



Seguridad en Aplicaciones Web Modernas



Introducción



Introducción

- Las aplicaciones web modernas usan APIs, microservicios y nube.
- Esto mejora el desarrollo, pero también incrementa los riesgos.
- Hoy abordaremos:
 - Seguridad en APIs RESTful
 - Seguridad en la nube
 - OWASP Top 10 y cómo mitigar riesgos







Seguridad en APIs RESTful



Seguridad en APIs RESTful

- Las APIs son esenciales pero vulnerables.
- Riesgos comunes:
 - SQL Injection
 - Cross-Site Scripting (XSS)
 - Cross-Site Request Forgery (CSRF)
- ValuationSoluciones:
 - Consultas preparadas / ORMs
 - Sanitización de entradas
 - Tokens CSRF y cookies con SameSite





Energiza! Autenticación y Autorización



Autenticación y Autorización

- Usa estándares modernos como:
 - JWT (JSON Web Tokens)
 - OAuth 2.0
- Aplica control de acceso por roles (RBAC)
- Representation of the second s





Validación y Sanitización en APIs



Validación y Sanitización en APIs

- Nunca confíes en los datos del cliente.
- Valida todos los datos entrantes y salientes.
- Protege tu API del mal uso.





Seguridad en la Nube



Seguridad en la Nube



AWS, Azure, Google Cloud Platform

Modelo de responsabilidad compartida:

- Proveedor: Infraestructura
- Tú: Datos, configuración y accesos









Buenas Prácticas Cloud



Buenas Prácticas Cloud

- Rotación de claves y tokens
- Cifrado en tránsito y en reposo
- Monitoreo con SIEM
- Pruebas de seguridad periódicas
- MFA para accesos críticos





OWASP Top 10 (2021)



OWASP Top 10 (2021)

- Broken Access Control
- 2. Cryptographic Failures
- 3. Injection (SQL, LDAP, OS...)
- 4. Insecure Design
- 5. Security Misconfiguration
- 6. Vulnerable Components
- 7. Auth Failures
- 8. Integrity Failures
- 9. Logging Failures
- 10. Server-Side Request Forgery (SSRF)





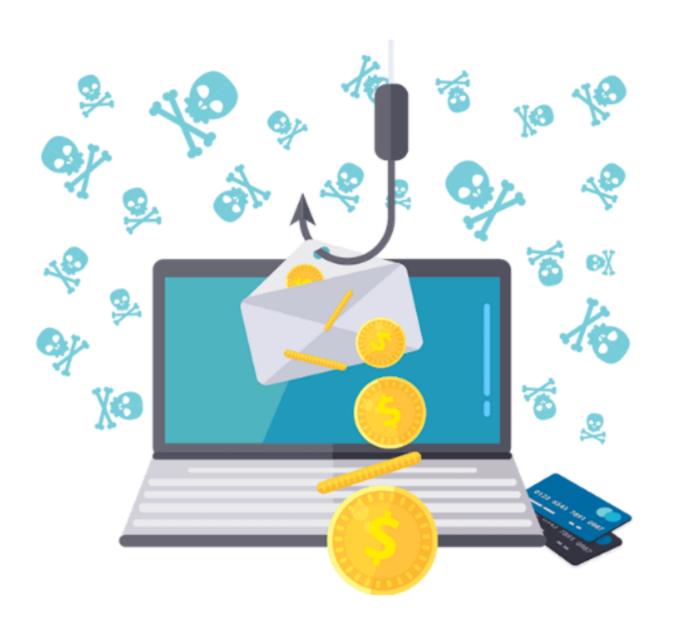
¿Por qué importa?



¿Por qué importa?

Las vulnerabilidades OWASP pueden provocar:

- Fugas de datos
- Robo de identidad
- Pérdidas económicas
- Daño a la reputación



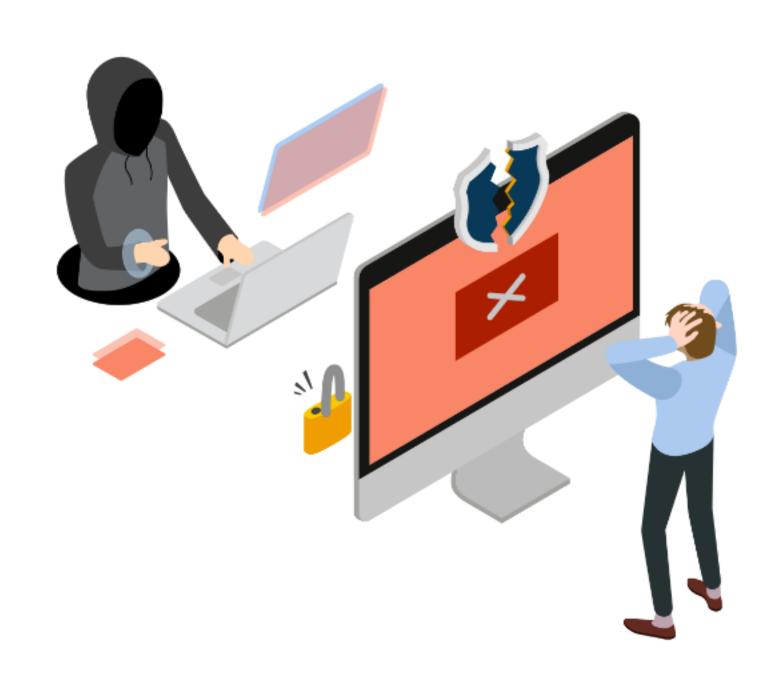


Mitigación según OWASP



Mitigación según OWASP

- Control de acceso fuerte
- Cifrado robusto
- Parches de seguridad frecuentes
- DevSecOps: pruebas + revisión continua
- Registro y monitoreo activo





Conclusión



Conclusión

- La seguridad moderna no es opcional.
- Debe aplicarse en:
 - Diseño
 - Desarrollo
 - Producción
- Cultura de prevención
- Equipos comprometidos
- Aplicaciones confiables y seguras



Energiza!