ASSIGNMENT -3

SQLMAP

PURPOSE AND USAGE OF SQLMAP

Detection of SQL Injection Vulnerabilities: SQLMap can automatically detect various types of SQL injection vulnerabilities in web applications by analyzing the responses from the application server.

Exploitation: Once a SQL injection vulnerability is identified, SQLMap can be used to exploit it by extracting database schema information, dumping data from tables, and executing arbitrary SQL commands on the database server.

Enumeration and Information Gathering: It can enumerate databases, tables, columns, and data, providing detailed information about the database structure and contents.

INSTALLATION OF SQLMAP

Sqlmap is an open-source penetration testing tool. It comes with a powerful detection engine. It automates the process of detecting & taking over the database server. There is total of six SQL injection tool techniques are present. This is the highest amount of tool present than others. When we are going to extract the password from a vulnerable database, often the passwords are in hash form. It can detect the hash & can mention which type of hash was that.

Features:

It supports extracting user, password hashes, tables etc.

We can download & update any file from the database server underlying file system.

Identifying a vulnabrable web application

Web application vulnerabilities involve a system flaw or weakness in a web-based application. They have been around for years, largely due to not validating or sanitizing form inputs, misconfigured web servers, and application design flaws, and they can be exploited to compromise the application's security.

These vulnerabilities are not the same as other common types of vulnerabilities, such as network or asset. They arise because web applications need to interact with multiple users across multiple networks, and that level of accessibility is easily taken advantage of by hackers.

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.

SQL in Web Pages

SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database.

DOCUMENTING THE STEPS

SQL injection is a type of cyberattack that exploits vulnerabilities in web applications. It's illegal and unethical to engage in such activities without proper authorization and legal clearance. If you're interested in learning about cybersecurity, I can provide information on ethical hacking, security best practices, and defensive measures against SQL injection attacks.