

DSA - OWASP

OWASP (OPEN WEB APPLICATION SECURITY PROJECT):

- Es un proyecto conformado por una comunidad mundial libre y abierta centrada en mejorar la seguridad del software.
- Tiene como fin ayudar a las organizaciones a desarrollar y mantener aplicaciones confiables.
- <https://www.owasp.org>

¿QUÉ OFRECE OWASP?

- **OWASP Top Ten**
 - Riesgos de seguridad más críticos para las aplicaciones web.
- **OWASP Web Security Testing Guide (WSTG)**
 - Controles de seguridad que se deben contemplar a la hora de realizar pentesting en aplicaciones web
- **OWASP Cheat Sheet Series**
 - Una colección concisa de información de alto valor sobre temas específicos de seguridad de aplicaciones.
 - Básicamente resúmenes sobre temáticas que complementan a los otros documentos.
- **OWASP Application Security Verification Standard (ASVS)**
 - Ofrece una lista completa de requisitos, controles y pruebas de seguridad de aplicaciones web que puede utilizar para determinar el alcance, crear y verificar aplicaciones web y móviles seguras.

¿QUÉ OFRECE OWASP?

- OWASP DefectDojo
 - tracking de pentesting y reporte
- OWASP Zed Attack Proxy (ZAP) (<https://www.zaproxy.org/>)
 - Herramienta de pentesting tipo burp
- OWASP in SDLC
 - Ejemplo del uso de mucha de las herramientas de owasp en el SDLC
- OWASP API Top 10
- OWASP Mobile Security
- OWASP Cloud-Native Application Security Top 10
- OWASP Kubernetes Top Ten
- OWASP Docker Top 10
- OWASP Top 10 Privacy Risks

¿QUÉ OFRECE OWASP?

- [OWASP Attacks list](#)
 - Enumeración de ataques a aplicaciones web
- [OWASP Vulnerabilities](#)
 - Enumeración de vulnerabilidades específicas
- [OWASP Proactive Controls](#)
 - Una lista de técnicas de seguridad que deben tenerse en cuenta para cada proyecto de desarrollo de software
 - Están ordenados por orden de importancia, siendo el control número 1 el más importante.
 - Fue escrito por desarrolladores para ayudar a nuevos desarrolladores a asegurar la seguridad en el desarrollo de software.
- [OWASP Vulnerable Web Applications Directory](#)
- [OWASP Automated Threats to Web Applications](#)
 - Enumeración de varios ataques automáticos a aplicaciones web
 - También define un lenguaje estándar para referenciar a estos ataques

ALGUNOS PROYECTOS QUE VAN DESAPARECIENDO O MUTANDO EN OWASP

- OWASP Top 10 Card Game
 - Juego de cartas del top ten y controles proactivos, black hats vs white hats
- OWASP Cornucopia
 - juego de cartas para ayudar al desarrollo de soft obteniendo requerimientos de seguridad a través del mismo.
- Latam Tour: <https://www.owasp.org/index.php/LatamTour2019>
- Latam Tour en casa: <https://www.owasp.org/index.php/LatamTour2020>
- Varios otros proyectos y muchísimo material de documentación.

OWASP TOP TEN

- El OWASP Top 10 es un documento de concientización para desarrolladores y seguridad de aplicaciones web.
- Representa un amplio consenso sobre los riesgos de seguridad más críticos para las aplicaciones web.
- Este documento contiene 10 categorías cada una contiene 5 secciones:
 1. Riesgo
 - Vectores de ataque
 - debilidades de seguridad
 - impacto tecnológico y del negocio.
 2. La aplicación es vulnerable?
 3. cómo se previene
 4. Ejemplos de escenarios de ataques
 5. Referencias.

OWASP TOP TEN

- En sí, cada categoría representa un riesgo de seguridad pero cada riesgo es genérico.
- Por ejemplo **A3: Injection** representa cualquier tipo de inyección a una aplicación pero existen muchísimas subcategorías de este riesgo (SQL injection , Command injection, Template injection, etc) que deben estudiarse específicamente para obtener resultados.
- Para estos casos deben usarse las referencias de la categoría que suelen ser muy útiles a la hora de estudiar el riesgo de la categoría de manera más específica.

OWASP TOP TEN

- Comúnmente en las referencias podemos encontrar:
 - OWASP Proactive Controls
 - Hace referencia a un control específico de la categoría.
 - OWASP Cheat Sheet:
 - Hace referencia a cheatsheet sobre temas de seguridad que amplían a la categoría.
 - OWASP ASVS
 - Hace referencia a requerimiento específico de ASVS relacionado con la categoría.
 - OWASP Testing Guide
 - En en OWASP Top Ten hace referencia al escenario específico de la WSTG relacionado con la categoría.
 - OWASP Automated Threats
 - hace referencia a un ataque automático específico que está relacionado con la categoría.
 - OWASP Vulnerabilities
 - En en OWASP Top Ten hace referencia a una vulnerabilidad relacionada con la categoría.
 - Documentos externos
 - MITRE: CWE/CVE
 - NIST

OWASP TOP TEN






- Se genera una nueva versión cada 3 o 4 años:
- Historial:
 - Top Ten 2003
 - Top Ten 2004
 - Top Ten 2007
 - Top Ten 2010
 - Top Ten 2013
 - Top Ten 2017
 - Top Ten 2021 (actual)
 - Planning to announce the release of the OWASP Top 10:2025 in the first half of 2025.

OWASP 2007-2017:

OWAPS TOP 10 - 2007		OWAPS TOP 10 - 2010		OWAPS TOP 10 - 2013		OWAPS TOP 10 - 2017
A1 – Secuencia de Comandos en Sitios Cruzados (XSS)	▲ 1	A1 – Inyección	■ 0	A1 – Inyección	■ 0	A1 – Inyección
A2 – Inyección	▼ -1	A2 – Secuencia de Comandos en Sitios Cruzados (XSS)	▲ 1	A2 – Pérdida de Autenticación y Gestión de Sesiones	■ 0	A2 – Pérdida de Autenticación
A3 – Ejecución Maliciosa de Ficheros	▲ 4	A3 – Pérdida de Autenticación y Gestión de Sesiones	▼ -1	A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	▲ 3	A3 – Exposición de Datos Sensibles
A4 – Referencia Directa Insegura a Objetos	▲ 1	A4 – Referencia Directa Insegura a Objetos	■ 0	A4 – Referencia Directa Insegura a Objetos	(*)	A4 - XML External Entities (XEE)
A5 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	■ 0	A5 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	▲ 1	A5 – Configuración de Seguridad Incorrecta	(**)	A5 - Perdida de Control de Acceso
A6 – Filtrado de Información y Manejo Inapropiado de Errores	(*)	A6 – Defectuosa Configuración de Seguridad	(*)	A6 – Exposición de Datos Sensibles	▼ -1	A6 – Configuración de Seguridad Incorrecta
A7 – Pérdida de Autenticación y Gestión de Sesiones	▲ 1	A7 – Almacenamiento Criptográfico Inseguro	(*)	A7 – Ausencia de Control de Acceso a las Funciones	↓ -4	A7 – Secuencia de Comandos en Sitios Cruzados (XSS)
A8 – Almacenamiento Criptográfico Inseguro	▲ 2	A8 – Falla de Restricción de Acceso a URL	↓ -3	A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	(*)	A8 - Deserialización insegura
A9 – Comunicaciones Inseguras	(*)	A9 – Protección Insuficiente en la Capa de Transporte	(*)	A9 – Uso de Componentes con Vulnerabilidades Conocidas	■ 0	A9 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Falla de Restricción de Acceso a URL	(*)	A10 – Redirecciones y reenvíos no validados	■ 0	A10 – Redirecciones y reenvíos no validados	(*)	A10 - Registro y monitorización insuficiente
(*) Nuevo (**) Fusionado						

TOP TEN 2007 / 2010

Cambia la metodología de selección: se centra en riesgos no en cantidad de vulnerabilidades.

OWASP Top 10 – 2007 (Anterior)	OWASP Top 10 – 2010 (Nuevo)
A2 – Fallas de Inyección	 A1 – Inyección
A1 – Secuencia de Comandos en Sitios Cruzados (XSS)	 A2 – Secuencia de Comandos en Sitios Cruzados (XSS)
A7 – Pérdida de Autenticación y Gestión de Sesiones	 A3 – Pérdida de Autenticación y Gestión de Sesiones
A4 – Referencia Directa Insegura a Objetos	= A4 – Referencia Directa Insegura a Objetos
A5 – Falsificación de Petición en Sitios Cruzados (CSRF)	= A5 – Falsificación de Petición en Sitios Cruzados (CSRF)
<era T10 2004 A10 – Gestión Insegura de la Configuración>	+ A6 – Configuración Defectuosa de Seguridad (NUEVO)
A8 – Almacenamiento Criptográfico Inseguro	 A7 – Almacenamiento Criptográfico Inseguro
A10 – Falla de restricción de acceso a URL	 A8 – Falla de restricción de acceso a URL
A9 – Comunicaciones Inseguras	= A9 – Protección Insuficiente en la Capa de Transporte
<no disponible en T10 2007>	+ A10 – Redirecciones y Destinos No Validados (NUEVO)
A3 – Ejecución de Ficheros Malintencionados	- <eliminado del T10 2010>
A6 – Revelación de Información y Gestión Incorrecta de Errores	- <eliminado del T10 2010>

¿QUÉ ES MITRE?

- Organización que con fondos del estado de EEUU trabaja en aspectos de seguridad informática.
- Lo importante es que administra el índice de Common Vulnerabilities and Exposure (CVE), identificador mundialmente utilizado.
- Ej: CVE-2014-0160
- [WebSite](#)
- También [Common vulnerabilities Enumeration](#)



April 15, 2025

Dear CVE Board Member,

We want to make you aware of an important potential issue with MITRE's enduring support to CVE.

On Wednesday, April 16, 2025, the current contracting pathway for MITRE to develop, operate, and modernize CVE and several other related programs, such as CWE, will expire. The government continues to make considerable efforts to continue MITRE's role in support of the program.

If a break in service were to occur, we anticipate multiple impacts to CVE, including deterioration of national vulnerability databases and advisories, tool vendors, incident response operations, and all manner of critical infrastructure.

MITRE continues to be committed to CVE as a global resource. We thank you as a member of the CVE Board for your continued partnership.

Sincerely,

Yosry Barsoum
VP and Director
Center for Securing the Homeland (CSH)

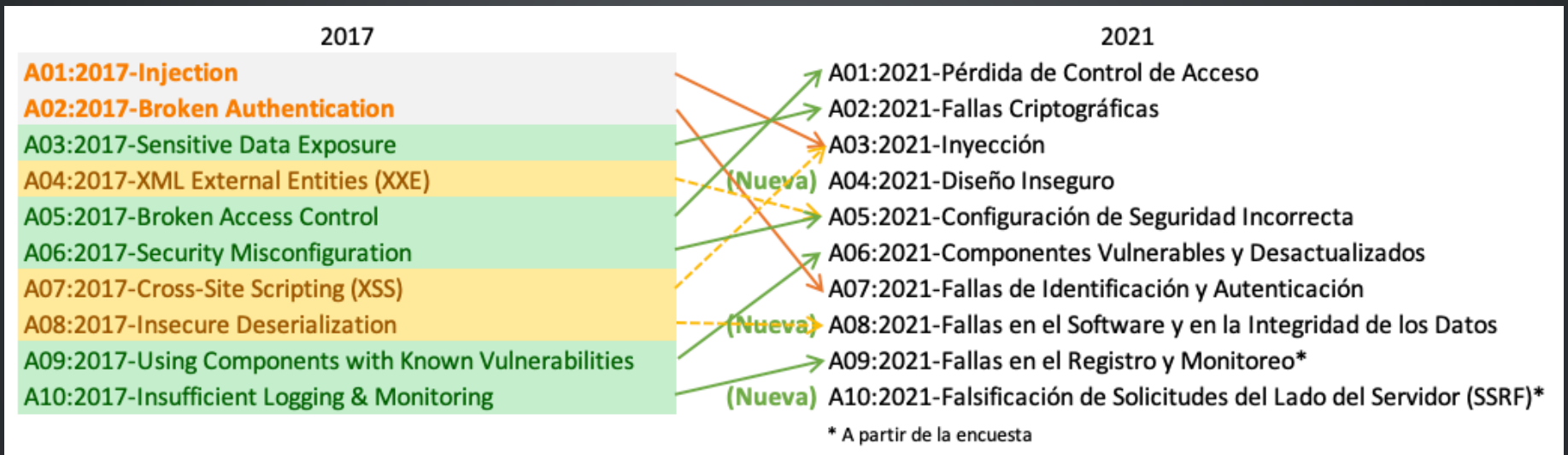
2010 VS 2013:

OWASP Top 10 – 2010 (Previo)	OWASP Top 10 – 2013 (Nuevo)
A1 – Inyección	A1 – Inyección
A3 – Pérdida de Autenticación y Gestión de Sesiones	A2 – Pérdida de Autenticación y Gestión de Sesiones
A2 – Secuencia de Comandos en Sitios Cruzados (XSS)	A3 – Secuencia de Comandos en Sitios Cruzados (XSS)
A4 – Referencia Directa Insegura a Objetos	A4 – Referencia Directa Insegura a Objetos
A6 – Defectuosa Configuración de Seguridad	A5 – Configuración de Seguridad Incorrecta
A7 – Almacenamiento Criptográfico Inseguro – Fusionada A9→	A6 – Exposición de Datos Sensibles
A8 – Falla de Restricción de Acceso a URL – Ampliada en →	A7 – Ausencia de Control de Acceso a las Funciones
A5 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)
<dentro de A6: – Defectuosa Configuración de Seguridad>	A9 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Redirecciones y reenvíos no validados	A10 – Redirecciones y reenvíos no validados
A9 – Protección Insuficiente en la Capa de Transporte	Fusionada con 2010-A7 en la nueva 2013-A6

2013 VS 2017:

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	⊗	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	⊗	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

OWASP 2017 A 2021:



¿CÓMO SE FORMA?

- Las 10 principales categorías fueron seleccionadas y priorizadas de acuerdo con estos datos de prevalencia, en combinación con estimaciones consensuadas de explotabilidad, detectabilidad e impacto.
- A partir de 2013 aparece la referencia directa a las CWE <https://cwe.mitre.org/> para reducir la complejidad de mapeo.
- (2017) Aparece la tasa de incidencia: se refiere al porcentaje de la población de aplicaciones que tiene al menos una instancia de un tipo de vulnerabilidad. No nos importa si fue algo puntual o sistémico.

¿CÓMO SE ELIGEN LAS 10 CATEGORÍAS?

- En 2017, categorías según la tasa de incidencia para determinar la probabilidad, y luego las clasificamos según la discusión del equipo basada en décadas de experiencia respecto a la Explotabilidad, la Detectabilidad (también probabilidad) y el Impacto técnico.
- Para 2021, queremos utilizar los datos de Explotabilidad e Impacto (técnico) si es posible.

2021

- Ocho de las diez categorías a partir de los **datos** aportados por partners encuestados
- Y dos categorías a partir de la votación/encuesta de la comunidad del Top 10 a un alto nivel
- Se uso número de aplicaciones analizadas para un año determinado (a partir de 2017) y el número de aplicaciones con al menos una instancia de una CWE encontrada en las pruebas.

¿QUÉ CAMBIÓ DE 2017 A 2021?

- Hay tres nuevas categorías
- Cuatro categorías con cambios de nombre y alcance
- Alguna consolidación en el Top 10 de 2021
- Cambiaron los nombres cuando ha sido necesario para centrarnos en la causa raíz en lugar del síntoma. Cambia la importancia de las CWE.



CWE: Knowing the weaknesses that result in vulnerabilities means software developers, hardware designers, and security architects can eliminate them before deployment, when it is much easier and cheaper to do so

CWE site

EL TOPTEN

[HTTPS://OWASP.ORG/TOP10/ES/](https://owasp.org/top10/es/)

DATA FACTORS

- CWEs mapeadas: El número de CWEs asignadas a una categoría por el equipo del Top 10.
- Tasa de incidencia: La tasa de incidencia es el porcentaje de aplicaciones vulnerables a esa CWE de la población analizada por esa organización para ese año.
- Cobertura (de pruebas): El porcentaje de aplicaciones que han sido testadas por todas las organizaciones para una determinada CWE.
- Explotabilidad ponderada: La sub-puntuación de explotabilidad de las puntuaciones CVSSv2 y CVSSv3 asignadas a las CVEs mapeadas a las CWEs, normalizados y colocados en una escala de 10 puntos.

DATA FACTORS

- Impacto ponderado: La sub-puntuación de Impacto de las puntuaciones CVSSv2 y CVSSv3 asignadas a las CVEs mapeadas a las CWEs, normalizados y colocados en una escala de 10 puntos.
- Total de ocurrencias: Número total de aplicaciones en las que se han encontrado las CWEs asignados a una categoría.
- Total de CVEs: Número total de CVEs en la base de datos del NVD que fueron asignadas a las CWEs asignados a una categoría.

RIESGOS: ¿QUÉ ANALIZA OWASP?

Agentes De Amenaza	Vectores De Ataque	Prevalencia de Debilidades	Detectabilidad de Debilidades	Impacto Técnico	Impacto Al Negocio
?	Fácil	Difundido	Fácil	Severo	?
	Medio	Común	Medio	Moderado	
	Difícil	Poco Común	Difícil	Menor	

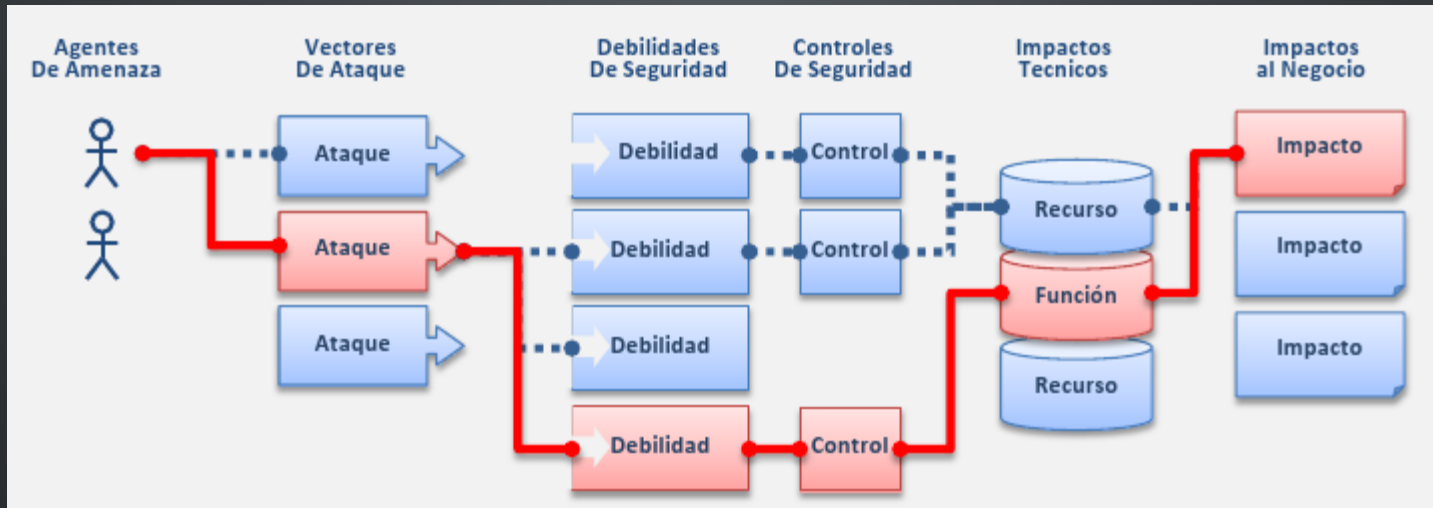
Sin embargo, solo usted sabe los detalles específicos de su ambiente y su negocio. Para una aplicación cualquiera, puede no haber un agente de amenaza que pueda ejecutar el ataque relevante, o el impacto técnico puede no hacer diferencia ninguna. Por tanto, usted debería evaluar cada riesgo, enfocándose en los agentes de amenaza, los controles de seguridad e impactos de negocio en su empresa.

EJEMPLO

- Recordemos por ejemplo el **Deface o defacement** manipular la página principal de un servidor web sin autorización, dejando algún tipo de mensaje en texto, imagen, vídeo...
- No siempre se trata de un motivo económico, puede ser de carácter reivindicativo político, lo que sería hacktivismo, o para avergonzar a los responsables del sitio, o simplemente un graffiti al estilo "estuve aquí".
- Por ejemplo en una fecha específica.

RIESGOS

- Los atacantes pueden potencialmente usar muchas diferentes rutas a través de su aplicación para causar daño.
- A veces, estas rutas son triviales de encontrar y explotar y a veces son extremadamente difíciles.
- De manera similar, el daño causado puede ir de ninguno hasta incluso sacarlo del negocio.
- Cada ruta es un riesgo



RIESGO TECNOLÓGICO

- Es la probabilidad de sufrir pérdidas por caídas o fallos en los sistemas informáticos o transmisión de datos, error desde programación u otros, siendo un componente del riesgo operativo

RIESGOS EN APLICACIONES

- Los atacantes pueden usar potencialmente rutas diferentes a través de la aplicación para hacer daño al negocio u organización, estas rutas representan un riesgo que puede, o no, ser lo suficientemente grave como para justificar la atención.

PÉRDIDA DE CONTROL DE ACCESO

- OWASP top 10 (2021): A01 (pérdida de control de acceso)
- OWASP top 10 (2017): A02 (pérdida de control de acceso y manejo de sesiones)
- OWASP top 10 (2010): A03 (pérdida de control de acceso y manejo de sesiones)
- OWASP top 10 (2007): A07 (pérdida de control de acceso y manejo de sesiones)

A2:2017

Pérdida de Autenticación

Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios (temporal o permanentemente).

¿La aplicación es vulnerable?

La confirmación de la identidad y la gestión de sesiones del usuario son fundamentales para protegerse contra ataques relacionados con la autenticación.

Pueden existir debilidades de autenticación si la aplicación:

- Permite ataques automatizados como la [reutilización de credenciales conocidas](#), cuando el atacante ya posee una lista de pares de usuario y contraseña válidos.
- Permite ataques de fuerza bruta y/o ataques automatizados.
- Permite contraseñas por defecto, débiles o muy conocidas, como "Password1", "Contraseña1" o "admin/admin".
- Posee procesos débiles o inefectivos en el proceso de recuperación de credenciales, como "respuestas basadas en el conocimiento", las cuales no se pueden implementar de forma segura.
- Almacena las contraseñas en texto claro o cifradas con métodos de *hashing* débiles (vea [A3:2017-Exposición de Datos Sensibles](#)).
- No posee autenticación multi-factor o fue implementada de forma ineficaz.
- Expone *Session IDs* en las URL, no la invalida correctamente o no la rota satisfactoriamente luego del cierre de sesión o de un periodo de tiempo determinado.

Cómo se previene

- Implemente autenticación multi-factor para evitar ataques automatizados, de fuerza bruta o reúso de credenciales robadas.
- No utilice credenciales por defecto en su software, particularmente en el caso de administradores.
- Implemente controles contra contraseñas débiles. Cuando el usuario ingrese una nueva clave, la misma puede verificarse contra la lista del [Top 10.000 de peores contraseñas](#).
- Alinear la política de longitud, complejidad y rotación de contraseñas con las recomendaciones de la [Sección 5.1.1 para Secretos Memorizados de la Guía NIST 800-63 B's](#) u otras políticas de contraseñas modernas, basadas en evidencias.
- Mediante la utilización de los mensajes genéricos iguales en todas las salidas, asegúrese que el registro, la recuperación de credenciales y el uso de APIs, no permiten ataques de enumeración de usuarios.
- Limite o incremente el tiempo de respuesta de cada intento fallido de inicio de sesión. Registre todos los fallos y avise a los administradores cuando se detecten ataques de fuerza bruta.
- Utilice un gestor de sesión en el servidor, integrado, seguro y que genere un nuevo ID de sesión aleatorio con alta entropía después del inicio de sesión. El *Session-ID* no debe incluirse en la URL, debe almacenarse de forma segura y ser invalidado después del cierre de sesión o de un tiempo de inactividad determinado por la criticidad del negocio.

A2:2017

Pérdida de Autenticación

Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios (temporal o permanentemente).

Ejemplos de escenarios de ataque

Escenario #1: el [relleno automático de credenciales](#) y el [uso de listas de contraseñas conocidas](#) son ataques comunes. Si una aplicación no implementa protecciones automáticas, podrían utilizarse para determinar si las credenciales son válidas.

Escenario #2: la mayoría de los ataques de autenticación ocurren debido al uso de contraseñas como único factor. Las mejores prácticas requieren la rotación y complejidad de las contraseñas y desalientan el uso de claves débiles por parte de los usuarios. Se recomienda a las organizaciones utilizar las prácticas recomendadas en la [Guía NIST 800-63](#) y el uso de autenticación multi-factor (2FA).

Escenario #3: los tiempos de vida de las sesiones de aplicación no están configurados correctamente. Un usuario utiliza una computadora pública para acceder a una aplicación. En lugar de seleccionar "logout", el usuario simplemente cierra la pestaña del navegador y se aleja. Un atacante usa el mismo navegador una hora más tarde, la sesión continúa activa y el usuario se encuentra autenticado.

Referencias

OWASP

- [OWASP Proactive Controls: Implement Identity and Authentication Controls](#)
- [OWASP ASVS: V2 Authentication, V3 Session Management](#)
- [OWASP Testing Guide: Identity, Authentication](#)
- [OWASP Cheat Sheet: Authentication](#)
- [OWASP Cheat Sheet: Credential Stuffing](#)
- [OWASP Cheat Sheet: Forgot Password](#)
- [OWASP Cheat Sheet: Session Management](#)
- [OWASP Automated Threats Handbook](#)

Externos

- [NIST 800-63b: 5.1.1 Memorized Secrets](#)
- [CWE-287: Improper Authentication](#)
- [CWE-384: Session Fixation](#)

IDOR

- OWASP top 10 (2013): A04 (referencia directa insegura a objetos)

A4 – Referencia Directa Insegura a Objetos

Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados.

A4 – Referencia Directa Insegura a Objetos

Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados.

¿Soy Vulnerable?

La mejor manera de poder comprobar si una aplicación es vulnerable a referencias inseguras a objetos es verificar que todas las referencias a objetos tienen las protecciones apropiadas. Para conseguir esto, considerar:

1. Para referencias **directas** a recursos **restringidos**, la aplicación necesitaría verificar si el usuario está autorizado a acceder al recurso en concreto que solicita.
2. Si la referencia es una referencia **indirecta**, la correspondencia con la referencia directa debe ser limitada a valores autorizados para el usuario en concreto.

Un análisis del código de la aplicación serviría para verificar rápidamente si dichas propuestas se implementan con seguridad. También es efectivo realizar comprobaciones para identificar referencias a objetos directos y si estos son seguros. Normalmente las herramientas automáticas no detectan este tipo de vulnerabilidades porque no son capaces de reconocer cuáles necesitan protección o cuáles son seguros e inseguros.

¿Cómo prevenirlo?

Requiere seleccionar una forma de proteger los objetos accesibles por cada usuario (identificadores de objeto, nombres de fichero):

1. **Utilizar referencias indirectas por usuario o sesión.** Esto evitaría que los atacantes accedieran directamente a recursos no autorizados. Por ejemplo, en vez de utilizar la clave del recurso de base de datos, se podría utilizar una lista de 6 recursos que utilizase los números del 1 al 6 para indicar cuál es el valor elegido por el usuario. La aplicación tendría que realizar la correlación entre la referencia indirecta con la clave de la base de datos correspondiente en el servidor. ESAPI de OWASP incluye relaciones tanto secuenciales como aleatorias de referencias de acceso que los desarrolladores pueden utilizar para eliminar las referencias directas a objetos.
2. **Comprobar el acceso.** Cada uso de una referencia directa a un objeto de una fuente que no es de confianza debe incluir una comprobación de control de acceso para asegurar que el usuario está autorizado a acceder al objeto solicitado.

A4 – Referencia Directa Insegura a Objetos

Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados.

Ejemplos de escenarios de ataques

La aplicación utiliza datos no verificados en una llamada SQL que accede a información sobre la cuenta:

```
String query = "SELECT * FROM accts WHERE account = ?";
```

```
PreparedStatement pstmt =  
    connection.prepareStatement(query , ... );
```

```
pstmt.setString( 1, request.getParameter("acct"));
```

```
ResultSet results = pstmt.executeQuery( );
```

Si el atacante modifica el parámetro “acct” en su navegador para enviar cualquier número de cuenta que quiera. Si esta acción no es verificada, el atacante podría acceder a cualquier cuenta de usuario, en vez de a su cuenta de cliente correspondiente.

```
http://example.com/app/accountInfo?acct=notmyacct
```

Referencias (en inglés)

OWASP

- [OWASP Top 10-2013 on Insecure Dir Object References](#)
- [ESAPI Access Reference Map API](#)
- [ESAPI Access Control API](#) (Ver `isAuthorizedForData()`, `isAuthorizedForFile()`, `isAuthorizedForFunction()`)

Para requisitos adicionales en controles de acceso, consultar la [sección de requisitos sobre Control de Acceso de ASVS \(V4\)](#).

Externas

- [CWE Entry 639 on Insecure Direct Object References](#)
- [CWE Entry 22 on Path Traversal](#) (que es un ejemplo de ataque de referencia a un objeto directo)