Nombre Taller: Lab 0x05

File Inclusion 0x01 (LFI)

## Detalles Prácticos:

Descripción: Este laboratorio tiene como objetivo demostrar una vulnerabilidad de Local File Inclusion(LFI) Se ha identificado un parámetro vulnerable(filename) que permite incluir archivos arbitrarios desde el servidor sin validación adecuada

Nivel(Básico/Intermedio o avanzado)

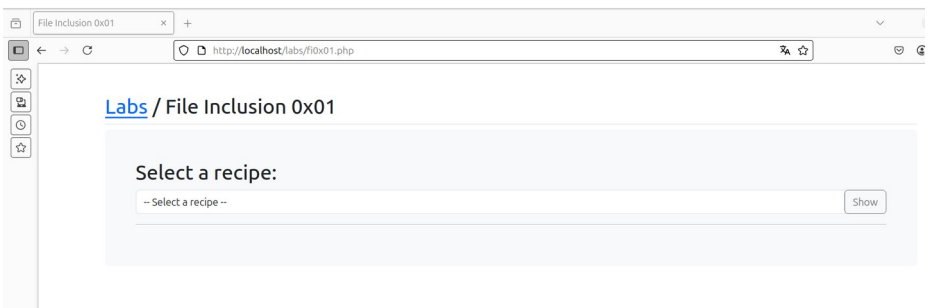
Instructores:Rieradipe

## Tabla de contenidos:



**Metodología aplicada:**

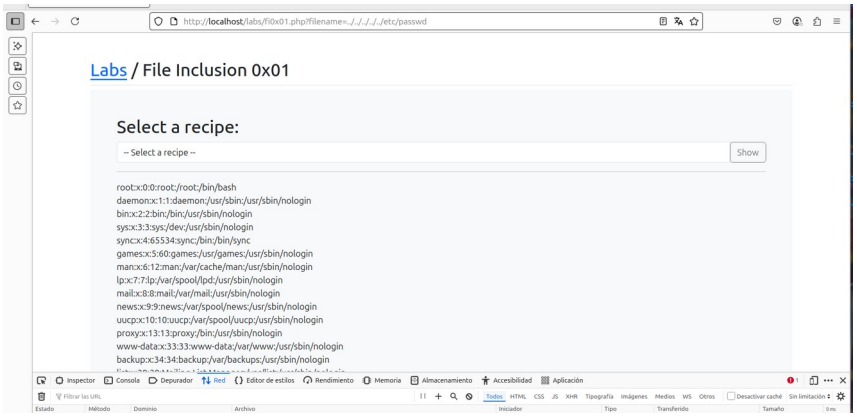
- **Identificación del parámetro vulnerable**



Al buscar recetas;
Se detecta que la aplicación hace uso de la URL.


Lo que indica que el contenido del parámetro *filename* se inserta directamente en una función de inclusión de archivos(include() o similar)

- **<u>Prueba de inclusión local</u>**
  Se prueba la siguiente URL manipulada: (../ 1vez. Hasta que muestra el contenido del archivo con información del sistema sobre usuarios locales)




**Conclusión:**

- La aplicación permite incluir archivos arbitrarios del sistema de ficheros, lo que representa una vulnerabilidad **critica** de seguridad.
  Un atacante podría acceder a archivos sensibles, logs o incluso cargar código malicioso.

**Recomendaciones:**

- Validar y sanitizar todas las entradas de usuarios, especialmente aquellas que interactúan con funciones de inclusión
- Utilizar listas blancas de archivos permitidos
- Desactivar allow_url_includer y allow_url_fopen en el archivo php.ini.
- Restringir los permisos de lectura del servidor web a los archivos realmente necesarios