20-04-2025

FORO DEBATE

Unidad de Trabajo 6

Francisco Javier Otero Herrero
Grupo ATU

FORO DEBATE

Mucho se ha hablado y se hablará de los controles de seguridad en el desarrollo de las aplicaciones web. En el documento adjunto encontrarás un artículo donde se exponen los 10 riesgos más críticos de las aplicaciones web.

http://unaaldia.hispasec.com/2013/11/owasp-los-diez-riesgos-mas-criticos-en.html

PREGUNTAS PARA EL DEBATE

I. ¿Estás de acuerdo o agregarías alguno más? ¿Por qué?

OWASP actualiza periódicamente una lista de los 10 riesgos de seguridad más críticos para las aplicaciones web. Esta lista proporciona una clasificación de los riesgos más comunes y peligrosos, y sirve como guía para desarrolladores y profesionales de seguridad.

La lista de ***OWASP*** *Top 10* ha evolucionado a lo largo de los años, pero algunos riesgos fundamentales permanecen, mientras que otros cambian de posición o se fusionan. Esto refleja los cambios en las tecnologías web y las tácticas de los atacantes.

En general, estoy de acuerdo con que la lista de OWASP Top 10 identifica los riesgos más críticos. Es una lista bien fundamentada y actualizada por expertos en seguridad. Si bien la lista de OWASP es muy completa, aquí hay algunas consideraciones y énfasis adicionales que podrían hacerse:

- ***Seguridad de APIs:*** Con el auge de las ***APIs,*** la seguridad de las interfaces de programación de aplicaciones se ha vuelto crucial. Los riesgos específicos de las ***APIs,*** como la falta de autorización granular, la limitación de velocidad inadecuada y la exposición excesiva de datos, merecen una atención especial.
- ***Seguridad en el desarrollo de microservicios:*** Las arquitecturas de microservicios introducen nuevos desafíos de seguridad debido a la mayor complejidad y la comunicación entre servicios.
- ***Seguridad en la nube:*** El despliegue de aplicaciones web en la nube plantea consideraciones de seguridad específicas, como la seguridad de la configuración de la nube, la gestión de identidades y accesos en la nube y la seguridad de los contenedores.
- ***DevSecOps:*** La integración de la seguridad en el ciclo de vida del desarrollo de software ***(DevSecOps)*** es cada vez más importante. La seguridad no debe ser una ocurrencia tardía, sino una parte integral del proceso de desarrollo.

FORO DEBATE

¿Por qué estas adiciones/énfasis?

- Las APIs son la base de muchas aplicaciones web modernas, y su seguridad es fundamental para proteger los datos y la funcionalidad.
- Los microservicios son una arquitectura popular, pero requieren una atención cuidadosa a la seguridad debido a su naturaleza distribuida.
- La nube es el entorno de despliegue dominante para las aplicaciones web, y su seguridad es esencial para proteger los datos y la infraestructura.
- DevSecOps es un enfoque esencial para construir aplicaciones web seguras en el mundo actual.

En resumen, la lista de ***OWASP Top 10*** es una excelente base, pero es importante complementarla con consideraciones adicionales sobre las tendencias actuales en el desarrollo web y la seguridad.