JAVA CODE QUALITY ASSIGNMENT

Secure coding standards are rules and guidelines used to prevent security vulnerabilities. Used effectively, these security standards prevent, detect, and eliminate errors that could compromise software security.

Secure Coding standards:

1.CWE:

- CWE stands for Common Weakness Enumeration. It identifies weakness in both software and hardware.
- It is a set of software weakness which can be found in any source codes so that it can be rectified. CWE is a community developed dictionary of weakness types. National Cyber Security of US is directly involved.
- Using CWE causes of security vulnerabilities were found and hence development become easier.
- J2EE environmental issues, path traversal, problems with Unix, Windows, MAC virtual file problems, improper Neutralizations were some of the weakness mentioned in CWE. It has over 1000 weakness where each and every weakness were explained clearly with its description.
- The list is regularly updated for every few months. It has over 600 categories of weakness.

2. OWASP Top 10:

- OWASP stands for **Open Web Application Security Project.**
- It is the documentation for developers to use to ensure that the web application is with minimal security vulnerability.
- Any organization can follow these standard to make the application more secure by reducing the security flaws.
- As the name suggests OWASP top 10 contains the top 10 security risks to be taken into consideration.
- The top 10 security risks are injection, Broken authentication, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting (XSS), Insecure

Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging & Monitoring.

3. CERT :

- CERT Is the secure coding standard that supports commonly used languages such as java, c, c++.
- The aim of the secure coding standard is to not only detect security risks with rules but also provide suggestions that can improve code quality with recommendations.
- By following the CERT, the entire program can be secured and protected from potential vulnerability.
- CERT is recommending that the code can be secured if SAST tool like Klocwok is used. These tool finds and eliminates the vulnerability in the development.
- CERT risk assessments like Severity, Likelihood, and Remediation Cost were used and based on the assessment result the degree of which the program is violating the rules can be found.

4.SANS 25:

- SANS 25 is the list of most dangerous errors that can lead to serious vulnerabilities in software. These 25 errors are easy to find and rectify it.
- Even though they are simple errors they are extremely dangerous as it can allow the attackers to take up the entire software. Attackers can also take the control and stop the application from working properly.
- Organizations like SANS institute, MITRE and many companies made this list. Over 20 organizations provided the input and they are analyzed based on likelihood, importance and so on, finally the list of top 25 was created.
- These 25 were categorized as three parts like Insecure Interaction Between Components, Risky Resource Management, Porous Defenses.
- Guidance and the complete information about 25 risks were provided in document for the users. Detail description of each and every error were also given.