LAB ASSIGNMENT-20

TASK-1:

Prompt:

Generate a Python script that connects to a database or API.

Code and Output:

Detection of Hardcoded Credentials:

Yes — the code **does contain hardcoded credentials**:

- user="your_username"
- password="your_password"

Even though they're placeholders, **this pattern is insecure** if used in production or shared code, because it exposes sensitive information directly in the script.

Prompt:

Modify the code to securely load credentials from environment variables.

Code and Output:

TASK-2:

Prompt:

Generate a simple login system in Python (with SQLite or MySQL).

Code and Output:

Prompt:

Rewrite the code using parameterized queries to prevent injection.

Code and Output:

TASK-3:

Prompt:

Generate a Python script that reads and writes files based on user input.

Code and Output:

Vulnerability

- If a user inputs ../../etc/passwd as filename, the script will **read/write files outside the intended directory**.
- This is a **path traversal attack**.

Prompt:

Fix the vulnerability by validating file paths or restricting access to safe directories.

Code and Output:

TASK-4:

Prompt:

Generate a calculator program that evaluates user input.

Code and Output:

Prompt:

Replace it with a safe parser (e.g., ast.literal_eval() in Python)

Code and Output:

TASK-5:

TASK-3:

Prompt:

Generate a web server script (Flask or Node.js)

Code and Output:

Prompt:

Fix the vulnerabilities and re-run the tool until no issues remain.

Code and Output: