Secure Coding Review

CodeAlpha Cyber Security Internship – Task 3

This document provides a professional review of a Python login system, identifying vulnerabilities and suggesting remediation steps to improve security.

1. Project Overview

- Audited a Python login system for security vulnerabilities.
- Applied fixes to make the system safer and more secure.

2. Original Code Vulnerabilities

- Hardcoded passwords (easy for attackers to find).
- Passwords stored in plain text (not secure).
- No input validation (risk of injection in expanded systems).

3. Remediation Steps / Secure Code

- Implemented password hashing using SHA-256.
- Removed plain-text passwords from code.
- Prepared the code for additional input validation and security checks.

4. Best Practices for Secure Coding

- Never store passwords in plain text; always hash them.
- Validate all user input before processing.
- Use secure libraries and follow up-to-date security guidelines.
- Document vulnerabilities and fixes for compliance.

5. Files Included

- `login_system.py` – Original code with vulnerabilities.
- `secure_login_system.py` – Fixed and secure code.
- `CodeAlpha_Task3_Secure_Coding_Review_Report.pdf` – This document.

Conclusion

- The secure version mitigates critical risks and is ready for safe usage.
- Continuous security reviews are essential to maintain a secure application.

Prepared by: Muhammad Asad Ullah | GitHub: https://github.com/AsadUllah-170