Puesta en Producción Segura

Práctica 2.7

UnrestrictedFileUpload

Jennifer Galván Bejarano

Índice

Indicaciones

<Incluye en un documento Word capturas de pantalla de todo el proceso>

Preparación:

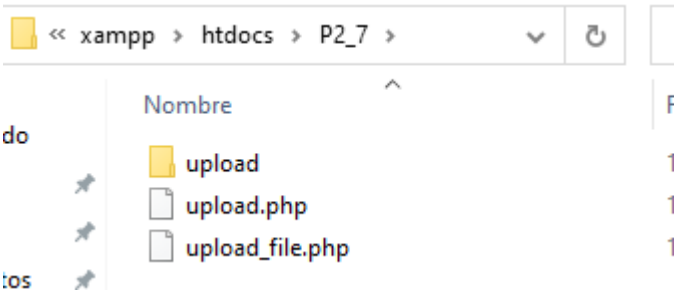
1) Despliega los ficheros upload.php y upload_file.php en el servidor.

2) En la misma donde has desplegado los archivos anteriores, crea una carpeta llamada “upload”.

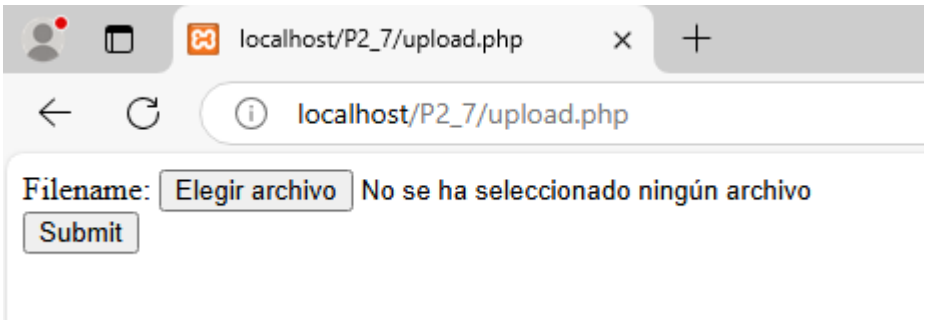
Actividades

1) Para realizar el ataque, usa upload.php para subir el archivo shell.php (terminal desde el navegador)

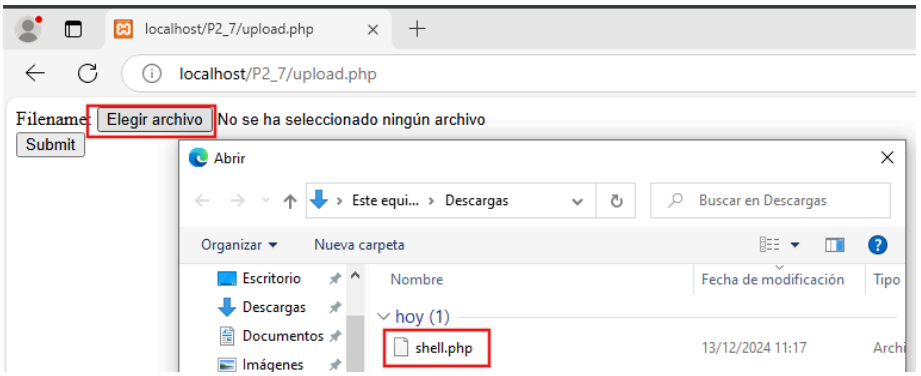
1. Primero subí los ficheros en Xampp donde despliegue el ejercicio del foro y cree la carpeta sugerida upload

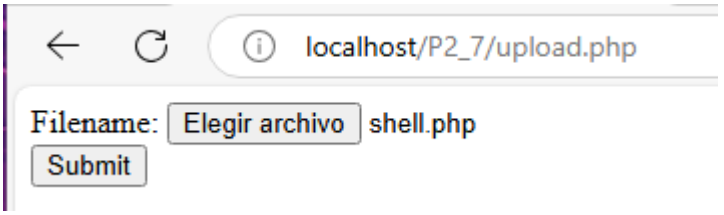


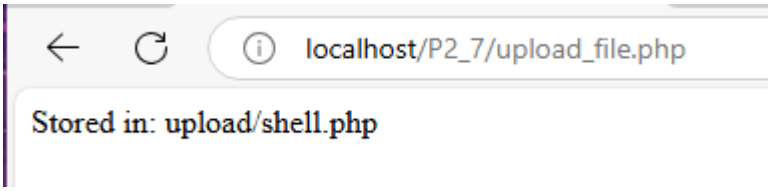
2. Entró a la página upload.php



3. Subo el archivo sugerido shell.php



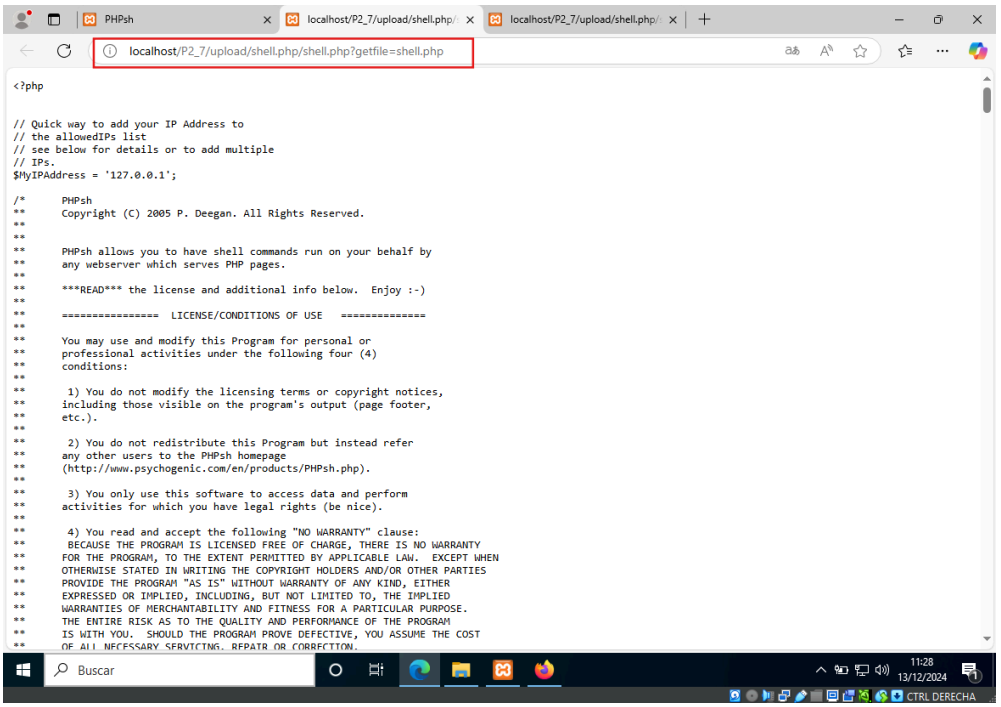




2) Una vez subido, usa la terminal de shell.php para navegar a través del servidor. Muestra el contenido del archivo de configuración del apache httpd.conf (contiene la configuración del servidor).

Cuando escribir en el area del signo de $ hhtpd.conf me salio lo siguiente:

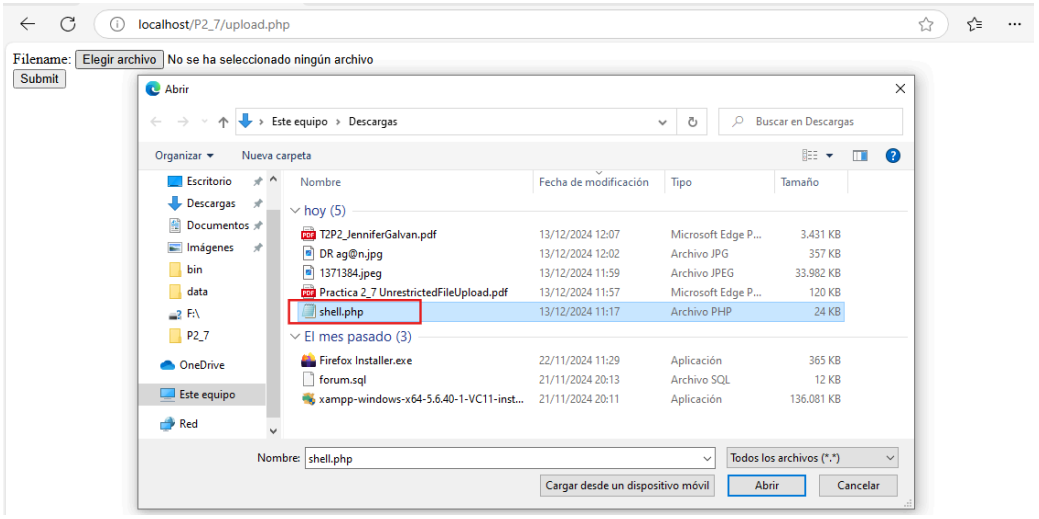
Si selecciono shell.php me sale lo siguiente, me abre otra ventana donde muestra el codigo completo de shell.php

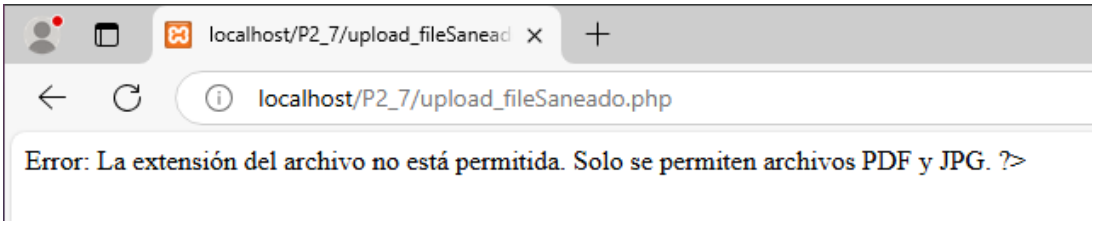


3) Mejora la subida de archivos en el servidor para evitar el ataque UnrestrictedFileUpload. Para ello modificar el archivo upload_file.php:

- Restringe la extensión y tipo de fichero a pdf y jpg.

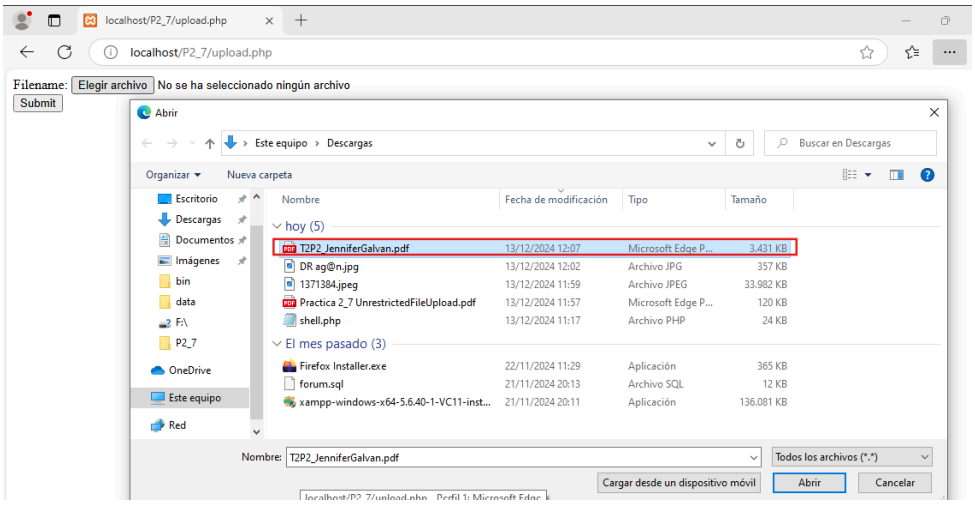
Compruebo que no pueda subir el fichero php

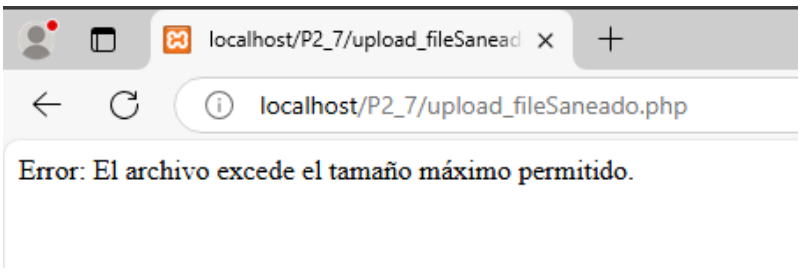




- Restringe el tamaño máximo de fichero a 2MB.

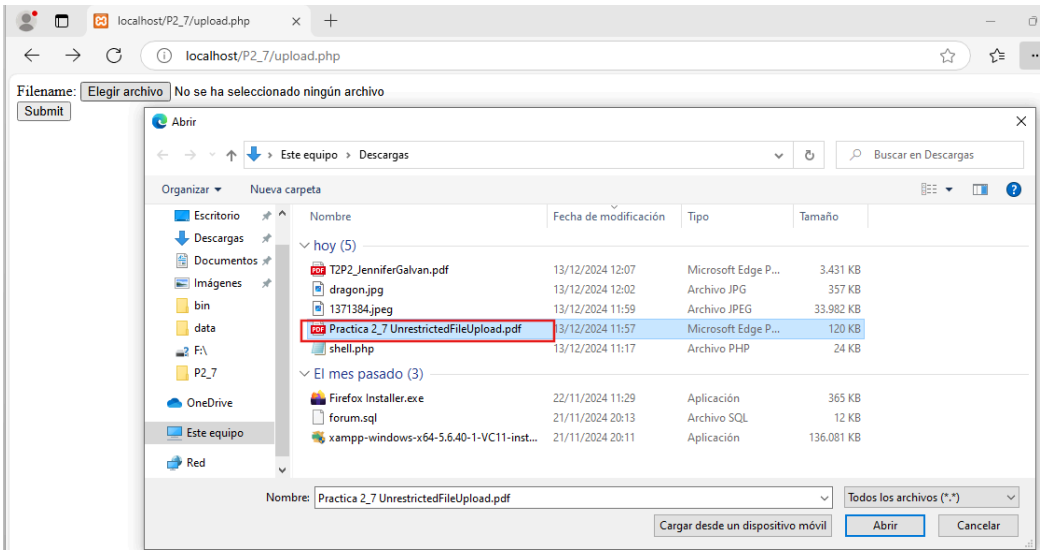
Compruebo que no pueda subir un fichero mayor a 2MB

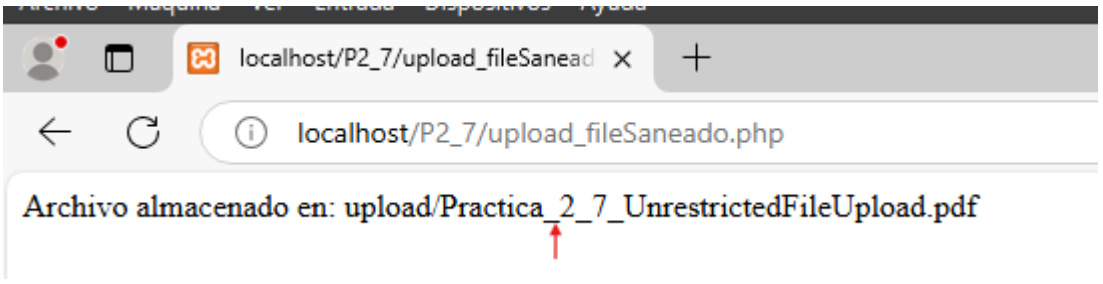


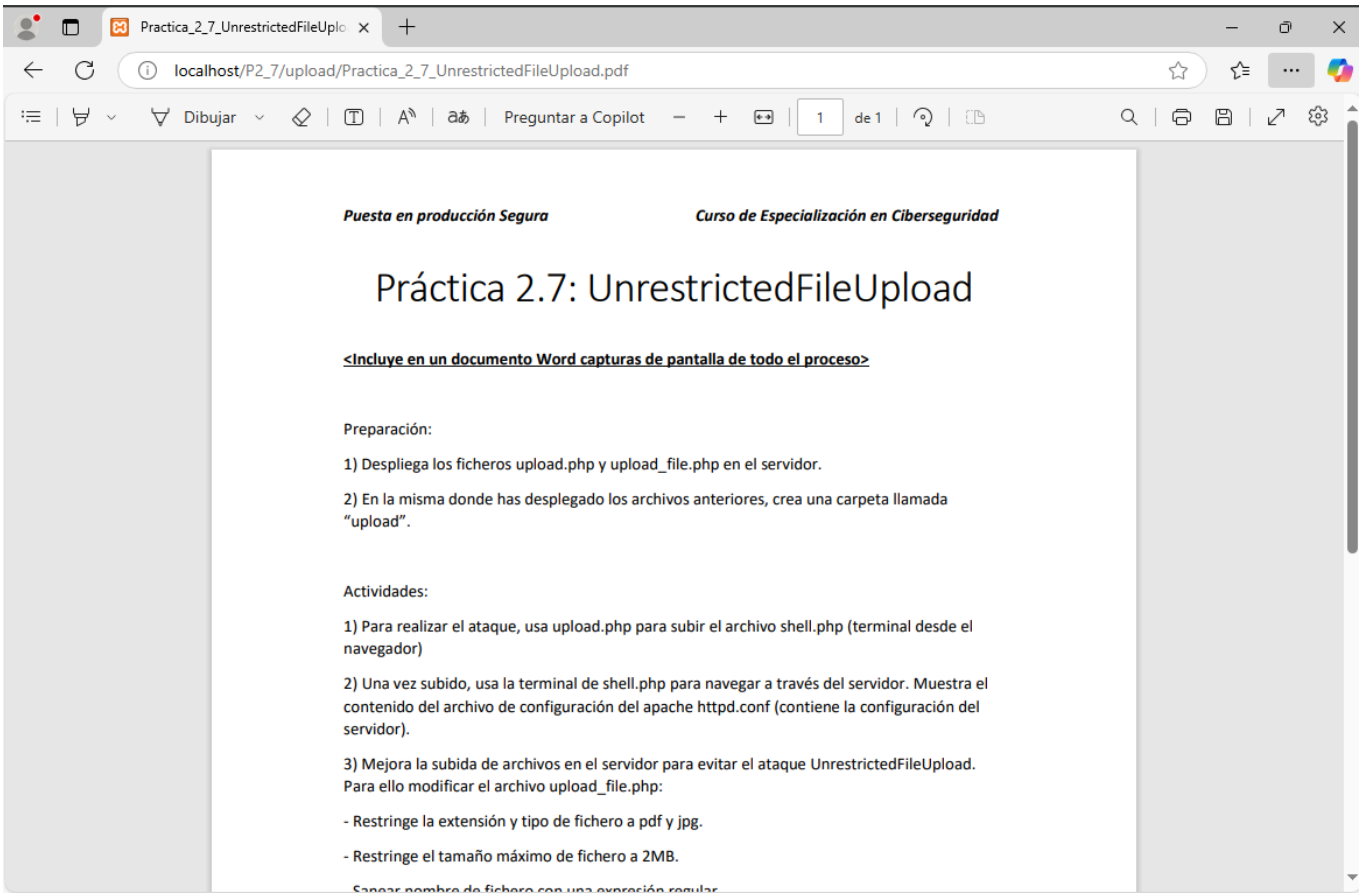


- Sanear nombre de fichero con una expresión regular.

Compruebo que se saneó el fichero con nombre irregular







Finalmente compruebo que suba el fichero con las indicaciones que se permiten.