OWASP: Lista de Verificación para Intrusión en Aplicaciones Web

Versión 1.1.17

14 de Julio de 2004

Contenidos

Introducción 1
Sobre OWASP 1
Sobre Traducción 2
Sugerencias 2
Lista de verificación para pruebas de penetración. 3
Uso de la lista de verificación como Solicitud de Oferta (RFP) 3
Uso de la lista de verificación como una comparativa 4
Uso de la lista de verificación como una lista de verificación 4
Sobre el Proyecto de Pruebas de OWASP (Partes Primera y Segunda) 4
El estándar OASIS WAS 4
Diagrama de flujo de las pruebas de penetración de seguridad 6
Lista de Verificación 8
Apéndice A – Tipos de vulnerabilidades OASIS WAS 15
Indice 20

Figuras

Figura 1: Diagrama de flujo de una prueba de penetración de seguridad 7

Tablas

Tabla 1: Lista de verificación para pruebas de intrusión 8

Introducción

Las pruebas de penetración de seguridad no van a ser nunca una ciencia exacta donde pueda definirse una lista completa de todos y cada uno de los puntos a comprobar. De hecho, una prueba de penetración de seguridad es solo una técnica apropiada para comprobar la seguridad de las aplicaciones Web bajo ciertas circunstancias. Por sí mismo, una prueba de penetración de seguridad no ayuda realmente a identificar vulnerabilidades de operación o de gestión. Para más información relativa a este tipo de vulnerabilidades de operación y gestión así como aprender a verificarlas, se recomienda leer:

- El manual "Entorno para Pruebas de OWASP Parte Uno" (*OWASP Testing Framework Part One* -http://www.owasp.org), que contiene información sobre cómo construir un entorno de trabajo de pruebas y qué técnicas de verificación se deberían considerar.
- La Guía "Manejo de Riegos para los Sistemas de Tecnologías de Información" (*Risk Management Guide for Information Technology Systems)*, NIST 800-30 [1], la cual describe vulnerabilidades de operación, técnicas y de gestión.

Sobre OWASP

OWASP es una organización formada por voluntarios dedicada a generar documentación basada en conocimiento y guías de implementación, así como software que pueda utilizarse por arquitectos de sistemas, desarrolladores y profesionales de la seguridad. El trabajo de OWASP promueve y ayuda a los usuarios a crear aplicaciones Web más seguras. Para más información sobre OWASP, consulte http://www.owasp.org.

[1] http://csrc.nist.gov/publications/nistpubs/index.html#sp800-30 (Inglés) La versión revisada puede encontrarse en: http://csrc.nist.gov/publications/drafts/SP800-30-RevA-draft.pdf (Inglés)

Sobre Traducción

La traducción de este documento fue realizada por (en orden alfabético):

- Juan Carlos Calderón Rojas
- Pedro Del Real López
- Raúl Mateos Martín
- Rogelio Miguel Morrell Caballero

Adicionalmente, agradecemos el apoyo como editor a:

- Christian Efrain Maldonado Sifuentes

Sugerencias

Para proporcionar alguna sugerencia sobre esta lista de verificación, envíe un correo a testing@owasp.org con el siguiente asunto [Pen Testing Checklist Feedback] (En ingles). o a owasp-spanish@list.sourceforge.net con el asunto "Sugerencia sobre Lista de Verificación para Intrusión en Aplicaciones"

Agradecemos todas las sugerencias y comentarios. Si su sugerencia es para una nueva prueba, detalle la prueba como quiere que aparezca en la lista de verificación. Si su sugerencia es una corrección o mejora, envíe sus comentarios y el texto completo que sugiere debe ser modificado. Como OWASP es un grupo de voluntarios, cuanto más sencillos sean los cambios a realizar más rápido se incorporarán dichos cambios a nuestras revisiones.

Lista de verificación para pruebas de penetración.

Muchos seguidores de OWASP, especialmente las compañías de servicios financieros, han pedido a OWASP desarrollar una lista de verificación para que puedan utilizarla en las pruebas de penetración de seguridad. La intención de esta lista de verificación es de promover la consistencia tanto entre los equipos de pruebas internos como entre los proveedores externos. Como tal, se pretende que se utilice esta lista de verificación de diferentes modos, incluyendo:

- Solicitud de oferta (RFP)
- Comparativas
- Lista de verificación para pruebas

Esta lista de verificación proporciona las pruebas a realizar, no las técnicas a utilizar.

Uso de la lista de verificación como Solicitud de Oferta (RFP)

Algunas personas han expresado la necesidad de una lista de verificación con la cual se puedan pedir servicios a los proveedores y compañías consultoras para asegurar la consistencia, y así, poder comparar soluciones y resultados a nivel de campo. Como tal, esta lista de verificación puede ser la base de una solicitud de oferta (RFP) de servicios a un proveedor. De esta forma se pide al proveedor que realice todos los servicios enumerados en la lista de verificación.

Nota: *Si usted o su compañía desarrolla una plantilla RFP a partir de esta lista, compártala con OWASP y la comunidad. Envíela a testing@owasp.org con asunto [Testing Checklist RFP Template].*

Uso de la lista de verificación como una comparativa

Algunas personas expresaron la necesidad de una lista de verificación desde la que podrían basar sus pruebas internas y utilizar el resultado de las pruebas para desarrollar métricas. Usar la misma lista de verificación permite a los usuarios comparar diferentes aplicaciones e incluso diferentes fuentes de desarrollo a un nivel de "manzanas con manzanas".

El proyecto de seguridad en aplicaciones Web OASIS (OASIS WAS por sus siglas en inglés) http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=was (En inglés) proporcionará un conjunto de tipos de vulnerabilidades que se pueden utilizar como un esquema de clasificación, y por tanto se podrán adoptar dentro de esta lista de verificación para ayudar al usuario a ordenar la información fácilmente. Para más información, vea el estándar OASIS WAS posteriormente en este documento.

Uso de la lista de verificación como una lista de verificación

Por supuesto muchos usuarios quieren utilizar esta lista de verificación simplemente como eso, como una lista de verificación. Como tal, la lista de verificación está escrita como un conjunto de categorías a verificar. Esto no dicta las técnicas que se deberían utilizar, aunque se proporcionan ejemplos.

Sobre el Proyecto de Pruebas de OWASP (Partes Primera y Segunda)

OWASP está trabajando actualmente en un entorno de trabajo de pruebas. En el momento en el que está leyendo este documento, la Primera Parte del Entorno de Trabajo de Pruebas estará cerca de su emisión y la Segunda Parte estará en camino. La primera parte describe el porqué, qué, dónde y cómo de las pruebas de seguridad en aplicaciones Web. La segunda parte proporciona detalles técnicos sobre cómo buscar problemas específicos utilizando el análisis de código fuente y pruebas de penetración de seguridad; Por ejemplo, como encontrar fallos de inyección SQL revisando código o a través de pruebas de intrusión. Esta lista de verificación se convertirá probablemente en el apéndice a la Segunda Parte de Entorno de Trabajo de Pruebas junto con listas de verificación similares para la revisión de código fuente.

El estándar OASIS WAS

Las pruebas identificadas en esta lista no están ordenadas de acuerdo a la importancia o criticidad. Algunos miembros del equipo OWASP están trabajando en un estándar XML para desarrollar una forma de describir coherentemente las pruebas para aplicaciones Web en OASIS.

La misión de OASIS es conducir la convergencia, desarrollo y adopción de estándares de información estructurada en las áreas de comercio electrónico, servicios Web (Web services), etc. Para más información acerca de OASIS, consulte http://www.oasis-open.org(En Inglés).

Creemos que OASIS WAS se convertirá en un estándar muy importante que permitirá a los usuarios desarrollar sistemas de gestión de riesgo y vulnerabilidades, así como procesos sobre datos. Dado que este trabajo se desarrolla dentro de un conjunto de estándares oficiales, y es independiente del proveedor o de la tecnología, así como el hecho de que su longevidad puede ser garantizada, hace de OASIS WAS un estándar conveniente para basar su trabajo.

Parte del estándar OASIS WAS será un conjunto de categorías de vulnerabilidades. Estas son problemas estándar sobre vulnerabilidades, las que tendrán definiciones textuales que van a permitir al usuario construir esquemas de clasificación y glosarios uniformes. Utilizando estas categorías de vulnerabilidad, los usuarios podrán crear presentaciones de datos útiles sobre sus datos de vulnerabilidad.

El estándar OASIS WAS XL se publicará en Agosto de 2004. Los tipos de vulnerabilidades WAS serán publicados en un borrador separado a finales de Abril de 2005. De esta forma esta lista de verificación podría cambiar cuando el estándar sea ratificado, aunque esto es improbable.

Dado que creemos que las categorías de vulnerabilidad WAS en el futuro se van a convertir en parte integral de la gestión de vulnerabilidades de las aplicaciones, será integrado debidamente a todo el trabajo en OWASP tal como esta lista de verificación o el entorno de trabajo de pruebas.

Diagrama de flujo de las pruebas de penetración de seguridad

Evidentemente, al promover una lista de verificación estamos promoviendo pruebas metódicas y repetibles.

Mientras que está fuera del alcance de esta lista prescribir una metodología de pruebas de intrusión (esto será presentado en la segunda parte del Proyecto de Pruebas de OWASP), se ha incluido un diagrama de flujo del modelo de pruebas, el cual se muestra en la Figura 1. El examinador podría encontrar útil el diagrama de flujo cuando se utilicen las pruebas técnicas descritas en este documento. Es importante apuntar que una prueba de intrusión a nivel de infraestructura debería ser realizada previamente a la prueba de la aplicación. En algunos casos, el sistema operativo del servidor puede ser explotado y puede dar al examinador mayor tracción en la explotación de la aplicación Web.

El diagrama de flujo de la Figura 1 se basa en varios pasos:

1. La prueba de penetración de seguridad se inicia recopilando toda la posible información relativa a la infraestructura y las aplicaciones involucradas. Este paso es fundamental, ya que sin un conocimiento sólido de la tecnología subyacente, podrían omitirse algunas pruebas durante la fase de pruebas.
2. La prueba debería seguir todas las diferentes fases mostradas en la Figura 1.
3. Los examinadores deberían intentar explotar todas las vulnerabilidades descubiertas. Aún cuando la explotación falle, el examinador obtendría un mayor conocimiento del riesgo de la vulnerabilidad.
4. Cualquier información obtenida verificando las vulnerabilidades (por ejemplo, errores de programación, obtención de código fuente, u otro descubrimiento de información interna) debería utilizarse para volver a evaluar el conocimiento general de la aplicación y como se ejecuta ésta.
5. Si, en cualquier punto durante la prueba, se detecta una vulnerabilidad que pueda llevar al compromiso del objetivo o pueda mostrar información crítica para el negocio, debe ponerse en contacto inmediatamente con el representante de la compañía y hacer que tome conciencia del riesgo involucrado.

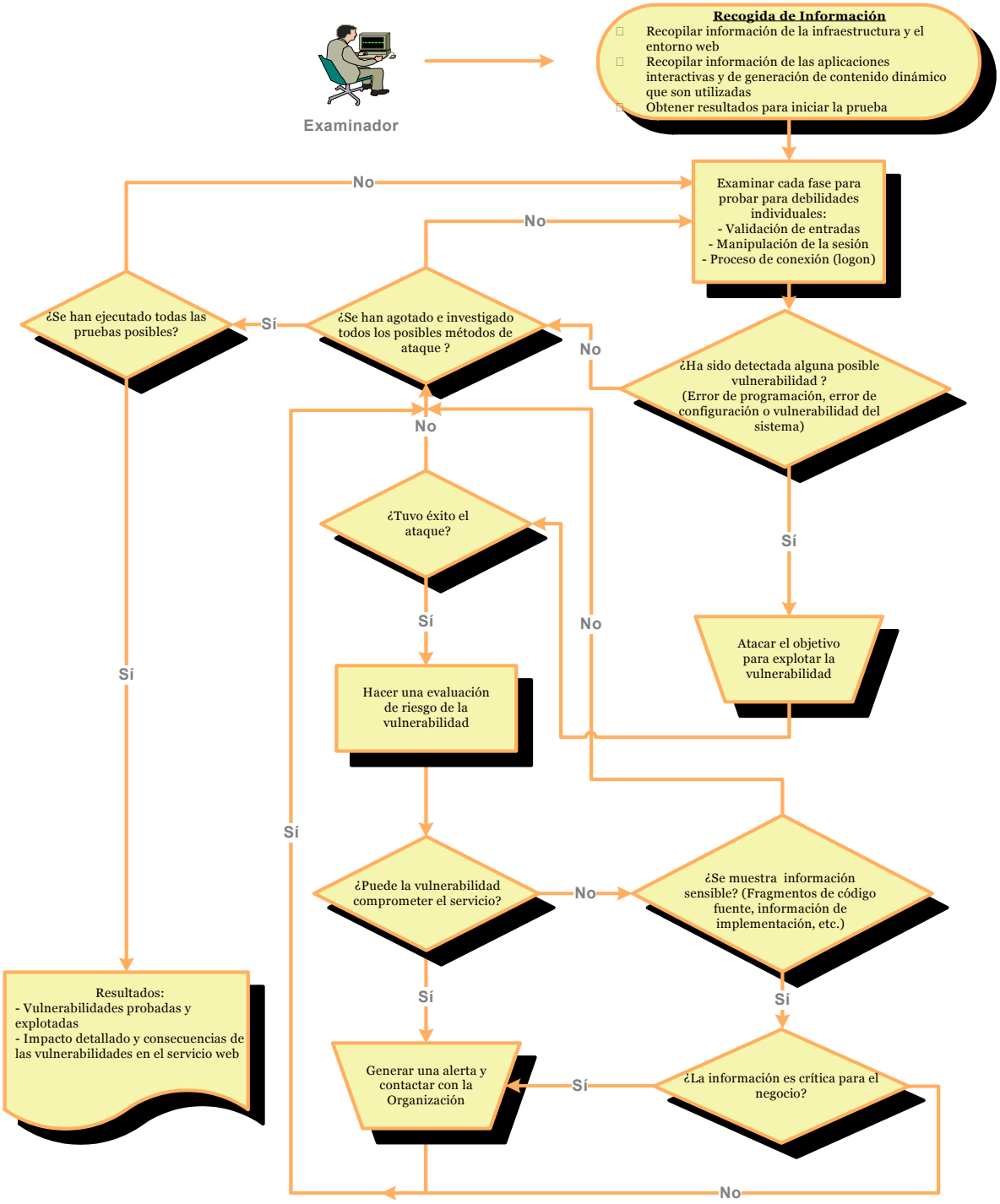

Figura 1: Diagrama de flujo de una prueba de penetración de seguridad.

Lista de Verificación

La siguiente tabla es la lista de verificación actual para pruebas de intrusión:

Tabla 1: Lista de verificación para pruebas de intrusión

Categoría	Número de ref.	Nombre	Objetivo	Notas
Negación de Servicio en Aplicaciones	OWASP-AD-001	Inundación de Aplicación	Asegúrese que la aplicación funciona correctamente cuando se presentan grandes volúmenes de peticiones, transacciones y/o tráfico de red.	**Usar varias herramientas de ofuscación para realizar esta prueba (por ej., SPIKE)**
	OWASP-AD-002	Bloqueo de aplicación	Asegúrese que la aplicación no permite a un atacante reiniciar o bloquear cuentas de usuario.	
Control de Acceso	OWASP-AC-001	Análisis de parámetros	Asegúrese que la aplicación refuerza su modelo de control de acceso asegurando que ningún parámetro disponible a un atacante proporcionará servicios adicionales.	**Típicamente esto incluye manipulación de los campos de formularios, valores en el URL, valores de scripts del lado del cliente y galletas (cookies).**
	OWASP-AC-002	Autorización	Asegúrese que los recursos que requieren autorización realicen las verificaciones de autorización adecuadas antes de ser enviadas al usuario.	
	OWASP-AC-003	Manipulación de los parámetros de autorización	Asegúrese que una vez que un usuario válido ha iniciado sesión, no sea posible cambiar el parámetro con el ID de sesión para reflejar otra cuenta de usuario.	**Por ej., número de cuenta, número de política, número de usuario, etc.**
	OWASP-AC-004	Funciones / páginas autorizadas	Verifique si es posible acceder páginas o funciones que requieren inicio de sesión (login) pero pueden ser evitada.	

Categoría	Número de ref.	Nombre	Objetivo	Notas
	OWASP-AC-005	Flujo de trabajo de la aplicación	Asegúrese que donde la aplicación requiera que el usuario realice acciones en una secuencia específica, la secuencia sea ineludible.	
Autenticación	OWASP-AUTHN-001	El punto final de la autenticación debe ser HTTPS	Asegúrese que a los usuarios se les pida dar credenciales de autenticación solo en páginas que proporcionen SSL.	**Esto asegura que el usuario sabe quien esta pidiendo sus credenciales así como a donde están siendo enviadas.**
	OWASP-AUTHN-002	Evasión de Autenticación	Asegúrese que el proceso de autenticación no puede ser evitado.	**Típicamente, esto sucede en conjunción con fallas tales como inyección SQL.**
Autenticación.usuario	OWASP-AUTHN-003	Las credenciales se transportan por un canal encriptado.	Asegúrese que los nombres de usuario y contraseñas son enviados por un canal encriptado.	**Típicamente, esto debe ser SSL.**
	OWASP-AUTHN-004	Cuentas predeterminadas	Verifique nombres de cuentas y contraseñas predeterminadas en uso.	
	OWASP-AUTHN-005	Nombre de usuario	Asegúrese que el nombre de usuario no es de información pública (o de cartera "*wallet*") tal como correo electrónico o SSN.	
	OWASP-AUTHN-006	Calidad de la contraseña	Asegúrese que la complejidad de la contraseña hace difícil adivinar las contraseñas.	

Categoría	Número de ref.	Nombre	Objetivo	Notas
	OWASP-AUTHN-007	Restauración de contraseña	Asegúrese que el usuario deba contestar a una respuesta secreta o pregunta secreta u otra información predeterminada antes de que las contraseñas puedan ser restauradas.	**Asegúrese que las contraseñas no son enviadas a los usuarios en correos electrónicos.**
	OWASP-AUTHN-008	Bloqueo de contraseñas	Asegúrese que las cuentas de usuario son bloqueadas por un período de tiempo cuando la contraseña incorrecta es ingresada por más de un número específico de veces (usualmente 5).	
	OWASP-AUTHN-009	Estructura de la contraseña	Asegúrese que los meta caracteres especiales no pueden ser usados en la contraseña.	**Puede ser útil cuando se realiza inyección de SQL.**
	OWASP-AUTHN-010	Contraseñas en blanco	Asegúrese que las contraseñas no estén en blanco.	
Autenticación. Gestión de Sesión.	OWASP-AUTHSM-001	Longitud de la ficha de sesión	Asegúrese que la ficha de sesión es de la longitud adecuada para proveer protección contra la adivinación durante una sesión autenticada.	
	OWASP-AUTHSM-002	Expiración de sesión	Asegúrese que las fichas de sesión solo son válidas para un período predeterminado después de la última solicitud del usuario.	

Categoría	Número de ref.	Nombre	Objetivo	Notas
	OWASP-AUTHSM-003	Re-utilización de sesión	Asegúrese que las fichas de sesión son cambiadas cuando el usuario se mueve de un recurso protegido por SSL a un recurso no protegido por SSL.	
	OWASP-AUTHSM-004	Eliminación de sesión	Asegúrese que la ficha de sesión es invalidada cuando el usuario sale del sistema.	
	OWASP-AUTHSM-005	Formato de la ficha de sesión	Asegúrese que la ficha de sesión es expirable y nunca es escrita en el historial del navegador o memoria rápida (caché).	
Gestión de la configuración	OWASP-CM-001	Métodos HTTP	Asegúrese que el servidor Web no soporte la habilidad de manipular recursos de Internet (por ej., PUT y DELETE).	
	OWASP-CM-002	Sitios virtuales	Trate de determinar si el sitio es virtualmente publicado.	**Si hay más sitios, podrían ser vulnerables y conducir a comprometer el servidor base.**
	OWASP-CM-003	Vulnerabilidades conocidas / Parches de seguridad	Asegúrese que las vulnerabilidades conocidas que los proveedores han parchado no están presentes.	
	OWASP-CM-004	Respaldo de archivos	Asegúrese que ningún archivo de respaldo de código fuente es accesible en la parte públicamente accesible de la aplicación.	

Categoría	Número de ref.	Nombre	Objetivo	Notas
	OWASP-CM-004	Configuración del Servidor Web	Asegúrese que los problemas de configuración comunes tales como listado de directorio y archivos de ejemplo han sido tratados.	
	OWASP-CM-005	Componentes del Servidor Web	Asegúrese que los componentes del servidor Web tales como Extensiones de Servidor Front Page o módulos Apache no introducen ninguna vulnerabilidad de seguridad.	
	OWASP-CM-006	Rutas comunes	Verifique la existencia de directorios comunes en la aplicación raíz.	**/backup & /admin pueden contener información.**
	OWASP-CM-007	Aspectos predefinidos de Lenguaje / aplicación	Por ej., peculiaridades del ambiente J2EE; Por ej., disponibilidad de snoop.jsp /*Spy.jsp y módulos cargados.	
Gestión de Configuración.Infraestructura	OWASP-CM-008	Infraestructura de las interfaces administrativas	Asegúrese que las interfaces administrativas para infraestructuras, tales como servidores Web y servidores de aplicación, no son accesibles a la Internet.	
Gestión de Configuración. Aplicación	OWASP-CM-009	Interfaces administrativas de aplicación	Asegúrese que las interfaces administrativas de las aplicaciones no son accesibles a la Internet.	

Categoría	Número de ref.	Nombre	Objetivo	Notas
Manejo de errores	OWASP-EH-001	Mensajes de error de la aplicación	Asegúrese que la aplicación no presenta mensajes de error de aplicación a un atacante que podrían ser usados en un ataque.	**Esto ocurre típicamente cuando las aplicaciones devuelven mensajes de error muy descriptivos tales como rastros de pila ("*stack*") o errores de BD.**
	OWASP-EH-002	Mensajes de error de usuario	Asegúrese que la aplicación no presenta mensajes de error de usuario a un atacante que podrían ser usados en un ataque.	**Esto típicamente ocurre cuando las aplicaciones devuelven un mensaje de error tal como "no existe el usuario" o "usuario correcto, contraseña incorrecta".**
Protección de datos	OWASP-DP-001	Datos sensibles en HTML	Asegúrese que no hay datos sensibles en el HTML (guardados en caché para el historial del navegador) que podrían conducir a un atacante a montar un ataque enfocado.	**Esto típicamente ocurre cuando los desarrolladores dejan información en comentarios HTML o la aplicación presenta nombres y direcciones en HTML.**
	OWASP-DP-002	Almacenamiento de datos	Asegúrese que los datos son protegidos para asegurar su confidencialidad e integridad, donde sea requerido.	
Protección de datos. Transporte	OWASP-DP-003	Versión SSL	Asegúrese que las versiones soportadas de SSL no tienen debilidades criptográficas.	**Típicamente, esto significa soportar solamente SSL 3 y TLS 1.0.**
	OWASP-DP-004	Métodos de intercambio de llave SSL	Asegúrese que el servidor Web no permite métodos de intercambio de llaves anónimas.	**Típicamente Diffie-Hellman anónimo (ADH por sus siglas en inglés).**

Categoría	Número de ref.	Nombre	Objetivo	Notas
	OWASP-DP-005	Algoritmos SSL	Asegúrese que los algoritmos débiles no están disponibles.	**Típicamente, algoritmos tales como RC2 y DES.**
	OWASP-DP-006	Longitud de las llaves SSL	Asegúrese que el sitio Web usa una longitud apropiada de llave.	**La mayoría de los sitios Web deben reforzar la encriptación de 128 bits.**
	OWASP-DP-007	Validez del certificado digital	Asegúrese que la aplicación usa certificados digitales válidos.	**Asegúrese que el certificado digital es válido; por ej., su firma, nombre de servidor, fecha, etc., son válidos.**
Validación de entradas	OWASP-IV-001	Inyección de scripts	Asegúrese que cualquier parte de la aplicación que permite entradas no procesa scripts como parte de la entrada.	**Caso clásico de ejecución inter-sitio (Cross Site Scripting) pero incluye también otros scripts.**
Validación de entradas.SQL	OWASP-IV-002	Inyección SQL	Asegúrese que la aplicación no procesará comandos SQL del usuario.	
Validación de entradas.SO	OWASP-IV-003	Inyección de comandos del SO	Asegúrese que las aplicaciones no procesen comandos de sistema operativo del usuario	**Esto típicamente incluye cuestiones como cruce de rutas ("*path traversal*"), sembrado de comandos de sistema ("*spawning command shells*") y funciones de SO.**
Validación de entradas LDAP	OWASP-IV-004	Inyección LDAP	Asegúrese que la aplicación no procesará comandos LDAP del usuario.	
Validación de entradas XSS	OWASP-IV-005	Ejecución inter-sitio	Asegúrese que la aplicación no guardará o reflejará código malicioso de script.	

Apéndice A – Tipos de vulnerabilidades OASIS WAS

Control de Acceso

Problemas que pueden permitir a usuarios acceder a activos o funciones a las cuales no están autorizados. Frecuentemente, no hay ningún mecanismo de control de acceso donde debería ser. Un mecanismo de control de acceso adecuado debería forzar los principios de un monitor de referencia: estos deberian ser resistentes a la manipulación y analizables.

Negación de servicio en aplicaciones

Fallas que pueden permitir a un atacante obstruir completa o parcialmente a los usuarios, el uso de una aplicación.

Negación de servicio en aplicaciones.Inundación

Usado para la negación de servicio en aplicaciones el cual involucra la saturación de un recurso limitado y compartido por todos los usuarios de la aplicación, tales como espacio en disco duro, CPU, ancho de banda de red, conexiones a base de datos o memoria.

Negación de servicio en aplicaciones.Bloqueo

Usado para la negación de servicio en aplicaciones el cual involucra el uso de un recurso o limite asignado a los usuarios, tal como cantidades de intentos fallidos, mensajes o transacciones.

Autenticación

Usado para problemas relacionados con determinar la identidad de los individuos o entidades, y la autenticidad de esa identidad.

Autenticación.Entidad

Usado para problemas con los sistemas automatizados de autenticación, tales como servicios Web, bases de datos, directorios y otros. Ejemplos incluyen almacenamiento seguro de credenciales, transporte seguro, cambio de credenciales y terminación de acceso.

Autenticación.Gestión de Sesión

Usado para problemas con la asignación, utilización, protección, modificación y terminación de identificadores de sesión. Los identificadores de sesión son como las credenciales de autenticación, aun así no son frecuentemente protegidas tan atentamente.

Autenticación.Usuario

Usado para los puntos relacionados con la identificación y autenticación de personas que puedan usar una aplicación. Problemas con nombre de usuarios, contraseñas, fichas (tokens), tarjetas inteligentes (smartcards), biometría y otras credenciales son ejemplos comunes.

Autenticación.Gestión de Usuarios

Usado para problemas relacionados con la gestión de conjuntos de usuarios, especialmente información relevante sobre la seguridad tales como los roles, privilegios, autorizaciones, grupos, números de identidad personal, números de tarjetas de crédito y otra información sensible; también, problemas con la creación de nuevos usuarios, registro, asignación de derechos, y terminación de acceso.

Desbordamiento de Pila

Fallas que pueden permitir a un atacante utilizar cadenas de caracteres formateadas para sobrescribir secciones de memoria, permitiendo cambiar los datos, cerrar inesperadamente o alterar el control del programa.

Desbordamiento de Pila.Formato

Fallas que pueden permitir a un atacante utilizar cadenas de caracteres formateadas para sobrescribir secciones de memoria, permitiendo cambiar los datos, cerrar inesperadamente o alterar el control del programa.

Desbordamiento de Pila.Memoria “Heap”

Fallas que pueden permitir a un atacante sobrescribir la memoria que es dinámicamente asignada por la aplicación.

Desbordamiento de Pila.Memoria “Stack”

Fallas que pueden permitir que un atacante escriba datos en la pila, causando que el programa caiga o transfiera el control.

Concurrencia

Usado para errores en ambientes multi-hilos que permiten que los datos sean compartidos o corrompidos. Ejemplos incluyen variables que son compartidas entre hilos y causan problemas “time-of-check-time-of-use (TOCTOU)”, patrones de singleton incorrectos y mal diseño de la cache.

Gestión de Configuración

Usado para describir problemas en la configuración de una aplicación o ambiente de aplicación.

Gestión de Configuración.Administración

Usado para problemas en los mecanismos de una aplicación que permite administración remota, tales como gestión de usuarios, administración de credenciales, gestión de base de datos y otras opciones de configuración.

Gestión de Configuración.Aplicación

Usado para describir problemas en la configuración de la aplicación, tales como mecanismos de seguridad mal configurados, programas predefinidos, código no utilizado y características habilitadas no necesarias.

Gestión de Configuración.Infraestructura

Usado para problemas con la configuración de la infraestructura de la aplicación, tales como servidores de Web y aplicación, filtros y mecanismos externos de seguridad.

Criptografía

Usado para problemas de encriptación, decriptación, firmado y verificación.

Criptografía.Algoritmo

Usado para la selección de algoritmos criptográficos, así como problemas de implementación y análisis.

Criptografía.Gestión de Llaves

Usado para asuntos de almacenamiento de certificados, fichas, revocación, almacenes de llaves, generación de llaves y otros puntos relacionados.

Protección de Datos

Usado para los puntos relacionados a la inapropiada revelación de datos.

Protección de Datos.Almacenamiento

Usado para problemas con el almacenamiento seguro de datos, incluyendo almacenamiento de credenciales, llaves y otra información sensible. Errores relacionados con los mecanismos de criptografía incluyendo fuentes pobres de aleatoriedad, mala selección de algoritmos e implementación deficiente.

Protección de Datos.Transporte

Usado para problemas relacionados a la transferencia segura de información. Frecuentemente, esto se referirá a problemas con la configuración SSL o TLS, pero pudiera incluir otros protocolos con características de seguridad.

Manejo de Errores

Usado para problemas en el manejo de errores, incluyendo impresión de rastros de pila ("stack traces") a la pantalla, mecanismos de seguridad abiertos incorrectamente, permitiendo que errores afecten la operación de la aplicación entera y revelando demasiada información acerca de una falla.

Validación de Entradas

Usado para asuntos relacionados a fallar en la validación de entradas de datos no seguras, antes de que sean enviadas a la aplicación.

Validación de Entradas.Archivos

Usado para los problemas de validación de entrada de datos donde la entrada viene de un archivo, tales como un archivo de propiedades, archivo de datos "batch", base de datos de archivo plano u otros datos basados en archivos.

Validación de Entradas.Usuario

Usado para los problemas de validación de entrada de datos donde la entrada viene de un usuario humano, tales como parámetros de llamadas HTTP, entrada de la línea de comandos y eventos de entrada en la interfaz gráfica de una aplicación.

Validación de Entradas.Red

Usado para los problemas de validación de entrada de datos donde la entrada viene de un protocolo de red, tales como los encabezados HTTP, números secuenciales y otros campos del protocolo.

Inyección

Problemas que pueden permitir a un atacante intercalar comandos en los datos y hacer que se interpreten por algún sistema al que alcancen los datos.

Inyección.HTML

Fallas que puede permitir a un atacante inyectar HTML hacia una aplicación y modificar la apariencia del HTML generado por esta aplicación. Por ejemplo, un atacante pudiera inyectar una etiqueta IMG no deseada dentro de un libro de visitas y ofender a otros usuarios.

Inyección.Comandos de SO

Fallas que pueden permitir a un atacante inyectar caracteres especiales y comandos hacia la consola de comandos del sistema operativo y modificar los comandos iniciales. El ataque pudiera intentar modificar la forma en que un programa es invocado o pudiera intentar encadenar comandos adicionales.

Inyección.LDAP

Fallas que pueden permitir a un atacante inyectar caracteres especiales y términos de búsqueda dentro de un servidor LDAP y modificar la consulta inicial.

Inyección.SQL

Fallas que pueden permitir a un atacante inyectar caracteres especiales y comandos hacia una base de datos SQL y modificar la consulta inicial. El ataque pudiera intentar cambiar el significado de la consulta o pudiera intentar de encadenar comandos adicionales.

Inyección.XSS

Fallas que pueden permitir a un atacante enviar o ejecutar un script malicioso a través de una aplicación Web. Los ataques de XSS almacenados guardan los scripts en la aplicación Web. Los ataques de XSS reflejados son rebotados de una aplicación Web en tiempo real y requieren que un usuario sea engañado a enviar una llamada conteniendo el ataque.

Monitoreo

Usado para los asuntos relacionados al monitoreo del estado de seguridad de una aplicación Web.

Monitoreo.Registro

Usados para los asuntos relacionados al registro adecuado de eventos, incluyendo lo que requiere ser registrado, como debería ser registrado, como los archivos de registros son revisados y otros asuntos relacionados a los registros.

Monitoreo.Detección

Usado para asuntos relacionados a la detección de ataques de una aplicación, cómo los ataques deben ser manejados, la información que debe ser colectada y quien deberia ser notificado.

Indice

C

comparativas
  lista de verificación, 4

D

diagrama de flujo de trabajo para pruebas de penetración, 7

F

flujo de trabajo
  pruebas de penetración, 6
flujo de trabajo para pruebas de penetración, 6

L

lista de verificación
  fundamento, 3
  usandola como lista de verificación, 4
lista de verificación como una comparativa, 4
lista de verificación para pruebas de penetracion, 3

M

marco de trabajo
  pruebas, 4
marco de trabajo para pruebas, 4

O

OASIS WAS
  estandard, 5
OWASP
  acerca de, 1
  proyecto de pruebas, 4

P

plantilla RFP, 3
proyecto de pruebas
  OWASP, 4

R

retroalimentación sobre lista de verificación, 1