forc?d - December 6, 2016, 3:07 pm

First attempt. (Kinda not legit method)

<https://gyazo.com/ff9cb8c422422001cf3ae6e60310f52f>

Update#2

Pretty darn close

<https://gyazo.com/66473a6385f016ea30c9fa61d4204f4c>

Just a matter of removing some "" ?

Faith Connors - December 6, 2016, 3:23 pm

Pretty sure I have a solution, will update in a bit.

Turns out I'm on Chrome Canary and they have all kinds of beta nightly shit for anti-xss going on and it's being a real nazi with me.

Firefox seems to let some stuff go through and a lot of the stuff I try /seems/ to work but I just don't get the alert.

EDIT: Now Firefox is letting my request go through but removing my code zzzz

EDIT2: I HAVE A WITNESS TO PROVE IM NOT A 100% RETARD

<https://i.gyazo.com/b51894698b25163110dc285974176aa4.png>

I HAD THE SOLUTION BEFORE BUT RAN INTO SOME PROBLEMS AND IM ONLY ABOUT 10-15% RETARDED

Untraceable_Pro - December 6, 2016, 5:53 pm

What are those variable `_0x6ffd` and how does the function spoiler work ?

Faith Connors - December 6, 2016, 6:02 pm

(Dec 6, 2016 06:53 PM)Untraceable_Pro Wrote: [\[CITE\]](#) What are those variable `_0x6ffd` and how does the function spoiler work ?

It's not really important to the solution at all, basically just prints the line.

Dunno why it had to be obfuscated lmao, maybe to try and throw people off?

redlightrouter - December 7, 2016, 12:46 am

(Dec 6, 2016 07:02 PM)Faith Connors Wrote: [\[CITE\]](#) It's not really important to the solution at all, basically just prints the line.

Dunno why it had to be obfuscated lmao, maybe to try and throw people off?

I actually did it for the people who didn't want to see spoilers or hints while watching the source code :))

(Dec 6, 2016 04:23 PM)Faith Connors Wrote: [\[CITE\]](#) Pretty sure I have a solution, will update in a bit.

Turns out I'm on Chrome Canary and they have all kinds of beta nightly shit for anti-xss going on and it's being a real nazi with me.

Firefox seems to let some stuff go through and a lot of the stuff I try /seems/ to work but I just don't get the alert.

EDIT: Now Firefox is letting my request go through but removing my code zzzz

EDIT2: I HAVE A WITNESS TO PROVE IM NOT A 100% RETARD

<https://i.gyazo.com/b51894698b25163110dc285974176aa4.png>

I HAD THE SOLUTION BEFORE BUT RAN INTO SOME PROBLEMS AND IM ONLY ABOUT 10-15% RETARDED

Haha nice! Mind sending me the vector?

(Dec 6, 2016 03:41 PM)redlightrouter Wrote: [\[CITE\]](#) Another hint and a pretty much a spoiler:

Spoiler [\(Click to View\)](#)

Imagine a guard on an airport that doesn't want H2o to be smuggled. The only thing he is checking for is H2o. So people with h2 can pass, people with o can pass, but once someone with H2o tries to get on the plane he gets denied. So if there's someone smart enough to think 'hey, let me bring h2 and o, and once I arrive in Columbia then I will make it H2o.' You pretty much get the same result, right?

This is the final hint since this is also a pretty big spoiler.

Succes ?

(Dec 6, 2016 04:07 PM)Forc?d Wrote: [\[CITE\]](#) First attempt. (Kinda not legit method)
<https://gyazo.com/ff9cb8c422422001cf3ae6e60310f52f>

Update#2

Pretty darn close

<https://gyazo.com/66473a6385f016ea30c9fa61d4204f4c>

Just a matter of removing some "" ?

Not sure how that didn't trigger the filter. Mind sending your steps that you did in a pm

NOTE: Some of you managed to get an alert box by a hex vector. That's patched.

ka\$h - December 7, 2016, 2:47 am

redlightrouter - December 7, 2016, 1:28 pm

(Dec 7, 2016 03:47 AM)Ka\$h Wrote: [\[CITE\]](#)

Nice! Don't forget to pm me your vector :)

ka\$h - December 7, 2016, 10:37 pm

(Dec 7, 2016 02:28 PM)redlightrouter Wrote: [\[CITE\]](#) Nice! Don't forget to pm me your vector :)

Just PMed you my vector now

redlightrouter - December 8, 2016, 9:44 am

(Dec 7, 2016 11:37 PM)Ka\$h Wrote: [\[CITE\]](#) Just PMed you my vector now

Thanks, I tried to patch that vector. Can you confirm that?

VAP3 - December 9, 2016, 11:43 am

Cant post links so I can show proof...

Faith Connors - December 9, 2016, 12:31 pm

(Dec 9, 2016 12:43 PM)VAP3 Wrote: [\[CITE\]](#) Cant post links so I can show proof...

Take off the http at the front or put spaces in it.

And don't put the url of the site as it will contain your vector, just a screenshot is fine.

Maxie - December 9, 2016, 1:09 pm

Cba to post pic, but nice challenge, had me a bit amused for a while! Probably vulnerable to more than one vector aswell.

B14ck_M4g1k - December 10, 2016, 2:07 am

Quite easy and fun! would love to see more.

Can't post images yet so here is the link

(http://imgur(.)com/a/Y2qpo

remove the ()

- B14cK_M4g1K ?

?Xe - December 10, 2016, 4:46 am

(Dec 8, 2016 10:44 AM)redlightrouter Wrote: [\[CITE\]](#) Thanks, I tried to patch that vector. Can you

confirm that?

What do you mean you tried to patch it? Are you just patching people's vectors they used? How is that fair if you are making it harder & harder lol ?

Faith Connors - December 10, 2016, 5:33 am

(Dec 10, 2016 05:46 AM)?Xeon Wrote: [\[CITE\]](#) What do you mean you tried to patch it? Are you just patching people's vectors they used? How is that fair if you are making it harder & harder lol ?
He didn't patch my vector lol

Hoodie+ - December 10, 2016, 5:37 am

<http://image.prntscr.com/image/a6661e68cf0149eca422fb33465b9a3a.png>

Easy challenge.

My payload:

Spoiler [\(Click to View\)](#)

Quote:*removed*

redlightrouter - December 10, 2016, 8:28 am

(Dec 10, 2016 05:46 AM)?Xeon Wrote: [\[CITE\]](#) What do you mean you tried to patch it? Are you just patching people's vectors they used? How is that fair if you are making it harder & harder lol ?
Because I want the vector to be identical as the one I had in mind. Faith's vector was good and so is hoodie's vector.

(Dec 10, 2016 06:37 AM)Hoodie+ Wrote: [\[CITE\]](#)
<http://image.prntscr.com/image/a6661e68cf0149eca422fb33465b9a3a.png>

Easy challenge.

My payload:

Spoiler [\(Click to View\)](#)

Nice! That's what I like to see. Mind removing your vector though? ^^

Andrew Carnegie - December 10, 2016, 1:27 pm

prntscr dot com/dhud0j easy did it again :P

xAnonymousxx - December 10, 2016, 4:15 pm

seems like a good one :))

redlightrouter - December 11, 2016, 10:57 am

(Dec 10, 2016 02:27 PM)Andrew Carnegie Wrote: [\[CITE\]](#) prntscr dot com/dhud0j easy did it again :P
Nice :) once you're able to pm, pm me your vector :)

Alim - July 22, 2017, 9:26 am

I don't send image, but I'll leave the link prntscr. com/fxyiyt

Please send me to pm your payload.

Nice challenge, thanks.

Akara Products - July 26, 2017, 9:40 am

i think im not good enough but thx anyways

redlightrouter - *July 27, 2017, 3:08 pm*

(Jul 26, 2017 09:40 AM)ImSeriousAF Wrote: [\[CITE\]](#) i think im not good enough but thx anyways
This one is very easy. Just try a bit harder :).