Academic Year: 2023-24 **Semester: V**
Class / Branch: TE IT
Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

EXPERIMENT NO. 8

Aim: To demonstrate SQL Injection using SQLMap

Theory:

SQL Injection is a code injection technique where an attacker executes malicious SQL queries that control a web application's database. With the right set of queries, a user can gain access to information stored in databases. SQLMAP tests whether a 'GET' parameter is vulnerable to SQL Injection.

SQLMap is an open source penetration test tool that automates the process of detecting and exploiting weaknesses in SQL injection and taking over the server database. So sqlmap is a tool thatcan automatically detect and exploit SQL injection bugs. by doing a SQL injection attack an attacker can take over and manipulate a database on a server.

sqlmap is able to detect and exploit different SQL injection types:

The types of attacks that sqlmap attempts are:

Boolean-based blind SQL injection
Time-based blind SQL injection
Error-based SQL injection
Union-based SQL injection
Stacked queries

Preventing SQL Injection

- User Authentication: Validating input from the user by pre-defining length, type of input, of the input field and authenticating the user.
- Restricting access privileges of users and defining how much amount of data any outsider can access from the database. Basically, users should not be granted permission to access everything in the database.
- Do not use system administrator accounts.