UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Open Web Application Security Project

Seguridad en la Red Informática Mundial

Metodología OWASP
Open Web Application Security Project.

Semana 8 clases 15 y 16

Mtra. María Noemí Araiza Ramírez

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Metodología OWASP

OWASP Open Web Application Security Project

- Tiene como objetivo ofrecer una metodología:

De libre acceso y utilización.

Que pueda ser utilizada como material de referencia por parte de los arquitectos de software, desarrolladores, fabricantes y profesionales de la seguridad.

Todos ellos involucrados en el diseño, desarrollo, despliegue y verificación de la seguridad de las aplicaciones y servicios web.

Metodología OWASP

- Organizado en proyectos y capítulos locales repartidos por todo el mundo, se desarrollan documentaciones, herramientas y estándares de fuentes abiertas (GPL, GFDL, LGPL). Cualquier persona y/o patrocinador puede participar.

- Patrocinadores principales:

Metodología OWASP

- Pretende que se desarrolle mejor Software mediante:

El desarrollo de herramientas útiles para identificar los fallos y corregirlos.

La educación de los grupos involucrados, para evitar que se produzcan fallos.

El fomento de la discusión de problemas a través de una comunidad abierta.

La definición de estándares.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Metodología OWASP

OWASP Open Web Application Security Project

- Proyectos más destacados:

OWASP Top Ten Project: Representa un consenso a nivel global sobre las 10 vulnerabilidades web más importantes.

WebGoat: Herramienta destinada a la educación y que permite practicar y explotar las vulnerabilidades más frecuentes de un sitio Web, con el fin de poner en práctica una metodología de desarrollo seguro.

WebScarab: Es un framework para el análisis de aplicaciones que utilizan como base los protocolos HTTP y HTTPS. Están escrito en Java y es multiplataforma.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Metodología OWASP

OWASP Open Web Application Security Project

- Guías más relevantes:

Development Guide: Guía para la construcción de aplicaciones Web seguras, Última versión completa 2.0.1 (Español e Inglés) (julio 2005) y Versión en desarrollo v3

Code Review Guide: Guía para la revisión de código para la garantía de software seguro y Última versión 2.0 (Enero 2011)

Testing Guide: Guía y herramientas para pruebas de intrusiones y garantía de software seguro, Última versión 3.0 (diciembre 2008) y Versión en desarrollo 4.0

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Open Web Application Security Project

¿Cuándo es un sistema seguro?

Un sistema es **seguro** si cumple las **expectativas** en un **contexto dado**

La seguridad total es algo que no existe

El riesgo no puede eliminarse por completo, pero puede reducirse

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Open Web Application Security Project

¿A quién le sirve OWASP?

- Desarrolladores de aplicaciones
- *Testers* de aplicaciones
- Analistas de seguridad

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Open Web Application Security Project

- Preguntas frecuentes sobre seguridad (OWASP *FAQ*)
- Guía de Desarrollo Seguro (OWASP *Development*)
- Guía de Pruebas (OWASP *Testing Guide*)
- Guía de Revision de Codigo (OWASP *Code Review*)
- OWASP TOP-10 (Los 10 riesgos mas importantes en aplicaciones web)
- OWASP Seguridad Movil (OWASP *Mobile Security*)
- Como detectar y responder en tiempo real los ataques a aplicaciones
- Estándar de Verificación de Seguridad en Aplicaciones

Metodología OWASP

Principios básicos de la seguridad de cualquier aplicación o servicio Web

Validación de la entrada y salida de información:

- La entrada y salida de información es el principal mecanismo que dispone un atacante para enviar o recibir código malicioso contra el sistema.
- Siempre debe verificarse que cualquier dato entrante o saliente es apropiado y en el formato que se espera.
- Las características de estos datos deben estar predefinidas y debe verificarse en todas las ocasiones.

Metodología OWASP

Principios básicos de la seguridad de cualquier aplicación o servicio Web

Diseños simples:

- Los mecanismos de seguridad deben diseñarse para que sean los más sencillos posibles, huyendo de sofisticaciones que compliquen excesivamente la vida a los usuarios.
- Si los pasos necesarios para proteger de forma adecuada una función o módulo son muy complejos, la probabilidad de que estos pasos no se ejecuten de forma adecuada es muy elevada.

Metodología OWASP

Principios básicos de la seguridad de cualquier aplicación o servicio Web

Utilización y reutilización de componentes de confianza:

- Debe evitarse “reinventar la rueda” constantemente.
- Cuando exista un componente que resuelva un problema de forma correcta, lo más inteligente es utilizarlo.

Metodología OWASP

Principios básicos de la seguridad de cualquier aplicación o servicio Web

Defensa en profundidad

- Nunca confiar en que un componente realizará su función de forma permanente y ante cualquier situación.
- Hemos de disponer de los mecanismos de seguridad suficientes para que cuando un componente del sistema fallen ante un determinado evento, otros sean capaces de detectarlo.

Principios básicos de la seguridad de cualquier aplicación o servicio Web

Verificación de privilegios

- Los sistemas deben diseñarse para que funcionen con los menos privilegios posibles.
- Igualmente, es importante que los procesos únicamente dispongan de los privilegios necesarios para desarrollar su función, de forma que queden compartimentados.

Metodología OWASP

Principios básicos de la seguridad de cualquier aplicación o servicio Web

Ofrecer la mínima información

- Ante una situación de error o una validación negativa, los mecanismos de seguridad deben diseñarse para que faciliten la mínima información posible.
- De la misma forma, estos mecanismos deben estar diseñados para que una vez denegada una operación, cualquier operación posterior sea igualmente denegada.

Metodología OWASP

Principios básicos de la seguridad de cualquier aplicación o servicio Web

Otros consideraciones

- De arquitectura.
- Mecanismos de autenticación.
- Gestión de sesiones de usuario.
- Control de acceso.
- Registro de actividad.
- Consideraciones de privacidad y criptografía.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Metodología OWASP

Elementos de la Guía de desarrollo

Para garantizar el desarrollo seguro de software, la Guía de Desarrollo OWASP proporciona una pautas para salvaguardar de amenazas en las aplicaciones Web en los siguientes elementos:

- Manejo de Pagos en el Comercio Electrónico
- Phising
- Servicios Web
- Autenticación
- Autorización
- Manejo de Sesiones
- Validación de Datos
- Intérprete de Inyección

Metodología OWASP

Elementos de la Guía de desarrollo

- Manejo de Errores, Auditoria y Generación de Logs
- Sistemas de Ficheros
- Desbordamientos de Memoria
- Interfaces Administrativas
- Cifrado
- Configuración
- Mantenimiento
- Ataques de Denegación de Servicio
- Licencia de Documentación Libre de GNU
- Directivas sobre PHP

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Metodología OWASP

OWASP Open Web Application Security Project

Elementos de la Guía de desarrollo

Manejo de Pagos en el Comercio Electrónico

Objetivos

- Manejar los pagos de una manera segura y equitativa de los usuarios de sistemas de comercio electrónico.
- Minimizar el fraude de los usuarios de tarjetas en pagos no presenciales. (CNP – Card Not Present).
- Maximizar la privacidad y confianza para los usuarios de sistemas de comercio electrónico.
- Cumplir con todas las leyes locales y normas PCI (Pay Card Industry)

Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Pagos en el Comercio Electrónico

Buenas prácticas

- Procese las transacciones online inmediatamente o pase el procesamiento a una tercera parte competente.
- Nunca almacene ningún número de tarjeta de crédito (CC). Si deben almacenarse, debe seguir las directivas de PCI al pie de la letra. Se recomienda encarecidamente que no almacene datos de tarjetas de crédito.
- Si se usa un servidor compartido para su sitio, no puede cumplir con las directivas PCI. Debe tener su propia infraestructura para cumplir con las directivas PCI.

Metodología OWASP

Elementos de la Guía de desarrollo

Phising

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

- 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.

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

Phising

Pautas para evitar el problema del Phising 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.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Metodología OWASP

OWASP Open Web Application Security Project

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 solo 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

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.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Metodología OWASP

OWASP Open Web Application Security Project

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

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.

Metodología OWASP

Elementos de la Guía de desarrollo

Manejo de Sesiones

Buenas prácticas:

- Datos sobre autorización y roles deben ser guardados solamente del lado del servidor.
- 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.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Metodología OWASP

OWASP Open Web Application Security Project

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.

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 limites de longitud, que contenga solo caracteres permitidos, si es numérico que tenga el signo correcto y dentro de los limites 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 esta ejecutando el código.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Metodología OWASP

OWASP Open Web Application Security Project

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 denegocio.

  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.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Metodología OWASP

OWASP Open Web Application Security Project

Elementos de la Guía de desarrollo

Validación de Datos

Ejemplo – Escenario (Validación de reglas de negocio)

- Usted va a llenar una lista con cuentas proporcionada por el backend del sistema:
- El usuario seleccionara una cuenta, selecciona un vendedor y presiona siguiente.

Solución incorrecta: La opción seleccionar cuenta es leída directamente y proporcionada en un mensaje de regreso al sistema backend sin validar si el número de cuenta es una de las cuentas proporcionadas por sistema de backend.

Un atacante puede cambiar el código HTML de cualquier manera que elija:

La carencia de validación requiere un viaje de vuelta al backend para proveer un mensaje de error que el código de la interfaz de usuario podría fácilmente haber eliminado.

El backend puede ser incapaz de enfrentarse a la carga útil de datos que la interfaz del usuario fácilmente podría haber eliminado. Por ejemplo desbordamientos de memoria, inyección de XML o similares.

Metodología OWASP

Elementos de la Guía de desarrollo

Validación de Datos

Solución aceptable: La opción de seleccionar el parámetro cuenta se lee por el código, y comparado con la lista previamente desplegada.

```
if ( account.inList(session.getParameter('payeelstid') ) {
            backend.performTransfer(session.getParameter('payeelstid'));
}
```

Esto evita la manipulación de parámetros, pero todavía hace que el navegador haga mucho trabajo.

Metodología OWASP

Elementos de la Guía de desarrollo

Validación de Datos

La mejor solución: El código original mostraba índices <option value=”1” … > en vez de nombres de cuenta.

```
int payeeLstId = session.getParameter('payeelstid');
accountFrom = account.getAcctNumberByIndex(payeeLstId);
```

Esto no sólo es más fácil que desplegar HTML, sino que hace trivial la validación y las reglas de negocio. El campo no puede ser manipulado.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Open Web Application Security Project

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)

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Open Web Application Security Project

Framework de Pruebas de OWASP

- **Fase 3: Durante el Desarrollo**
  - 3.a: Inspección de Código por Fases
  - 3.b: Revisiones de Código
- **Fase 4: Durante la Implementación**
  - 4.a: *Testing de Penetración de Aplicaciones*
  - 4.b: *Testing de Gestión de Configuraciones*
- **Fase 5: Mantenimiento y Operación**
  - 5.a: Ejecución de Revisiones de la Gestión Operativa
  - 5.b: Ejecución de Comprobaciones Periódicas de Mantenimiento
  - 5.c: Asegurar la Verificación de Cambios
- Flujo de Pruebas típico en un SDLC

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Open Web Application Security Project

Framework de Pruebas de OWASP

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

1.a: 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*

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Open Web Application Security Project

Framework de Pruebas de OWASP

1.b: 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

Fase 2: Durante el Diseño y Definición

2.a: Revisión de los Requisitos de Seguridad

- Los requisitos de seguridad definen cómo funciona una aplicación desde la perspectiva de la seguridad

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Open Web Application Security Project

Framework de Pruebas de OWASP

- 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*
  - *Integridad*
  - *Contabilidad*
  - *Gestión de Sesiones*
  - *Seguridad de Transporte*
  - *Segregación de Sistemas en Niveles*
  - *Privacidad*

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Open Web Application Security Project

Framework de Pruebas de OWASP

2.b: 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

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Open Web Application Security Project

2.c: 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

2.d: 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