Universidad Autónoma "Gabriel Rene Moreno"

INF513-SC: Tecnologia Web

Seguridad Web

Docente:
Ing. Evans Balcazar Veizaga M.Sc.

Alumno:
Mauricio Elian Delgadillo Garcia (Cod. 217015689)

Santa Cruz - Bolivia

Índice

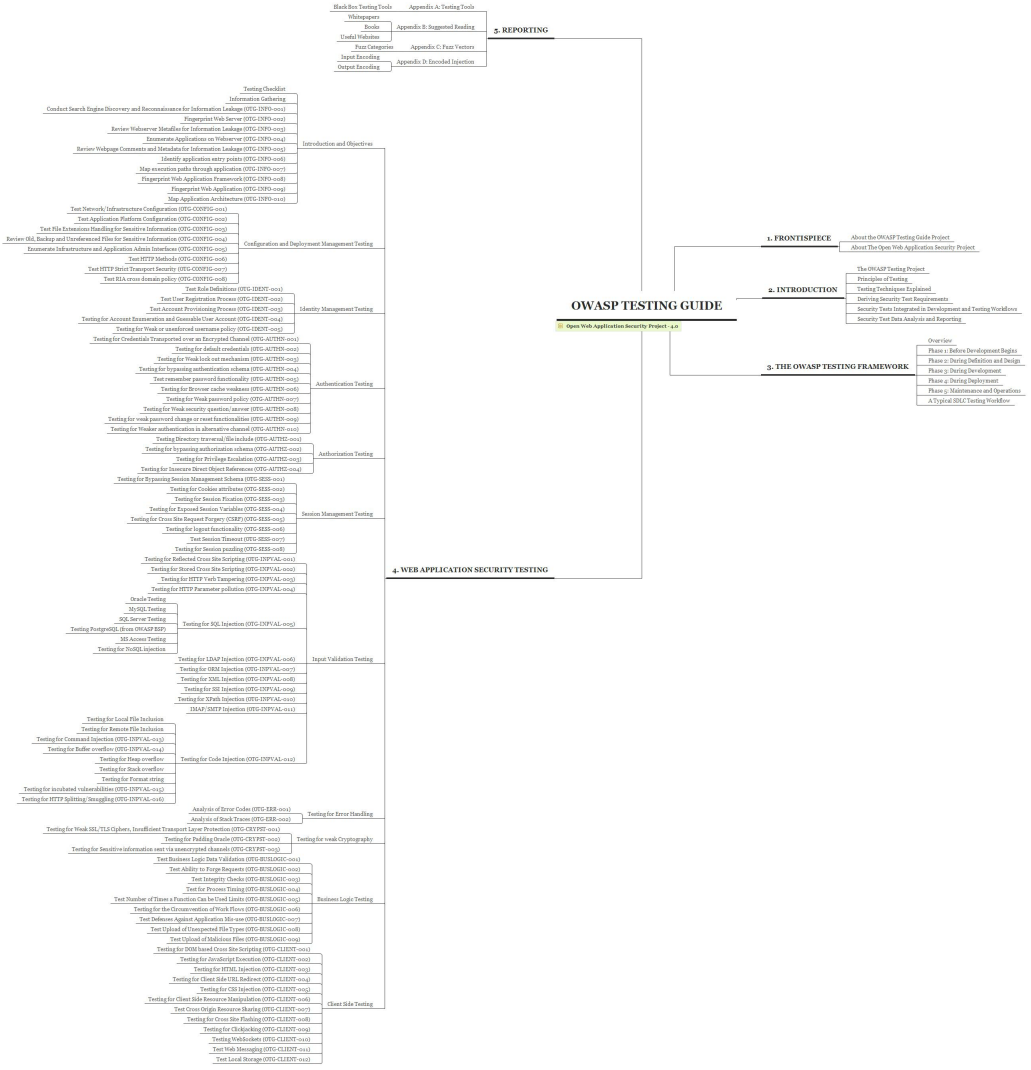
1. The OWASP Foundation

Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo mundo. Juntos constituyen una comunidad de seguridad informática que trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera.

OWASP es un nuevo tipo de entidad en el mercado de seguridad informática. Estar libre de presiones corporativas facilita que OWASP proporcione información imparcial, práctica y reedítable sobre seguridad de aplicaciones informáticas. OWASP no está afiliado a ninguna compañía tecnológica, si bien apoya el uso informado de tecnologías de seguridad. OWASP recomienda enfocar la seguridad de aplicaciones informáticas considerando todas sus dimensiones: personas, procesos y tecnologías.

Los documentos con más éxito de OWASP incluyen la Guía OWASP y el ampliamente adoptado documento de autoevaluación OWASP Top 10. Las herramientas OWASP más usadas incluyen el entorno de formación WebGoat, la herramienta de pruebas de penetración WebScarab y las utilidades de seguridad para entornos .NET OWASP DotNet. OWASP cuenta con unos 50 capítulos locales por todo el mundo y miles de participantes en las listas de correo del proyecto. OWASP ha organizado la serie de conferencias AppSec para mejorar la construcción de la comunidad de seguridad de aplicaciones web.

A continuacion una grafica que representa un mapa mental de la guia sobre el Testing



1.1. OWASP Top Ten

El OWASP Top 10 es un documento de concientización estándar para desarrolladores y seguridad de aplicaciones web. Representa un amplio consenso sobre los riesgos de seguridad más críticos para las aplicaciones web.

Las empresas deben adoptar este documento e iniciar el proceso para garantizar que sus aplicaciones web minimicen estos riesgos. Usar OWASP Top 10 es quizás el primer paso más efectivo para cambiar la cultura de desarrollo de software dentro de su organización a una que produzca un código más seguro.

1.1.1. Inyección

Las fallas de inyección, como la inyección de SQL, NoSQL, OS y LDAP, ocurren cuando se envían datos que no son de confianza a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete para que ejecute comandos no deseados o acceda a los datos sin la debida autorización.

1.1.2. Autenticación rota

Las funciones de la aplicación relacionadas con la autenticación y la administración de sesiones a menudo se implementan de manera incorrecta, lo que permite a los atacantes comprometer contraseñas, claves o tokens de sesión, o explotar otras fallas de implementación para asumir las identidades de otros usuarios de forma temporal o permanente.

1.1.3. Exposición de datos sensibles

Muchas aplicaciones web y API no protegen adecuadamente los datos confidenciales, como los financieros, la atención médica y la PII. Los atacantes pueden robar o modificar esos datos débilmente protegidos para cometer fraude con tarjetas de crédito, robo de identidad u otros delitos. Los datos confidenciales pueden verse comprometidos sin protección adicional, como el cifrado en reposo o en tránsito, y requieren precauciones especiales cuando se intercambian con el navegador.

1.1.4. Entidades externas XML (XXE)

Muchos procesadores XML más antiguos o mal configurados evalúan las referencias de entidades externas dentro de los documentos XML. Se pueden utilizar entidades externas para divulgar archivos internos mediante el controlador de URI de archivos, recursos compartidos de archivos internos, escaneo de puertos internos, ejecución remota de código y ataques de denegación de servicio.

1.1.5. Control de acceso roto

Las restricciones sobre lo que pueden hacer los usuarios autenticados a menudo no se aplican correctamente. Los atacantes pueden aprovechar estas fallas para acceder a funciones y / o datos no autorizados, como acceder a las cuentas de otros usuarios, ver archivos confidenciales, modificar los datos de otros usuarios, cambiar los derechos de acceso, etc.

1.1.6. Configuración incorrecta de seguridad

La mala configuración de seguridad es el problema más común. Esto suele ser el resultado de configuraciones predeterminadas inseguras, configuraciones incompletas o ad hoc, almacenamiento en la nube abierta, encabezados HTTP mal configurados y mensajes de error detallados que contienen información confidencial. No solo todos los sistemas operativos, marcos, bibliotecas y aplicaciones deben estar configurados de manera segura, sino que también deben ser parcheados / actualizados de manera oportuna.

1.1.7. Secuencias de comandos entre sitios (XSS)

Las fallas de XSS ocurren cuando una aplicación incluye datos que no son de confianza en una nueva página web sin la validación o el escape adecuados, o actualiza una página web existente con datos proporcionados por el usuario mediante una API de navegador que puede crear HTML o JavaScript. XSS permite a los atacantes ejecutar scripts en el navegador de la víctima que pueden secuestrar sesiones de usuario, desfigurar sitios web o redirigir al usuario a sitios maliciosos.

1.1.8. Deserialización insegura

La deserialización insegura a menudo conduce a la ejecución remota de código. Incluso si las fallas de deserialización no dan como resultado la ejecución remota de código, se pueden usar para realizar ataques, incluidos ataques de reproducción, ataques de inyección y ataques de escalada de privilegios.

1.1.9. Uso de componentes con vulnerabilidades conocidas

Los componentes, como bibliotecas, marcos y otros módulos de software, se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, dicho ataque puede facilitar la pérdida de datos o la toma de control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden socavar las defensas de las aplicaciones y permitir varios ataques e impactos.

1.1.10. Registro y monitoreo insuficientes

El registro y la supervisión insuficientes, junto con una integración faltante o ineficaz con la respuesta a incidentes, permite a los atacantes atacar aún más los sistemas, mantener la persistencia, cambiar a más sistemas y manipular, extraer o destruir datos. La mayoría de los estudios de infracciones muestran que el tiempo para detectar una infracción es de más de 200 días, generalmente detectados por partes externas en lugar de procesos internos o monitorio. [1]

2. SSL (Secure Sockets Layer)

SSL (Secure Sockets Layer) y su sucesor TLS (Transport Layer Security) son métodos utilizados para proteger y cifrar información confidencial como tarjetas de crédito, nombres de usuario, contraseñas y otros datos privados enviados a través de Internet. Páginas del sitio web aseguradas con SSL y TLS son aquellos marcados con el HTTPS en su dirección URL.[3]

Quien necesita un certificado SSL?

Cualquier cosa (incluidas personas, software, computadoras y dispositivos) que intercambien información confidencial en cualquier red, incluida Internet y la Web, debe utilizar SSL /TLS. La información confidencial incluye cosas como nombre de usuario y contraseñas, números de tarjetas de crédito o cualquier otro dato que deba mantenerse privado.[4]

¿Cómo funciona el SSL/TLS?

- Con el fin de brindar un alto nivel de privacidad, el SSL encripta los datos que se transmiten a través de la web. Esto significa que cualquiera que intente interceptar estos datos únicamente verá una mezcla confusa de caracteres que es casi imposible de descifrar.
- SSL inicia un proceso de autenticación llamado enlace entre dos dispositivos de comunicación para garantizar que ambos sean realmente quienes dicen ser.
- SSL también firma digitalmente los datos para proporcionar integridad de datos, al verificar que los datos no sean alterados antes de llegar a su destinatario.

Ha habido varias iteraciones de SSL, cada una más segura que la anterior. En 1999, SSL se actualizó para convertirse en TLS.

¿Por qué es importante el SSL/TLS?

Originalmente, los datos de la web se transmitían en texto sin formato que cualquiera podía leer si interceptaba el mensaje. Por ejemplo, si un consumidor visitaba un sitio web de compras, hacía un pedido e ingresaba su número de tarjeta de crédito en el sitio web, ese número de tarjeta de crédito se transmitía por Internet sin ser ocultado.

SSL se creó para corregir este problema y proteger la privacidad del usuario. Al

encriptar cualquier dato que se interponga entre un usuario y un servidor web, SSL garantiza que cualquiera que intercepte los datos solo podrá ver un desorden de caracteres mezclados. El número de la tarjeta de crédito del consumidor ahora está seguro y solo es visible en el sitio web de compras en el que se ingresó.

El SSL también detiene ciertos tipos de ataques cibernéticos: autentica los servidores web, lo que es importante porque los atacantes suelen crear sitios web falsos para engañar a los usuarios y robarles los datos. También evita que los atacantes manipulen los datos en tránsito, como el sello a prueba de manipulaciones de un envase de medicamentos.

¿SSL y TLS son lo mismo?

SSL es el predecesor directo de otro protocolo llamado TLS (Seguridad de la capa de transporte). En 1999, Internet Engineering Task Force (IETF) propuso una actualización de SSL. Debido a que IETF desarrollaba esta actualización y a que Netscape ya no participaba, el nombre se cambió a TLS. Las diferencias entre la versión final de SSL (3.0) y la primera versión de TLS no son significativas. El cambio de nombre se hizo para indicar el cambio de propiedad.

Debido a que están tan estrechamente relacionados, los dos términos se suelen usar de manera indistinta y se confunden. Algunas personas aún usan el término SSL para referirse a TLS, otras usan "encripción SSL/TLS"porque SSL aún es un nombre muy reconocido. ¿SSL aún está actualizado?

SSL no se ha actualizado desde la versión SSL 3.0 en 1996 y ahora se considera obsoleto. Existen varias vulnerabilidades conocidas en el protocolo SSL y los expertos en seguridad recomiendan descontinuar su uso. De hecho, la mayoría de navegadores web modernos ya no son compatibles con SSL.

TLS es el protocolo de encripción actualizado que aún se implementa en línea, aunque muchas personas aún se refieren a este como "encripción SSL". Esto podría resultar confuso para los usuarios que buscan comprar soluciones de seguridad. La verdad es que cualquier proveedor que ofrece "SSL" en estos días seguramente está ofreciendo protección TLS, que es un estándar de la industria desde hace casi veinte años. Sin embargo, como muchas personas aún buscan "protección SSL", el término aún se usa bastante en muchas páginas de productos.[2]

3. Sistema de Respaldo

Los sistemas de respaldo consisten en el resguardo de ciertas cantidades de datos digitales que están almacenados en el disco duro de una computadora, aunque también esta la protección a documentos físicos de información.

Importancia del Respaldo de Información

- Robos
- Perdida de Información
- Accidentes

3.1. Métodos para el Respaldo de la información

- **Manual:** El usuario copia los archivos que quiere respaldar por medio de comandos.
- **Automático:** Con aplicaciones especializadas donde el usuario programa los archivos que quiere guardar y este respaldo se va a ir actualizando conforme se realicen modificaciones al documento

3.2. Según Granularidad:

- Respaldo Completo: Copia la totalidad de la información, ya sea en disco, cintas, DVD, CD o cualquier medio
- Respaldo Parcial: Respaldo realiza la copia solamente de una parte de la información
- Respaldo Incremental: Realiza una copia de todos los archivos que fueron modificando o que han cambiado después del ultimo Backup
- Respaldo Diferencial: Respaldo trabaja en una forma similar que el incremental. La primera vez copia los archivos que han sido modificados desde el ultimo Backup. Luego cada vez que se vuelva a ejecutar copiara todos los datos que hayan sido modificados desde el primer Backup completo

3.3. Segun la Operatividad del Sistema:

- Respaldo frio (cold) u off-line: El sistema se detiene para realizar la copia.
- Respaldo caliente (hot) u on-line: El sistema no se detiene y la copia se realiza con el sistema en producción.[6]

3.4. Respaldo y almacenamiento en la nube

A la inversa, la copia de seguridad fuera del sitio transmite copias de datos a una ubicación remota, que puede incluir el centro de datos secundario de una empresa o la instalación de colocación arrendada. Cada vez más, la copia de seguridad de datos fuera del sitio equivale al almacenamiento en la nube basado en suscripción como un servicio, que proporciona una capacidad escalable y de bajo costo y elimina la necesidad del cliente de comprar y mantener hardware de respaldo. A pesar de su creciente popularidad, la elección de la copia de seguridad como un servicio requiere que los usuarios cifren los datos y tomen otras medidas para salvaguardar la integridad de los datos.

El respaldo en la nube se divide en lo siguiente:

1. Almacenamiento público en la nube: los usuarios envían datos a un proveedor de servicios en la nube, que les cobra una tarifa de suscripción mensual basada en el almacenamiento consumido. Hay tarifas adicionales por ingreso y egreso de datos. Amazon Web Services (AWS), Google Compute Engine y Microsoft Azure son actualmente los mayores proveedores de nube pública.

2. Almacenamiento en la nube privada: se realiza un respaldo de los datos en diferentes servidores dentro del firewall de la compañía, generalmente entre un centro de datos local y un sitio de recuperación de desastres secundario. Por esta razón, el almacenamiento en la nube privada a veces se denomina almacenamiento interno en la nube.

3. Almacenamiento híbrido en la nube: una empresa usa almacenamiento local y externo. Las empresas suelen utilizar el almacenamiento en la nube pública de forma selectiva para el archivo de datos y la retención a largo plazo. Utilizan el almacenamiento privado para el acceso local y la copia de seguridad para un acceso más rápido a sus datos más críticos.

La copia de seguridad de datos de nube a nube es un enfoque alternativo que ha ido ganando impulso. Con este método, los datos de un cliente se copian de una plataforma de copia de seguridad en la nube a otra nube. También se refiere a las copias de seguridad basadas en la nube de datos almacenados en plataformas de software como servicio (SaaS).[5]

Referencias

[1] OWASP Pagina Oficial. https://owasp.org/. 2021.

[2] Cloudfare. What is SSL. https://www.cloudflare.com/es-la/learning/ssl/what-is-ssl/. 2021.

[3] Netscape. THE SSL PROTOCOL. http://home.netscape.com/newsref/std/SSL.html. 1997.

[4] SSL.com. Informacion General. https://www.ssl.com/es/. 2021.

[5] TechTarget. Copia de seguridad o respaldo. https://searchdatacenter.techtarget.com/es/definicion/Copia-de-seguridad-o-respaldo. Septiembre, 2018.

[6] Andres Aguero Vargas. Sistemas de Respaldo. https://prezi.com/nabrjhcenryf/sistemas-de-respaldo-y-recuperacion-de-informacion/. Abril, 2015.