EasyAudit™
KNOW THE RISK

WHITE PAPER EASYAUDIT

Las 10 reglas de OWASP para la seguridad de aplicaciones Web

OWASP es la entidad internacional que produce recursos y materiales para mejorar la seguridad del software web. La Top 10 ayuda a desarrolladores, profesionales IT y directivos a reconocer las principales amenazas para las aplicaciones.

OWASP Top 10

- Injection: entradas no controladas pueden ejecutar comandos o consultas arbitrarias.
- Broken Authentication: sesiones, credenciales y cookies mal gestionados exponen cuentas.
- Cross Site Scripting (XSS): scripts maliciosos roban credenciales o fuerzan acciones.
- Insecure Direct Object Reference: referencias directas abren accesos no previstos.
- Security Misconfiguration: servidores y aplicaciones mal configurados crean brechas.
- Sensitive Data Exposure: datos no protegidos exponen clientes y empresa.
- Missing Function Level Access Control: cada función debe verificar permisos.
- Cross Site Request Forgery: el usuario autenticado es inducido a acciones no deseadas.
- Components with Known Vulnerabilities: librerías vulnerables comprometen la aplicación.
- Unvalidated Redirects and Forwards: redirecciones no controladas llevan a malware o phishing.

EasyAudit WEB sigue la metodología OWASP para verificar portales, áreas reservadas, sitios web y aplicaciones, entregando un informe claro y accionable.