OWASP

Open Web Application Security Project

FILE UPLOAD EXPLOTATION

Randy Ortega

ortega571@gmail.com

https://www.linkedin.com/in/randy-ortega-10b54a61

OWASP
Open Web Application Security Project

ACERCA DE MI

- Ingeniero de Sistemas Unexpo
- Especialista en Seguridad de la Información

  Mercantil Banco Universal
- Instructor de Ethical Hacking Vsoft Learning
- CE|H V7

OWASP

Open Web Application Security Project

Qué es un archivo?

- Un archivo o fichero informático es un conjunto de bits guardados en un dispositivo de almacenamiento (memoria, disco duro, pen drive, entre otros).
- Se caracterizan por presentar:
  - Un tamaño definido
  - Una extensión de acuerdo a su contenido
  - En el caso de las imágenes, presentan bits de inicio y bits de fin denotativos.

OWASP
Open Web Application Security Project

Qué es una subida de archivos?

- Se conoce como subida de archivos a todo proceso de carga de archivos a un servidor (local o remoto) a través de un formulario tipo Web.

OWASP
Open Web Application Security Project

Es peligrosa una subida de archivos?

Si, la subida de archivos representa un riesgo grande a la aplicación.

Entre los riesgos más significativos están:

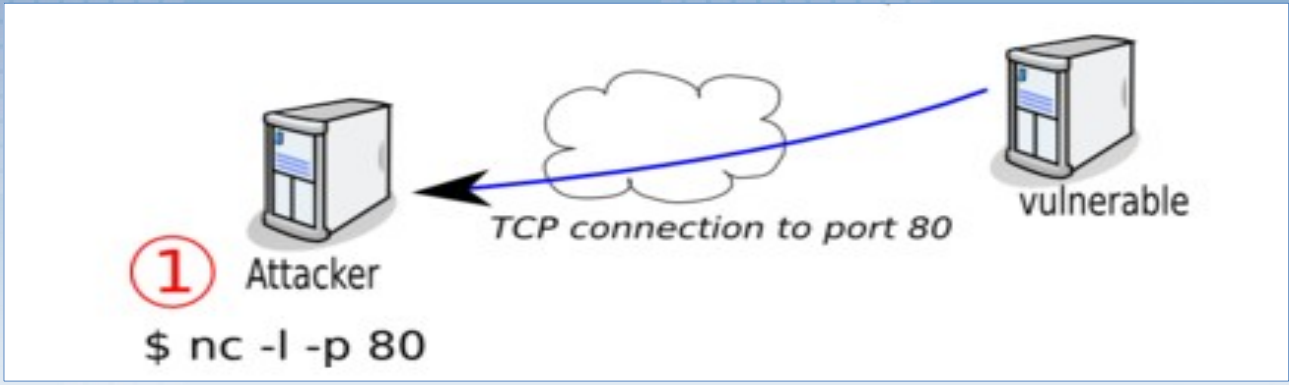
- El servidor Web puede ser comprometido por la subida de una **web shell**, con la cual se puedan ejecutar comandos, navegar por los archivos del sistema, explotar vulnerabilidades locales, entre otras.
- El portal puede ser comprometido a un defacement.

OWASP
Open Web Application Security Project

Es peligrosa una subida de archivos?

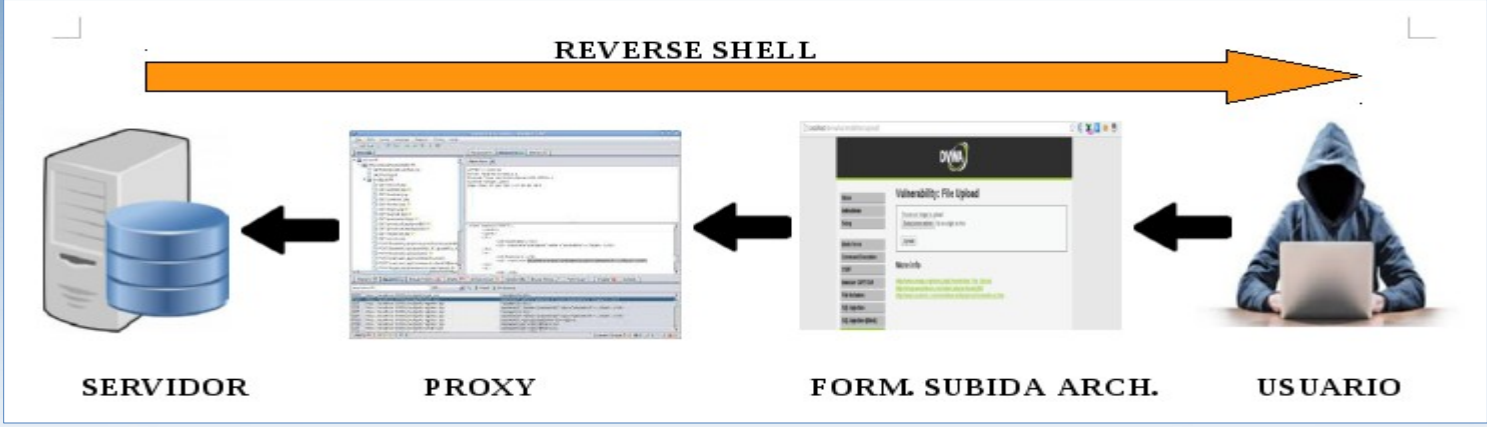
- El atacante puede ser capaz de colocar una página de phishing en el sitio web.
- El servidor web puede ser utilizado como un servidor con el fin de acoger malware, pornografía, entre otros.
- El atacante puede ser capaz de causar **Denegación de Servicios** al subir archivos de gran tamaño.
- El atacante al subir una **reverse shell** puede tomar control del servidor y ejecutar comandos como administrador.

Qué es una reverse shell?



Una **reverse shell** (shell inversa) se le dice a la conexión establecida desde la máquina destino (víctima) al cliente (atacante), donde el cliente obtiene una shell de la máquina destino, ganando acceso al sistema.

Ataque de subida de archivos (Lab)



El atacante se saltará la validación del formato de archivos permitidos por el formulario de subida de archivos y subirá una reverse shell con el cual tomará control del sistema.

OWASP

Open Web Application Security Project

Métodos de protección para la subida de archivos

- Comprobar la extensión del archivo de subida
- Comprobar el tamaño del archivo de subida.
- Usar una lista blanca para las extensiones de archivos permitidos.
- Verificar el tipo de contenido del archivo a través del Content Type, además verificar a nivel tanto del lado del cliente como del lado del servidor el MIME del archivo.

OWASP

Open Web Application Security Project

Métodos de protección para la subida de archivos

- Subir los archivos a un directorio que esté fuera del directorio raíz de la aplicación.
- Generar un nombre de archivo aleatorio y añada la extensión previamente generada
- Cifrar los archivos al momento de almacenarlos en el servidor.

OWASP
Open Web Application Security Project

Conclusiones

La subida de archivos en una aplicación representa un riesgo grande en una organización, por lo que deben ser cautelosos y tomar las medidas preventivas a la hora de realizar la validación del tipo de archivos que permiten subir para evitar ser vulnerados. Puede complementar la información ingresando al siguiente enlace

https://www.owasp.org/index.php/Unrestricted_File_Upload

OWASP

Open Web Application Security Project

PREGUNTAS


THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
DANKSCHEEN
BÏYAN
SHUKRIA
TINGKI
YAQHANYELAY
TASHAKKUR ATU
SUKSAMA
EKHMET
MEHRBANI
GRAZIE
MAAKE
KOMAPSUMNIDA
GOZAIMASHITA
EFCHARISTO
JUSPAXAR
BOLZÏN
MERCI
PALDIES