Practical 7

SQL Injection (Manual & SQLmap)

* Theory

• Purpose :-

-> SQL Injection (SQLi) is a web security vulnerability that allows attackes to manipulate backend databases by injecting malicious SQL queries.

• How it Works :-

-> SQLi occurs when a web application does not properly sanitize user input, allowing attackers to execute arbitrary SQL commands.

• Types of SQL Injection :-

-> Boolean-based : `SELECT * FROM users WHERE id = 1' OR '1' = '1`

-> Union-based : `SELECT username, password FROM users WHERE id = 1 UNION SELECT null, null -`

-> SQLmap Usage : `sqlmap -u "http://example.com/login.php?id=1" --dbs`

* Practical

To check if a Website is vulnerable

- sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1 --dbs