3. Metodologías de Seguridad

Lorenzo Elguea
Febrero 2024

Tema 3

3. Metodologías de Seguridad

    1. Controles CIS
    2. NIST
    3. OWASP

Controles CIS

Los **Controles** de Seguridad Críticos de **CIS** comprenden un conjunto de 18 (19 en la UP) controles informáticos en torno a la seguridad de las organizaciones

CIS_Controls_v8_Spanish.22.01.pdf y CIS_Controls_Version_8.xlsx

Cada control, tiene una función específica que lo identifica. Aunque algún control puede tener partes de otras funciones, una de ellas es la principal. Las funciones son:

1. Identificar (22)

2. Proteger (94)

3. Recuperar (7)

4. Responder (13)

5. Detectar (20)

Controles CIS

Los controles CIS, se enfocan en proteger los activos

Tipo de Activo a proteger

1. Aplicaciones (31)
2. Datos (23)
3. Dispositivos (27)
4. Redes (35)
5. Usuarios (15)
6. No Aplica (25)

NIST

NIST es el acrónimo de Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, en inglés) dependiente del Departamento de Comercio de EE. UU.

El Marco de Ciberseguridad del NIST ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Este Marco es voluntario. Le brinda a su negocio una reseña de las mejores prácticas para ayudarlo a decidir dónde tiene que concentrar su tiempo y su dinero en cuestiones de protección de ciberseguridad.

https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

Marco NIST

El Marco de Ciberseguridad del NIST en su negocio en estas cinco áreas:

1. Identificación
2. Protección
3. Detección
4. Respuesta
5. Recuperación.

cybersecurity_sb_nist-cyber-framework-es.pdf

NIST

1. Identificación

Haga una lista de todos los equipos, programas software y datos que use, incluyendo computadoras portátiles, teléfonos inteligentes, tablets y dispositivos utilizados en puntos de venta.

Elabore y comparta una política de ciberseguridad de la compañía que cubra los siguientes puntos:

Funciones y responsabilidades de los empleados, proveedores y todo aquel que tenga acceso a datos delicados.

Pasos a seguir para protegerse contra un ataque y limitar el daño si se produce un ataque.

NIST

2. Protección

Controle quiénes acceden a su red y usan sus computadoras y otros dispositivos.

Use programas de seguridad para proteger los datos.

Codifique los datos delicados, tanto cuando estén almacenados o en tránsito.

Haga copias de seguridad de los datos con regularidad.

Actualice los programas de seguridad con regularidad, en lo posible, automatice estas actualizaciones.

Implemente políticas formales para la eliminación segura de archivos electrónicos y dispositivos en desuso.

Capacite sobre ciberseguridad a todas las personas que usen sus computadoras, dispositivos y redes. Usted puede ayudar a los empleados a comprender su riesgo personal además de la función crucial que cumplen en el lugar de trabajo.

NIST

3. Detección

Monitoree sus computadoras para controlar si detecta acceso de personal no autorizado a sus computadoras, dispositivos (soportes de almacenamiento de datos de tipo USB) y software.

Revise su red para controlar si detecta usuarios o conexiones no autorizados.

Investigue cualquier actividad inusual en su red o por parte de su personal.

NIST

4. Respuesta

Implemente un plan para:

Notificar a los clientes, empleados y otros cuyos datos pudieran estar en riesgo.

Mantener en funcionamiento las operaciones del negocio.

Reportar el ataque a los encargados del cumplimiento de la ley y otras autoridades.

Investigar y contener un ataque.

Actualizar su política y plan de ciberseguridad con las lecciones aprendidas.

Prepararse para eventos inadvertidos (como emergencias climáticas) que puedan poner en riesgo los datos.

Ponga a prueba su plan con regularidad.

NIST

5. Recuperación

Después de un ataque:

Repare y restaure los equipos y las partes de su red que resultaron afectados.

Mantenga informados a sus empleados y clientes de sus actividades de respuesta y recuperación.

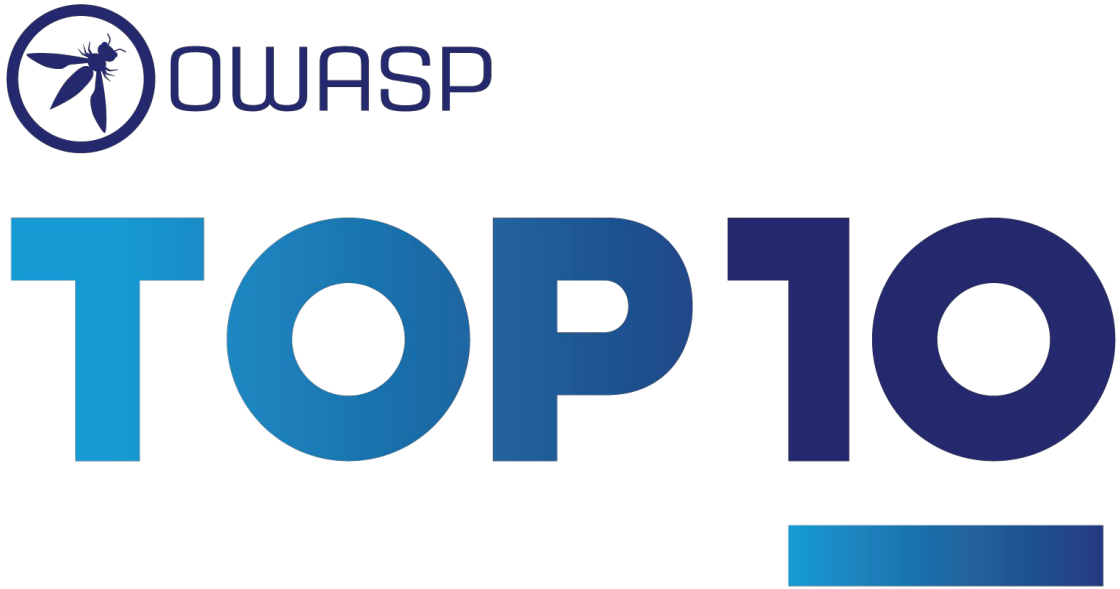
Open Web Application Security Project: OWASP

Lorenzo Elguea

OWASP

OWASP es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. Wikipedia

Periódicamente actualiza el TOP 10

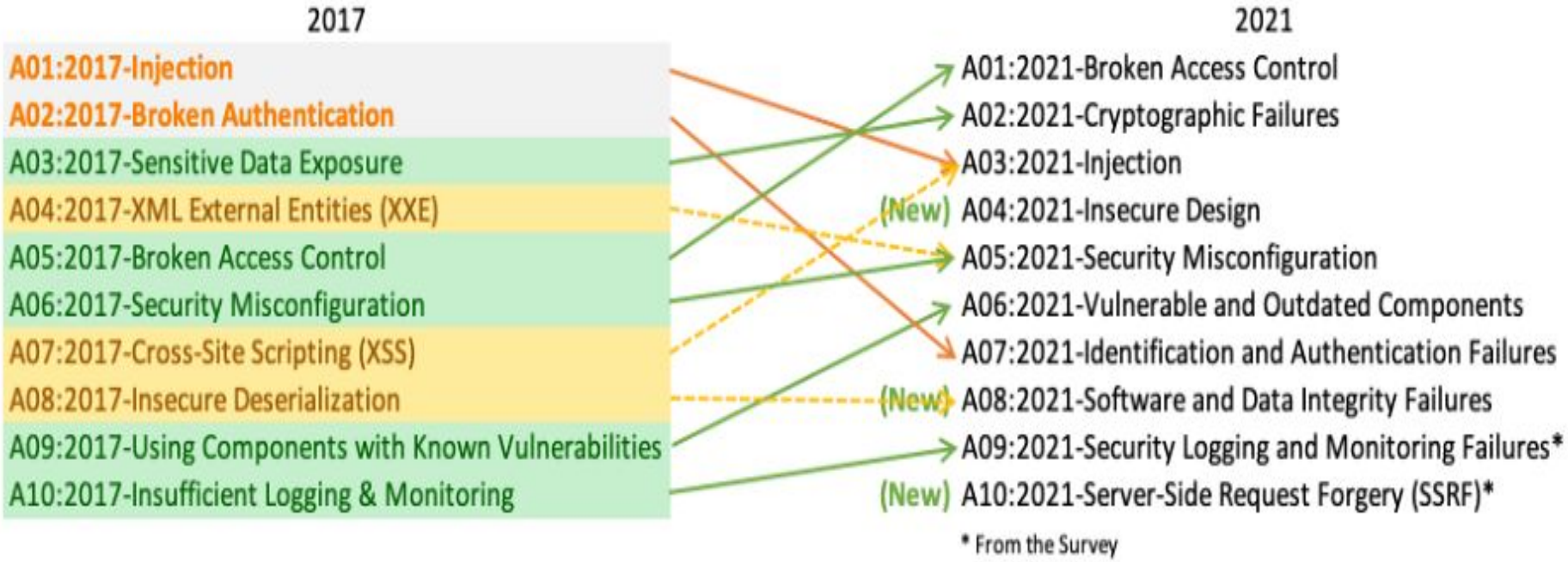


TOP 10 2021

Top 10:2021 List

- A01 Broken Access Control
- A02 Cryptographic Failures
- A03 Injection
- A04 Insecure Design
- A05 Security Misconfiguration
- A06 Vulnerable and Outdated Components
- A07 Identification and Authentication Failures
- A08 Software and Data Integrity Failures
- A09 Security Logging and Monitoring Failures
- A10 Server Side Request Forgery (SSRF)

TOP 10


2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

OWASP: qué es y cómo usar esta metodología para mejorar la seguridad de nuestra aplicación web - Blog de arsys.es

OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation

OWASP Top 10:2021