

Seguridad en la Red Informática Mundial

Metodología OWASP Open Web Application Security Project.

Semana 9 clases 17 y 18

Mtra. María Noemí Araiza Ramírez

Elementos de la Guía de desarrollo

Phishing

El phishing es una tergiversación donde el criminal utiliza ingeniería social para aparecer como una identidad legítima.



- Los ataques de phishing son uno de los mayores problemas para los sitios bancarios y de comercio electrónico, con el potencial de destruir los medios de subsistencia y calificaciones crediticias de un cliente.
- Hasta un 5% de los usuarios parecen ser atraídos en este tipo de ataques.





Debido a nuevas medidas de seguridad implementadas en nuestros **Servicios en Línea** y modificación de nuestra banca electrónica, es necesario seguir ciertos pasos para que sus Servicios en Línea funcionen correctamente.

Es necesario que ingrese a sus servicios en línea **SuperNet** y active nuevamente su **Dispositivo Token Santander**.

Para operar sus servicios en línea de manera normal es necesario realizar la activación y sincronización de sus Servicios en Línea.

El proceso tiene valdes de 24 horas, de lo contrario deberá acudir a su sucursal.

Ingresa a sus Servicios en Línea en el siguiente enlace para realizar el proceso.

SUPERNET

SUPERMÓVIL



Microsoft account team (account-security-noreply@account.microsoft.com)

To:



Dear User,

All Hotmail customers have been upgraded to Outlook.com. Your Hotmail Account services has expired.

Due to our new system upgrade to Outlook. In order for it to remain active follow the link Sign in Re-activate your account to Outlook. <https://account.live.com>

Thanks,
The Microsoft account team

Metodología OWASP

Elementos de la Guía de desarrollo

Phising

Pautas para evitar el problema del Phising en el desarrollo de aplicaciones Web:

- Educación del usuario.
 - Haga fácil a sus usuarios informar de estafas.
 - Informe a los clientes a través de correo electrónico de lo siguiente:
 - *Deben escribir la URL en sus navegadores para acceder su sitio.
 - *Usted nunca proporciona enlaces para que ellos hagan clic.
 - *Usted nunca preguntara por sus datos confidenciales.
 - *Y en el caso que los usuarios reciban tales mensajes, deberán comunicarse inmediatamente con usted para informar a las autoridades competentes.
-

Metodología OWASP

Elementos de la Guía de desarrollo

Phising

Pautas para evitar el problema del Phising en el desarrollo de aplicaciones Web:

- Nunca solicitar información secreta a sus clientes.
- Solucionar todos los problemas de XSS.
- No utilice ventanas emergentes.
- No utilice frames (frames ni iframes).
- Mueva su aplicación a un enlace de distancia de su página principal.
- Imponga el uso de referencias locales para imágenes y otros recursos.
- Mantenga la barra de direcciones, utilice SSL, no utilice direcciones IP



Metodología OWASP

Elementos de la Guía de desarrollo

Phishing

Pautas para evitar el problema del Phishing en el desarrollo de aplicaciones Web:

- No sea la fuente de robos de identidad.
 - Implemente protecciones dentro de su aplicación.
 - Monitorice actividad inusual en las cuentas.
 - Tome control de los nombres de dominio fraudulentos.
 - Trabaje con las autoridades competentes
 - Sea amable con su cliente cuando ocurre un ataque – él es la víctima.
-

Metodología OWASP

Elementos de la Guía de desarrollo

Pruebas de Servicios WEB

Los servicios web y SOA (Arquitectura Orientada a Servicios) son aplicaciones en expansión que están permitiendo que los negocios interoperen y crezcan a un ritmo sin precedentes.

Los clientes de servicios web generalmente no son frontales web, sino otros servidores.

Metodología OWASP

Elementos de la Guía de desarrollo

Pruebas de Servicios WEB

Los servicios web están expuestos a la red como cualquier otro servicio, pero pueden ser utilizados en HTTP, FTP, SMTP o acompañados de cualquier otro protocolo de transporte.

Las vulnerabilidades en servicios web son similares a otras vulnerabilidades como la inyección SQL, revelación de información, etc, pero también tienen vulnerabilidades de XML.

Metodología OWASP

Elementos de la Guía de desarrollo

Autenticación

La ***identificación*** es la capacidad de identificar a un usuario dentro de un sistema o aplicación.

Por ejemplo, cuando un usuario se conecta a una aplicación con un nombre de usuario y una contraseña. El sistema utiliza el nombre de usuario para identificarlo.

La ***autenticación*** es la capacidad de demostrar que un usuario es quién asegura ser.

El sistema autentica al usuario en el momento de la conexión, comprobando que la contraseña es correcta.

Metodología OWASP

Elementos de la Guía de desarrollo

Autenticación

Objetivo:

Proveer servicios de autenticación segura a las aplicaciones Web, mediante:

- Vinculando una unidad del sistema a un usuario individual mediante el uso de una credencial
 - Proveyendo controles de autenticación razonables de acuerdo al riesgo de la aplicación.
 - Denegando el acceso a atacantes que usan varios métodos para atacar el sistema de autenticación.
-

Metodología OWASP

Elementos de la Guía de desarrollo

Autenticación

Buenas prácticas:

- La autenticación es sólo tan fuerte como los procesos de administración de usuarios a los que afecte dicha autenticación.
 - Use la forma más apropiada de autenticación para su clasificación de recursos.
 - Re-autenticar al usuario para transacciones de alto valor y acceso a áreas protegidas.
 - Autenticar la transacción, no el usuario.
 - Las contraseñas son un mecanismo débil por sí sólo y no son adecuadas para sistemas de alto valor.
-

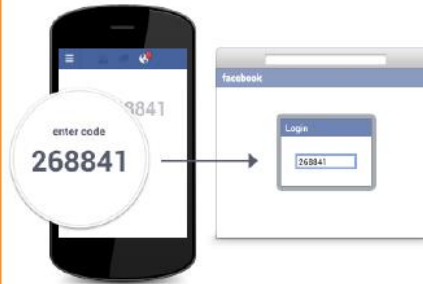
Metodología OWASP

Elementos de la Guía de desarrollo

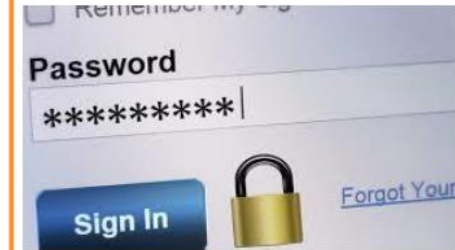
Autenticación



Lo que soy



Lo que tengo



Lo que sé

Metodología OWASP

Elementos de la Guía de desarrollo

Autenticación en aplicaciones



Elementos de la Guía de desarrollo

Autenticación en dos pasos

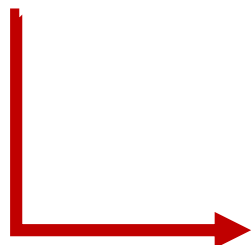
Seguridad

Cambia la contraseña y toma otras medidas para proteger más tu cuenta.



Seguridad e inicio de sesión

Cambia la contraseña y toma otras medidas para proteger más tu cuenta.



Usar autenticación en dos pasos

Usa el teléfono como una medida adicional de seguridad para evitar que otras persona...



Activado



Autenticación en dos pasos activada

Desde el 18 de septiembre de 2018

[Desactivar](#)

Seguridad adicional

Una vez que hayas ingresado la contraseña, se te pedirá un código de inicio de sesión.



Mensaje de texto

Enviaremos un código al +52 ...
*****21 para realizar la configuración.



App de autenticación

Recibirás un código de inicio de sesión a través de una app de autenticación.



Códigos de recuperación

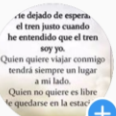
Usa estos códigos cuando

Metodología OWASP

Elementos de la Guía de desarrollo

Autenticación en dos pasos

arnoammi ▾



125197132
Publicaci...SeguidoresSeguidos

Noemi Araiza

Editar perfil

arnoammi

📁 Archivo

🕒 Tu actividad

📄 Tarjeta de identificación

🔖 Guardado

🌟 Mejores amigos

+👤 Descubrir personas

📘 Abrir Facebook

⚙️ Configuración

← Configuración

+👤 Seguir e invitar a amigos

🔔 Notificaciones

🔒 Privacidad

🛡️ Seguridad

📢 Anuncios

💳 Pagos

👤 Cuenta

❓ Ayuda

ℹ️ Información

Inicios de sesión

← Autenticación en dos pasos



Agrega seguridad adicional con la autenticación en dos pasos

Agrega protección a tu cuenta cada vez que inicies sesión en un teléfono o una computadora que no reconozcamos.

Te enviaremos un mensaje de texto con un código de inicio de sesión, o bien puedes usar la app de seguridad que elijas, como Duo Mobile o Google Authenticator.

[Más información](#)

Empezar

Metodología OWASP

Elementos de la Guía de desarrollo

Autenticación en dos pasos

← Autenticación en dos pasos

Elige un método de seguridad

Elige cómo quieres recibir el código de seguridad cuando necesitemos confirmar que eres tú quien inicia sesión. [Más información](#)

Autenticación en dos pasos

Mensaje de texto

Enviaremos un código al número que elijas.



App de autenticación

Comprobaremos si tienes una. Si no tienes ninguna, te recomendaremos una para que la descargues.



← Código de confirmación

Ingresar código

Ingresa el código de seis dígitos que enviamos al número terminado en 3521 para terminar de configurar la autenticación en dos pasos.

— — — — —

Siguiente

[Reenviar código](#) • [Cambiar número de teléfono](#)

← Código de confirmación

Ingresar código

Ingresa el código de seis dígitos que enviamos al número terminado en 3521 para terminar de configurar la autenticación en dos pasos.

0 3 4 1 2 6

Siguiente

Confirmación



Autenticación en dos pasos activada

Te pediremos un código cada vez que inicies sesión desde un teléfono o una computadora que no reconozcamos.

[Más información](#)

Listo

Ventajas

- Se aumenta mucho la seguridad de la aplicación.
- Si alguien se sabe la contraseña del usuario, no le servirá para entrar a la aplicación.
- Se puede realizar por SMS o por la versión móvil de la aplicación.

Desventajas

- El envío por SMS puede resultar costoso para el proveedor de la aplicación.
 - El usuario puede tardar en escribir el código y pensar que no funciona.
 - Si se usa el *smartphone* y se pierde, no podrá entrar a las aplicaciones.
-

Metodología OWASP

Elementos de la Guía de desarrollo

Autorización

Objetivos:

- Asegurar que únicamente usuarios autorizados puedan realizar acciones permitidas con su correspondiente nivel de privilegio.
 - Controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
 - Prevenir ataques de escalada de privilegios, como por ejemplo utilizar funciones de administrativas siendo un usuario anónimo o incluso un usuario autenticado.
-

Metodología OWASP

Elementos de la Guía de desarrollo

Autorización

Prácticas para garantizar la autorización:

- Principio de mínimo privilegio
 - Listas de Control de Acceso
 - Controles de autorización personalizados
 - Rutinas de autorización centralizadas
 - Matriz de autorización
 - Control y Protección de acceso a recursos
-

Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Sesiones

¿Qué es una Sesión?

Una sesión es una serie de comunicaciones entre un cliente y un servidor, en la que intercambia información.

El tiempo de vida de una sesión comienza cuando un usuario se conecta por primera vez a un sitio web.

Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Sesiones

La finalización de una sesión puede estar relacionada con tres circunstancias.

- 1) Cuando se abandona el sitio web
 - 2) Cuando se alcanza un tiempo de inactividad que es previamente establecido, en este caso la sesión es automáticamente eliminada
 - 3) Se ha cerrado o reiniciado el servidor
-

Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Sesiones

Aplicaciones

Comercio electrónico: En este caso una sesión permite ir eligiendo una serie de productos e irlos añadiendo a un carrito “, hasta que se finaliza la compra”

Identificación de usuarios: Donde se introduce nombre de usuario y contraseña, el usuario tendrá permisos sobre las páginas a visitar, de forma que si el usuario intenta pasar a una página sin haberse identificado, el sistema comprobará que no se ha identificado y será redireccionado a la página de identificación.

Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Sesiones

Objetivos:

- Asegurarse de que los usuarios autenticados tengan una asociación con sus sesiones robusta y criptográficamente segura.
 - Garantizar que se hagan cumplir los controles de autorización.
 - Se tienen que prevenir los típicos ataques web, tales como la reutilización, falsificación e interceptación de sesiones.
 - Autorización
-

Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Sesiones

Buenas prácticas:

- Los datos sobre autorización y roles deben ser guardados solamente del lado del servidor.
 - Los datos sobre la navegación son ciertamente aceptables en la URL siempre y cuando los controles de validación y autorización sean efectivos.
 - Las preferencias del usuario (ej. temas y lenguaje del usuario) puede ser almacenado en cookies.
 - Datos de formularios no deberían contener campos ocultos, si se encuentran ocultos, probablemente necesiten estar protegidos y sólo disponibles del lado del servidor.
-

Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Sesiones

Sin embargo, los campos ocultos pueden (y deben) ser utilizados para la protección de secuencias y ataques de Pharming.

- Los datos contenidos en formularios de varias páginas pueden ser enviados de vuelta al usuario en los siguientes dos casos:

Cuando existen controles de integridad para prevenir la manipulación.

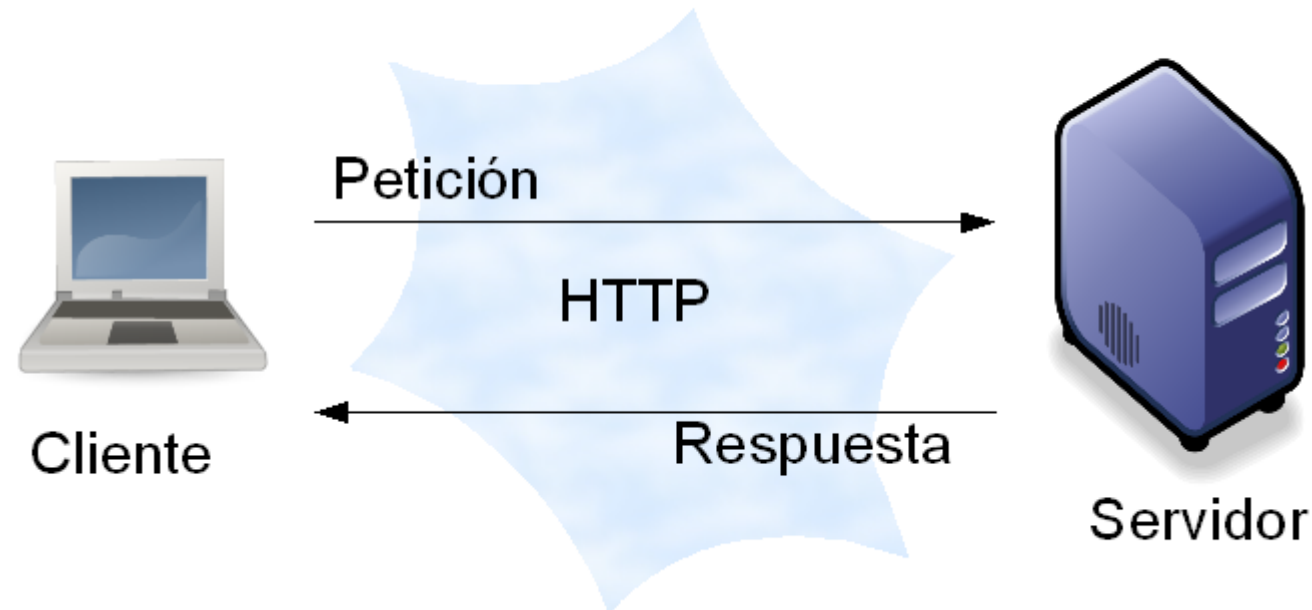
Cuando los datos son validados después de cada envío del formulario, o al menos al final del proceso de envío.

Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Sesiones (cookies)

HTTP es un protocolo sin manejo de estados Tras responder el servidor cierra de inmediato la conexión.



Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Sesiones (cookies)

El servidor almacenará la información necesaria para llevar el seguimiento de la sesión.

- Identificador de la sesión
 - Identificador del usuario en sesión
 - Tiempo de expiración de la sesión
 - Dirección donde se encuentra localizado el cliente
 - Variables asociadas a la sesión
 - Otras variables temporales
-

Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Sesiones (cookies)

Cuando se usa la interfaz HttpSession de forma interna y totalmente transparente al programador, se está haciendo uso de cookies.

Cuando a través de una página JSP se comienza una sesión, se crea un cookie llamado JSSESSIONID.

La diferencia es que esta cookie es temporal y durará el tiempo que permanezca el navegador ejecutándose, borrándose cuando el usuario cierre el navegador.

Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Sesiones (cookies)

El uso de cookies es para reconocer al usuario en el momento en el que se conecta al servidor.

Una de las páginas que recoge la petición del usuario puede comprobar si existe una cookie que ha dejado anteriormente, si la encuentra sabe que ese usuario ya ha visitado ese sitio web y por lo tanto puede leer valores que le identifiquen.



Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Sesiones (cookies)

Otro uso de las cookies es ofrecer personalización del usuario, es decir, en muchos sitios web es posible elegir color de fondo, tipo de letra, entre otros recursos.

Estos valores pueden almacenarse en cookies, de forma que cuando acceda de nuevo al sitio web, se compruebe la existencia de esos valores y recuperarlos para utilizarlos en la personalización de la página tal y como el usuario estableció en su momento.

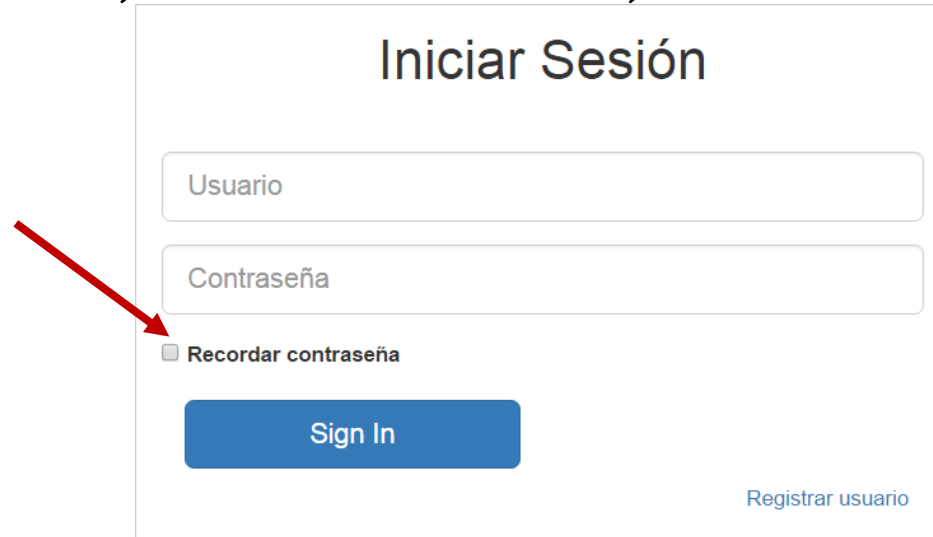


Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Sesiones (cookies)

Un ejemplo que está en varios sitios web es en el momento de realizar un registro o solicitar el alta en un área restringida por clave, en donde pueden colocar un checkbox que cuando se selecciona permite recordar el nombre de usuario, sin la contraseña, la cual debe ser tecleada por él



A diagram of a login form titled "Iniciar Sesión". It contains two input fields: "Usuario" and "Contraseña". Below the "Contraseña" field is a checkbox labeled "Recordar contraseña", which is pointed to by a red arrow. Below the checkbox is a blue "Sign In" button. At the bottom right of the form is a link that says "Registrar usuario".

Metodología OWASP

Elementos de la Guía de desarrollo

Validación de Datos

La debilidad de seguridad más común en aplicaciones web es la falta de validación apropiada de las entradas del cliente o del entorno.

Esta debilidad lleva a casi todas las principales vulnerabilidades en las aplicaciones, tales como intérprete de inyección, ataques Locale/Unicode, ataques al sistema de archivos y desbordamientos de memoria.

Nunca se debe confiar en los datos introducidos por el cliente, ya que tiene todas las posibilidades de manipular los datos.

Metodología OWASP

Elementos de la Guía de desarrollo

Validación de Datos

Objetivo

Garantizar que la aplicación sea robusta contra todas las formas de ingreso de datos, ya sea obtenida del usuario, de la infraestructura, de entidades externas o de sistemas de base de datos.

Metodología OWASP

Elementos de la Guía de desarrollo

Validación de Datos

Contramedidas:

- Revisiones de integridad:
 - ✓Aseguran que los datos no han sido manipulados y que siguen siendo los mismos.
 - ✓Las revisiones de integridad deben ser incluidas en cualquier lugar en que los datos pasen de una frontera confiable a una menos confiable.

Por ejemplo, en la aplicación al navegador del usuario en un campo oculto, o hacia un método de pago ofrecido por terceros, tal como un identificador utilizado internamente a su regreso.

Metodología OWASP

Elementos de la Guía de desarrollo

Validación de Datos

✓El tipo de control de integridad (checksum, HMAC, encriptación, firma digital) se debe seleccionar en relación directa con el riesgo que representa la transición de los datos a través de una frontera confiable.

Metodología OWASP

Elementos de la Guía de desarrollo

Validación de Datos

- Validación
 - ∞ Asegura que los datos están sólidamente escritos, con la sintaxis correcta, dentro de los límites de longitud, que contenga solo caracteres permitidos, si es numérico que tenga el signo correcto y dentro de los límites del rango.
 - ∞ La validación debe ser llevada a cabo en cada capa de la aplicación. Sin embargo, la validación debería llevarse a cabo en función del servidor que está ejecutando el código.
-

Metodología OWASP

Elementos de la Guía de desarrollo

Validación de Datos

Por ejemplo, la capa de web/presentación debe validar problemas relacionados con la web, las capas de persistencia deberían validar problemas de persistencia tales como inyección de SQL/HQL; las operaciones de búsqueda en directorio deberían revisar inyección de LDAP y así sucesivamente.

Metodología OWASP

Elementos de la Guía de desarrollo

Validación de Datos

- Validación de reglas de negocio
 - Garantizan que los datos no solamente sean validos, sino que cumplas con las reglas de negocio.
Por ejemplo, las tasas de interés entran dentro de los límites permitidos..
 - Las reglas de negocio se conocen durante el diseño e influyen durante la implementación. Sin embargo, hay enfoques malos, buenos y “mejores”.
 - Frecuentemente el mejor enfoque es el más simple en términos de código.
-

Metodología OWASP

Elementos de la Guía de desarrollo

Pruebas de Denegación de Servicio

El tipo más común de ataque de Denegación de Servicio (Dos) es del tipo empleado en una red para hacer inalcanzable a la comunicación a un servidor por parte de otros usuarios válidos.

El concepto fundamental de un ataque DoS de red es un usuario malicioso inundando con suficiente tráfico una máquina objetivo para conseguir hacerla incapaz de sostener el volumen de peticiones que recibe.

Cuando el usuario malicioso emplea un gran número de máquinas para inundar de tráfico una sola máquina objetivo, se conoce generalmente como ataque denegación de servicio distribuidos (DDoS).

Metodología OWASP

Framework de Pruebas

Describe un marco de pruebas típico que puede ser desarrollado en una Organización

Hay que verla como un marco de referencia que comprende tanto técnicas como tareas que es apropiado realizar en varias fases del ciclo de vida de desarrollo del software (SDLC)

Metodología OWASP

Framework de Pruebas OWASP

Está estructurado de la siguiente forma:

Fase 1 Antes de Empezar el Desarrollo

- 1a Revisión de Estándares y Políticas
- 1b Desarrollo de Métricas y Criterios de Medición (Asegurar la Trazabilidad)

Fase 2 Durante el Diseño y Definición

- 2a Revisión de los Requisitos de Seguridad
- 2b Diseño de una Arquitectura de Revisión
- 2c Creación y Revisión de Modelos UML
- 2d Creación y Revisión de Modelos de Amenaza

Metodología OWASP

Framework de Pruebas OWASP

Fase 3 Durante el Desarrollo

- 3a Inspección de Código por Fases
- 3b Revisiones de Código

Fase 4 Durante la Implementación

- 4a Testing de Penetración de Aplicaciones
- 4b Testing de Gestión de Configuraciones

Fase 5 Mantenimiento y Operación

- 5a Ejecución de Revisiones de la Gestión Operativa
- 5b Ejecución de Comprobaciones Periódicas de Mantenimiento
- 5c Asegurar la Verificación de Cambios

Flujo de Pruebas típico en un SDLC (Software Development Life Cycle)

Framework de Pruebas

Fase 1 Antes de Empezar el Desarrollo

Comprobar que existe un SDLC adecuado, donde la seguridad sea inherente.

Comprobar que están implementados la política y estándares de seguridad adecuados para el equipo de desarrollo.

Desarrollar las métricas y criterios de medición.

Framework de Pruebas

1a Revisión de Estándares y Políticas

- Asegurar que las políticas, documentación y estándares adecuados están implementados.
- Las personas pueden hacer las cosas correctamente, sólo si saben que es lo correcto.

1b Desarrollo de Métricas y Criterios de Medición (Asegurar la Trazabilidad)

- Antes de empezar el desarrollo, planificar el programa de medición.
 - Definir los criterios que deben medirse proporciona visibilidad de los defectos tanto en el proceso como en el producto.
-

Framework de Pruebas

Fase 2 Durante el Diseño y Definición

2a Revisión de los Requisitos de Seguridad

- Los requisitos de seguridad definen cómo funciona una aplicación desde la perspectiva de la seguridad
- Es indispensable probar los requisitos de seguridad
- Al buscar inconsistencias en los requisitos, tener en cuenta mecanismos de seguridad, como:

Gestión de Usuarios

Autenticación

Autorización

Confidencialidad de los Datos

Framework de Pruebas

Integridad

Contabilidad

Gestión de Sesiones

Seguridad de Transporte

Privacidad

2b Diseño de una Arquitectura de Revisión

- Las aplicaciones deben tener documentados su arquitectura y diseño.
 - Se deben identificar fallos de seguridad en la fase de diseño No es sólo una de las fases más efectivas por costos a la hora de identificar errores, sino que también puede ser la fase más efectiva para realizar cambios.
-

Framework de Pruebas

2c Creación y Revisión de Modelos UML

- Una vez completados el diseño y arquitectura, construye modelos UML que describan cómo funciona la aplicación
 - Emplea estos modelos para confirmar junto a los diseñadores de sistemas una comprensión exacta de cómo funciona la aplicación
 - Si se descubre alguna vulnerabilidad, debería serle transmitida al arquitecto del sistema para buscar alternativas
-

Framework de Pruebas

2d Creación y Revisión de Modelos de Amenaza

- Desarrolla escenarios de amenazas realistas
 - Analiza el diseño y la arquitectura para asegurarte que esas amenazas son mitigadas, aceptadas por negocio, o asignadas a terceros como puede ser una aseguradora)
 - Cuando las amenazas identificadas no tienen estrategias de mitigación, revisa el diseño y la arquitectura con los arquitectos de los sistemas para modificar el diseño
-

Framework de Pruebas

Fase 3 Durante el Desarrollo

3a Inspección de Código por Fases

- El equipo de seguridad debería realizar una inspección del código por fases con los desarrolladores y, en algunos casos, con los arquitectos del sistema
 - El propósito de una inspección es entender el flujo de programación a alto nivel, su esquema y la estructura del código que conforma la aplicación.
-

Framework de Pruebas

3b Revisiones de Código

- El probador puede examinar ahora el código real en busca de defectos de seguridad
 - Las revisiones de código estático validan el código contra listas de comprobación, que incluyen:
 - a) Requisitos de negocio de disponibilidad, confidencialidad e integridad
 - b) Guía del OWASP o Lista de Comprobación de los Top 10 de exposición técnica
-

Framework de Pruebas

- c) Incidencias específicas relativas al lenguaje o marco de trabajo en uso, como el Scarlet paper para PHP o las Microsoft Secure Coding checklists para ASP NET
- d) Cualquier requisito específico de la industria, como Sarbanes Oxley 404 COPPA, ISO 17799 APRA, HIPAA, Visa Merchant guidelines o cualquier otro

Framework de Pruebas

Fase 4 Durante la Implementación

4a Testing de Penetración de Aplicaciones

- Tras haber comprobado los requisitos, analizado el diseño y realizado la revisión de código, cabría esperar que se hayan identificado todas las incidencias, pero no hay que darlo por hecho!
 - El test de penetración de la aplicación después de que haya sido implementada nos proporciona una última comprobación
-

Framework de Pruebas

4b Testing de Gestión de Configuraciones

- El test de penetración de la aplicación debería incluir la comprobación de como se implementó y aseguró su infraestructura.

Aunque la aplicación puede ser segura, un pequeño detalle de la configuración podría estar en una etapa de instalación por defecto, y ser vulnerable a explotación

Ventajas	Desventajas
<ul style="list-style-type: none">•Puede ser rápida (y por lo tanto económica).•Requiere de un conjunto de habilidades relativamente inferior al requerido para revisión de código fuente.•Prueba el código que realmente se está exponiendo	<ul style="list-style-type: none">•Se realiza demasiado tarde en el SDLC.•Es solamente una prueba de impacto frontal.

Framework de Pruebas

Fase 5 Mantenimiento y Operación

5a Ejecución de Revisiones de la Gestión Operativa

- Debe existir un proceso que detalle cómo se gestiona la sección operativa de la aplicación y su infraestructura

5b Ejecución de Comprobaciones Periódicas de Mantenimiento

- Deberían realizarse comprobaciones de mantenimiento mensuales o trimestrales, sobre la aplicación e infraestructura, para asegurar que no se han introducido nuevos riesgos de seguridad y que el nivel de seguridad sigue intacto

5c Asegurar la Verificación de Cambios

- Es vital que como parte del proceso de gestión de cambios, el cambio sea comprobado para asegurar que el nivel de seguridad no haya sido afectado por dicho cambio
-

Referencias

<https://www.owasp.org>