XSS Reflected Attacks on DVWA

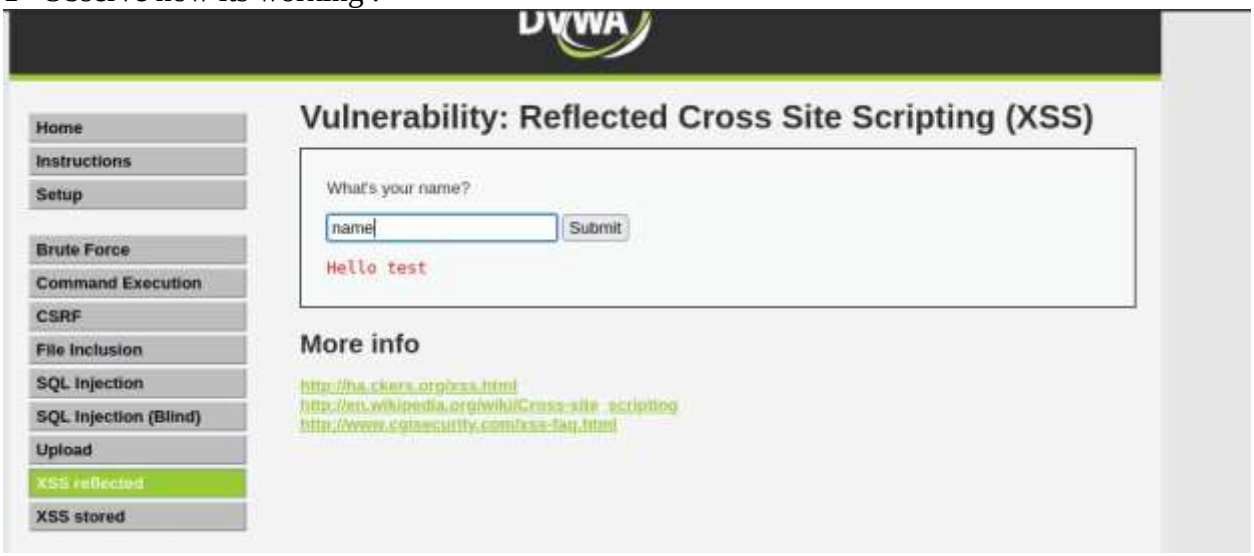
Prepared by Md Jobarul Islam

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 :

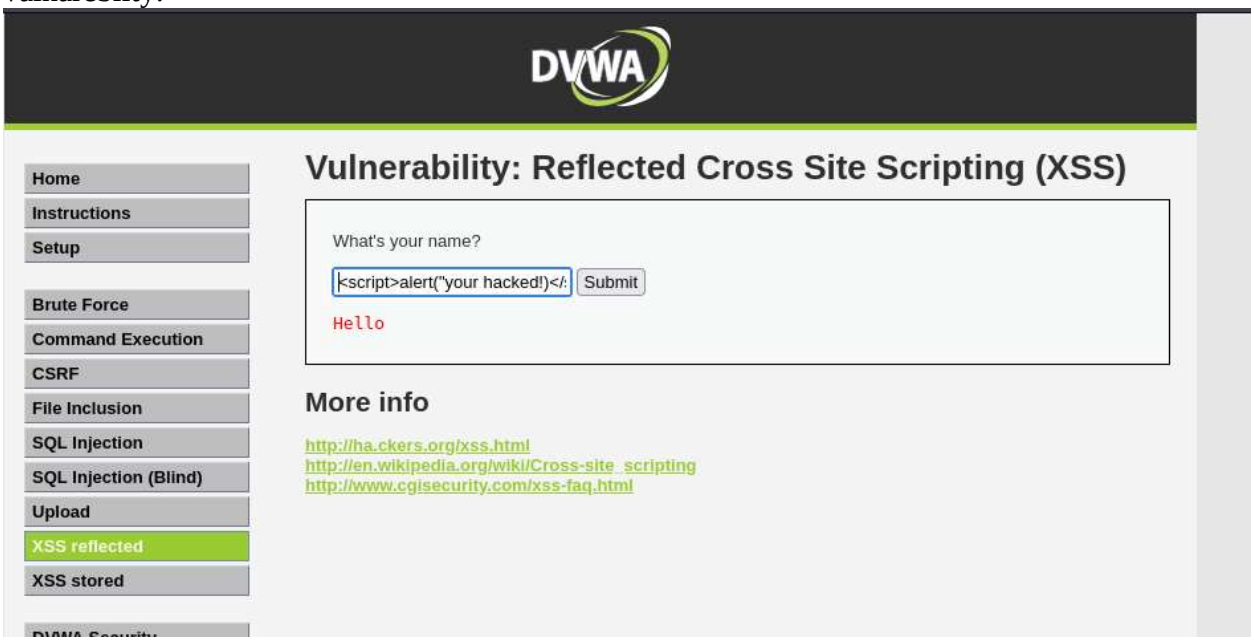
Low security XSS Reflected Attack

1st Observe how its working :

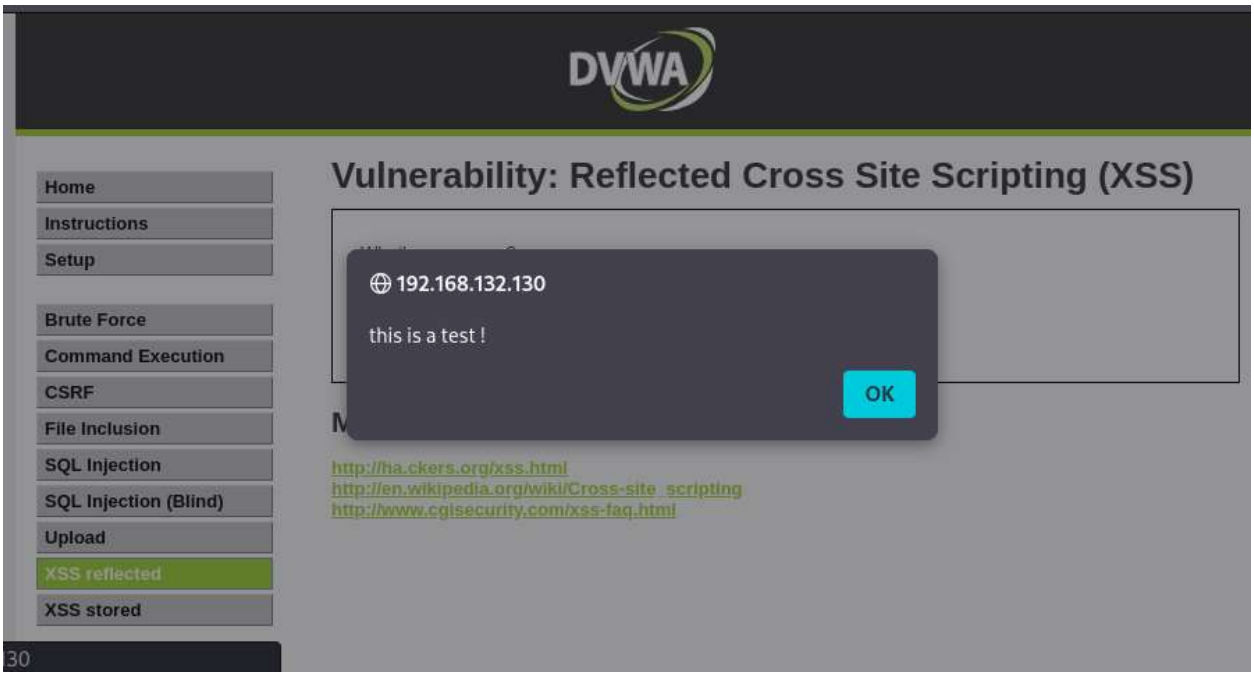


Use (Ctrl + u) for open source code:
(Ctrl + f) for search [hello reflected_text]
Back to Render window by (Ctrl + w)

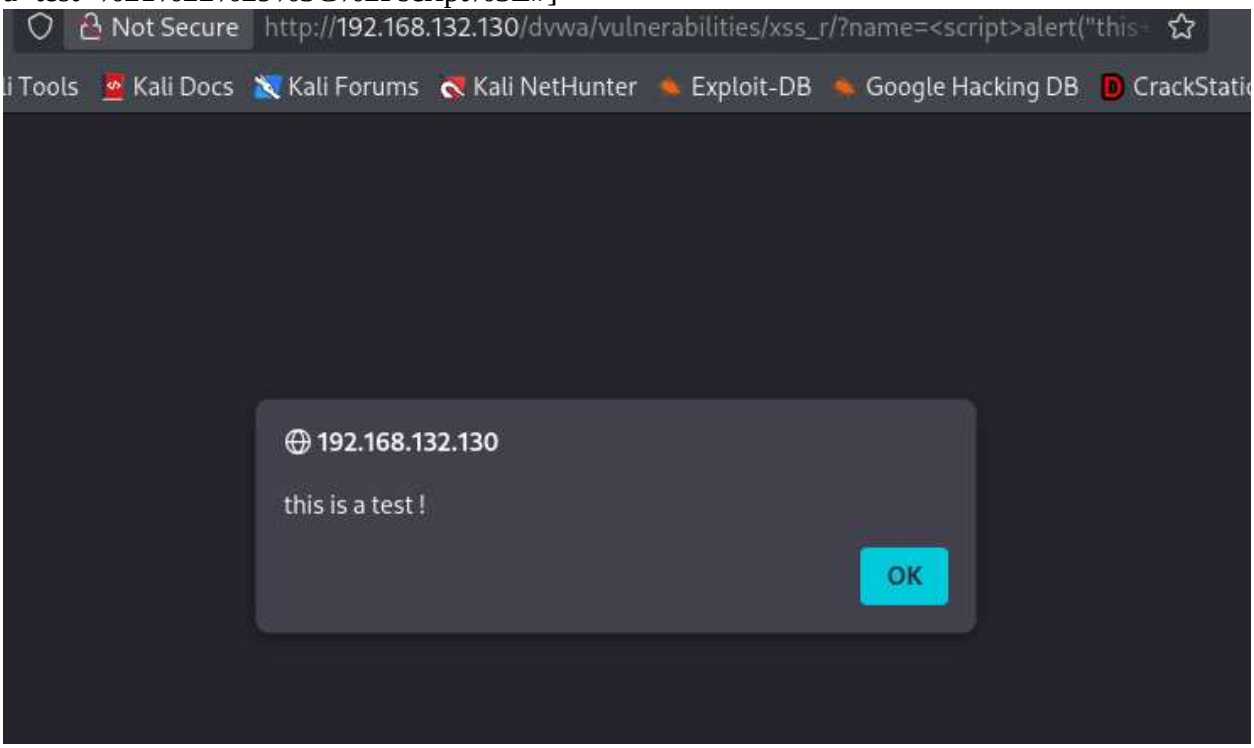
Submit [<script>alert("this is a test! ")</script>] code in input box for check for Xss valnareblity:



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#]



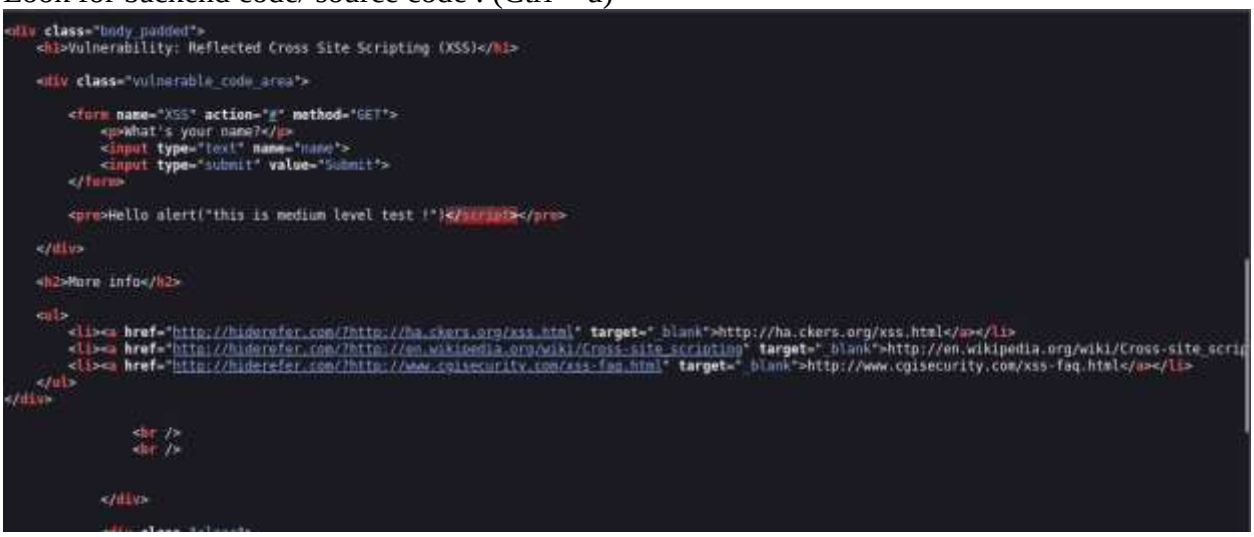
Its seems that this page have vulnerability of XSS Reflected and I found it. So it's can by compromised by attacker.

Medium security XSS Reflected Attack

Submit security level low to medium:

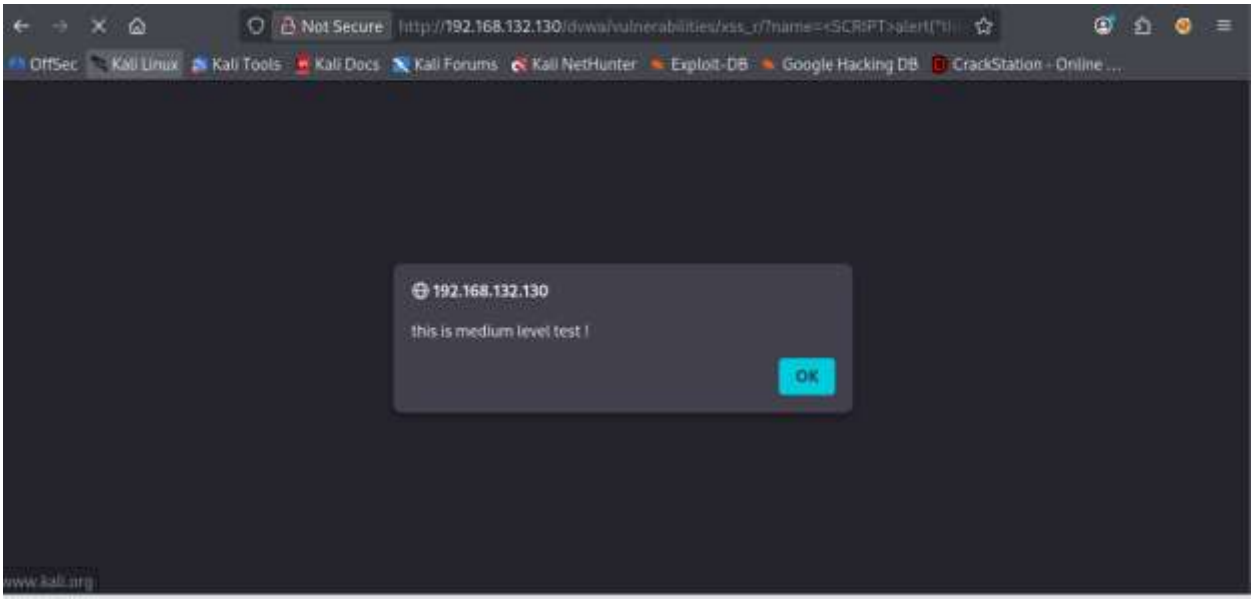
Its same as low level. Take look how the page work and the inject malicious code for check the vulnerability.
Code: [<script>alert("this is medium level test !")</script>] this time not working its do what its mean to be:

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 lavel page have vulnerability of XSS Reflected and I found it. So it's can by compromised by attacker.

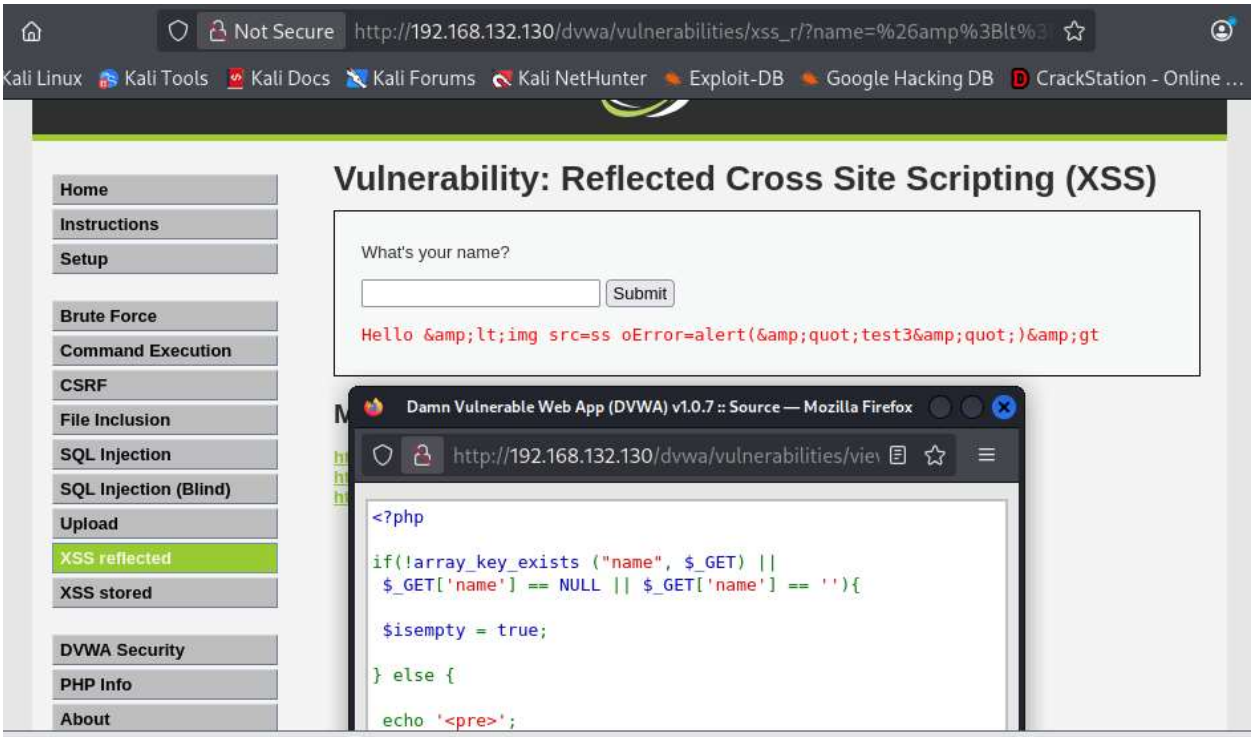
High security XSS Reflected Attack

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:

Lets take look its source code :

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



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

----------End----------