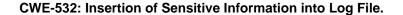
Suggestions for CWE-532:



- **Resolution:**
- * Avoid logging sensitive information directly.
- * Use secure logging practices such as masking or encrypting sensitive data before logging.
- * Implement access controls to limit who can view log files.
- * Regularly review and audit log files for sensitive information.

Suggestions for CWE-276:

- **CWE-276: Incorrect Default Permissions**
- **Description:** Ensure that files and directories have appropriate permissions set by default, preventing unauthorized access or accidental changes.
- **Resolution:**
- 1. **Verify Permissions:** Check and set correct permissions (e.g., `chmod 755` for directories) during installation or deployment.
- 2. **Use Default Settings:** Ensure platform-specific defaults are secure.
- 3. **Automate Permissions:** Implement scripts or configuration management tools to enforce correct permissions.
- 4. **Review Policies:** Regularly audit and update permission policies.

By following these steps, you can mitigate the risk associated with CWE-276, enhancing the security of your application.