Secure Coding Review Project Summary

This project is part of the CodeAlpha Cyber Security Internship. The goal of this task was to conduct a Secure Coding Review of a simple login script written in Python.

Objective:

To identify security vulnerabilities in the code and apply best practices to enhance its security.

Original (Insecure) Code Issues:

1. Hardcoded credentials (admin/admin123)
2. Plain text password comparison
3. No input validation or sanitization

Security Risks:

- Easy for attackers to guess hardcoded passwords
- Exposes system to unauthorized access
- No protection against brute force or input abuse

Improvements Made:

- Used bcrypt for password hashing and verification
- Replaced hardcoded passwords with securely hashed equivalents
- Input is securely handled and verified

Improved Code Summary:

- The new version uses the bcrypt library to hash passwords and check them securely.
- This improves protection against password theft and unauthorized access.

Conclusion:

Secure coding practices are essential to build applications that resist cyber threats. Even a simple script can pose major risks if written without security in mind.