OWASP

Open Web Application Security Project

What is OWASP

- A non-profit organization dedicated to providing unbiased practical information about application security.
    - Meeting OWASP Compliance Standards is the First Step Toward Secure Code.

OWASP Top 10 Application Security Risks

- The OWASP top 10 is a list of flaws so prevalent and severe that no web application should be delivered to customers without some evidence that the software does not contain these errors.
    - Although the Veracode Platform detects hundreds of software security flaws, OWASP provides razor focus on problems that are worth fixing.

OWASP Projects

- It is one of many projects managed by the OWASP Foundation, which provides these resources as part of OWASP:
    - Articles
    - Documentation
    - Methodologies
    - Tools
    - Technologies

OWASP Community

- The community has a goal to generate open, workable standards for individual web-based technologies. OWASP projects are essentially a collection of correlated tasks with a well-defined roadmap and members. Organizations can use the provided information to practice more secure development practices.

OWASP

Open Web Application Security Project

OWASP Secure Coding and Vulnerability Detection

- OWASP secure coding focuses on the early detection of vulnerabilities within a program. The community defines security vulnerabilities as a hole or weakness within program code that is a direct result of a design flaw or implementation bug. These weaknesses make it possible for an attacker to harm software users, owners, or additional entities relying on the application. OWASP lists various types of vulnerability categories on their website, including:
    - Authentication
    - Availability
    - Code Quality
    - Error Handling
    - General Logic Errors
    - Input Validation
    - Protocol Errors

Comply With OWASP Secure Coding Through Static and Architectural Analysis

- Static Application Security Testing (SAST) and architectural analysis software such as CAST Application Intelligence Platform (AIP) helps organizations build security into their software by integrating security vulnerability feedback at the development stage. CAST AIP analytical capability is not available through open source code quality checkers or utilities provided as part of the developer environment. Deep understanding of systems security is only possible when analysis techniques such as Data Flow Analysis, Architecture Analysis, Transaction Risk, and Propagation Risk Analysis are employed to identify vulnerabilities.
    - Some key highlights of CAST AIP Secure Programming capabilities include:
        - Design flaws account for 50% of security problems and cannot be found by code review, or open source code quality tools. CAST AIP's holistic, system-level analysis is required to understand architectural risks that pose security threats and vulnerabilities.
        - Security training and guidance to development teams improves application security. CAST supports continuous improvement through automated feedback and training based on 300+ security best practices
            - CAST's insight includes benchmarking scores for consistent monitoring and offers the opportunity to improve these areas: Risk, Technical Debt, Complexity, Efficiency, Stability, and Resilience.
            - **APPLICATION SECURITY CANNOT BE AN AFTERTHOUGHT**