SECUINFOR

Centro de Operaciones
de Ciberseguridad

#SiempreAlerta

APRENDIENDO QUE SON LOS RIESGOS DE SEGURIDAD EN APLICACIONES WEB

Autor: Christian Mendoza Bonzo

Objetivo: Instruir a Organizaciones, Gerentes, Desarrolladores, Arquitectos de seguridad; sobre las consecuencias de seguridad más importantes en aplicaciones WEB.

Fecha: Septiembre 5, 2016.

www.secuinfor.com

Cuando se habla de riesgo en aplicaciones es imposible no acudir al proyecto abierto de seguridad en aplicaciones web, esto se debe a que este proyecto si bien es de código abierto, se mantiene en constante actualización gracias a las empresas que aportan con su detallado análisis, modelamiento y categorización de las amenazas.

Dado que el software inseguro está debilitando y socavando entidades financieras, de salud, defensa, energía y otras infraestructuras críticas, como resultado de la evolución tecnológica que crece y se hace cada vez más complicada e interconectada, la dificultad por lograr aplicaciones que brinden confidencialidad, disponibilidad e integridad, que son los pilares de la seguridad, incrementa exponencialmente.

Por ende vamos a desarrollar el tema de riesgo en aplicaciones web desde el punto de vista de esta entidad.

Pero ***¿Qué son los riesgos de seguridad en aplicaciones?.*** El riesgo es un valor que nos indica qué tan probable o cercano está un evento, es decir la magnitud o probabilidad de ocurrencia de un evento, mientras las consecuencias o impacto pueden variar dependiendo de su análisis cualitativo o cuantitativo, un claro ejemplo de esto es cuando nuestra aplicación se degrada o deja de funcionar, eso puede ocasionar un perjuicio directo que puede ser cuantificado en un valor que sólo cada organización es capaz de determinar, mientras que un valor cualitativo ocurre cuando esa aplicación que dejó de funcionar por algún motivo afecta directamente a la imagen o credibilidad de la institución.

Los atacantes sin importar su motivación, pueden potencialmente usar métodos diferentes a través de una o varias aplicaciones para impactar negativamente a la organización o entidad objetivo, cada uno de estos caminos representa un riesgo posible que puede, o no, ser lo suficientemente grave como para justificar la atención de una entidad, como se ilustra a continuación:

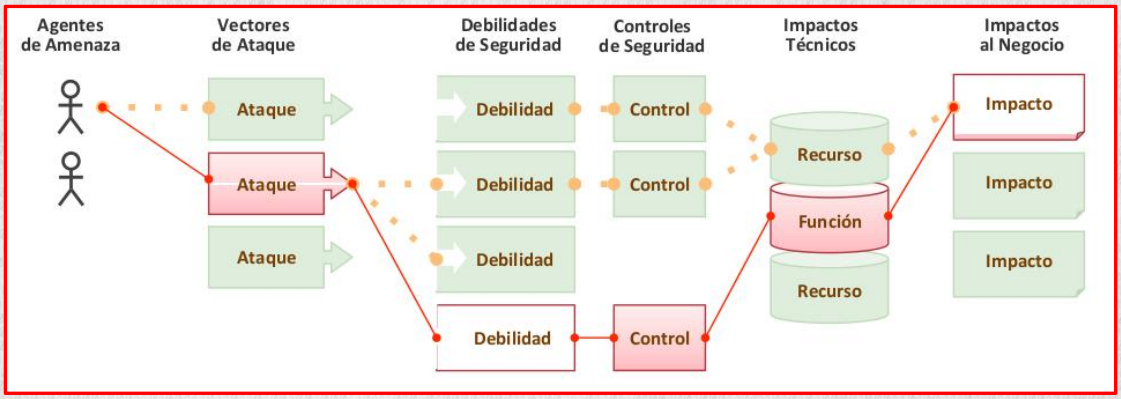

Fig 1. Riesgo de Seguridad en Aplicaciones. Copyright por: OWASP. Re-impreso con Permiso.

Sin embargo, no está demás recordar que un evento de baja probabilidad de ocurrencia pero que se ejecuta de forma recurrente o consecutiva puede tener un impacto muy alto cada vez que se logra el objetivo.

Un ejemplo pueden ser los recurrentes intentos de un usuario sin privilegios por ganar acceso a una base de datos financiera, este usuario estaría en plena capacidad de modificar o alterar los registros bancarios favoreciendo al mejor postor; como pueden darse cuenta, se trataba de una acción de baja probabilidad o leve que muchos administradores de sistemas no le prestan atención; sin embargo, la recurrencia sumada al éxito que se ha logrado, incrementa el riesgo, esto puede ocurrir cuando no se tiene identificado un óptimo control así como los mecanismos de identificación de ese riesgo.

Una inquietud que surge es ***¿Cuál es MI RIESGO? ó ¿Cómo lo identifico?***, para la identificación del nivel de riesgo revisaremos la metodología ya existente del proyecto abierto de seguridad en aplicaciones web .

Agente de Amenaza	Vectores de Ataque	Prevalencia de Debilidades	Detectabilidad de Debilidades	Impacto Técnico	Impacto al Negocio
Específico de la aplicacion	Fácil	Difundido	Fácil	Severo	Específico de la aplicación /negocio
	Promedio	Común	Promedio	Moderado	
	Difícil	Poco Común	Difícil	Menor	

Fig 2. Metodología de Evaluación de Riesgos OWASP. Copyright por: OWASP. Re-impreso con Permiso.

Cada entidad sabe los detalles específicos de su organización, para una aplicación determinada podría no existir un agente de amenaza que pueda ejecutar el ataque o el impacto técnico, podría no hacer ninguna diferencia en su negocio, por lo tanto, el oficial de riesgo de cada organización debe evaluar cada riesgo, enfocándose en los agentes de amenaza, los controles de seguridad y el impacto al negocio. En el gráfico antes descrito se menciona los ***Agentes de Amenazas*** como específicos de la aplicación mientras el ***Impacto al Negocio*** como específico de la aplicación/negocio, con el fin de indicar que estos son claramente dependientes de los detalles específicos de las aplicaciones en su empresa.

Top 10 de Riesgos de Seguridad en Aplicaciones

La clasificación que presentamos a continuación proviene del ***OWASP TOP 10 de Riesgos de Seguridad en Aplicaciones***, los cuales derivan del tipo de ataque, debilidad o el tipo de impacto que causan, dichos nombres reflejan o describen los riesgos.

A1 Inyección.- Ocurre cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta, el resultado es engañar a este intérprete para que ejecute dichos comando y así acceder a datos no autorizados.

A2 Pérdida de Autenticación y Gestión de Sesiones.- Cuando en una aplicación los mecanismos que proveen autenticación y gestión de sesiones son implementados incorrectamente, permitiendo a los atacantes comprometer contraseñas, claves, sesiones o explorar otras fallas para asumir la identidad de otros usuarios.

A3 Secuencia de Comandos en Sitios Cruzados (XSS).- Este tipo de fallas ocurren cuando datos no confiables son enviados al navegador sin una validación y codificación apropiada, puede permitir a un atacante ejecutar secuencia de comandos en el navegador de la víctima los cuales pueden secuestrar las sesiones del usuarios, destruir sitios web o dirigirlos a sitios maliciosos.

A4 Referencia Directa Insegura a Objetos.- Esta falla se presenta cuando un desarrollador expone una referencia a un objeto de implementación interno sin un control de acceso u otra protección, el atacante puede manipular estas referencias para acceder a datos no autorizados.

A5 Configuración de Seguridad Incorrecta.- Está presente por la ausencia o carencia de una configuración segura para las aplicaciones.

A6 Exposisción de datos sensibles.- Este tipo de fallas se produce por que muchas aplicaciones web no protegen adecuadamente los datos sensibles tales como: número de tarjeta de crédito, credenciales de acceso, permitiendo a los atacantes obtener y modificar tales datos para llevar a cabo fraudes informáticos.

A7 Ausencia de Control de Acceso a Funciones .- se debe a que muchas aplicaciones no verifican el control de acceso en su infraestructura, permitiendo el acceso a funciones especiales desde la misma interfaz de usuario.

A8 Falsificación de Peticiones en Sitios Cruzados (CSRF).- Esta falla permite al atacante forzar que el navegador de la víctima genere pedidos que la aplicación vulnerable considera son peticiones legítimas provenientes de la víctima.

A9 Utilización de componentes con vulnerabilidades conocidas.- La mayoría de software contiene módulos que normalmente se ejecutan con privilegios de administrador, si esto no se modifica o personaliza puede facilitar la intrusión a un atacante quien podría acceder a datos sensibles, adicionalmente es un mecanismo que debilita las defensas de la aplicación.

A10 Redirecciones y Reenvíos no válidos.- Las páginas web contienen enlaces que dirigen a los usuarios hacia otra página dentro del mismo sitio, sin una correcta validación de estas redirecciones, un atacante podría redirigir a las víctimas hacia sitios de suplantación de identidad o malware y hurtar información financiera o personal.

RECOMENDACIONES.-

Sobre aplicaciones web y cómo protegerse existen un sinnúmero de mecanismos que le permitirán salvaguardar la confidencialidad, integridad y disponibilidad de las aplicaciones así como de sus datos.

Entre los mecanismos de protección podemos destacar los siguientes puntos:

a. **Análisis y Valoración de Riesgos.-** Esto permitirá a cada organización no sólo conocer el riesgo e impacto, sino qué acciones son posibles tomar y los recursos necesarios, con lo cual ya pueden armar planes a corto, mediano y largo plazo.
b. **Análisis de código.-** Esto les permitirá revisar las vulnerabilidades en su código fuente.
c. **Pruebas de Intrusión.-** Aquí se pretende descubrir las vulnerabilidades internas y externas que se encuentran expuestas, también le permitirá descubrir posibles falencias en su arquitectura de seguridad.
d. **Aseguramiento (hardening).-** Con este tipo de servicio, se pretende proteger o minimizar el riesgo de exposición de sus activos de información, aplicaciones, datos, etc.
e. **Seguridad perimetral.-** Estos dispositivos le permitirán controlar el acceso a sus aplicaciones; dependiendo la estrategia y su ubicación deberá añadir componentes complementarios.
f. **Web Application Firewall (WAF).-** Este dispositivo les permitirá contener ataques dirigidos a sus aplicaciones web.
g. **Anti-DDoS.-** Esta herramienta es de mucha utilidad cuando las

aplicaciones web son transaccionales, dado que puede minimizar ataques de denegación de servicio contra éstas.

h. **Respaldos.-** Efectúe respaldos periódicos de todos sus sistemas.

i. **Plan de Contingencia.-** Este plan debe contener las tareas necesarias para recuperarse de un incidente serio, así como las responsabilidades de cada persona para lograrlo, es de mencionar que este plan debe ser preparado teniendo en mente el tiempo máximo de recuperación así como el punto de recuperación.

Si desea conocer cómo podemos ayudarlo a proteger su información confidencial contáctenos a:

Email: info@secuinfor.com
PBX: +593-4-3726620
Website: http://www.secuinfor.com