UNIVERSIDAD AUTÓNOMA GABRIEL RENÉ MORENO

FACULTAD DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN Y TELECOMUNICACIONES

INVESTIGACION U5: SEGURIDAD WEB

MATERIA Tecnología Web

NOMBRE Pablo Michael Tardio Ventura

CODIGO 217064957 **GRUPO** SC

FECHA 14/03/2021

DOCENTE Ing. Evans Balcázar Veizaga

CONTENIDO

INTRODUCCION

En pocas palabras, seguridad web son las medidas aplicadas para proteger una página web y garantizar que los datos no están expuestos ante los cibercriminales. En este sentido, la seguridad web es un proceso continuo y una parte esencial de administrar un sitio web

OBJETIVOS

OBJETIVO GENERAL

Investigar sobre Seguridad web en su conjunto

OBJETIVOS ESPECIFICO

Realizar la siguiente tarea

- Que es el OWASP, cite y explique cada uno.
- Que es SSL, explique.
- Que es el Sistema de Respaldo, explique.

DESARROLLO

OWASP

QUÉ ES OWASP ?

OWASP (Open Web Application Security Project), es un proyecto sin ánimo de lucro a nivel mundial que busca mejorar la seguridad del software en general. Para esto, la organización se ha provisto de una serie de herramientas y documentos que explican cuáles son las brechas de seguridad más comunes en cualquier sistema de información. Sobra decir, que todos los materiales de OWASP están disponibles de manera libre (gratuita) para su libre consulta y uso.

¿POR QUÉ ES IMPORTANTE CONOCERLO?

OWASP es una organización de talla mundial, no encontrarás un compendio de vulnerabilidades más grande que las que menciona OWASP tan bien documentadas. Muchas empresas dedicadas al desarrollo de software están conscientes de esto, por lo cual, no es nada raro que las buenas ofertas para nosotros los desarrolladores estén cargadas de un componente que incluya conocimientos en OWASP.

CUÁLES SON EXACTAMENTE SUS CONTENIDOS ?

Actualmente OWASP tiene en realidad varios proyectos en los que resaltan las categorías Tool Projects, Code Projects y Documentation Projects. El proyecto de documentación más conocido es el TOP TEN, en el cuál se listan las 10 vulnerabilidades (security risks) más habituales y cómo prevenirlas. En este top, reconocerás términos como SQL INJECTION, Cross-Site Scripting (XSS) y Broken Authentication. Sin más, te dejo con esta lista de diez riesgos de seguridad o vulnerabilidades.

PRINCIPALES 10 OWASP

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.

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.

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.

ENTIDADES EXTERNAS XML (XXE)

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

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.

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.

SECUENCIAS DE COMANDOS ENTRE SITIOS (XSS)

Los defectos 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.

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.

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.

REGISTRO Y MONITOREO INSUFICIENTES

El registro y la supervisión insuficientes, junto con una integración faltante o ineficaz con la respuesta a incidentes, permiten 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 monitoreo.

SSL

¿QUÉ ES UN CERTIFICADO SSL?

SSL es el acrónimo de Secure Sockets Layer (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal. Los dos sistemas pueden ser un servidor y un cliente (por ejemplo, un sitio web de compras y un navegador) o de servidor a servidor (por ejemplo, una aplicación con información que puede identificarse como personal o con datos de nóminas).

Esto lo lleva a cabo asegurándose de que todos los datos que se transfieren entre usuarios y sitios web o entre dos sistemas sean imposibles de leer. Utiliza algoritmos de cifrado para codificar los datos que se transmiten e impedir que los hackers los lean al enviarlos a través de la conexión. Esta información podría ser cualquier dato confidencial o personal, por ejemplo, números de tarjeta de crédito y otros datos bancarios, nombres y direcciones.

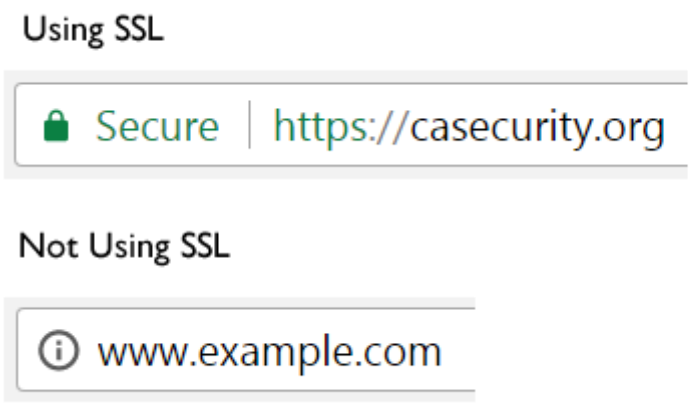
El protocolo TLS (Transport Layer Security, seguridad de la capa de transporte) es solo una versión actualizada y más segura de SSL. Si bien aún denominamos a nuestros certificados de seguridad SSL porque es un término más común, al comprar certificados SSL en DigiCert, en realidad se compran los certificados TLS más actualizados con la opción de cifrado ECC, RSA o DSA.

HTTPS (Hyper Text Transfer Protocol Secure o protocolo seguro de transferencia de hipertexto) aparece en la dirección URL cuando un sitio web está protegido por un certificado SSL. Los detalles del certificado, por ejemplo la entidad emisora y el nombre corporativo del propietario del sitio web, se pueden ver haciendo clic en el símbolo de candado de la barra del navegador.

¿CÓMO SÉ SI UN SITIO WEB ESTÁ PROTEGIDO MEDIANTE SSL?

Desde el punto de vista técnico, el protocolo SSL es un método transparente para establecer una sesión segura que requiere una intervención mínima por parte del usuario final. En el caso de los navegadores, es posible determinar si un sitio web usa SSL cuando se muestra el candado o la barra de direcciones presenta la URL como HTTPS, en lugar de HTTP.

A continuación, se muestra un ejemplo de sitio web protegido mediante SSL en Chrome 56 y otro ejemplo de sitio web no protegido.



¿POR QUÉ NECESITO LA SEGURIDAD SSL?

Son muchas las transacciones y comunicaciones que realizamos cada día a través de Internet, por lo que usar SSL es en realidad lo más lógico. El SSL es compatible con los siguientes principios de seguridad de la información:

- Cifrado: protege la transmisión de datos (p. ej., de navegador a servidor, de servidor a servidor, de aplicación a aplicación, etc.).
- Autenticación: garantiza que el servidor al que se conecta es, en efecto, el servidor correcto.
- Integridad de los datos: garantiza que los datos solicitados o enviados son realmente los datos legítimos.

El SSL puede utilizarse para proteger:

- Las transacciones mediante tarjeta de crédito a través de Internet u otros pagos a través de Internet.
- El tráfico a través de una intranet, por ejemplo, una red interna, la función de compartir archivos, las extranets o las conexiones con bases de datos.
- Los servidores de correo web, como el acceso web a Outlook o los servidores Exchange y Office Communications.
- La conexión entre un cliente de correo electrónico como Microsoft Outlook y un servidor de correo electrónico como Microsoft Exchange.
- La transferencia de archivos mediante HTTPS y los servicios de FTP, como las actualizaciones de nuevas páginas por parte del responsable del sitio web o la transferencia de archivos de gran tamaño.
- Los accesos al sistema en aplicaciones y paneles de control como Parallels, cPanel y muchos otros.
- Los procesos de trabajo y la virtualización de aplicaciones como las plataformas Citrix Delivery o las plataformas de computación basadas en la nube.
- Los accesos y la actividad en paneles de control de hosting, como Parallels o cPanel, entre otros.

SISTEMA DE RESPALDO

¿QUÉ ES UN BACKUP?

Un backup es una copia de seguridad de tu información. Éstas pueden ser periódicas o puntuales y tú decides el tipo de información que quieres copiar, ya sea en un backup online o local, para que en caso de pérdida o robo puedas recuperar los datos.

Gracias a las copias de seguridad podemos tener un plan de acción o Disaster Recovery Plan (DRP) en caso de que surja algún problema con tu servidor o sistema, para evitar la pérdida de información confidencial o datos sensibles en situaciones similares como la que te hemos puesto de ejemplo al principio.

Disponer de una copia de seguridad ayuda a reducir el tiempo de respuesta frente a incidencias y minimizar los daños y errores que éstas puedan conllevar. De esta forma, seguirás garantizando la seguridad de tu empresa y la continuidad de su actividad.

RAZONES PARA REALIZAR COPIAS DE BACKUP

Si pierdes información confidencial o datos sensibles, que no sea por la falta de copias de seguridad. Los backup son una medida muy fácil y ágil y te garantizan la recuperación de archivos o documentos perdidos o robados y gracias a ellos te evitarás infinidad de problemas. Vamos a explicarte unas cuantas razones por las que deberías implementar un sistema de respaldo automático en tu empresa.

- Recuperación de los datos y la información en caso de desastres de forma rápida y eficaz, minimizando el alcance de la incidencia.
- Detección de errores o comprobar diferencias entre las actualizaciones.
- De forma indirecta, una copia de seguridad nos da mucha información del estado de nuestro sitio y de nuestro servidor.
- Ahorro de costes y tiempo en la recuperación de información.
- Gracias a los backups automáticos y a la nube no necesitas un tiempo o espacio físico para hacer tu backup.
- Ten tu sitio web protegido frente a desastres naturales.
- Seguridad contra errores humanos, como por ejemplo equivocarse en el código que puede conllevar a la pérdida total de un sitio web.

¿CÓMO REALIZAR COPIAS DE BACKUP?

Puedes realizar copias de seguridad tanto en backups locales como en backups online. Disponer de copias de seguridad en backups locales sigue siendo una necesidad para las empresas gracias a su accesibilidad y su capacidad de restauración, que combinadas con copias de seguridad en remoto (backup online), basadas en automatización, ayudan a tener una copia de seguridad de los servidores siempre actualizada.

Actualmente, las copias de seguridad en dispositivos externos siguen siendo el método más utilizado por las empresas, a pesar de que los backup online se encuentran en pleno crecimiento. Antes de escoger un sistema de respaldo automático para tu empresa, te recordamos que existen diferentes tipos de copias de seguridad, que puedes implementar en función de tus necesidades:

- Copias de seguridad completas: Son aquellas que copian la totalidad de los archivos y carpetas seleccionados al soporte que le indiquemos para su posterior recuperación.
- Copias de seguridad diferenciales: Se trata de una copia de los datos creados y modificados a partir de la última copia de seguridad completa.
- Copias de seguridad incrementales: Es una copia de los datos creados y modificados desde la última ejecución de la copia de seguridad, tanto en copias incrementales como completas.

La periodicidad de las copias de seguridad también es importante. Realizar una copia cada hora será más efectivo, a la hora de recuperar datos, que si se realizan una vez al mes o una al año. La realización de copias de seguridad en períodos de tiempo largos puede suponer pérdida de información por el camino.

En caso de realizar copias de seguridad diarias o con mucha frecuencia, insistimos en comprobar los históricos que vamos guardando para no almacenar información redundante o ir grabando lo mismo una y otra vez. De esta manera mejorarás la eficiencia a la hora de realizar copias de seguridad y no saturarás el espacio.

BACKUP EN SERVIDORES PROPIOS VS CLOUD BACKUP. ¿CUÁL ES LA MEJOR OPCIÓN?

A continuación vamos a explicarte las ventajas del backup en servidores y el cloud backup, para que encuentres la mejor solución para ti.

VENTAJAS BACKUP EN SERVIDORES PROPIOS

SEGURIDAD PARA UNA COMPAÑÍA

La seguridad es la ventaja más destacable a la hora de contratar un servicio de copia de seguridad en servidores. La tecnología más avanzada y la monitorización las 24 horas del día, 7 días a la semana, hacen de este servicio una opción 100% recomendable.

DATOS CIFRADOS

Toda la información enviada a los servidores remotos se hace de manera cifrada para garantizar su privacidad y seguridad.

MAYOR EFICIENCIA

Cuando se implementa una copia de seguridad en servidores remotos, el espacio de almacenamiento en los servidores de la empresa se reduce de manera considerable. Mejorando así, la rapidez.

ALMACENAJE SEGURO

Al contratar un servicio de backup, ya sea en la nube o físico, una de sus grandes ventajas es que todos los datos se almacenan fuera de la propia empresa, y así se evitan los posibles robos de información y la fuga de datos.

AUTOMATIZACIÓN

Tú decides la periodicidad con la que quieres realizar copias de seguridad y éstas se harán de manera automática sin necesidad de estar pendiente, optimizando así el tiempo de hacerlo manualmente.

VENTAJAS DEL CLOUD BACKUP

REDUCE LOS RIESGOS

Apostar por un disco duro a la hora de almacenar los datos tiene grandes riesgos. Los más comunes, que el dispositivo externo se estropee o que nos lo roben. Gracias a las copias de seguridad en la nube, los datos no se graban en una ubicación física, por tanto aumentan notablemente su seguridad.

CIFRADO DE LA INFORMACIÓN

El software de backup se encarga de cifrar los datos, para así enviarlos de manera segura al servicio de almacenamiento en la nube.

ESPACIO DE ALMACENAMIENTO ILIMITADO

Los backups en la nube disponen de almacenamiento ilimitado. En la mayoría de casos, estos ofrecen planes para poder ajustarse a las necesidades de cada empresa y que sólo pagues por aquello que de verdad necesitas. No pagues por un elefante si necesitas una hormiga.

CONCLUSIONES

Se ha podido aprender acerca del uso de Jetstream y Tailwind Y poder aprender el concepto de un CRUD y su respectiva implementación en laravel y con esto poder concluir la investigación dada para la materia de Tecnología web

BIBLIOGRAFIA

1. Seguridad web: https://co.godaddy.com/blog/que-es-seguridad-en-la-web-manual-basico/
2. OWASP: https://owasp.org/www-project-top-ten/
3. SSL https://www.globalsign.com/es/ssl-information-center/what-is-ssl
4. Sistema de respaldo: https://www.esedsl.com/blog/por-que-es-importante-para-tu-empresa-tener-un-sistema-de-respaldo-automatico