Assignment-SQLMAP

Step -1 Purpose and Usage of SQLMap:

- SQLMap is a tool used for detecting and exploiting SQL injection vulnerabilities in web applications.
- It automates the process of identifying and exploiting SQL injection flaws, making it easier for penetration testers to assess the security of web applications.

Step -2 Installation of SQLMap:

- SQLMap is written in Python and can be easily installed on most operating systems.
- You can install SQLMap by cloning its GitHub repository or by using package managers like apt (for Debian-based systems) or yum (for Red Hat-based systems).
- For example, on Debian-based systems, you can install SQLMap using the following command:

  sudo apt-get install sqlmap

Step -3 Identifying a Vulnerable Web Application:

- You can use intentionally vulnerable web applications like DVWA (Damn Vulnerable Web Application) or WebGoat for practicing SQL injection attacks.
- Install and set up DVWA on your local machine or use online platforms like OWASP Juice Shop.

Step -4 Performing a Basic SQL Injection Attack:

- Use SQLMap to perform a basic SQL injection attack against the chosen target.
- Example command:

  sqlmap -u "http://target.com/page.php?id=1" --dbs
- This command will identify the databases present in the target application by exploiting the SQL injection vulnerability.

Step -5 Documenting the Steps:

- Document the commands you used, the responses you received, and any observations you made during the attack.
- Describe the potential impact of SQL injection vulnerabilities and suggest mitigation strategies.