OWASP
Secure Coding Practices - Quick Reference Guide

A quick overview

The Secure Coding Practices Quick Reference Guide is a technology agnostic set of general software security coding practices, in a comprehensive checklist format, that can be integrated into the development lifecycle. At only 17 pages long, it is easy to read and digest.

The focus is on secure coding requirements, rather then on vulnerabilities and exploits. It is designed to serve as a quick reference or review for the developers, as opposed to being a tool for the security community.

It includes a brief overview of security and risk principles, a glossary of important application security related terminology and links to useful resources.

The guide does not cover implementation of an entire secure software development lifecycle, but instead targets just the coding practices that enable secure development. The primary focus is on web applications and their supporting infrastructure, but most of the guidance can be applied to any software deployment platform.

Key areas covered in the guide include:

- Input Validation
- Output Encoding
- Authentication and Password Management
- Session Management
- Access Control
- Cryptographic Practices
- Error Handling and Logging
- Data Protection
- Communication Security
- System Configuration
- Database Security
- File Management
- Memory Management
- General Coding Practices

I think you will find this guide can be extremely useful defining general security requirements for a software project. It may also be helpful as a resource when developing an organization's secure coding standards or when defining secure coding requirements in contracts for outsources software development.

Place : mumbai

Date : 22-112-2023