redeszone.net

Cuáles son los principales ataques a aplicaciones web y cómo evitarlos

8-10 minutos

Son muchas las amenazas que podemos sufrir a la hora de navegar por Internet. Hay muchos tipos de ataques, variedades de malware, técnicas que utilizan los piratas informáticas… Todo esto puede afectarnos como usuarios domésticos, poner en riesgo a una empresa u organización, así como también afectar a las páginas y aplicaciones web. Los **servidores de los sitios web** pueden sufrir muchos tipos de ataques. Vamos a explicar cuáles son los principales que pueden poner en riesgo el buen funcionamiento y la seguridad.

Ataques que pueden afectar a los servidores Web

Un servidor web es el encargado de gestionar todo el contenido de

un sitio y permitir que los usuarios finales puedan ver el contenido. Si no funciona bien, el visitante no podría entrar en la página o no vería correctamente todo. En caso de que ese servidor haya sufrido algún ataque de seguridad, no solo no funcionaría bien sino que podría incluso ser un riesgo para los visitantes. Podrían ser utilizados para robar datos, romper contraseñas, ataques de denegación de servicios…

Cross-Site Request

Lo podemos traducir al español como falsificación de solicitudes entre sitios, también conocida como ataque con un solo clic o sesión y abreviado como CSRF («sea-surf») o XSRF. Se trata de un tipo **de exploit malicioso de un sitio web** a través del cual se transmiten comandos no autorizados de un usuario en el que el sitio web confía. A diferencia de los scripts de sitios cruzados (XSS), que explota la confianza que un usuario tiene para de un sitio en particular, CSRF explota la confianza que un sitio tiene en el navegador de un usuario.

De esta forma, el atacante es capaz de realizar una acción en nombre de la víctima. Es, básicamente, como si lo estuviera ejecutando ese usuario. Es uno de los ataques más peligrosos por

las consecuencias que podría tener para la víctima.

Inyección SQL

Este ataque es uno de los más populares en las aplicaciones web. Los piratas informáticos van a basarse en una vulnerabilidad, como podría ocurrir en la capa de la base de datos de la aplicación web. Ese código podría comprometer a esa herramienta y llegar a filtrar datos confidenciales, información, etc.

Lógicamente esto va a provocar que el programa funcione incorrectamente. A fin de cuentas lo que hace el atacante con la inyección SQL es modificar el código que ya previamente ha sido programado. Va a modificar la función principal que tiene.

Ataque de envenenamiento de cookies

Los ataques de envenenamiento de cookies implican **la modificación de los contenidos de una cookie** (información personal almacenada en el equipo de la víctima) para eludir los mecanismos de seguridad. Al usar ataques de envenenamiento de cookies, los atacantes pueden obtener información no autorizada sobre otro usuario y robar su identidad.

Con el envenenamiento de cookies, por tanto, el atacante podría obtener información confidencial, como podrían ser datos financieros. Esto puede poner en riesgo la privacidad del usuario.

Robo de cookies

El robo de cookies es un tipo de ataque que se realiza mediante **scripts del lado del cliente** como JavaScript**.** Cuando el usuario hace clic en un enlace, el script buscará la cookie almacenada en la memoria del equipo para todas las cookies activas y las enviará al pirata informático que está llevando a cabo ese ataque.

Hay que tener en cuenta que las cookies son un elemento muy importante. Pueden almacenar información de nuestro equipo, de los programas que utilizamos, los datos personales… Tienen un gran valor en la red.

Ataques de phishing

Sin duda estamos ante un clásico de los ataques cibernéticos. El **Phishing** es el proceso en el que un atacante intenta robar datos sensibles, contraseñas, credenciales… Busca que los usuarios introduzcan información como nombres de usuario, contraseñas y

detalles de tarjetas de crédito haciéndose pasar por una entidad fiable en una comunicación electrónica. Sin embargo todo eso que pone la víctima termina en un servidor controlado por los atacantes.

Cuando hablamos de robo de información, de datos sensibles, debemos recordar siempre el Phishing. Es uno de los métodos más utilizados por los piratas informáticos para recopilar todo tipo de información personal.

Web Defacement

Otro ataque que puede comprometer seriamente una página es lo

que se conoce como **Web Defacement**. En español lo podemos traducir como desfiguración de un sitio web. Es cambiar la apariencia a una página para que parezca lo que no es. Pueden acceder a un servidor y modificar o reemplazar todo el contenido que hay.

Esto podría afectar seriamente a la reputación de un sitio web. Un atacante podría modificar totalmente la apariencia, los artículos publicados, el contenido… Lógicamente se trata de un problema muy importante al que hay que hacer frente.

Desbordamiento de buffer

Un tipo de ataque más es lo que se conoce como desbordamiento de buffer. Se trata de un problema en el que un **proceso almacena datos** en un búfer fuera de la memoria que el programador reservó para ello. Es otra variedad de amenaza muy común. Los datos adicionales sobrescriben la memoria que puede contener otros datos, incluidas variables de programa y datos de control de flujo del programa.

Esto podría provocar errores de acceso a la memoria, resultados incorrectos, finalización del programa o una violación de la

seguridad del sistema. Hay que tener en cuenta que este tipo de vulnerabilidades puede estar presente en todo tipo de sistemas, aplicaciones y servidores.

Navegación forzada

En este caso estamos ante un ataque cuyo objetivo es enumerar y acceder a los recursos a los que la aplicación no hace referencia, pero que aún son accesibles. Podríamos nombrar como ejemplos los directorios como config, backup, logs a los que se puede acceder y que pueden revelar mucha información sobre la aplicación en sí, contraseña, actividades, etc.

Este método también lo debemos incluir como uno de los más utilizados por los piratas informáticos para comprometer la seguridad de servidores. Lo pueden usar para controlar y modificar directorios.

División de respuesta HTTP

También se conoce como **separación de respuesta HTTP**. En esta ocasión un atacante pasa datos maliciosos a una aplicación vulnerable**,** y la aplicación incluye los datos en un encabezado de

respuesta HTTP. Este ataque en sí no causa ningún daño, pero daría lugar a otros ataques sensibles como XSS.

Por tanto, podemos decir que este método es más bien una estrategia para dar lugar a otros ataques. Es una puerta de entrada a través de una aplicación que tenga algún fallo de seguridad explotable.

Como hemos visto, son muchos los **ataques** que podemos sufrir. No importa si somos usuarios domésticos o una gran organización. Además, cualquier dispositivo, sistema o servidor puede ser atacado por un ciberdelincuente. Esto hace que debamos tomar precauciones y no cometer errores de ningún tipo que nos

comprometan.

Existen diferentes **métodos y herramientas** que los desarrolladores de aplicaciones web y servidores web usan para proteger una página. Además, también existen soluciones para ataques específicos y mejores prácticas que se pueden aplicar de forma continua para proteger las aplicaciones y los usuarios. Las revisiones de código, los programas de recompensa de errores y los escáneres de código deberían implementarse durante todo el ciclo de vida de la aplicación.

Las **revisiones de códigos** pueden ayudar a detectar códigos vulnerables al principio de la fase de desarrollo, los escáneres de códigos dinámicos y estáticos pueden hacer comprobaciones automáticas de vulnerabilidades, así como los programas de bonificación de errores permite a los testers o hackers éticos encontrar errores en el sitio web.

Usar procedimientos almacenados con parámetros que se puedan llevar a cabo automáticamente. Un ejemplo sería implementar CAPTCHA o hacer que los usuarios tengan que responder preguntas. Esto asegura que un formulario y una solicitud sean enviados por un humano y no por un bot.

Otro aspecto muy importante es el de utilizar un **cortafuegos de aplicación web** (WAF) para supervisar la red y bloquear posibles ataques. Algunos ejemplos pueden ser el WAF de Cloudflare, Sucuri o AWS. Es una medida de seguridad que conviene aplicar en nuestros servidores. Así evitaremos la entrada de atacantes que puedan llegar a romper nuestra privacidad y seguridad.

No obstante, hay que tener en cuenta que ninguno de estos métodos puede reemplazar al otro. Esto significa que cada uno aporta su propio valor a la tabla y agrega protección contra ciertos escenarios de ataque. No se pueden encontrar todas las vulnerabilidades mediante revisiones de código o programas de bonificación de errores, ni solo mediante un cortafuegos de aplicación web ya que ninguna herramienta es 100% segura. Todo esto hace que debamos tener en cuenta una combinación de todos estos métodos para proteger las aplicaciones y a los usuarios de la manera más eficiente posible.