Programación de Servicios y Procesos

U.D.5 – TÉCNICAS DE PROGRAMACIÓN SEGURA

Buenas prácticas programación segura

- Evitar fallos leyendo errores de otros programadores.
- Revisar y participar en foros de detección errores.
- Leer formas de codificación segura.
- Leer software de código abierto para aprender.

Precaución manejo datos

- Limpiar los datos → Trabajar en formato datos pueden introducirse.
- Realizar la comprobación límites → Para evitar, por ejemplo, desbordamiento de buffer.
- Comprobar parámetros de línea de comandos.
- Incializar correctamente las variables con datos válidos.

Revisión de procesos

- Intentar revisión por pares en nuestro modelo de desarrollo.
- Hacer verificación independiente en proyectos críticos.
- Usar herramientas automáticas de revisión siempre que sea posible.

Usar listas de control de seguridad

- Uso de contraseñas. (2024 sistemas 2 pasos o token)
- Inicios de sesión de usuario únicos.
- Usar listas de control de acceso basados en roles.
- Nunca intercambio de contraseñas en texto plano.
- Contraseñas en BD siempre encriptadas.
- Usar cifrado para transferencias de datos.

Marco de referencia en Seguridad Software

- En la industria del software tanto compañías como instituciones tienen tienen peso en cada área de desarrollo de software.
- En áreas críticas como la seguridad las compañías pueden tener parte interesada, como fabricantes.
- Organizaciones sin ánimo de lucro como OWASP, ofrecen una opinión más objetiva del estado de un arte.

OWASP

- Open Worldwide Application Security Project
- Organización sin ánimo de lucro centrada en impulsar la construcción de software seguro.
- Tiene alrededor de 250 capítulos locales alrededor del mundo.
- Su misión: To be the global open community that powers secure software through education, tools, and collaboration.

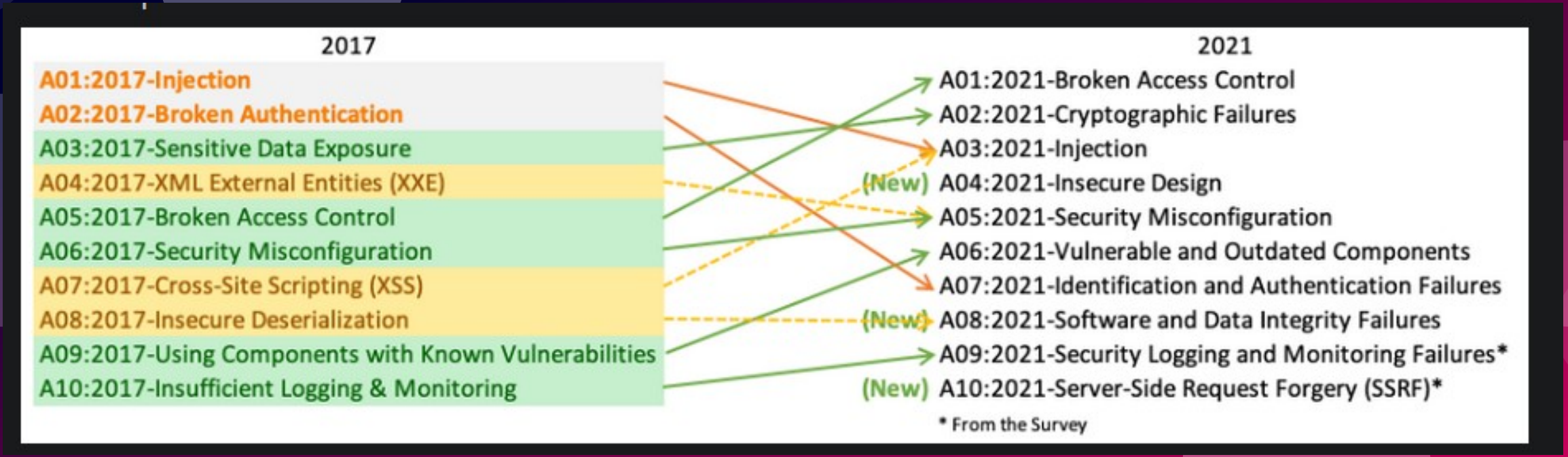
https://owasp.org

OWASP II

- OWASP ofrece herramientas para impulsar el desarrollo de software seguro.
- Guía OWASP establece un marco de trabajo para comprobar y aumentar seguridad.
- OWASP Top ten → 10 riesgos de seguridad más importantes
- OWASP MAS → Marco para desarrollar y testear aplicaciones móviles seguras.

https://owasp.org

Ejemplo: Top 10 Web Application Security Risks



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

ISO/IEC 27001:2022

- La web de AENOR indica sobre esta certificación:

"Los Sistemas de Gestión de Seguridad de la Información (SGSI) son el medio más eficaz de minimizar los riesgos, al asegurar que se identifican y valoran los procesos de negocio y/o servicios de TI, activos y sus riesgos, considerando el impacto para la organización, y se adoptan los controles y procedimientos más eficaces y coherentes con la estrategia de negocio, considerando la mejora continua.

Una gestión eficaz de la seguridad de la información permite garantizar:

- su confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información,
- su integridad, asegurando que la información y sus métodos de proceso son exactos y completos, y
- su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

La certificación del Sistema de Gestión de Seguridad de la Información de AENOR, de acuerdo a ISO/IEC 27001:2022, contribuye a fomentar las actividades de protección de sus sistemas y su información en las organizaciones, mejorando su imagen y generando confianza frente a terceros. "

https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion