EasyAudit™
KNOW THE RISK

EASYAUDIT WHITE PAPER

OWASP's 10 Rules for Web Application Security

OWASP is the international organization that produces resources and materials to improve web software security. The Top 10 helps developers, IT professionals and managers recognize the main threats to applications.

OWASP Top 10

- Injection: unchecked input can execute arbitrary commands or queries.
- Broken Authentication: badly managed sessions, credentials and cookies expose accounts.
- Cross Site Scripting (XSS): malicious scripts steal credentials or force actions.
- Insecure Direct Object Reference: direct references open unintended access.
- Security Misconfiguration: poorly configured servers and applications create openings.
- Sensitive Data Exposure: unprotected data exposes customers and the company.
- Missing Function Level Access Control: every function must check permissions.
- Cross Site Request Forgery: authenticated users are pushed into unwanted actions.
- Components with Known Vulnerabilities: vulnerable libraries compromise the application.
- Unvalidated Redirects and Forwards: unchecked redirects lead to malware or phishing.

EasyAudit WEB follows the OWASP methodology to check portals, reserved areas, websites and applications, returning a clear and actionable report.