EasyAudit™
KNOW THE RISK

WHITE PAPER EASYAUDIT

Le 10 regole di OWASP per la sicurezza delle applicazioni Web

OWASP è l'ente internazionale che produce risorse e materiali per migliorare la sicurezza del software web. La Top 10 aiuta sviluppatori, professionisti IT e dirigenti a riconoscere le principali minacce per le applicazioni.

OWASP Top 10

- Injection: input non controllati possono eseguire comandi o query arbitrarie.
- Broken Authentication: sessioni, credenziali e cookie gestiti male espongono gli account.
- Cross Site Scripting (XSS): script malevoli rubano credenziali o forzano azioni.
- Insecure Direct Object Reference: riferimenti diretti aprono accessi non previsti.
- Security Misconfiguration: server e applicazioni non configurati bene creano varchi.
- Sensitive Data Exposure: dati non protetti espongono clienti e azienda.
- Missing Function Level Access Control: ogni funzione deve verificare i permessi.
- Cross Site Request Forgery: l'utente autenticato viene indotto ad azioni non volute.
- Components with Known Vulnerabilities: librerie vulnerabili compromettono l'applicazione.
- Unvalidated Redirects and Forwards: redirect non controllati portano a malware o phishing.

EasyAudit WEB segue la metodologia OWASP per verificare portali, aree riservate, siti web e applicazioni, restituendo un report chiaro e azionabile.