

Seguridad en la Red Informática Mundial

Top-Ten Vulnerabilidades según OWASP

Semana 15 clases 29 y 30

Mtra. María Noemí Araiza Ramírez

Top-Ten Vulnerabilidades según OWASP



Objetivos:

¿Qué es OWASP Top 10?

¿Qué objetivos y motivaciones tiene?

¿Qué ha cambiado de 2013 a 2017?

¿Qué son los Riesgos de Seguridad de Aplicaciones?

¿Conocer cómo me afectan o cuál es mi riesgo?

¿Conocer los 10 Riesgos más importantes?

OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Inyección	→	A1:2017 – Inyección
A2 – Pérdida de Autenticación y Gestión de Sesiones	→	A2:2017 – Pérdida de Autenticación y Gestión de Sesiones
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	↘	A3:2017 – Exposición de Datos Sensibles
A4 – Referencia Directa Insegura a Objetos [Unido+A7]	U	A4:2017 – Entidad Externa de XML (XXE) [NUEVO]
A5 – Configuración de Seguridad Incorrecta	↘	A5:2017 – Pérdida de Control de Acceso [Unido]
A6 – Exposición de Datos Sensibles	↗	A6:2017 – Configuración de Seguridad Incorrecta
A7 – Ausencia de Control de Acceso a las Funciones [Unido+A4]	U	A7:2017 – Secuencia de Comandos en Sitios Cruzados (XSS)
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	✗	A8:2017 – Deserialización Insegura [NUEVO, Comunidad]
A9 – Uso de Componentes con Vulnerabilidades Conocidas	→	A9:2017 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Redirecciones y reenvíos no validados	✗	A10:2017 – Registro y Monitoreo Insuficientes [NUEVO, Comunidad]

Top-Ten Vulnerabilidades según OWASP



¿Cuál es mi Riesgo?

Top 10 2013

Agente de Amenaza	Vectores de Ataque	Prevalencia de Debilidades	Detectabilidad de Debilidades	Impacto Técnico	Impacto al Negocio
Específico de la aplicación	Fácil	Difundido	Fácil	Severo	Específico de la aplicación /negocio
	Promedio	Común	Promedio	Moderado	
	Difícil	Poco Común	Difícil	Menor	

Agente de Amenaza	Explotabilidad	Prevalencia de Vulnerabilidad	Detección de Vulnerabilidad	Impacto Técnico	Impacto de Negocio
Específico de la Aplicación	Fácil 3	Difundido 3	Fácil 3	Severo 3	Específico del Negocio
	Promedio 2	Común 2	Promedio 2	Moderado 2	
	Difícil 1	Poco Común 1	Difícil 1	Mínimo 1	

Top 10 2017

A10

Redirecciones y reenvíos no válidos

Recordemos que está ubicada en la tabla de amenazas de 2013, para 2017 esta amenaza desaparece y se integra una nueva.

A10
:2017

Registro y Monitoreo Insuficientes

A10

Redirecciones y reenvíos no válidos

Las aplicaciones web frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, y utilizan datos no confiables para determinar la página de destino.

Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de phishing o malware, o utilizar reenvíos para acceder páginas no autorizadas.

A10

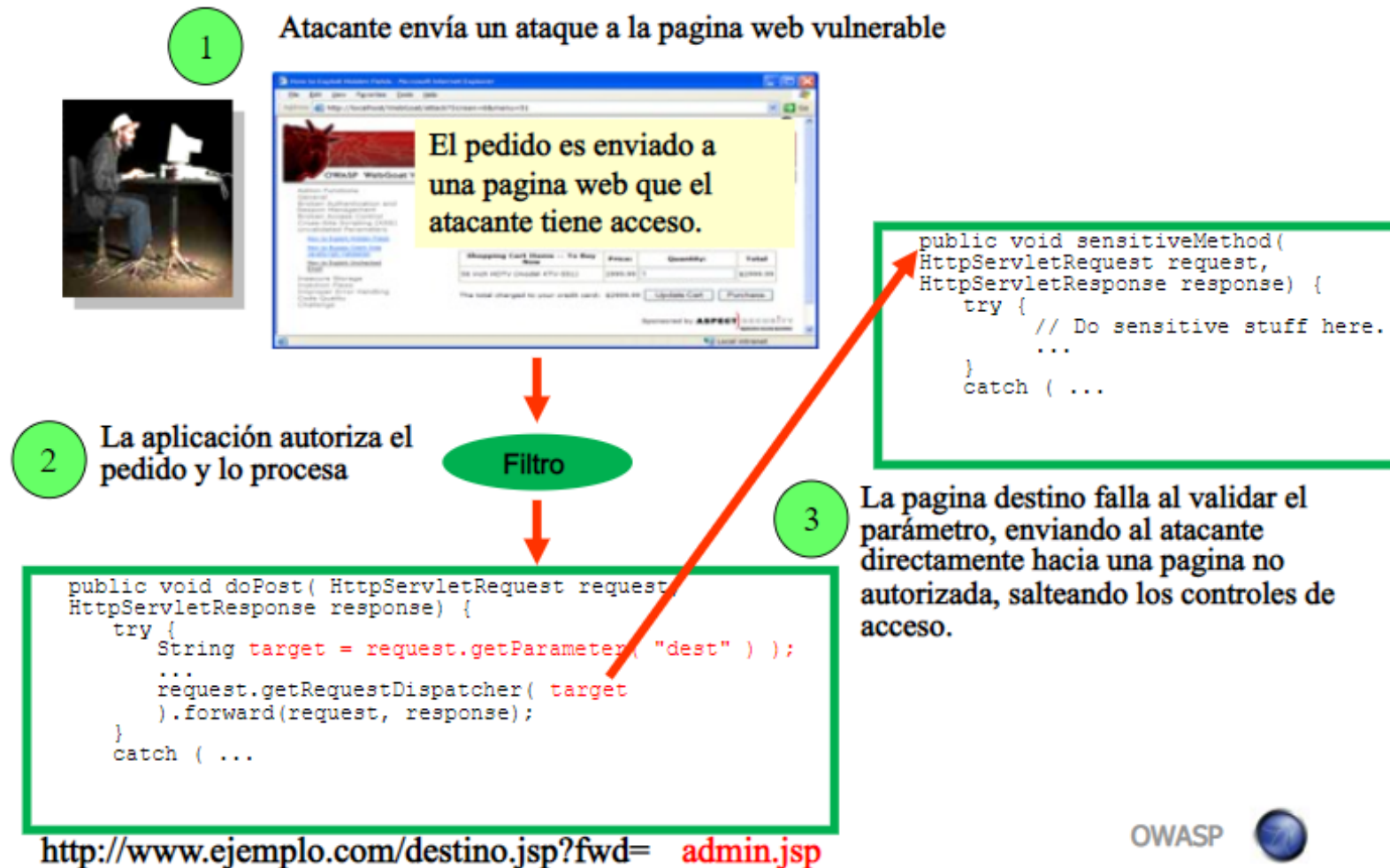
Redirecciones y reenvíos no válidos

¿Por qué se producen estas redirecciones?

Bien, no es difícil encontrar una aplicación que en determinadas ocasiones, por necesidad de la propia aplicación se realice una redirección legítima a través de un valor obtenido por un parámetro.



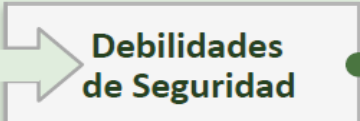


Top-Ten Vulnerabilidades según OWASP

A10 Redirecciones v reenvíos no válidos



Top-Ten Vulnerabilidades según OWASP

A10 Redirecciones y reenvíos no válidos

 <p>Agentes de Amenaza</p>	 <p>Vectores de Ataque</p>	 <p>Debilidades de Seguridad</p>		 <p>Impactos Técnicos</p>	 <p>Impactos al negocio</p>
Específico de la Aplicación	Explotabilidad PROMEDIO	Prevalencia POCO COMÚN	Detección FÁCIL	Impacto MODERADO	Específico de la Aplicación / Negocio
<p>Considere la probabilidad de que alguien pueda engañar a los usuarios a enviar una petición a su aplicación web. Cualquier aplicación o código HTML al que acceden sus usuarios podría realizar este engaño</p>	<p>Un atacante crea enlaces a redirecciones no validadas y engaña a las víctimas para que hagan clic en dichos enlaces. Las víctimas son más propensas a hacer clic sobre ellos ya que el enlace lleva a una aplicación de confianza. El atacante tiene como objetivo los destinos inseguros para evadir los controles de seguridad.</p>	<p>Con frecuencia, las aplicaciones redirigen a los usuarios a otras páginas, o utilizan destinos internos de forma similar. Algunas veces la página de destino se especifica en un parámetro no validado, permitiendo a los atacantes elegir dicha página.</p> <p>Detectar redirecciones sin validar es fácil. Se trata de buscar redirecciones donde el usuario puede establecer la dirección URL completa. Verificar reenvíos sin validar resulta más complicado ya que apuntan a páginas internas.</p>		<p>Estas redirecciones pueden intentar instalar código malicioso o engañar a las víctimas para que revelen contraseñas u otra información sensible. El uso de reenvíos inseguros puede permitir evadir el control de acceso.</p>	<p>Considere el valor de negocio de conservar la confianza de sus usuarios.</p> <p>¿Qué pasaría si sus usuarios son infectados con código malicioso?</p> <p>¿Qué ocurriría si los atacantes pudieran acceder a funciones que sólo debieran estar disponibles de forma interna?</p>

A10

Redirecciones y reenvíos no válidos

¿Soy vulnerable?

La mejor forma de averiguar si una aplicación dispone de redirecciones y re envíos no validados, es verificar que:

1. Revisar el código para detectar el uso de redirecciones o reenvíos (llamados transferencias en .NET). Para cada uso, identificar si la URL objetivo se incluye en el valor de algún parámetro. Si es así, si la URL objetivo no es validada con una lista blanca, usted es vulnerable.

A10

Redirecciones y reenvíos no válidos

¿Soy vulnerable?

2. Recorrer la aplicación para observar si genera cualquier redirección. Analizar los parámetros facilitados antes de la redirección para ver si parecen ser una URL de destino o un recurso de esa URL. Si es así, modificar la URL de destino y observar si la aplicación redirige al nuevo destino.
 3. Si el código no está disponible, se deben analizar todos los parámetros para ver si pudieran formar parte de una redirección o destino y modificarlos para comprobar su comportamiento.
-

A10

Redirecciones y reenvíos no válidos

¿Soy vulnerable?

Evidentemente, lo más fácil es hacer esto en tiempo de desarrollo, pero en caso de tener que solventarlo una vez desplegado el proyecto o aplicación, bastaría con hacer una revisión de código para encontrar y comprobar la validación de todas las redirecciones que permitan introducir URLs completas.

A10

Redirecciones y reenvíos no válidos

¿Cómo se puede evitar?

Puede realizarse un uso seguro de redirecciones y re envíos de varias maneras:

1. Simplemente, evitando el uso de redirecciones y reenvíos.
2. Si se utiliza, no involucrar parámetros manipulables por el usuario para definir el destino Generalmente, esto puede realizarse.
3. Si los parámetros de destino no pueden evitarse, asegúrese de que el valor facilitado es válido y autorizado para el usuario.

A10

Redirecciones y reenvíos no válidos

¿Cómo se puede evitar?

Se recomienda que el valor de cualquier parámetro de destino sea un valor de mapeo, en lugar de la dirección, o parte de la dirección, de la URL y en el código del servidor traducir dicho valor a la dirección URL de destino.

Las aplicaciones pueden utilizar ESAPI para sobrescribir el método sendRedirect y asegurarse de que todos los destinos redirigidos son seguros.

A10

Redirecciones y reenvíos no válidos

¿Cómo se puede evitar?

Evitar estos problemas resulta extremadamente importante ya que son un blanco preferido por los phishers que intentan ganarse la confianza de los usuarios.

Como mínimo se debería aplicar lo siguiente:

1. Requerir SSL para todas las páginas sensibles Las peticiones sin SSL a estas páginas deben ser redirigidas a las páginas con SSL

A10

Redirecciones y reenvíos no válidos

¿Cómo se puede evitar?

2. Establecer el atributo secure en todas las cookies sensibles.
 3. Configurar el servidor SSL para que acepte únicamente algoritmos considerados fuertes (por ejemplo, que cumpla FIPS 140-2).
 4. Verificar que el certificado sea válido, no se encuentre expirado o revocado y que se ajuste a todos los dominios utilizados por la aplicación.
 5. Conexiones a sistemas finales back end y otros sistemas también deben utilizar SSL u otras tecnologías de cifrado.
-

A10

Redirecciones y reenvíos no válidos

Ejemplos de escenarios de ataques

Escenario 1: La aplicación tiene una página llamada “redirect.jsp” que recibe un único parámetro llamado url. El atacante compone una URL maliciosa que redirige a los usuarios a una aplicación que realiza el phishing e instala código malicioso.

<http://www.example.com/redirect.jsp?url=evil.com>

A10

Redirecciones y reenvíos no válidos

Ejemplos de escenarios de ataques

Escenario 2: La aplicación utiliza reenvíos para redirigir peticiones entre distintas partes de la aplicación. Algunas páginas utilizan un parámetro para indicar dónde será dirigido el usuario si la transacción es correcta.

Entonces, el atacante compone una URL que evadirá el control de acceso de la aplicación y lo llevará a una función de administración a la que en una situación habitual no debería acceder.

<http://www.example.com/boring.jsp?fwd=admin.jsp>



Registro y Monitoreo Insuficientes

Para 2017 se integra esta amenaza dada por la comunidad.

A10
:2017

Registro y Monitoreo Insuficientes

El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permiten a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos.

Los estudios muestran que el tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de por procesos internos.

Top-Ten Vulnerabilidades según OWASP

A10
:2017

Registro y Monitoreo Insuficientes

App. Específica	Explotabilidad: 2	Prevalencia: 3	Detectabilidad: 1	Técnico: 2	¿Negocio?
<p>El registro y monitoreo insuficientes es la base de casi todos los grandes y mayores incidentes de seguridad.</p> <p>Los atacantes dependen de la falta de monitoreo y respuesta oportuna para lograr sus objetivos sin ser detectados.</p>		<p>Este punto se incluye en el Top 10 basado en la encuesta a la industria. Una estrategia para determinar si usted no posee suficiente monitoreo es examinar los registros después de las pruebas de penetración.</p> <p>Las acciones de los evaluadores deben registrarse lo suficiente como para comprender los daños que podrían haber causado.</p>		<p>Los ataques más exitosos comienzan con la exploración de vulnerabilidades. Permitir que el sondeo de vulnerabilidades continúe puede aumentar la probabilidad de una explotación exitosa. En 2016, la identificación de brechas tardó una media de 191 días, un tiempo más que suficiente para infligir daño.</p>	

A10
:2017

Registro y Monitoreo Insuficientes

¿La aplicación es vulnerable?

El registro y monitoreo insuficientes ocurren en cualquier momento:

- Eventos auditables, tales como los inicios de sesión, fallos en el inicio de sesión, y transacciones de alto valor no son registrados.
- Advertencias y errores generan registros poco claros, inadecuados o ninguno en absoluto.

A10
:2017

Registro y Monitoreo Insuficientes

¿La aplicación es vulnerable?

- Registros en aplicaciones o APIs no son monitoreados para detectar actividades sospechosas.
 - Los registros son almacenados únicamente de forma local.
 - Los umbrales de alerta y de escalamiento de respuesta no están implementados o no son eficaces.
-

A10
:2017

Registro y Monitoreo Insuficientes

¿La aplicación es vulnerable?

- Las pruebas de penetración y escaneos utilizando herramientas DAST (como OWASP ZAP) no generan alertas.
- La aplicación no logra detectar, escalar o alertar sobre ataques en tiempo real.

También es vulnerable a la fuga de información si registra y alerta eventos visibles para un usuario o un atacante.

A10
:2017

Registro y Monitoreo Insuficientes

¿Cómo se previene?

Según el riesgo de los datos almacenados o procesados por la aplicación:

- Asegúrese de que todos los errores de inicio de sesión, de control de acceso y de validación de entradas de datos del lado del servidor se pueden registrar para identificar cuentas sospechosas. Mantenerlo durante el tiempo suficiente para permitir un eventual análisis forense.

A10
:2017

Registro y Monitoreo Insuficientes

¿Cómo se previene?

- Asegúrese de que las transacciones de alto impacto tengan una pista de auditoría con controles de integridad para prevenir alteraciones o eliminaciones.
 - Asegúrese que todas las transacciones de alto valor poseen una traza de auditoría con controles de integridad que permitan detectar su modificación o borrado, tales como una base de datos con permisos de inserción únicamente u similar.
 - Establezca una monitorización y alerta efectivos de tal manera que las actividades sospechosas sean detectadas y respondidas dentro de períodos de tiempo aceptables.
-

A10
:2017

Registro y Monitoreo Insuficientes

¿Cómo se previene?

- Establezca o adopte un plan de respuesta o recuperación de incidentes.

Existen frameworks de protección de aplicaciones comerciales y de código abierto tales como OWASP AppSensor, firewalls de aplicaciones web como ModSecurity utilizando el Core Rule Set de OWASP, y software de correlación de registros con paneles personalizados y alertas.

A10
:2017

Registro y Monitoreo Insuficientes

Ejemplos de escenarios de ataques

Escenario 1: El software de un foro de código abierto es operado por un pequeño equipo que fue atacado utilizando una falla de seguridad.

Los atacantes lograron eliminar el repositorio del código fuente interno que contenía la próxima versión, y todos los contenidos del foro.

Aunque el código fuente pueda ser recuperado, la falta de monitorización, registro y alerta condujo a una brecha de seguridad peor.

A10
:2017

Registro y Monitoreo Insuficientes

Ejemplos de escenarios de ataques (Top 10 2017)

Escenario 2: Un atacante escanea usuarios utilizando contraseñas por defecto, pudiendo tomar el control de todas las cuentas utilizando esos datos.

Para todos los demás usuarios, este proceso deja solo un registro de fallo de inicio de sesión.

Luego de algunos días, esto puede repetirse con una contraseña distinta.

A10
:2017

Registro y Monitoreo Insuficientes

Ejemplos de escenarios de ataques (Top 10 2017)

Escenario 3: De acuerdo a reportes, un importante minorista tiene un sandbox de análisis de malware interno para los archivos adjuntos de correos electrónicos.

Este sandbox había detectado software potencialmente indeseable, pero nadie respondió a esta detección.

Se habían estado generando advertencias por algún tiempo antes de que la brecha de seguridad fuera detectada por un banco externo, debido a transacciones fraudulentas de tarjetas.

Próximos pasos para Desarrolladores

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Desarrolladores

Establezca y utilice procesos de seguridad repetibles y controles estándar de seguridad

En el caso de que usted sea nuevo en la seguridad de aplicaciones web o ya se encuentre familiarizado con estos riesgos, la actividad de producir una aplicación web segura o arreglar una ya existente puede ser difícil.

Hay que gestionar una gran cartera de aplicaciones, esta tarea puede resultar desalentadora.

OWASP ha producido un gran número de recursos gratuitos y abiertos, que los puede utilizar para gestionar la seguridad de las aplicaciones en su organización.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Desarrolladores

Establezca y utilice procesos de seguridad repetibles y controles estándar de seguridad

Lo anterior con la finalidad de apoyar a las organizaciones y desarrolladores a reducir los riesgos de seguridad de sus aplicaciones de un modo rentable

Algunos de los recursos que OWASP ha producido para ayudar a las organizaciones a generar aplicaciones web y APIs seguras o en su defecto a verificar la seguridad de sus aplicaciones ya existentes.

A continuación veremos estos recursos:

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Desarrolladores

Establezca y utilice procesos de seguridad repetibles y controles estándar de seguridad

Requisitos de Seguridad en Aplicaciones

Para producir aplicaciones web seguras, se debe definir qué significa “seguro” para una aplicación en particular.

OWASP recomienda utilizar el Estándar de Verificación de Seguridad en Aplicaciones de OWASP (ASVS), como una guía para ajustar los requisitos de seguridad de sus aplicaciones.

Si el servicio es externo, vea el Anexo Contrato de software seguro de OWASP.

Nota: ese anexo toma en cuenta las leyes de los EE.UU. y por lo tanto se recomienda realizar las consultas legales correspondientes a cada país antes de utilizarlo.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Desarrolladores

**Establezca y utilice procesos de seguridad repetibles y
controles estándar de seguridad**

Arquitectura
de seguridad
en
aplicaciones

Es mucho más rentable diseñar la seguridad desde el principio y en todo el SDLC que añadir seguridad a sus aplicaciones y APIs. OWASP recomienda la serie de hoja de trucos de prevención de prevención como puntos de inicio óptimos para guiarlo en el diseño seguro de aplicaciones.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Desarrolladores

Establezca y utilice procesos de seguridad repetibles y controles estándar de seguridad

Controles de Seguridad Estándar

Construir controles de seguridad fuertes y usables es difícil. Un conjunto de controles estándar de seguridad simplifican radicalmente el desarrollo de aplicaciones y APIs seguras.

Los controles proactivos de OWASP son un buen punto de inicio para desarrolladores, y muchos de los frameworks modernos incluyen controles estándares y efectivos para autorización, validación, prevención de CSRF, etc.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Desarrolladores

Establezca y utilice procesos de seguridad repetibles y controles estándar de seguridad

**Ciclo de vida
de desarrollo
seguro**

Para mejorar el proceso que su organización utiliza para crear aplicaciones y APIs, OWASP recomienda el Modelo de Garantía de la Madurez del Software (SAMM).

Este modelo ayuda a las organizaciones a formular e implementar estrategias para el software seguro, adaptado a los riesgos específicos para su negocio y organización.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Desarrolladores

Establezca y utilice procesos de seguridad repetibles y controles estándar de seguridad

Educación de la Seguridad en Aplicaciones

El proyecto educativo de OWASP proporciona material de formación para ayudar a educar a los desarrolladores en seguridad en aplicaciones web.

Para una formación práctica acerca de vulnerabilidades, pruebe los proyectos OWASP WebGoat, WebGoat.NET, OWASP NodeJS Goat, OWASP Juice Shop Project o el OWASP Broken Web Applications Project.

Para mantenerse al día, asista a una Conferencia AppSec de OWASP, entrenamientos de OWASP o a las reuniones de los capítulos locales de OWASP.

Próximos pasos para Testers

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Testers

Establecer revisiones continuas de seguridad de las aplicaciones

Construir código de modo seguro es importante. Sin embargo es crítico verificar que la seguridad que pretende construir está realmente presente, correctamente implementada, y es utilizada en todos los lugares donde se supone que debe serlo.

El objetivo de la revisión de seguridad es proveer esta evidencia. El trabajo es difícil y complejo, además, los procesos modernos de desarrollo a alta velocidad como Agile y DevOps han colocado una presión extrema en los enfoques y las herramientas tradicionales.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Testers

Establecer revisiones continuas de seguridad de las aplicaciones

Por lo tanto lo alentamos a pensar en cómo va a enfocarse en lo que es importante para su portafolio de aplicaciones, y hacerlo efectivo en términos de costo.

Por otro lado, los riesgos modernos cambian rápidamente, así que los días de escanear o hacer un test de penetración a una aplicación para encontrar vulnerabilidades una vez al año han pasado hace tiempo.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Testers

Establecer revisiones continuas de seguridad de las aplicaciones

El desarrollo moderno de software requiere revisión continua de seguridad de la aplicación a través de todo el ciclo de vida del desarrollo de software.

Debemos analizar cómo mejorar los canales de desarrollo existentes automatizando la seguridad para que no retrase el desarrollo.

Independientemente del enfoque que elija, hay que considerar el costo anual de revisar, clasificar, remediar, revisar de nuevo, y volver a poner en producción una sola aplicación, esto multiplicado por la cantidad de aplicaciones.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Testers

Establecer revisiones continuas de seguridad de las aplicaciones

Comprender el Modelo de Amenazas

Antes de comenzar la revisión, asegúrese de comprender en qué es importante emplear el tiempo.

Las prioridades vienen del Modelado de Amenazas, así que si Ud. no tiene uno, necesita crearlo antes de la revisión.

Considere usar OWASP ASVS y la Guía de Revisión OWASP como un insumo y no confíe en vendedores de herramientas para decidir qué es importante para su negocio.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Testers

Establecer revisiones continuas de seguridad de las aplicaciones

Comprender su SDLC

Su enfoque de la revisión de seguridad de aplicaciones debe ser altamente compatible con las personas, procesos y herramientas que usa en su SDLC.

Intentos de forzar pasos, flujos de autorizaciones y revisiones extra probablemente causarán fricción, serán evitados y difíciles de superar. Busque oportunidades naturales para recabar información de seguridad y retroalimente su proceso con ella.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Testers

Establecer revisiones continuas de seguridad de las aplicaciones

Estrategias de pruebas

Escoja la técnica más simple, rápida y precisa para verificar cada requerimiento.

El Marco de Trabajo de Conocimiento de Seguridad de OWASP y el Estándar de Verificación de Seguridad de Aplicaciones de OWASP (ASVS) pueden ser buenas fuentes de requerimientos de seguridad funcionales y no funcionales en la revisión y en las pruebas de integración.

Considere los recursos humanos requeridos para lidiar con falsos positivos provenientes del uso de herramientas automáticas, así como con los serios peligros de los falsos negativos.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Testers

Establecer revisiones continuas de seguridad de las aplicaciones

Lograr
cobertura y
precisión

No comience por probarlo todo. Concéntrese en lo que es importante y amplíe su programa de verificación con el tiempo.

Esto significa ampliar el conjunto de defensas y riesgos de seguridad que se prueban automáticamente, así como ampliar el conjunto de aplicaciones y APIs que se incluyen en el alcance.

El objetivo es lograr un estado en el que la seguridad esencial de todas sus aplicaciones y API se verifique continuamente

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para Testers

Establecer revisiones continuas de seguridad de las aplicaciones

Comunicar
los
mensajes
claramente

No importa que tan buena sea su revisión, no hará ninguna diferencia a menos que la comunique efectivamente.

Construya confianza mostrando que comprende cómo funciona la aplicación.

Describa claramente y sin jerga técnica como puede ser abusada e incluya un escenario de ataque para hacerlo real.

Haga una estimación realista de qué tan difícil es descubrir una vulnerabilidad y explotarla, y que tan malo podría ser.

Finalmente, distribuya los hallazgos.

Próximos pasos para las Organizaciones

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para las Organizaciones

Comenzar con su programa de seguridad en aplicaciones

La seguridad en las aplicaciones ya no es opcional, con el aumento de los ataques y las presiones de cumplimiento normativo, las organizaciones deben establecer un mecanismo eficaz para asegurar sus aplicaciones.

Por el número de líneas de código que ya están en producción, muchas organizaciones luchan para conseguir gestionar un enorme volumen de vulnerabilidades.

OWASP recomienda establecer un programa para aumentar el conocimiento y mejorar la seguridad en todo su catálogo de aplicaciones

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para las Organizaciones

Comenzar con su programa de seguridad en aplicaciones

Conseguir un nivel de seguridad adecuado requiere que diversas partes de la organización trabajen juntos de manera eficiente, incluidos los departamentos de seguridad y auditoria, desarrollo, gestión y el negocio.

Se requiere que la seguridad sea visible y medible, para que todos los involucrados puedan entender la postura de la organización en cuanto a la seguridad en aplicaciones.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para las Organizaciones

Comenzar con su programa de seguridad en aplicaciones

También es necesario centrarse en las actividades y resultados que realmente ayuden a mejorar la seguridad de la empresa mediante la reducción de riesgo de la forma más rentable posible.

Algunas de las actividades clave en la efectiva aplicación de los programas de seguridad incluyen OWASP SAMM y la Guía de OWASP de Seguridad para CISOs.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para las Organizaciones

Comenzar con su programa de seguridad en aplicaciones

Inicio

- Documentar todas las aplicaciones y sus activos de información asociados.
- Las organizaciones grandes deben considerar el uso de una Base de Datos de Gestión de la Configuración (CMDB).
- Establecer un programa de seguridad de aplicaciones e impulsar su adopción.
- Realizar un análisis de brecha de capacidades entre su organización y otras similares para definir las áreas clave de mejora y un plan de ejecución.
- Obtener la aprobación de la dirección y establecer una campaña de concienciación de seguridad en las aplicaciones para toda la organización y TI.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para las Organizaciones

Comenzar con su programa de seguridad en aplicaciones

Enfoque
basado en el
catálogo de
riesgos

- Identificar y establecer prioridades en su catalogo de aplicaciones en base al riesgo inherente asociado al negocio, guiadas por las leyes de privacidad aplicables y otras regulaciones relevantes a los activos de datos a ser protegidos.
- Establecer un modelo de calificación de riesgo común, con un conjunto consistente de factores de impacto y probabilidad, que reflejen la tolerancia al riesgo de la organización.
- Medir y priorizar de forma acorde todas las aplicaciones y APIs. Adicionar los resultados al CMDB.
- Establecer directrices para garantizar y definir los niveles de cobertura y rigor requeridos.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para las Organizaciones

Comenzar con su programa de seguridad en aplicaciones

Contar con
una base
sólida

- Establecer un conjunto de políticas y estándares que proporcionen una base de referencia de seguridad de las aplicaciones, a las cuales todo el equipo de desarrollo debe adherirse.
- Definir un conjunto de controles de seguridad reutilizables, que complementen esas políticas y estándares y proporcionen una guía en su uso en el diseño y desarrollo.
- Establecer un perfil de formación en seguridad en aplicaciones que sea un requisito, dirigido a los diferentes roles y tecnologías de desarrollo.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para las Organizaciones

Comenzar con su programa de seguridad en aplicaciones

Integrar la
Seguridad en
los procesos
existentes

- Definir actividades de implementación segura y verificación en los procesos operativos y de desarrollo existentes.
- Definir actividades como el modelado de amenazas, diseño y revisión de seguridad, revisión de código, pruebas de intrusión y remediación.
- Para tener éxito, proporcionar expertos en la materia y servicios de apoyo a los equipos de desarrollo y del proyecto.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para las Organizaciones

Comenzar con su programa de seguridad en aplicaciones

Proporcionar
visibilidad a
la gestión

- Gestionar a través de las métricas. Manejar las decisiones de mejora y provisión de recursos económicos, basándose en las métricas y el análisis de los datos capturados.
- Las métricas incluyen el seguimiento de las prácticas y actividades de seguridad, las vulnerabilidades presentes y las mitigadas, la cobertura de la aplicación, densidad de defectos por tipo y cantidad de instancias, etc.
- Analizar los datos de las actividades de implementación y verificación para buscar el origen de la causa y los patrones en las vulnerabilidades, para poder determinar mejoras estratégicas en la organización y el negocio.

Próximos pasos para los Administradores de Aplicaciones

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para los Administradores de Aplicaciones

Administrar el Ciclo de Vida Completo de la Aplicación

Las aplicaciones son algunos de los sistemas más complejos que los humanos crean y mantienen.

La administración TI para una aplicación debería ser ejecutada por especialistas en TI que sean responsables por el ciclo de vida completo de la misma.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para los Administradores de Aplicaciones

Administrar el Ciclo de Vida Completo de la Aplicación

Sugerimos la creación de un administrador para cada aplicación a los efectos de proveer una contraparte técnica al dueño de la aplicación.

El administrador se encarga de todo el ciclo de vida de la aplicación desde el punto de vista de TI, desde la recopilación de los requisitos hasta el proceso de retiro de los sistemas, que a menudo se pasa por alto.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para los Administradores de Aplicaciones

Administrar el Ciclo de Vida Completo de la Aplicación

Administración de Requisitos y Recursos

- Recolectar y negociar los requisitos de negocios para una aplicación, incluyendo confidencialidad, autenticidad, integridad y disponibilidad de todos los activos de datos y de las funciones de negocio.
- Recopilar los requerimientos técnicos incluyendo requerimientos de seguridad funcionales y no funcionales.
- Planear y negociar el presupuesto que cubre todos los aspectos de diseño, construcción, testeo y operación, incluyendo actividades de seguridad.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para los Administradores de Aplicaciones

Administrar el Ciclo de Vida Completo de la Aplicación

Solicitud de
Propuestas
(RFP) y
Contrataciones

- Negociar requisitos con desarrolladores internos y externos, incluyendo lineamientos y requerimientos de seguridad con respecto a su programa de seguridad. Por ej. SDLC, mejores prácticas.
- Evaluar el cumplimiento de todos los requerimientos técnicos, incluyendo las fases de planificación y diseño.
- Negociar todos los requerimientos técnicos incluyendo diseño, seguridad y acuerdos de nivel de servicio (SLA).
- Considerar usar plantillas y listas de comprobación, como el Anexo de Contrato de Software Seguro.

Nota: este anexo toma en cuenta las leyes de los EE.UU. y por lo tanto se recomienda realizar las consultas legales correspondientes a cada país antes de utilizarlo.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para los Administradores de Aplicaciones

Administrar el Ciclo de Vida Completo de la Aplicación

Planificación y Diseño

- Negociar la planificación y diseño con los desarrolladores, interesados internos y especialistas de seguridad.
- Definir la arquitectura de seguridad, controles y contramedidas adecuadas a las necesidades de protección y el nivel de amenazas planificado. Esto debería contar con el apoyo de especialistas en seguridad.
- Asegurar que el propietario de la aplicación acepta los riesgos remanentes o bien que provea recursos adicionales.
- En cada etapa (sprint), asegurar que se creen casos de uso con requisitos de seguridad y restricciones para requerimientos no funcionales..

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para los Administradores de Aplicaciones

Administrar el Ciclo de Vida Completo de la Aplicación

Despliegue,
Pruebas y
Puesta en
Producción

- Automatizar el despliegue seguro de la aplicación, interfaces y todo componente, incluyendo las autorizaciones requeridas.
- Probar las funciones técnicas, integración a la arquitectura de TI, y coordinar pruebas de funciones de negocio.
- Crear casos de “uso” y de “abuso” tanto desde el punto de vista netamente técnico como del negocio.
- Administrar pruebas de seguridad de acuerdo a los procesos internos, las necesidades de protección y el nivel de amenazas asumido para la aplicación.
- Poner la aplicación en operación y migrar las aplicaciones usadas previamente en caso de ser necesario.
- Actualizar toda la documentación, incluyendo la Base de Datos de Gestión de la Seguridad (CMDB) y la arquitectura de seguridad.

Top-Ten Vulnerabilidades según OWASP



Próximos pasos para los Administradores de Aplicaciones

Administrar el Ciclo de Vida Completo de la Aplicación

Operación y Gestión del cambio

- Operar incluyendo la administración de seguridad de la aplicación (por ej. administración de parches).
- Aumentar la conciencia de seguridad de los usuarios y administrar conflictos de usabilidad vs seguridad.
- Panificar y gestionar cambios, por ejemplo la migración a nuevas versiones de la aplicación u otros componentes como sistema operativo, interfaces de software y bibliotecas.
- Actualizar toda la documentación, incluyendo la Base de Datos de Gestión de la Seguridad (CMDB) y la arquitectura de seguridad.

Próximos pasos para los Administradores de Aplicaciones

Administrar el Ciclo de Vida Completo de la Aplicación

Retiro de Sistemas

- Cualquier dato requerido debe ser almacenado. Otros datos deben ser eliminados de forma segura.
- Retirar la aplicación en forma segura, incluyendo el borrado de cuentas, roles y permisos no usados.
- Establecer el estado de la aplicación a “retirada” en la CMDB.

Referencias

<https://www.owasp.org>