Tipos De Ataques Más Comunes A Sitios Web Y Servidores

Si estas leyendo este articulo, es por que de seguro estas interesado en conocer las técnicas ó métodos que se usan para realizar un ataque a una pagina ó sitio web, como también a los servidores. Ya sea que tus intenciones no sean ~~buenas~~ malas, te explicaremos los tipos de ataques mas comunes que se realizan en los sitios y servidores web.

¿Qué puedes hacer con lo que conocerás? Simple, conocer como funciona el ataque y así evitar ser víctima de un ataque en especifico. De seguro con este articulo te preguntarás: ¿Mi Sitio Web Esta Preparado Para Cualquier Ataque De Hackers?. No te queremos sembrar una duda, solo deseamos abrirte los ojos y que seas capaz de lograr un protección a tus recursos web.

Ataque Por Injection

Los **ataques de inyección**, más específicamente sqli (Structured Query Language Injection) es una técnica para modificar una cadena de consulta de base de datos mediante la **inyección de código en la consulta**. El **SQLI** explota una posible vulnerabilidad donde las consultas se pueden ejecutar con los datos validados.

SQLI siguen siendo una de las técnicas de sitios web más usadas y se pueden utilizar para obtener **acceso a las tablas**

de bases de datos, incluyendo información del usuario y la contraseña. Este tipo de ataques son particularmente comunes en los sitios de empresas y de comercio electrónico donde los hackers esperan grandes bases de datos para luego extraer la información sensible.Los **ataques sqli** también se encuentran entre los **ataques más fáciles de ejecutar**, que no requiere más que un solo PC y una pequeña cantidad de conocimientos de base de datos.

DDoS

La Denegación de Servicio (DoS) ó Denegación de Servicio Distribuida (DDoS) son las formas más comunes para congelar el **funcionamiento de un sitio web**. Estos son los intentos de inundar un sitio con solicitudes externas, por lo que ese sitio no podría estar disponible para los usuarios reales. Los ataques de denegación de servicio por lo general se dirigen a puertos específicos, rangos de IP o redes completas, pero se pueden dirigir a cualquier dispositivo o servicio conectado.

Los **ataques de denegación de servicio** funcionan cuando una computadora con una conexión a Internet intenta inundar un servidor con paquetes. **DDoS**, por otro lado son cuando muchos dispositivos, a menudo ampliamente distribuidos, en un intento de botnet para inundar el objetivo con cientos, a menudo miles de peticiones.

Los ataques DDoS vienen en 3 variedades principales:

1. Los ataques de volumen, donde el ataque intenta desbordar el ancho de banda en un sitio específico.
2. Los ataques de protocolo, donde los paquetes intentan consumir servicios o recursos de la red.
3. Ataques a aplicaciones, donde las peticiones se hacen con la intención de «explotar» el servidor web, mediante

la capa de aplicación.

Fuerza Bruta

Estos son básicamente intenta «**romper**» todas las combinaciones posibles de nombre de usuario + contraseña en una página web. Los **ataques de fuerza bruta** buscan contraseñas débiles para ser descifradas y tener acceso de forma facil. Los atacantes cuentan con buen tiempo, así que el truco es hacer que tus contraseñas sean lo bastante seguras y así el atacante se cansaría antes de descifrar tu contraseña. Mientras que las computadoras se vuelven más y más poderosa la necesidad de contraseñas más fuertes se vuelve cada vez más importante. El caso mas reciente de esta vulnerabilidad, se ha visto en cuanto a la vulneración de cuentas de algunos famosos alojadas en iCloud.

Cross Site Scripting

Los atacantes utilizan Cross-site Scripting (XSS) para **inyectar scripts maliciosos** en lo que serían sitios web inofensivos. Debido a que estos scripts parecen provenir de sitios web de confianza, el navegador de los usuarios finales casi siempre ejecuta la secuencia de comandos, la concesión de los piratas informáticos el acceso a la información contenida en las cookies o tokens de sesión utilizados con ese sitio. El

XSS generalmente se utiliza para obtener acceso de un usuario de la cuenta.

¿Por Qué Hackean Los Sitios Web?

Simple, por que hay personas buenas y personas malas, bueno, para no ser tan tajantes con la explicación, es por que existen **White Hack** y **Black Hack**. Has escuchado alguna vez, mentiras son mentiras, ya sean blancas o negras? Pues bien, en este caso, puede aplicar esto, con la variación, de que los White Hack tienen un motivo bueno para vulnerarla seguridad, en contraparte, los Black Hack, no. Los White Hack, son aquellos profesionales que prueban que tan vulnerable es un sistema, y realizar un reporte detallado el cual servira para mejorar el sistema, son conocidos como auditores de seguridad informática.

Los Black Hack, vulneran un sistema, extraen información sensible, y ni te avisan. Pero por que tendrían que avisarte? De eso se trata ;) En un mundo de malos y buenos tenemos que estar prevenidos y conocer los diferentes métodos por los cuales podrán ser vulnerados nuestros sitios web. ¿Usas algún método o herramienta en particular para prevenir los ataques? Siéntete en la libertad de compartirlo en un comentario.