Nombre Taller:Lab 6

File Inclusion 0x02

Detalles Prácticos:

Descripción: El objetivo de este laboratorio es explorar una vulnerabilidad de inclusión de archivos en una aplicación web, utilizando técnicas de bypass y normalización para acceder a archivos sensibles del servidor que no deberían ser visibles
Nivel(Básico/Intermedio o avanzado)
Instructores:Rieradipe

Tabla de contenidos:

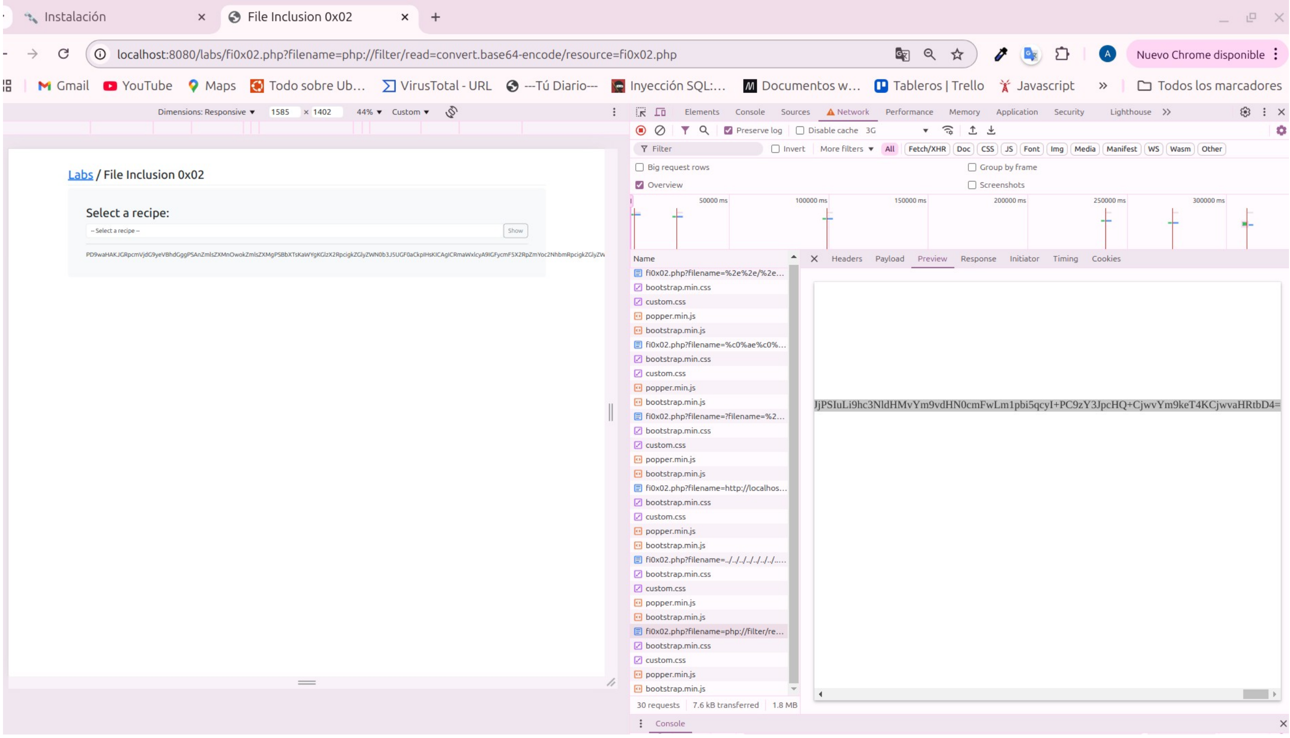
Explotación exitosa #1 🧠
Lectura de archivo fuente con php://filter

- Vector utilizado:

```
?filename=php://filter/read=convert.base64-encode/resource=fi0x02.php
```

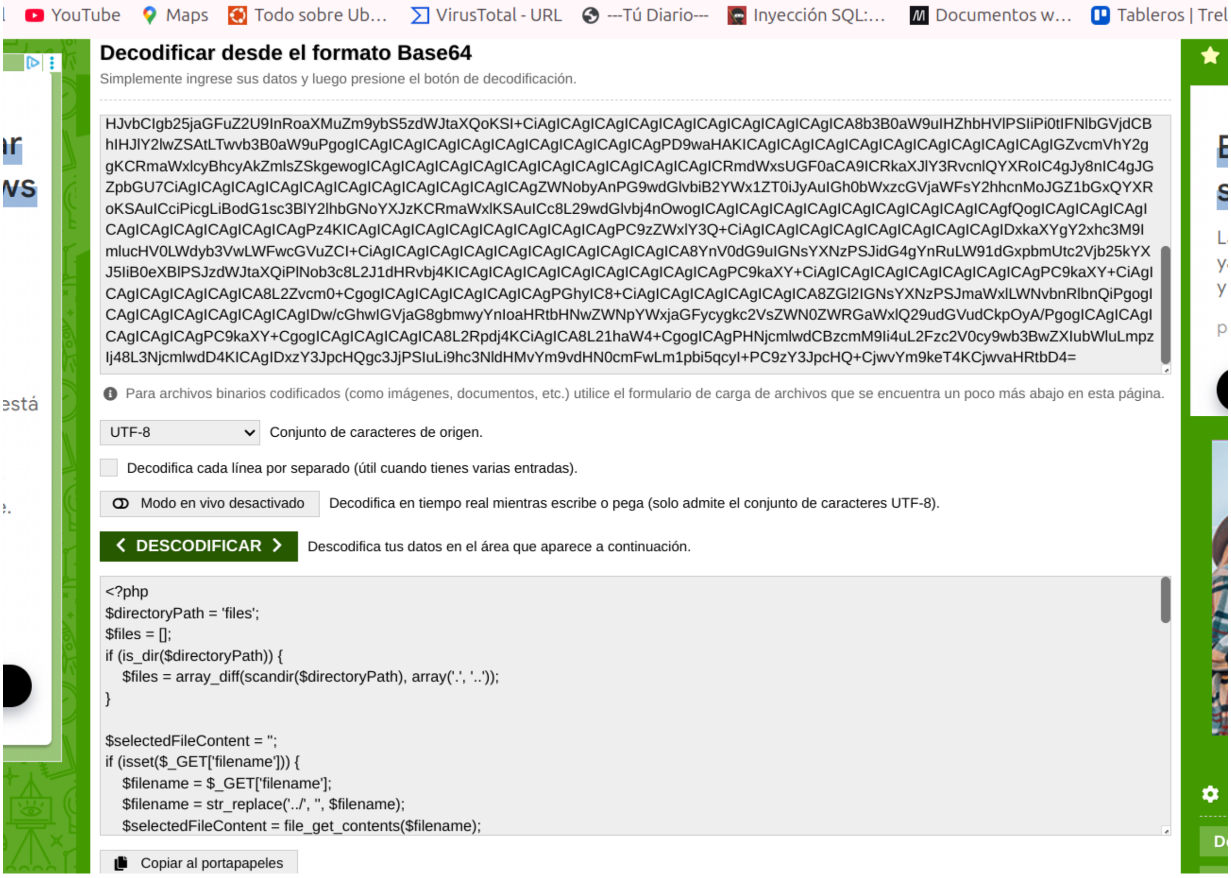
- Resultado:

1. Se obtuvo una cadena codificada en Base64 como respuesta del servidor
2. Est cadena representa el **código fuente real del archivo** *fi0x02.php*



- <u>Validación:</u>

  - Se utiliza la herramienta gratuita https://www.base64decode.org para decodificar el contenido



  - El resultado es el código PHP completo, confirmado el acceso a un archivo interno del servidor

✅ Justificación del éxito:

Esta técnica demuestra:
- El parámetro filename permite inclusión arbitraria de archivos.
- Que no hay restricciones sobre wrappers como *php://*
- Qué es posible acceder al código interno pudiendo revelar estructuras, rutas o vulnerabilidades mayores

Esto se considera una **vulnerabilidad crítica,** incluso sin acceder a /etc/passwd

🧠 Valor añadido / diferencial

- Se identificó y entendió que el resultado codificado en **Base64,** sin que el lab lo indique explicitamente.
- Se aplica lógica y herramientas externas para interceptar el contenido y confirmar el acceso no autorizado

🔐 Medidas de protección recomendadas

I. **Bloquear** el uso de **wrappers especiales** como php:·
II. **Validar** entradas mediante listas blancas estrictas de rutas permitidas.
III. **Nunca** mostrar archivos fuente ni errores detallados en producción.
IV. **Escapar o filtrar** caracteres especiales y coodificaciones peligrosas