PROJECT REPORT

Secure Coding Password Manager (Python GUI)

Intern Name: Nikita Vaishnav
Project Type: Secure Coding Review & Implementation
Technology Used: Python, Tkinter, bcrypt

1. Objective

The objective of this internship project is to design and implement a secure GUI-based password manager by applying secure coding principles. The project focuses on preventing common security vulnerabilities such as plaintext password storage, unauthorized access, and sensitive data exposure.

2. Project Description

This project is a Python GUI-based Secure Password Manager that provides secure user registration, login, and password storage functionality. The application enforces authentication before access and ensures that sensitive data is handled using secure coding techniques.

3. Secure Coding Practices Implemented

- Password hashing using bcrypt instead of plaintext storage
- Input validation to prevent invalid or malicious input
- Authentication-based access control
- Masked password display to avoid data exposure
- No hardcoded credentials or sensitive information
- Controlled GUI-based access to sensitive functionality

4. Secure Coding Review Summary

During the secure coding review, potential vulnerabilities such as plaintext password storage and unauthorized access were identified. These issues were mitigated by applying hashing techniques, input validation, and authentication mechanisms.

5. Tools & Technologies

- Python 3 Programming Language
- Tkinter for GUI development
- bcrypt library for secure password hashing
- Manual secure code inspection

6. Conclusion

This internship project successfully demonstrates the application of secure coding practices in a real-world GUI-based application. By following secure coding standards, the project minimizes common security risks and ensures safe handling of sensitive user data.