SEG 118 – Desarrollo Seguro basado en OWASP

Ing. Carlos Carreño

Nov, 2021

MODULO 5: SEGURIDAD EN LA CODIFICACIÓN DE SOFTWARE

- Vulnerabilidades más comunes. ¿Cómo prevenirlas?
- Vulnerabilidades del ranking OWASP Top 10
- Otras vulnerabilidades
- Recursos de OWASP para seguridad en la codificación

Vulnerabilidades más comunes. ¿Cómo prevenirlas?

- **Errores en la gestión de recursos**: Una aplicación permite que se consuman un exceso de recursos afectando a la disponibilidad de los mismos.
- **Error de configuración**: Problemas de configuración de software o de los servicios web.
- **Factor humano**: Negligencias causadas generalmente por la falta de formación y concienciación.
- **Validación de entrada**: Fallo en la validación de datos introducidos en aplicaciones.
- **Salto de directorio**: Fallo en la depuración de un programa, en la validación de caracteres especiales.
- **Permisos, privilegios y/o control de acceso**: Fallos en la protección y gestión de permisos

Vulnerabilidades del ranking OWASP Top 10

- OWASP Top 10 es un documento de los diez riesgos de seguridad más importantes en aplicaciones web según la Open Web Application Security Project, un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.
- Creado a mediados de la década de 2000, el OWASP Top 10, la última actualización de la que disponíamos fechaba del 2017 y ahora se ha actualizado después de cuatro años y, después de más de una década, hay una nueva vulnerabilidad encabezando el ranking.

Vulnerabilidades Top Ten según OWASP

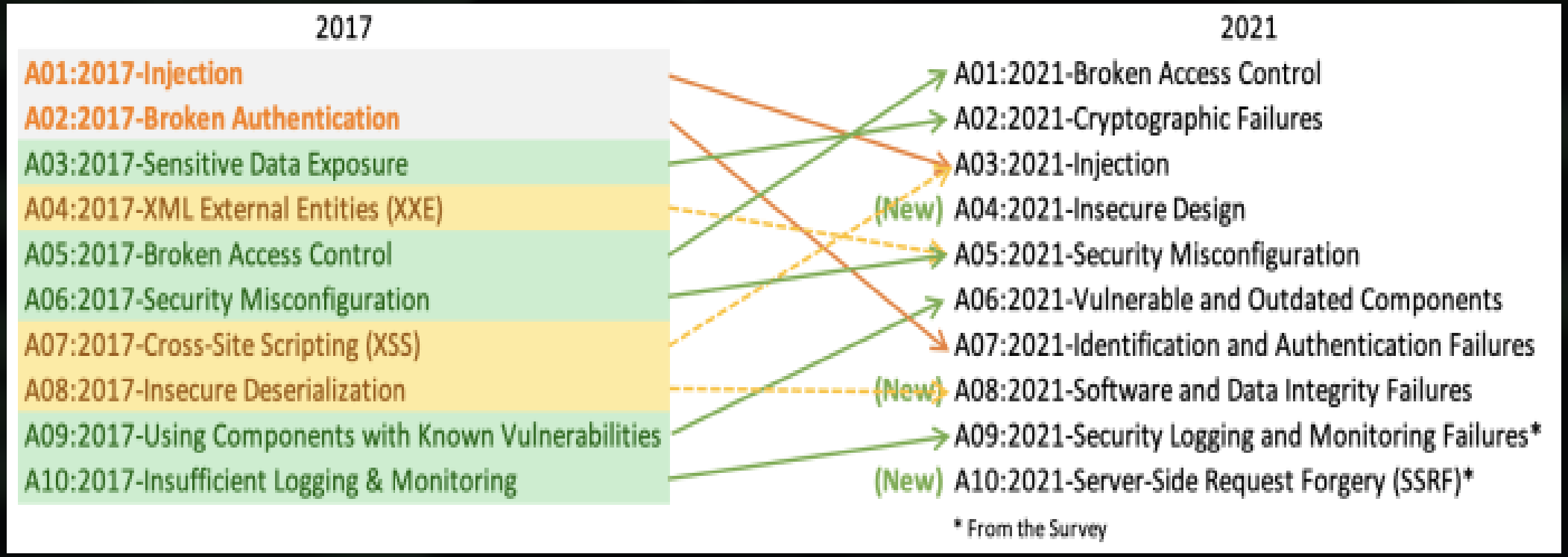
- **A1:2017 Inyección**
- **A2:2017 Pérdida de Autenticación**
- **A3:2017 Exposición de datos sensibles**
- **A4:2017 Entidades Externas XML (XXE)**
- **A5:2017 Pérdida de Control de Acceso**

Vulnerabilidades Top Ten según OWASP

- **A6:2017 Configuración de Seguridad Incorrecta**
- **A7:2017 Secuencia de Comandos en Sitios Cruzados (XSS)**
- **A8:2017 Deserialización Insegura**
- **A9:2017 Componentes con vulnerabilidades conocidas**
- **A10:2017 Registro y Monitoreo Insuficientes**

New top 10 OWASP 2021

- Habrá algunos cambios.



Otras vulnerabilidades

- **Lista de las 20 principales vulnerabilidades críticas en software de SANS**
- **CWE : Enumeración de Debilidades Comunes (**The Common Weakness Enumeration)

Lista de las 20 principales vulnerabilidades críticas en software de SANS

- **CWE-119** : Error de búfer de memoria
- **CWE-79** : Secuencias de comandos entre sitios
- **CWE-20** : Error de entrada no validado
- **CWE-200** : Error de exposición de información sensible
- **CWE-125** : Error de lectura fuera de límites
- **CWE-89** : Inyección SQL
- **CWE-416** : Error de memoria libre
- **CWE-190** : Error de desbordamiento de enteros
- **CWE-352** : Falsificación de solicitudes entre sitios

… continua

- **CWE-22** : Recorrido de directorio
- **CWE-78** : Inyección de comandos del sistema operativo
- **CWE-787** : Error de escritura fuera de los límites
- **CWE-287** : Error de autenticación inadecuado
- **CWE-476** : Desreferenciación del puntero NULL
- **CWE-732** : Asignación de permisos incorrecta
- **CWE-434** : Carga de archivos sin restricciones
- **CWE-611** : Exposición de información a través de entidades XML
- **CWE-94** : Inyección de código
- **CWE-798** : Clave de acceso codificada
- **CWE-400** : Consumo incontrolado de recursos

Recursos de OWASP para seguridad en la codificación

- OWASP Secure Coding Practices Quick Reference Guide
- OWASP Top 10
- OWASP ZAP
- OWASP Guía de Pruebas

Practica

- Hacer la lectura del documento ***OWASP Secure Coding Practices Quick Reference*** realizar un grafo o “mapa mental” en Power Point con las principales practicas de codificacion segura recomendadas por **OWASP**

Referencias

- https://owasp.org/www-project-top-ten/2017/Top_10
- https://es.myservername.com/sans-top-20-security-vulnerabilities-software-applications
- https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html
- https://www.zaproxy.org/