



03/04/2021

XSS Reflected Attacks on DVWA

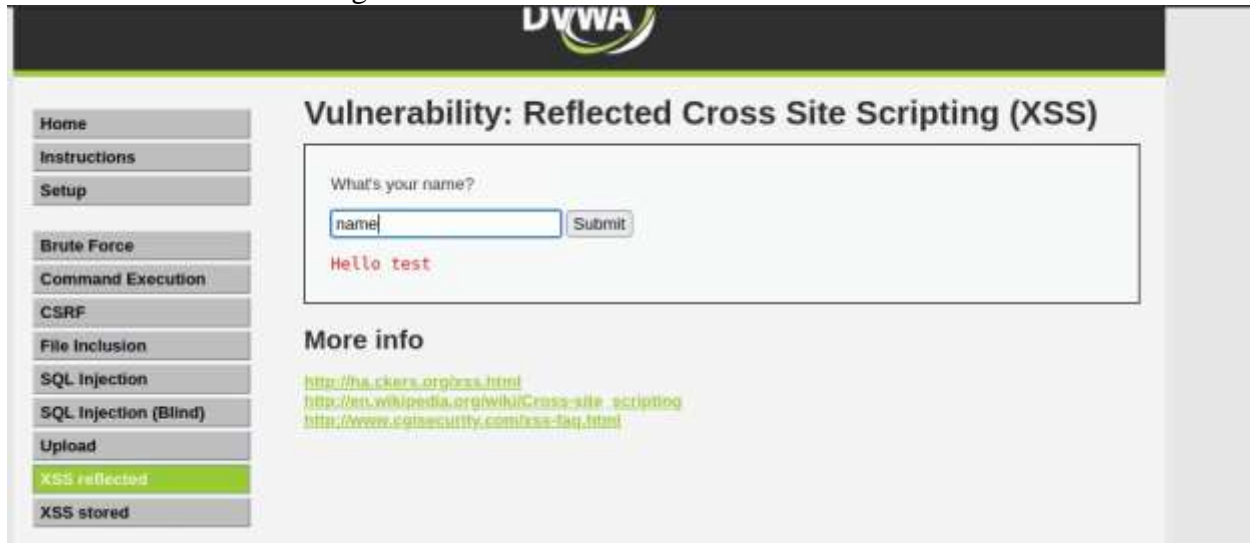
Prepared by Md Jobarul Islam

Md Jobarul Islam
Mirpur, Dhaka
email: jobarulislam1203@gmail.com
linkedIn: <https://www.linkedin.com/in/jobarulislam/>
GitHub: <https://github.com/jobarulislam>
Phone: 01312-678017

LogIn to the dvwa and select XSS reflected :

Low security XSS Reflected Attack

1st Observe how its working :



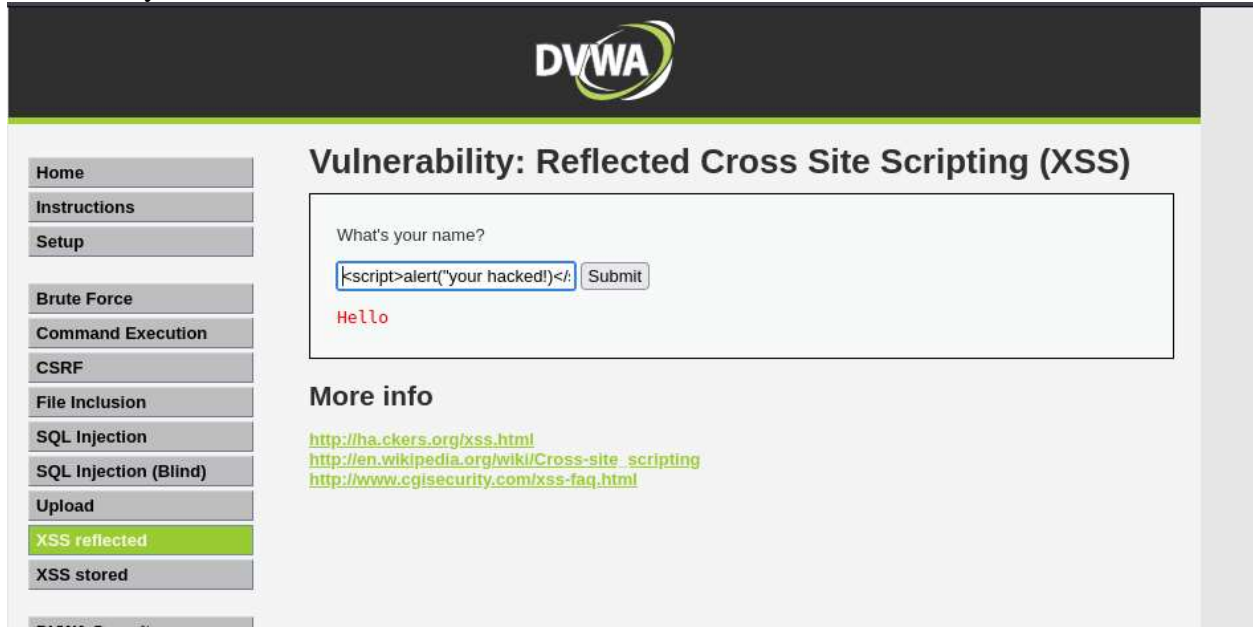
Use (Ctrl + u) for open source code:

(Ctrl + f) for search [hello reflected_text]

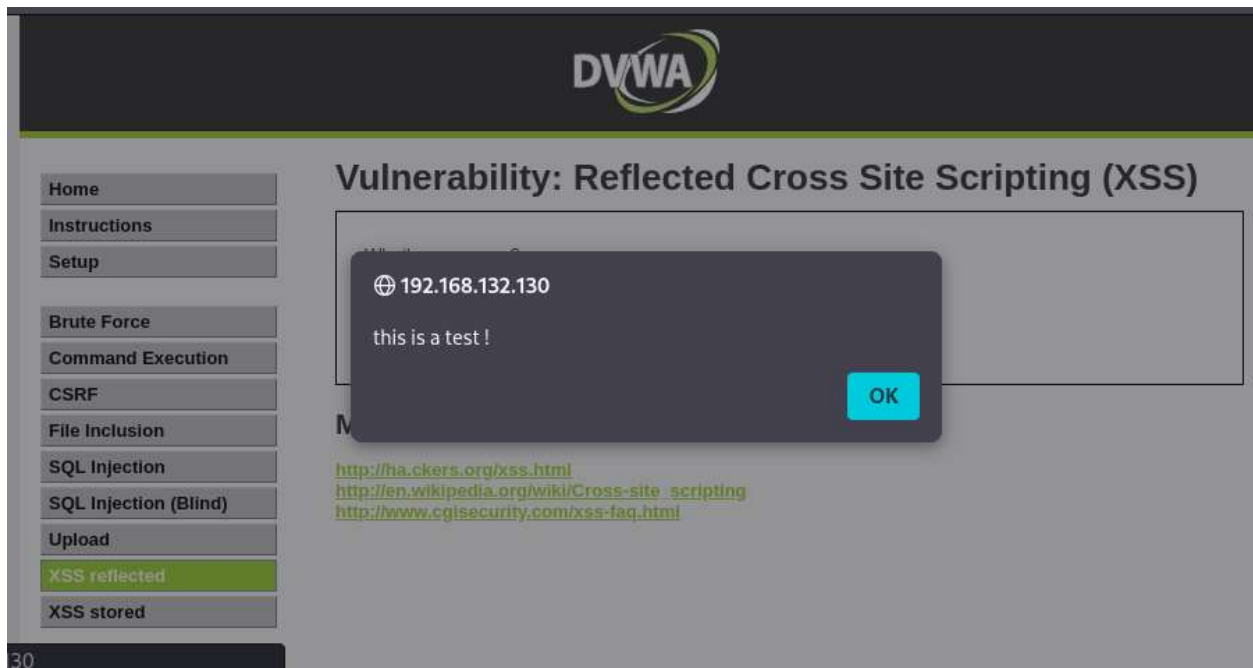
Back to Render window by (Ctrl + w)

```
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB CrackStation - Online ...
36 <div id="main body">
37
38
39 <div class="body padded">
40 <h1>Vulnerability: Reflected Cross Site Scripting (XSS)</h1>
41
42 <div class="vulnerable code area">
43
44 <form name="XSS" action="#" method="GET">
45 <p>What's your name?</p>
46 <input type="text" name="name">
47 <input type="submit" value="Submit">
48 </form>
49
50 <pre>Hello test</pre>
51
52 </div>
53
54 <h2>More info</h2>
55
56 <ul>
57 <li><a href="http://hiderefer.com/?http://ha.ckers.org/xss.html" target="_blank">http://ha.ckers.org/xss.html</a></li>
58 <li><a href="http://hiderefer.com/?http://en.wikipedia.org/wiki/Cross-site_scripting" target="_blank">http://en.wikipedia.org/wiki/Cross-site_scripting</a></li>
59 <li><a href="http://hiderefer.com/?http://www.cgisecurity.com/xss-faq.html" target="_blank">http://www.cgisecurity.com/xss-faq.html</a></li>
60 </ul>
61 </div>
62
63 <br />
64 <br />
Hello name ^ v Highlight All Match Case Match Diacritics Whole Words 1 of 1 match Reached end of page, co X
```

Submit [`<script>alert("this is a test! ")</script>`] code in input box for check for Xss vulnerability:

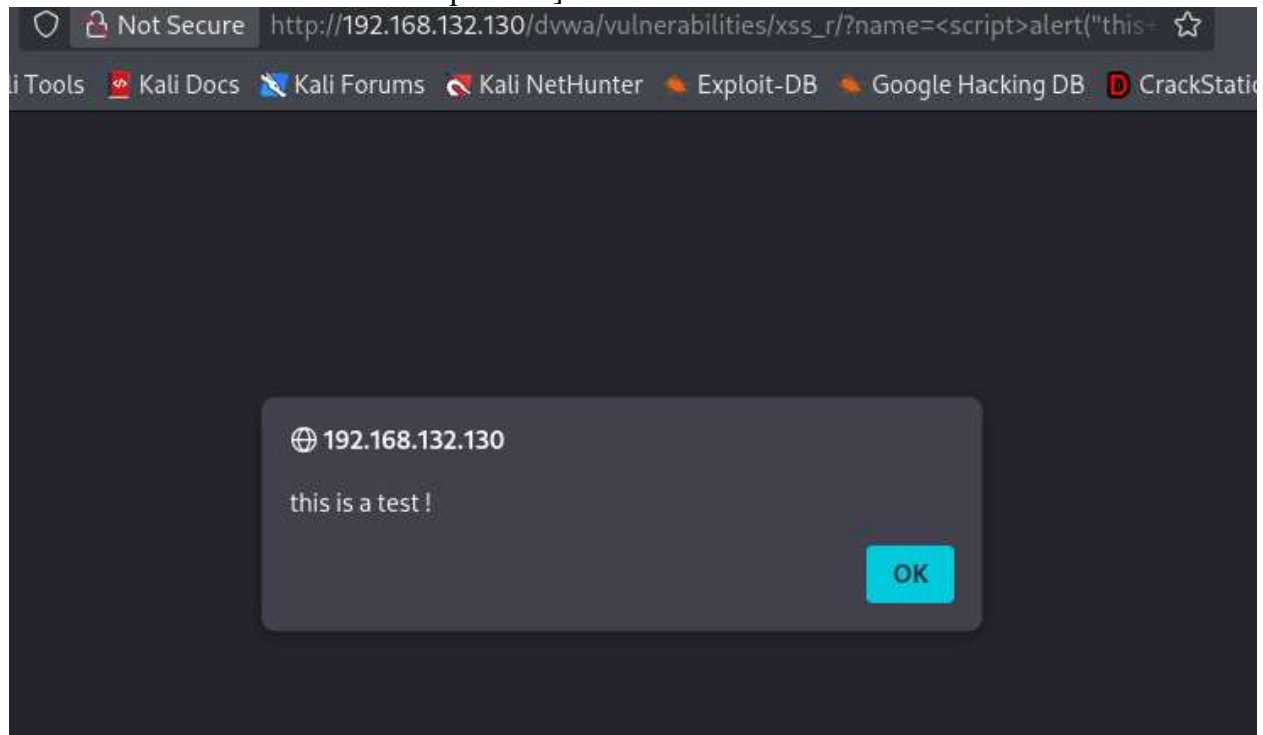


Code Inject work so this is vulnerable :



Url of this page :

[http://192.168.132.130/dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22this+is+a+test+%21%22%29%3C%2Fscript%3E#]



It seems that this page has vulnerability of XSS Reflected and I found it. So it can be compromised by an attacker.

Medium security XSS Reflected Attack

Submit security level low to medium:

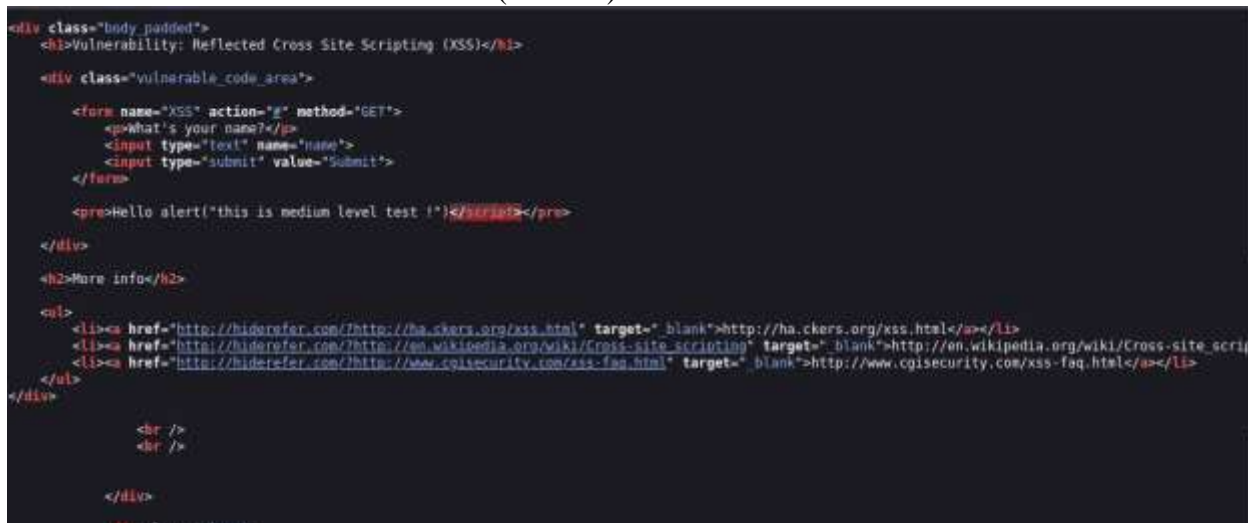


Its same as low level. Take look how the page work and the inject malicious code for check the vulnerability.

Code: [`<script>alert("this is medium level test !")</script>`] this time not working its do what its mean to be:

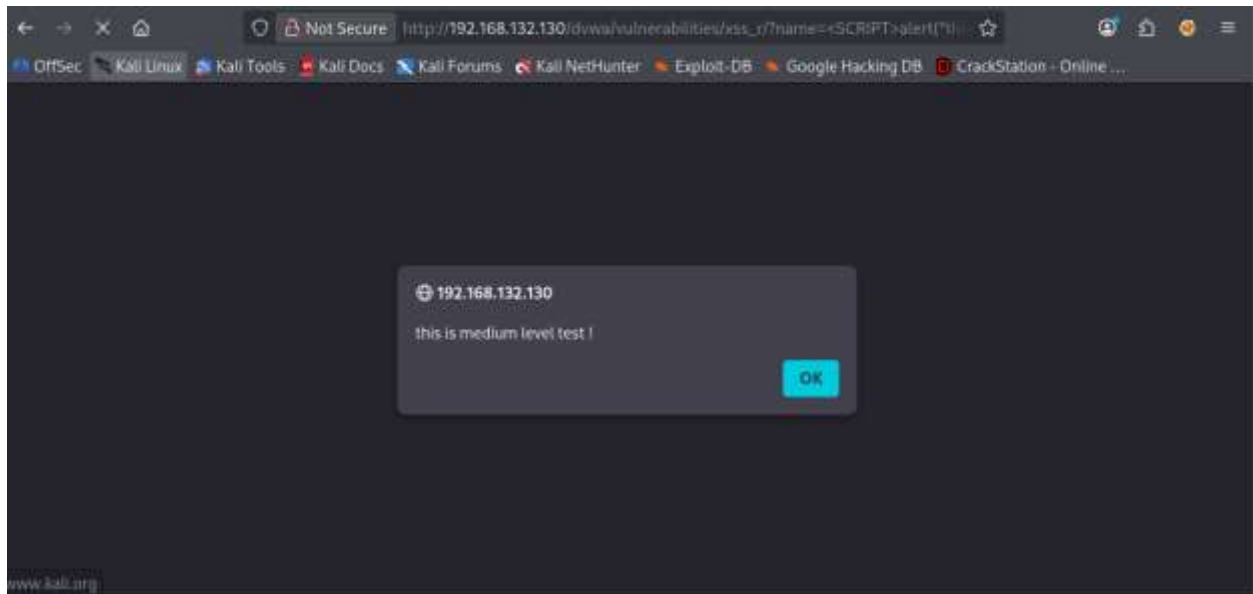


Look for backend code/ source code : (Ctrl + u)



In this code seems my `<script>` tag vanished by [`$name = str_replace('<script>', '', $_GET['name'])`]; , this piece of JavaScript code. This source code creates a filter, with `str_replace()` function, that removes the `<script>` tag in our payload and replaces it with a null value. This renders the payload script ineffective, so the attack failed, and no popup window is displayed. Because this script is only filtering out `<script>` in lower case, we can try and get around the filter by using a different tag in the payload. We will use `<ScRipt>`.

This time I use [`<SCRIPT>alert("this is medium level test !")</script>`] code and its work .This time its work because [`str_replace()`] function active or null value only when its value is exactly as [`<script>`] tag . when I use uppercase then the function can not detracted it as a tag so its work.so its also compromised by attack.



Its seems that this medium level page have vulnerability of XSS Reflected and I found it. So it's can by compromised by attacker.

High security XSS Reflected Attack

Submit security level medium to high :



Its same as previous two level. Take look how the page work and the inject malicious code for check the vulnerability.

Code: [`<script>alert("this is medium level test !")</script>`] and [`<SCRIPT>alert("this is medium level test !")</script>`] this time not working its do what its mean to be:



DVWA

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello [<SCRIPT>alert("this is medium level test !")</script>]

More info

<http://hacker.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

Lets take look its source code :



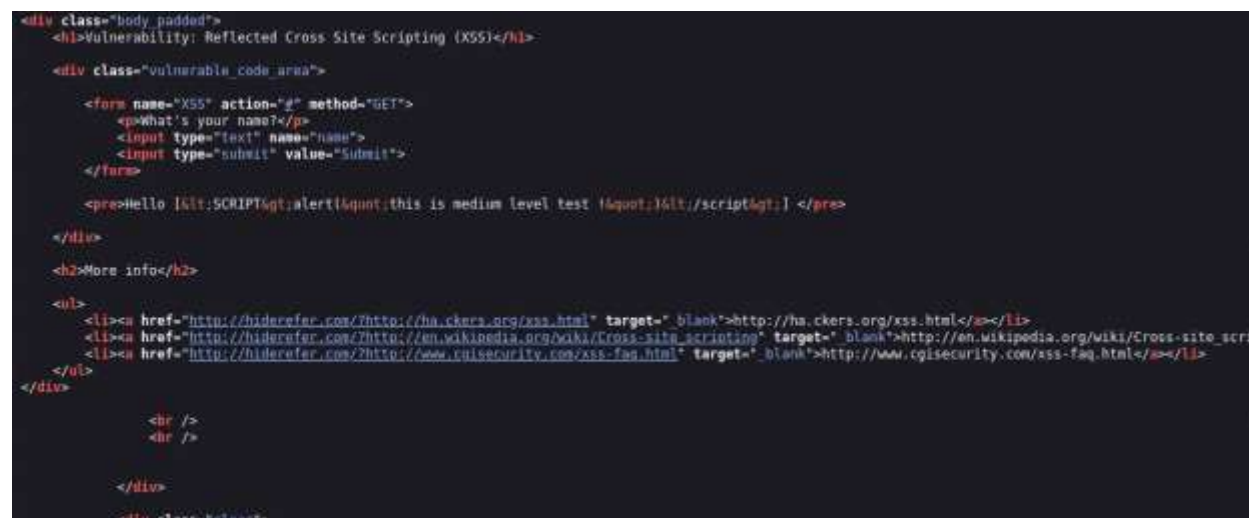
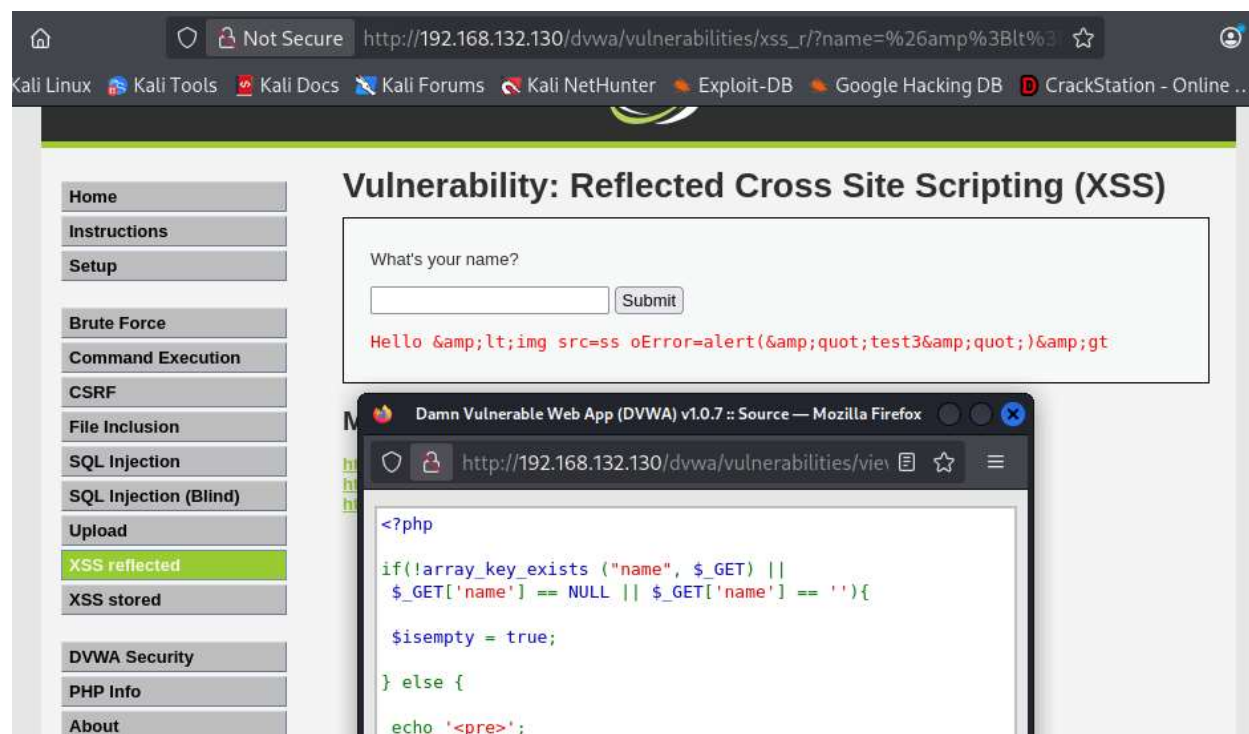
http://192.168.132.130/dvwa/vulnerabilities/view_source.php?id=xss_r&

Reflected XSS Source

```
<?php
if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL ||
$_GET['name'] == ''){
    $isempty = true;
} else {
    echo '<pre>';
    echo 'Hello ' . htmlspecialchars($_GET['name']);
    echo '</pre>';
}
?>
```

Compare

Its validation code (!array_key_exists ("name", \$_GET) || \$_GET['name'] == NULL || \$_GET['name'] == "") and (echo 'Hello ' . htmlspecialchars(\$_GET['name'])); make all the input value as a string and make all the special character like alternate. so, those Not respond like tag anymore. so malicious code didn't work as before low and medium levels.



It seems that this high level page has no vulnerability of XSS Reflected and I found it. So it's cannot be compromised by XSS attack.

-----End-----