

Forum:[Hack Forums](#)

Thread: [XSS Challenge 4 | Test your skills](#)

redlightrouter - March 25, 2017, 8:31 am

Hey all,

I've made another xss challenge. Difficulty level is low to medium, but do not underestimate it.
[XSS Challenge](#)

Don't forget to PM me your solution :)

Good luck ?

Spoiler ([Click to View](#))

Faith Connors - March 25, 2017, 9:02 am

you were right i am getting a headache

edit: figured out a possible vector. took a bit of setup though lol. pming soon and adding screenshot.

screenshot added:

redlightrouter - March 25, 2017, 11:02 am

(Mar 25, 2017 09:02 AM)Faith Connors Wrote: [\[CITE\]](#) *****Nice one, but unfortunately it's not what I had in mind.

HINT: Look at the source code

Kashmiri Hunter - March 25, 2017, 10:35 pm

0x00 - Payload Sent !

Thanks !

Nomad.Null - March 25, 2017, 10:58 pm

(Mar 25, 2017 11:02 AM)redlightrouter Wrote: [\[CITE\]](#) Nice one, but unfortunately it's not what I had in mind.

HINT: Look at the source code

An XSS is an XSS ?

redlightrouter - March 26, 2017, 8:50 am

(Mar 25, 2017 10:58 PM)True Demon Wrote: [\[CITE\]](#) An XSS is an XSS ?

I guess that's what you could call it, yeah :p.

(Mar 25, 2017 10:35 PM)Kashmiri Hunter Wrote: [\[CITE\]](#) 0x00 - Payload Sent !

Thanks !
Nice, you got it right :)

Lsd-r2 - March 26, 2017, 11:22 am

Bro have you a sql test/games??

redlightrouter - March 31, 2017, 12:00 pm

(Mar 26, 2017 11:22 AM)Lsd-r2 Wrote: [CITE](#) Bro have you a sql test/games??

Nope sorry. I consider myself a noob in SQL, so I don't really know how to make an interesting challenge. I know how to make the standard/basic/too often used challenge, but like I said it's literally everywhere.

THC - March 31, 2017, 12:30 pm

Belongs here I think.

[Website Hacking](#)

redlightrouter - March 31, 2017, 12:52 pm

I guess it's time for a little write up.

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

So these are being filtered:

PHP Code

```
<?php
$blacklist = array('(',')','alert','eval','prompt','confirm','atob','&lt;script&gt;','&','javascript','data','\u{61}',
'http','https');
```

Changing those words to uppercase won't work since it will be treat as lowercase.

PHP Code

```
<?php
foreach($blacklist as $i)
{
    if(strpos(strtolower($_GET['xss']), $i))
    {
        $_GET['xss'] = '1';
    }
}
```

EDIT: Something went wrong so I made a shorter version.

So what basically happens is that the once we try our basic img src payload it filters parentheses and alert,confirm and prompt.

In javascript it's possible to use unicoded letters in functions etc.
so instead of a normal alert I use `\u{6C}ert()` (or `\u006cert()`)

Now the only thing that gets filtered are the parentheses.

In javascript it is also possible to use backticks (`) as parentheses. The only thing is that the given argument will be handles as a string.

so the final payload is:

PHP Code

```
<?php
&lt;img src=x on*error="\u{6C}ert``" &gt;
```

REMOVE *

Thanks for your submissions!

Alim - *July 22, 2017, 10:25 am*

Sorry, again i arrived later.

I found the solution before seeing the answers.

[prntscr .com/fyy613](https://prntscr.com/fyy613)

Thanks.