Cryptography and Network Security Lab 11

Perform the SQL Injection attack on Damm Vulnerable Web Application (DVWA)

SQL injection (also known as SQL fishing) is a technique often used to attack data driven applications. This is done by including portions of SQL statements in an entry field in an attempt to get the website to pass a newly formed rogue SQL command to the database (e.g., dump the database contents to the attacker). SQL injection is a code injection technique that exploits a security vulnerability in an application's software.

The vulnerability happens when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

In this lab we will do the following:

- **Always inject SQL statements into the SQL Injection User ID field with security set to low.**
- **Obtain the username and raw-MD5 password contents from the users' table.**
- **Crack the raw-MD5 password HASH for each user.**

SQL Statements:

- Input "1" into the text box.
- Input the below text into the User ID Textbox .

%' or '0'='0

(mysql> SELECT first_name, last_name FROM users WHERE user_id ='%' or '0'='0';)

- Obtain user name and password**.**

-1' union select user,password from users#

- Input the below text into the User ID Textbox**:**

Display Database Version

Display Database Name

Resources:

- ✓ **https://www.programmersought.com/article/70775062690/**
- ✓ **https://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson6/index.html**
- ✓ **https://www.youtube.com/watch?v=GLvrieLufTA**