Prácticas de Programación Segura

Seguridad por Diseño

Prácticas de programación segura

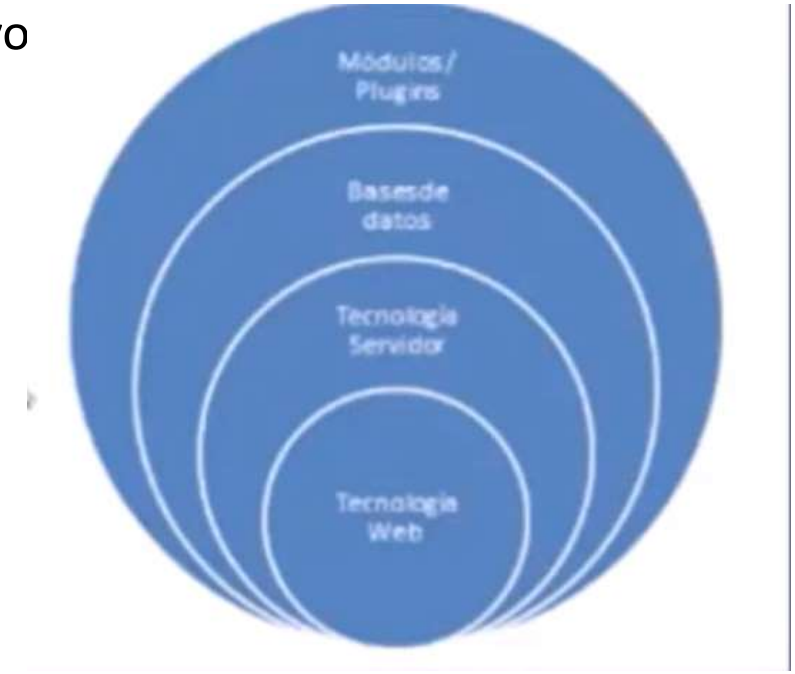
- Deben aplicarse las políticas de seguridad dentro de la arquitectura del software e implementar teniendo en cuenta que hay que analizar todo el código durante el ciclo de vida del desarrollo para obtener un código seguro.
- Puntos de un desarrollo seguro
  - Evaluación de riesgos
  - Autenticación
  - Autorización y control de acceso
  - Administración de sesiones
  - Validación de datos de entrada
  - Desbordamiento de buffer
  - Uso inseguro de criptografía
  - Manejo de errores
  - Loggining
  - Administración remota
  - Aplicaciones web y configuraciones del servidor

Programación segura

- Modelado de Amenazas: determinar activos y evaluar los riesgos.
- Seguridad Simple: modelar una estructura simple de seguridad.
- Defensa en profundidad: tener varias capas de seguridad por si alguna falla.
- Menor privilegio: cada usuario tiene que tener los mismos privilegios.
- Seguridad positiva: hacer uso de listas blancas
- Fallar de forma segura: controlar los fallos y no dar información alguna a los atacantes.
- Evitar la Seguridad por Oscuridad; ocultar un banner de un servicio puerto no implica que estés a salvo.
- Corrección completa: llevar a cabo el hardening del servidor antes de su puesta online.

¿Cómo empezar una Auditoria Web?

- Depende del objetivo



¿Qué buscamos en la Auditoría Web?

1. Vulnerabilidades y fallos en la configuración en la propia aplicación web.
2. Vulnerabilidades y fallos de configuración en el servidor
3. Comunicaciones inseguras entre cliente y servidor.

OWASP – Open Web Application Security Project

- https://owasp.org/www-project-top-ten/

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

OWASP Web Security Testing Guide

- Checklist

OWASP

- https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf

- https://owasp.org/2020/12/03/wstg-v42-released

How Do You Safeguard Against Malicious Code?

- Enterprise management and security teams have their work cut out for them in protecting against web application vulnerabilities and malware code.

- Providing continuous protection includes a comprehensive approach to application, network and data security that includes:

Recomendaciones finales

How Do You Safeguard Against Malicious Code?

- Stress to employees the importance of never opening unexpected emails from external sources. It's especially important to avoid opening attachments or clicking links from such sources.
- Install and update antivirus software on all computers as a first defense
- Block pop-ups to prevent some incidents of intentional or accidental clicking on potentially harmful links
- Use minimal permissions on web applications to limit the authority and prevent hackers from having the potential to spread malicious code to critical systems

How Do You Safeguard Against Malicious Code?

- Keep software updated to ensure any applicable security patches or improvements are included
- Scan websites and code for malicious code regularly
- Implement secure firewalls for all network traffic
- Utilize software tools to monitor suspicious activity, especially any use of unauthorized web sites, access to bank accounts, or emails to or from unrecognized email accounts

How Do You Safeguard Against Malicious Code?

- Utilize secure VPN software for mobile employees who may utilize business systems from home, customer or job sites, or on public networks
- Overall, ensure that there are authorized and accountable resources that monitor system logs for suspicious activity to be proactive in detecting potential security issues or the presence of malicious software.