

Die 10 OWASP-Regeln für die Sicherheit von Webanwendungen

OWASP ist die internationale Organisation, die Ressourcen und Materialien zur Verbesserung der Websoftware-Sicherheit erstellt. Die Top 10 hilft Entwicklern, IT-Fachleuten und Führungskräften, die wichtigsten Bedrohungen zu erkennen.

OWASP Top 10 2013

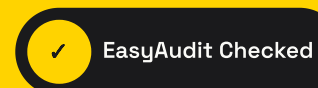
- Injection: etwa SQL Injection, wenn ungefilterte Queries Daten verändern oder stehlen können.
- Broken Authentication and Session Management: fehlerhafte Verwaltung von Zugangsdaten, Token und Cookies.
- Cross Site Scripting (XSS): gefährliche Skripte werden an den Browser des Nutzers gesendet.
- Insecure Direct Object Reference: direkte Referenzen ohne Kontrollen öffnen unbefugten Zugriff.
- Security Misconfiguration: Server und Software sind nicht korrekt konfiguriert oder aktualisiert.
- Sensitive Data Exposure: sensible Nutzerdaten werden nicht angemessen geschützt.
- Missing Function Level Access Control: Funktionen sind ohne korrekte Berechtigungsprüfung erreichbar.
- Cross Site Request Forgery: Nutzer werden zu ungewollten Aktionen gezwungen.
- Components with Known Vulnerabilities: verwundbare Komponenten werden weiterverwendet.
- Unvalidated Redirects and Forwards: Nutzer werden auf gefährliche Seiten umgeleitet.

Eine professionelle Prüfung zeigt, ob Website, Portal oder Anwendung von diesen Problemen betroffen sind.

Möchten Sie wissen, ob Ihr Unternehmen wirklich geschützt ist?

EasyAudit prüft Anwendungen, Infrastrukturen und E-Commerce-Plattformen mit einem klaren, konkreten Audit, das technische Risiken in einfache Entscheidungen übersetzt.

Audit auf easyaudit.de anfordern



Das sichtbare Zeichen eines ernsthaften Engagements für Sicherheit.