ASSIGNMENT-2

SQL MAP

1. Purpose and Usage of SQLMap:

Vulnerability Assessment: SQLMap helps security professionals identify SQL injection vulnerabilities in web applications by automating the process of detecting and exploiting these weaknesses in database security.

Automated Exploitation: Once a SQL injection vulnerability is identified, SQLMap can automate the exploitation process, extracting data from the database, manipulating tables, and even providing access to unauthorized users if proper security measures are not in place.

2.Installation of SQLMap:

To install SQLMap for cybersecurity purposes, you can follow these general steps:

Download SQLMap:

You can download the latest version of SQLMap from its official GitHub repository.Use git or download the ZIP file from the repository.Navigate to the SQLMap directory:

Open a terminal and move to the directory where SQLMap is downloaded.

Install dependencies:

Ensure you have Python installed. SQLMap requires Python 2.7.

Install required dependencies using:

pip install -r requirements.txt

Run SQLMap:

Execute SQLMap by running the following command:

python sqlmap.py

Now, you have SQLMap installed and ready to use for penetration testing and ethical hacking. Remember to use such tools responsibly and only on systems you have explicit permission to test.

3. Identifying a Vulnerable Web Application:

Reconnaissance: Gather information about the target, such as subdomains and technologies used.

Scanning: Use tools like Nessus or OpenVAS to perform vulnerability scans on the web application.

Enumeration: Identify exposed services, directories, and files through tools like Dirb or Gobuster.

Fingerprinting: Determine the web server, framework, and CMS versions to find known vulnerabilities. 4. Performing a Basic SQL Injection Attack:

SQL injection is a code injection technique that might destroy your database.

SQL injection is one of the most common web hacking techniques.

SQL injection is the placement of malicious code in SQL statements, via web page input.

5.Documenting the Steps:

Introduction:

Briefly explain the purpose of SQL mapping.

Mention the importance of identifying and fixing SQL injection vulnerabilities.

Setup:

Provide details on the environment setup (e.g., target URL, database type).

Specify tools used (e.g., SQLmap).

Target Analysis:

Identify the target website or application.

Explore the input fields susceptible to SQL injection.