CWE (Common Weakness Enumeration) e **WASC (Web Application Security Consortium)** são duas classificações amplamente utilizadas no campo da segurança da informação para categorizar e descrever vulnerabilidades de segurança. Aqui está um detalhamento de cada um:

CWE (Common Weakness Enumeration)

Definição:
CWE é uma lista de fraquezas de software mantida pela MITRE Corporation. Ela fornece uma linguagem comum para identificar, descrever e categorizar vulnerabilidades de segurança em software.

Objetivos:
- **Facilitar a comunicação:** Proporciona uma terminologia comum para profissionais de segurança e desenvolvedores discutirem e documentarem vulnerabilidades.
- **Educação e Treinamento:** Auxilia no ensino e na compreensão das vulnerabilidades de software.
- **Ferramentas de Segurança:** Facilita a integração de ferramentas de segurança, como scanners de vulnerabilidades e ferramentas de análise de código.

Estrutura:
- Cada entrada CWE descreve uma fraqueza específica, como "SQL Injection" (CWE-89) ou "Buffer Overflow" (CWE-120).
- As fraquezas são categorizadas hierarquicamente para permitir uma navegação mais fácil.

Exemplo de Entradas CWE:
- **CWE-79:** Cross-Site Scripting (XSS)
- **CWE-89:** SQL Injection
- **CWE-20:** Improper Input Validation

WASC (Web Application Security Consortium)

Definição:
WASC é uma organização que criou a "WASC Threat Classification", uma lista de categorias de ameaças e vulnerabilidades específicas para aplicações web.

Objetivos:
- **Estabelecer um padrão:** Proporciona uma classificação padrão para vulnerabilidades de aplicações web.
- **Aprimorar a segurança web:** Facilita a compreensão e a mitigação de vulnerabilidades específicas da web.
- **Orientação:** Fornece informações detalhadas e orientações sobre como prevenir e mitigar essas ameaças.

Estrutura:
- A classificação WASC agrupa vulnerabilidades em categorias gerais.
- Cada categoria descreve um tipo de ameaça ou vulnerabilidade, seus impactos potenciais, e métodos de mitigação.

Exemplo de Categorias WASC:
- **WASC-01:** SQL Injection
- **WASC-10:** Cross-Site Scripting (XSS)
- **WASC-33:** Path Traversal

Diferenças e Complementaridade

Escopo:
- **CWE:** Abrange uma ampla gama de fraquezas de software, não se limitando apenas a vulnerabilidades web.
- **WASC:** Foca especificamente em vulnerabilidades e ameaças relacionadas a aplicações web.

Detalhamento:
- **CWE:** Fornece descrições detalhadas e técnicas das fraquezas, incluindo exemplos, métodos de exploração, e técnicas de mitigação.
- **WASC:** Oferece uma visão mais generalizada das vulnerabilidades web, adequada para uma compreensão mais ampla das ameaças.

Utilização

CWE é frequentemente usado por:
- Desenvolvedores de software para identificar e corrigir fraquezas no código.
- Ferramentas de análise de código e scanners de vulnerabilidades para relatar fraquezas.

WASC é frequentemente usado por:
- Profissionais de segurança web para categorizar e entender ameaças web específicas.
- Consultores de segurança para educar sobre as principais ameaças às aplicações web.

Exemplos de Utilização em Ferramentas de Segurança

OWASP ZAP e outras ferramentas de segurança:
- Utilizam ambas as classificações para relatar vulnerabilidades detectadas.
- **Relatórios de vulnerabilidades:** Muitas ferramentas mapeiam suas descobertas para as categorias CWE e WASC para facilitar a compreensão e a ação corretiva.

Conclusão

CWE e WASC são ferramentas importantes na segurança da informação, cada uma com seu foco específico. CWE é uma classificação abrangente de fraquezas de software, enquanto WASC se concentra em vulnerabilidades de aplicações web. Ambas são utilizadas para melhorar a comunicação, a educação e a mitigação de vulnerabilidades no desenvolvimento de software e segurança web.