
Nombre Taller: Lab 15

Lab: Insecure File Upload 0x01

## Detalles Prácticos:

Descripción: En este laboratorio subimos archivos malicosos .PHP desde shell.
Nivel(Básico/Intermedio o avanzado)
Instructores:Rieradipe

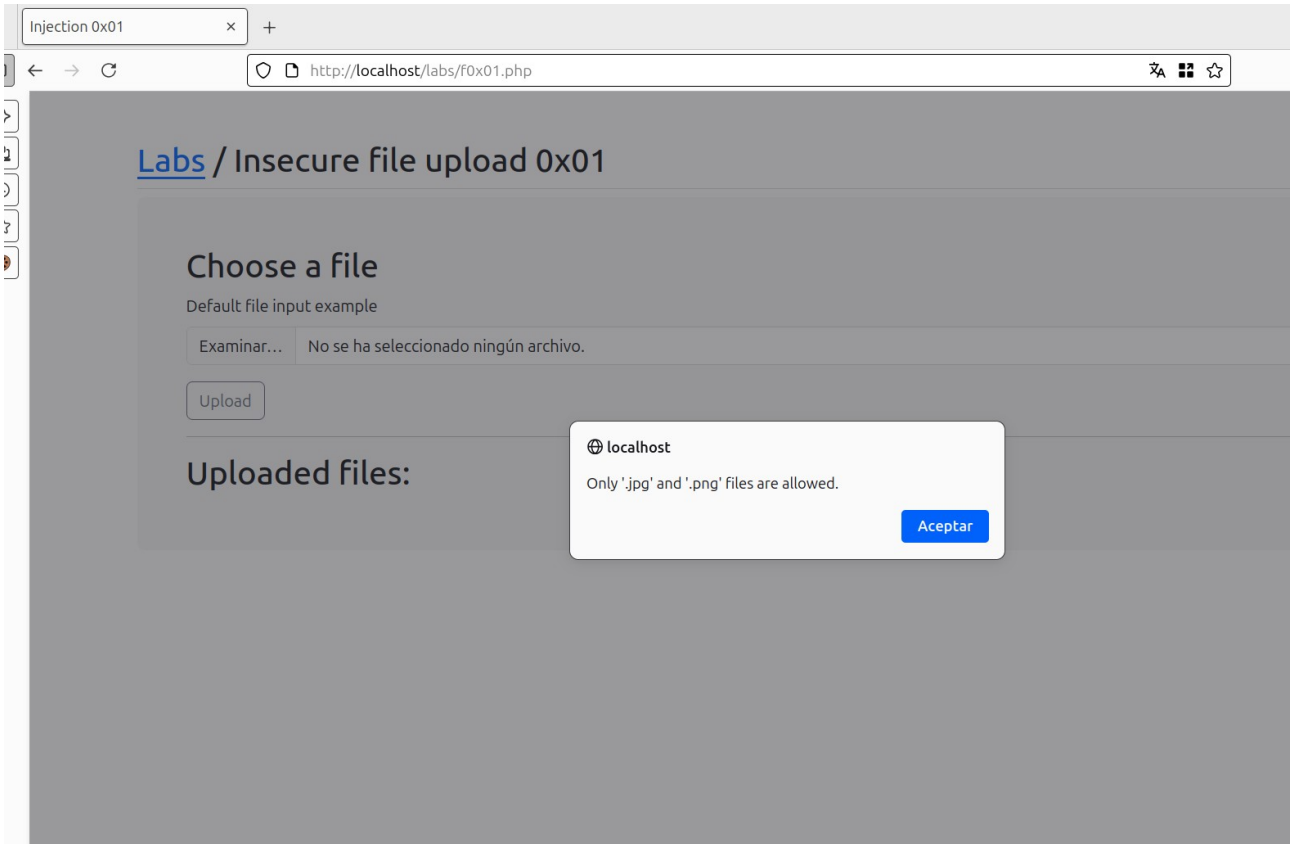
## Tabla de contenidos:

**Ojetivo:**

Subir un archivo PHP malicioso (web shell) evadiendo las restricciones de tipo de archivo para ejecutar comandos en el servidor

**Análisis inicial:**

- El formulario permite subir archivos
- Muestra un error



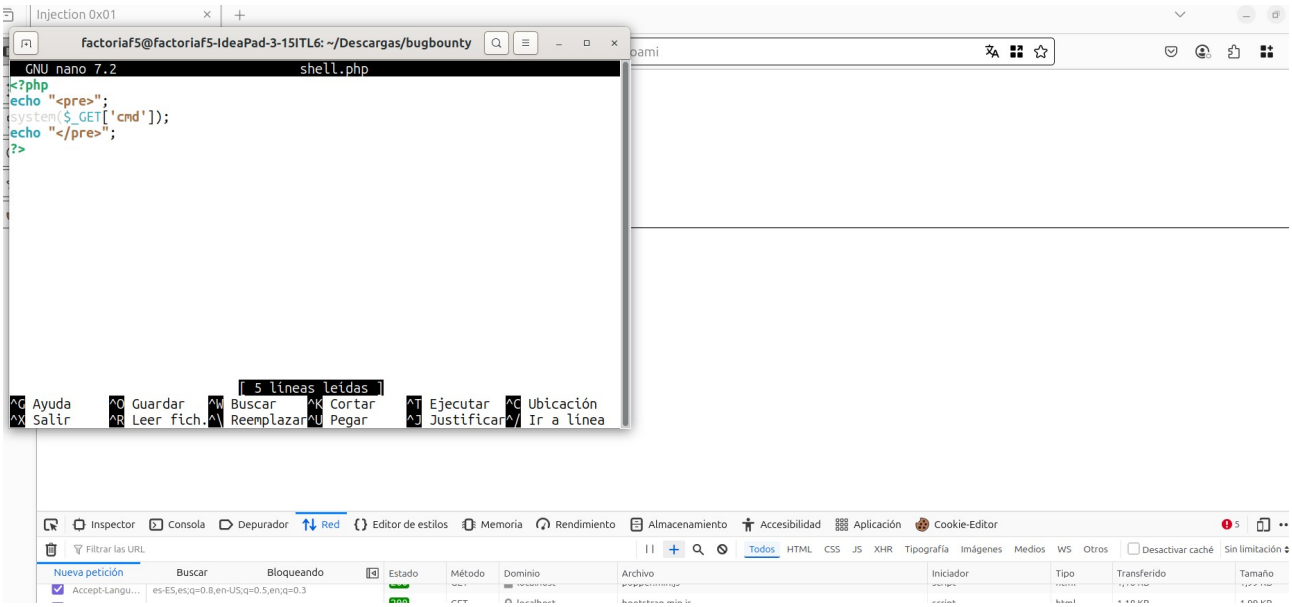

- Las restricciones son visibles desde el lado cliente y se validan también en lado servidor

**Herramientas usadas:**

- Navegador Firefox
- DevTools(red e inspector)
- Editor de textos nano
- PHP shell básico
- Servidor local(Docker + Apache)

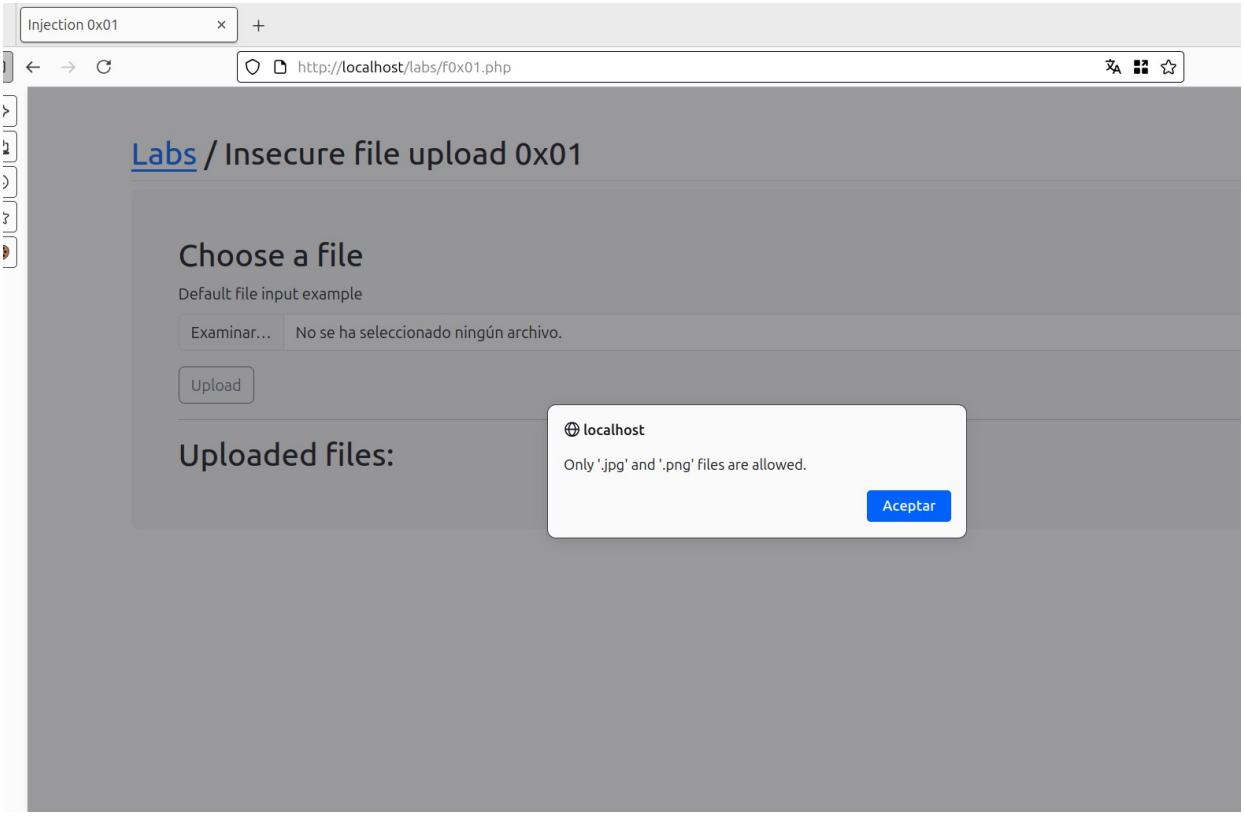
## Fases de la explotación:

1. Preparamos el archivo malicioso
   Creamos shell.php
   Este archivo se guarda en Descargas/bugbunty/shell.php




2. Subido inicial bloqueada

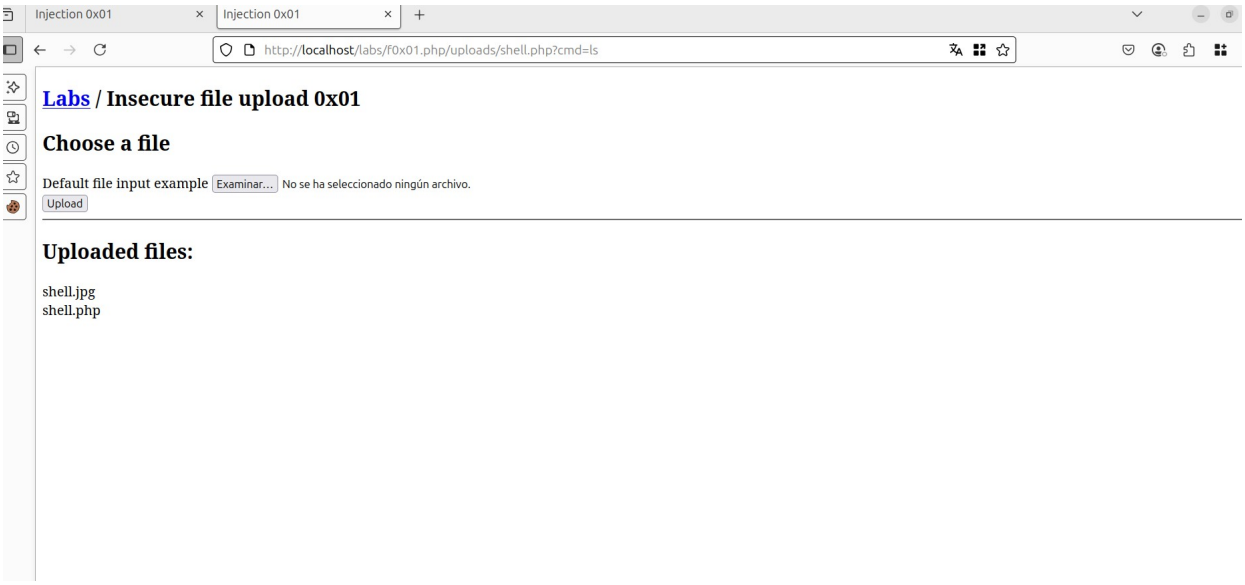
- Al intentar subir shell.php se muestra el mensaje de error




- Cambiamos la extension a .jpg → shell.jpg pero el codigo php deja de ejecutarse

3. Bypass con DevTools

- En DevTools → pestaña Red, interceptamos la petición Post
- Modificamos el filename=”shell.jpg” por filename=”shell.php”
- Enviamos la peticion

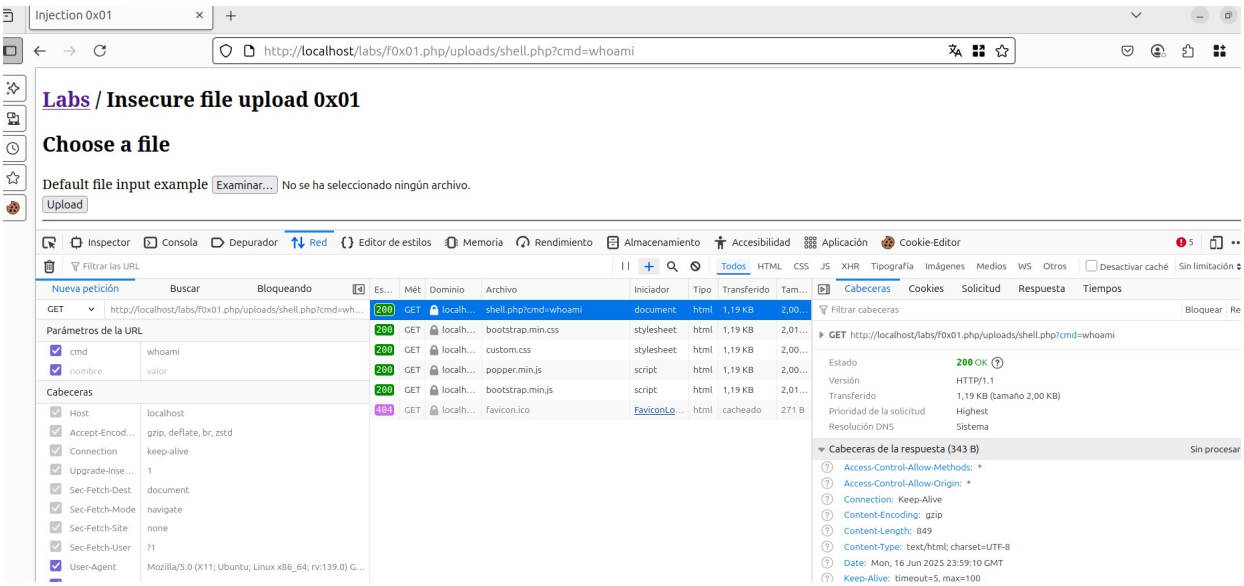



4. Ejecución del payload

Accedemos al payload desde la url

| http://localhost/labs/f0x01.php/uploads/shell.php?cmd=whoami |
|---|

Respuesta esperada: salida del comando whoami
Aunque no se mosro visualmente, el servidor responde con un 200 OK y se confirma que el archivo esta activo



5. Archivos subidos

- shell.jpg prueba bloqueada
- shell.php web shell funcional
- kero.jpg y kero2.jpg pruebas de subida

**Conclusión:**

El servidor es vulnerable a subida de archivos maliciosos si se modifican los encabezados desde el cliente.
No hay validación por contenido real del archivo, solo por extensión y tipo MIME superficial

**Medidas de mitigación:**

| |
|---|
| **V**alidar en el servidor el contenido del archivo |
| **R**enombrar archivos al subirlos |
| **P**rohibir la ejecución en el directorio de subida (uploads /) |
| **V**alidar extensiones y tipos MIME con seguridad, no solo en el cliente |
| **Escaneo antivirus de archivos subidos** |