Seguridad en Apache
Vulnerabilidades actuales: DoS, CSS

Universidad de Granada

9 de octubre de 2015

Contenidos

¿Qué es un servidor web Apache?

- Un **servidor web** es un programa que procesa una aplicación del lado del servidor y realiza conexiones con un cliente.
- Un **servidor Apache** es un servidor web HTTP de **código abierto** y **multiplataforma** que es usado para la creación de sitios o servicios web.

Seguridad en Apache

La configuración por defecto de Apache deja al descubierto mucha cantidad de información que pueda ser usado para un posterior ataque. Por ejemplo:

- **Información acerca del servidor**: Normalmente incluso puede conocerse el sistema sobre el que el servidor está trabajando y la versión de este.
- **Listado de directorios**: En un principio si el servidor es capaz de mostrar una listado de directorios y ficheros que sería necesario bloquear para los visitantes que no poseen permisos de administrador.

Por lo que la primera tarea del administrador del servidor será realizar una adecuada configuración del servicio httpd.

Tipos y formas de ataque

- **Information Leakage:** Es una forma de obtener información para posteriormente atacar el servidor web haciendo uso de alguna otra técnica.
- **Bypass:** La idea predominante en este ataque es el de tomar un atajo u otra ruta para saltarse algun tipo de seguridad.
- **DoS:** o Ataque de denegación de servicios, es uno de los más frecuente actualmente consiste en provocar la perdida de conectividad a una red de ordenadores por la sobrecarga de los recursos de la misma.
- **XSS o CSS:** o Cross-site scripting, consiste en aprovechar una inseguridad o agujero de seguridad en una aplicación web para inyectar código JavaScript u otro lenguaje.
- **SQL injection:** La inyección SQL tiene una idea muy parecida a la de XSS intenta acceder a una información contenida en una base de datos.

¿Qué es un ataque DoS?

- Un ataque de **denegación de servicio** se produce cuando un usuario normalmente malintencionado intenta producir la pérdida de conectividad de una red de ordenadores consumiendo algún tipo de recurso limitado.
- El objetivo que se quiere alcanzar es deshabilitar el computador víctima, el nombre a este ataque viene dado por la propuesta:
  "Se pretende negar la capacidad de una institución o empresa para dar servicio a sus usuarios, afiliados o clientes."

Diferencia entre DDoS y DoS

Los ataques DDoS son distribuidos, esto quiere decir que no es una sola computadora produciendo peticiones a un servidor sino que el atacante posee unos computadores manejadores que se encargan de que el número de computadores manejados envien simultaneamente peticiones al servidor víctima.

Principales Métodos de ataque

- **Consumición de recursos escasos o limitados:** Ancho de banda, memoria, espacio de disco entre otros, incluso condiciones ambientales.
  - **Conexión de Red**.
  - **Usar tus propios recursos contra ti**.
  - **Consumición de ancho de banda**.
  - **Consumición de otros recursos**.
- **Destrucción o alteración de la información de configuración:** Una mala configuración de un servidor puede no operar completamente, un atacante puede alterar o destruir la información para que se impida el acceso directo a una máquina o red.
- **Destrucción o alteración de componenentes físicos:** La seguridad física es muy importante a la hora de recibir ataques y prevenirlos, ya que existen computadores que están autorizados a cambiar condiciones ambientales del lugar donde se encuentran los servidores.

Prevención y respuesta en Apache

- La herramienta más eficaz para evitar ataques DoS es un **firewall**.
- Directiva **RequestReadTimeout**.
- Directiva **TimeOut**.
- Podemos configurar los valores de las siguientes directivas de manera apropiada con el fin de evitar un consumo excesivo de recursos provocada por la entrada de clientes: LimitRequestBody, LimitRequestFields, LimitRequestFieldSize, LimitRequestLine y LimitXMLRequestBody
- Directiva **acceptfilter** (solo disponible en algunos sistemas operativos).
- Directiva **MaxRequestWorkers**.
- Por último hacer uso de **mpm** (multi-Processiong Modules).

¿Qué es un ataque XSS?

Los ataques de este tipo incluyen normalmente tres partes, el atacante, la web que se va a aprovechar para ejecutar el código malicioso y la victima cliente, la meta que queremos alcanzar es obtener los cookies u otra información que permita la identificación de la victima cliente en la web.

Técnica

Prevención y respuesta

- **Filtrado de entrada**: Se filtran las etiquetas que pueden aparecer en un determinado parametro.
- **Filtrado de salida**: Es similar al anterior pero en este caso se filtran los datos en la versión que se envia de vuelta al usuario como respuesta.
- **Instalación de una aplicación firewall**: Se dedica a interceptar los ataques CSS antes de que alcancen el servidor web y los bloquee. Pueden cubrir todos los métodos de entrada incluyendo las cabeceras HTTP.