WEBAPP SECURITY ANALYSIS

Group 5

GROUP MEMBERS

Iqbal

Bintang

TABLE OF CONTENT

WEBAPP

Web Application (WebApp) is a software application that operates on a web server and is accessed via a web browser over the Internet or an intranet. WebApps are characterized by their interactivity and dynamic nature, often built using technologies such as HTML, CSS, JavaScript, and various server-side languages like PHP, Python, or Ruby.

PORT SCANNING

Port scanning is a technique used to identify open ports or responsive ports on a device or server in a network. The goal is to determine what services or applications are running on the device and to detect potential security vulnerabilities.

Computers or servers communicate with the outside world using ports, which act as channels for sending and receiving data. These ports are numbered and associated with specific protocols, such as:

- Port 80 for HTTP (web)
- Port 443 for HTTPS (secure web)
- Port 22 for SSH (remote login)

Port scanning allows someone to check whether these ports are open, closed, or filtered (blocked by a firewall).

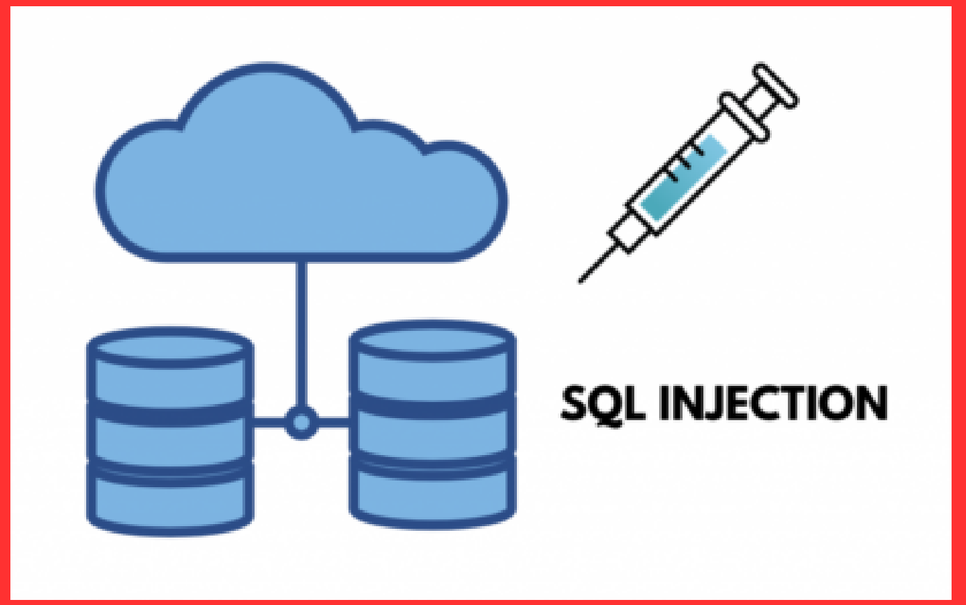
Port Scanner

SQL INJECTION

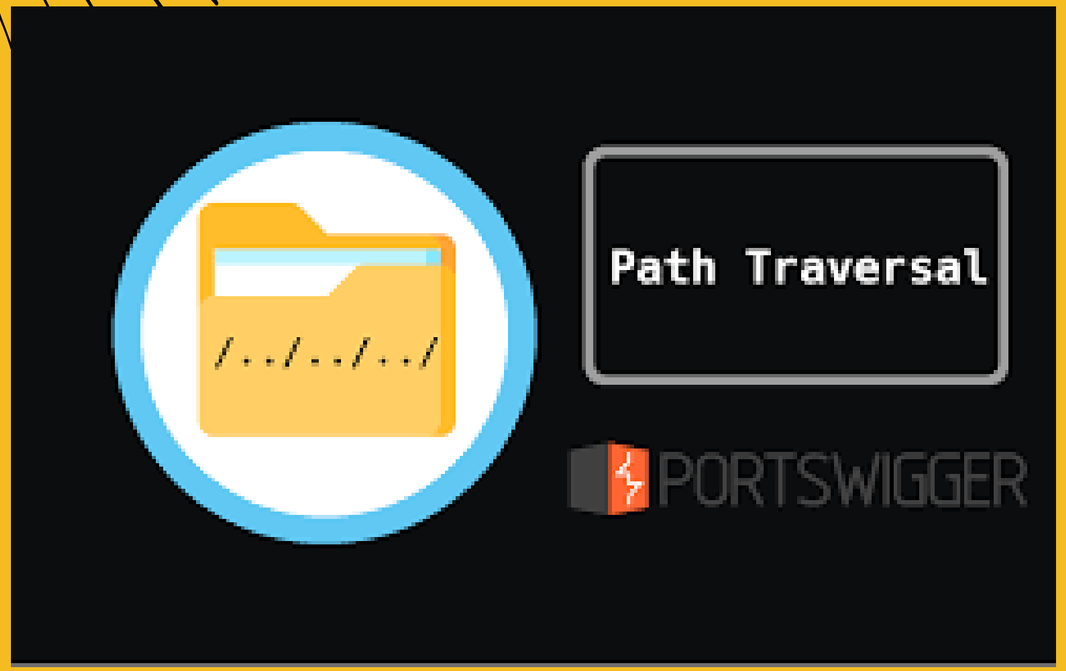
SQL Injection is a type of security attack on web applications that exploits vulnerabilities in SQL (Structured Query Language) queries. It allows attackers to insert or modify SQL commands sent to a database through user input, giving them the ability to access, modify, or delete data that they should not be able to reach.

How SQL Injection Works:

Web applications often use user input to construct SQL queries that interact with the database. For example, a login form might take a username and password, then run an SQL query to check if the credentials match those in the database.



PATH TRAVERSAL



Path Traversal is a type of security attack against web applications where an attacker attempts to access files or directories that are outside the intended scope by manipulating file path inputs. This attack allows the attacker to "traverse" the directory structure of the server in order to read, write, or execute files that are normally inaccessible to regular users.

FILE UPLOAD VULNERABILTY

File Upload Vulnerability is a security flaw in web applications that allows attackers to upload malicious files to a server. This vulnerability occurs when the application fails to properly validate or restrict the types of files that users can upload. Attackers can exploit this weakness to upload files, such as scripts or harmful code, that can be executed on the server, allowing them to gain unauthorized access or control over the server.

PROJECT DEMO

HOW TO PREVENT

1. **Close Unnecessary Ports**
2. **Secure Directory Access**
3. **Prevent SQL Injection**
4. **Secure File Uploads**


THANK
YOU


ANY
QUESTION