Assignment-12 SQL Injection

CYSE450-Ethical Hacking and Penetration Testing

(Total 100 Points)

In this lab, you will understand how to test a web application for SQL injection. You will learn how to execute error-based and UNION-based SQL injection using Burp Suite.

SQL injection is one of the most common web-based attack which is used to execute malicious SQL statements.
This exercise requires Metasploitabl2 VM.

Task A: [50 points] Get Familiar with SQL statements. DO NOT forget to put a semi colon (;) after each SQL query in the command line terminal.

1. Login to metasploitable2 VM
2. Login to MySQL as root [NOTE: There is no password for root in Metasploitable2. So, when it prompts for password, just hit an "Enter" Key.]
3. Execute SQL query to retrieve the database available in Metasploitable2 VM
4. Execute SQL query, **use dvwa; (**to select dvwa database.)
5. Execute SQL query to retrieve the available tables in dvwa database.
6. Execute the SQL query, SELECT * FROM **user;** (to retrieve all the rows and columns that are present in the user table. Here "*" is nothing but all.)
7. Execute query that retrieves the data where name attributes match admin'. This query retrieves all the columns associated with name 'admin'.

   SELECT * FROM table where user="admin";
8. Execute, SELECT * FROM user where user="any" or 1=1;

Here 1=1 always returns true. So, it retrieves all the rows from the database. which is not supposed to be done.

Task B: [50 Points] SQL Injection Attack from Webpage (as a front end user)

1. In a browser (in Kali Linux), type the ip address of Metasploitable 2 VM. [DO not Power off metasploitable2 VM)
2. Login to DVWA
3. Select DVWA Security tab and change the security level to "**Low**"
4. Select on the "**SQL Injection**" tab.
5. In the "User ID" box, type the query using "union" to combine multiple select statements, to fetch the database name and the username logged in to metasploitable 2 VM.

   any' union select database(),user()'

6. Once you know the name of the database, execute the query to retrieve the tables available in this database:

   any' union select table_name,1 from information_schema.tables where table_schema='dvwa'#'

7. After retrieving the table names in dvwa database, retrieve the colum names in user table using the following sql query:

   any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name="users"#'

8. Using the information retrieved for column names, retrieve/display the username and password for all the users in the users table.