OWASP (Open Web Application Security Project)

OWASP je otevřená komunita, která funguje jako hlavní zdroj informací o kybernetické bezpečnosti pro vývojáře a provozovatele webů. Jejím cílem je činit bezpečnost softwaru „viditelnou“, aby lidé a organizace mohli činit informovaná rozhodnutí o rizicích. Veškeré jejich výstupy (metodiky, dokumentace, nástroje) jsou k dispozici zdarma pod otevřenou licencí.

Projekt OWASP Top 10

Nejznámějším a nejdůležitějším projektem této nadace je **OWASP Top 10**. Jde o pravidelně aktualizovaný seznam deseti nejkritičtějších bezpečnostních rizik pro webové aplikace.

Slouží jako základní standard pro testování bezpečnosti. Pokud aplikace splňuje ochranu proti těmto deseti bodům, považuje se za solidně zabezpečenou.

Příklady kategorií z aktuálního seznamu:

```
1. **Broken Access Control:** Uživatel se dostane k datům, ke kterým by neměl mít přístup.
2. **Cryptographic Failures:** Špatné šifrování nebo ochrana citlivých dat (např. hesel).
3. **Injection:** Zahrnuje [[sql_injection|SQL Injection]] a [[command_injection|Command Injection]].
4. **Insecure Design:** Chyby vzniklé již ve fázi návrhu aplikace.
```

Další významné projekty

Kromě seznamu Top 10 spravuje OWASP stovky dalších užitečných projektů:

- **OWASP ZAP (Zed Attack Proxy):** Jeden z nejoblíbenějších open-source nástrojů pro automatizované hledání zranitelností ve webových aplikacích.
- **OWASP ASVS (Application Security Verification Standard):** Podrobný rámec pro testování úrovně bezpečnosti (vhodný pro certifikace).
- **OWASP SAMM (Software Assurance Maturity Model):** Model pro firmy, jak postupně zlepšovat své procesy vývoje softwaru z hlediska bezpečnosti.
- **OWASP Core Rule Set (CRS):** Sada pravidel pro firewally jako ModSecurity.

Proč je OWASP důležitý?

- **Standardizace:** Poskytuje jednotný jazyk pro vývojáře a auditory (všichni vědí, co se myslí pod pojmem „OWASP Top 1“).
- **Vzdělávání:** Nabízí návody, jak se útokům bránit, nejen jak je najít.
- **Komunita:** Po celém světě existují lokální „chapters“ (pobočky), kde se odborníci setkávají a sdílejí zkušenosti.

Srovnání: OWASP Top 10 vs. ASVS

Metodika	Účel	Pro koho
OWASP Top 10	Seznam nejčastějších rizik.	Vývojáři a manažeři (povědomí).
ASVS	Komplexní kontrolní seznam (checklist).	Bezpečnostní auditoři a testeři.

Související pojmy: SQL Injection, ModSecurity, WAF, Kybernetická bezpečnost, Šifrování, Penetrační testování.