XSS -- MUNA

Contenido

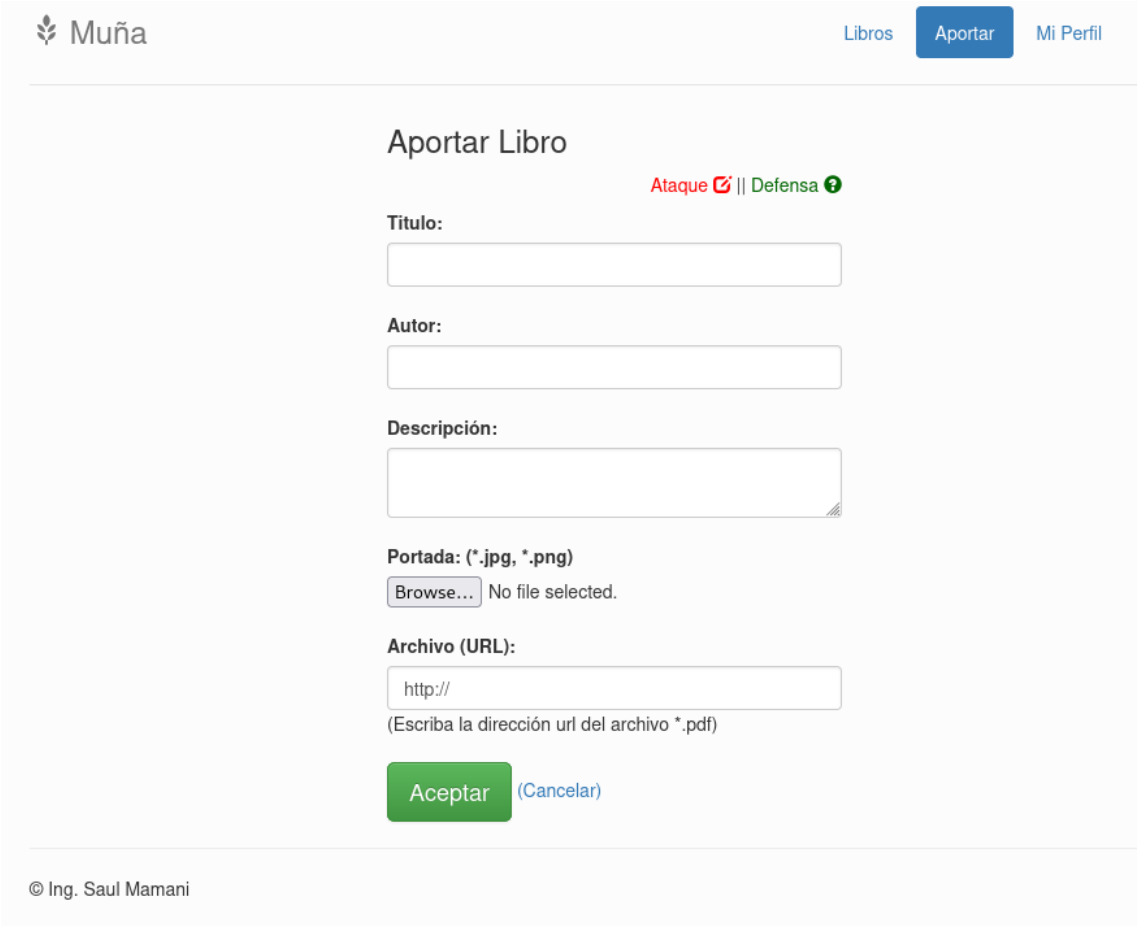
Introducción

Solucionar un error en la página de Muna para subir un libro y poder realizar un ataque XSS.

Registrar Aporte en Muna paso a paso.

En la pestaña Aportar de nuestra página web Muña se encuentran varios apartados que rellenar como vemos a continuación.

Joaquim Chagas Neto CCIEX 08/02/2024

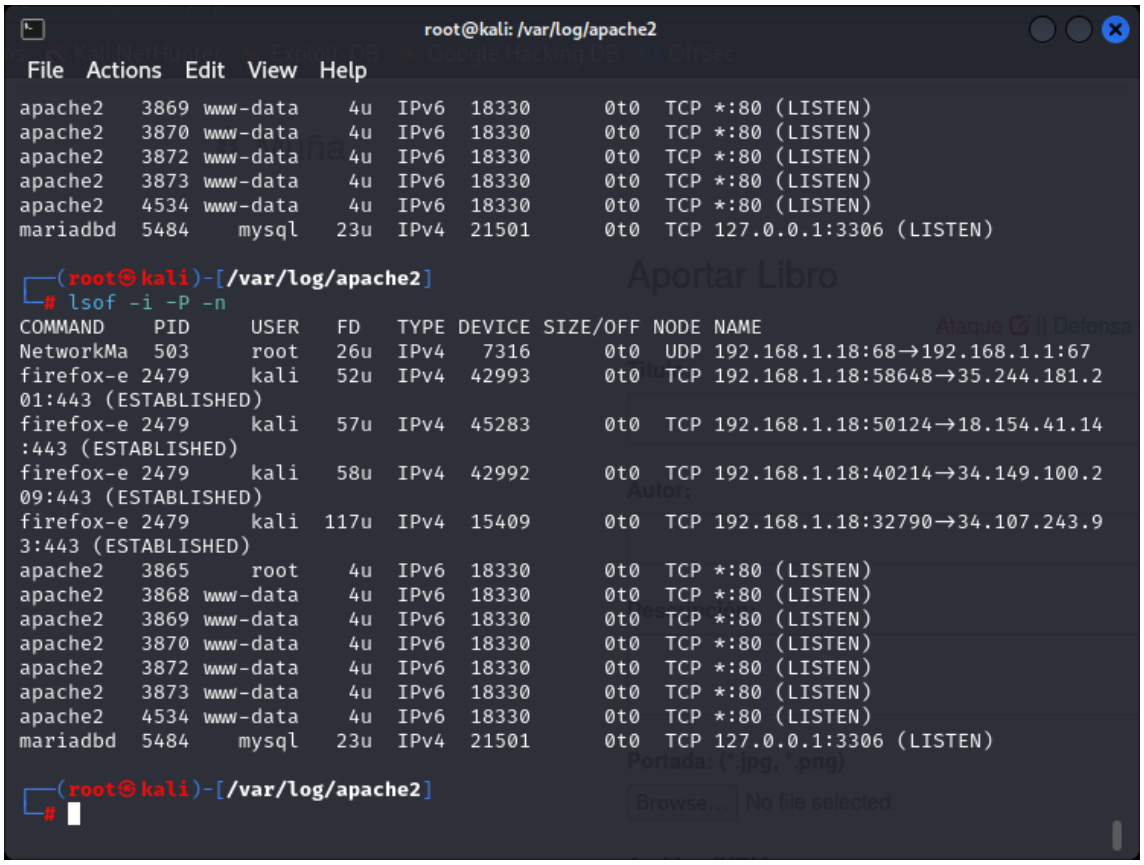


Al intentar Aportar un libro cualquiera nos saltaba un error en el registro.

Solución.

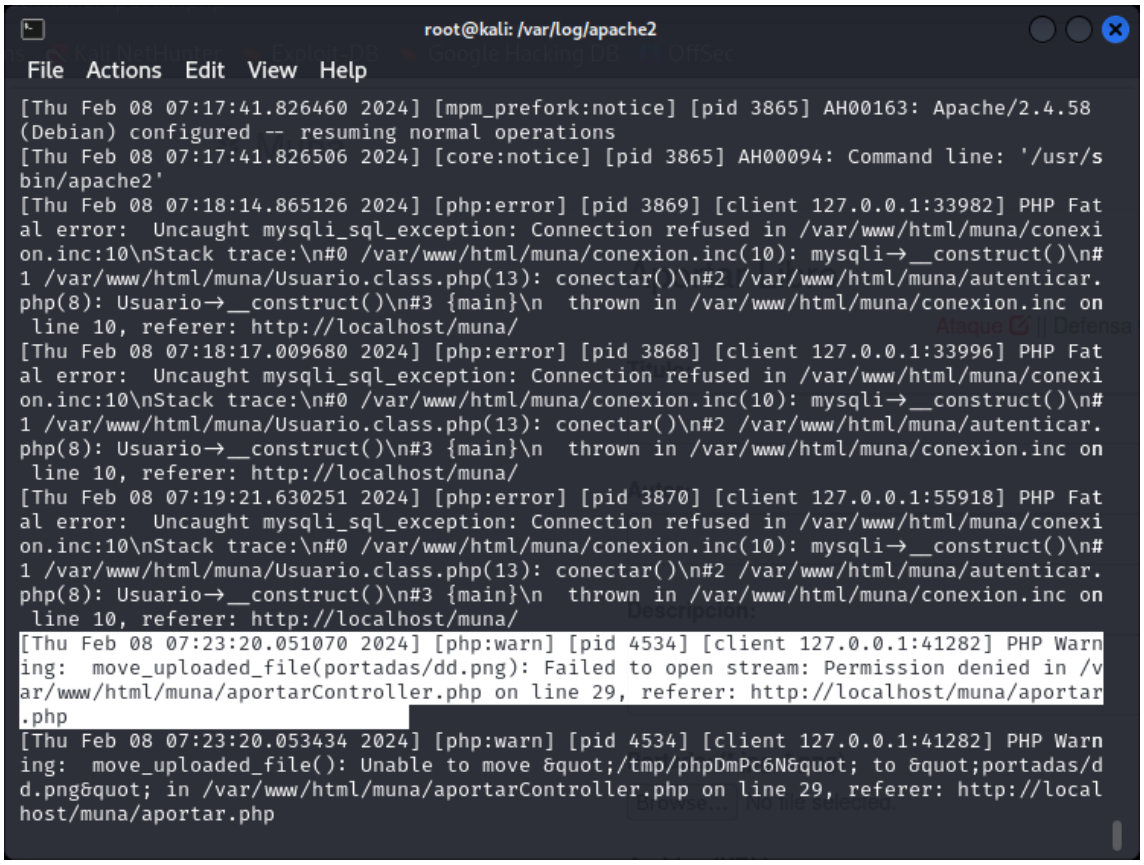
Ver quién tiene permisos para acceder a apache2.
En este caso haremos un lsof -i -P -n para poder ver quién puede acceder a ello.

Joaquim Chagas Neto CCIEX 08/02/2024



Seguidamente nos moveremos a la carpeta de logs de apache con el comando cd /var/log/apache2 y haremos un cat error.log para ver donde se produjo el error.

Joaquim Chagas Neto CCIEX 08/02/2024



Viendo el log de error nos dice básicamente que hubo un permission denied en var/www/html/muna/aportarController.php.

Por lo tanto, tendremos que modificar los permisos de los grupos y usuarios que puedan utilizar este recurso.

Con un ls -l vemos quienes son los propietarios de los archivos de ../muna. No obstante, como ya vimos antes en el lsof -i -P -n apache utiliza el grupo www-data.

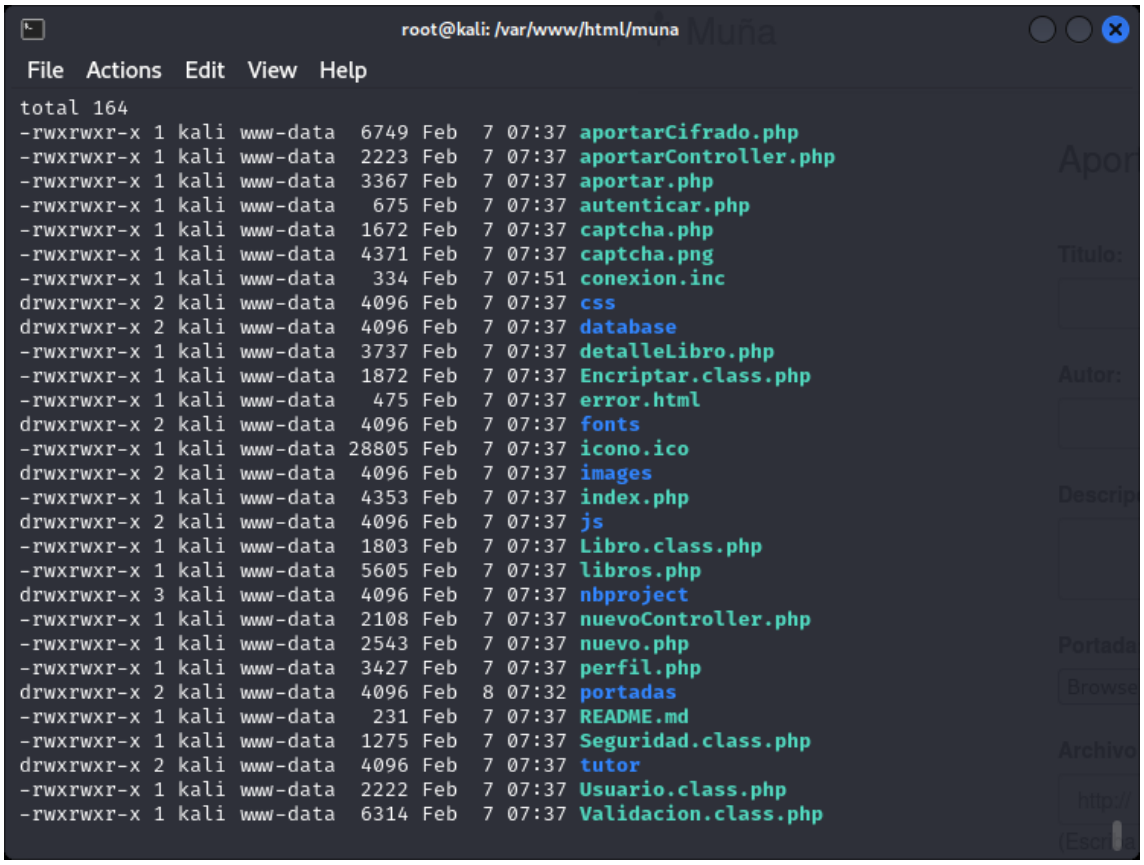
Siguiendo esta línea tendremos que otorgar privilegios de manera recursiva al grupo www-data con el comando chgrp -R www-dat * en la carpeta de muna.

Aún así no tenemos el privilegio de poder escribir en la página con este usuario/grupo. Para solucionar esta situación tendremos que ejecutar el comando chmod -R g+w * dentro de la carpeta muna.

Después de haber realizado estos pasos tendríamos ya el poder de escribir y leer archivos como grupo www-data en Muna.

Verificamos que esto es así con un ls -l.

Joaquim Chagas Neto CCIEX 08/02/2024

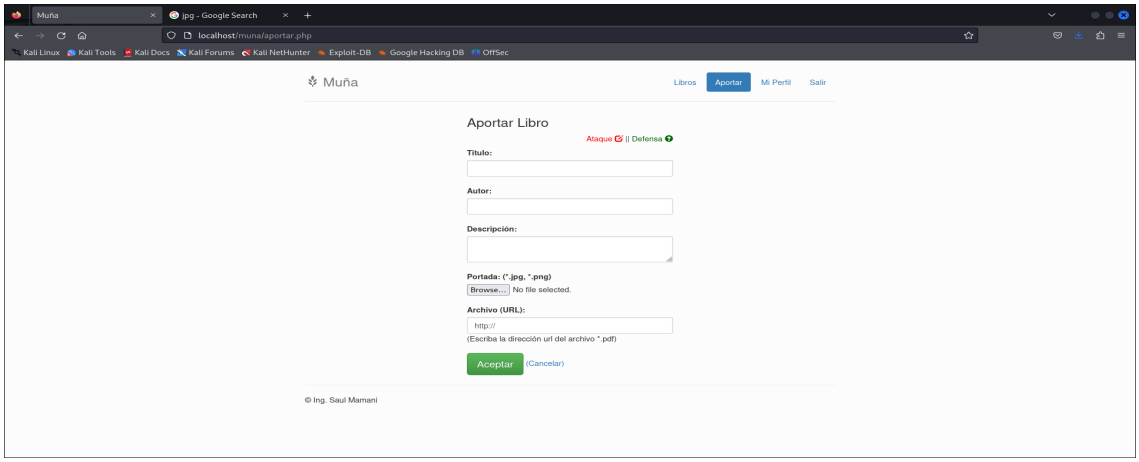


Vemos que el propietario de la carpeta es Kali pero www-data tiene permisos en ella.

Prueba Final.

Accedemos a la página de Muna, en mi caso 127.0.0.1/muna.

Creamos un usuario y entramos en la pestaña aportar.

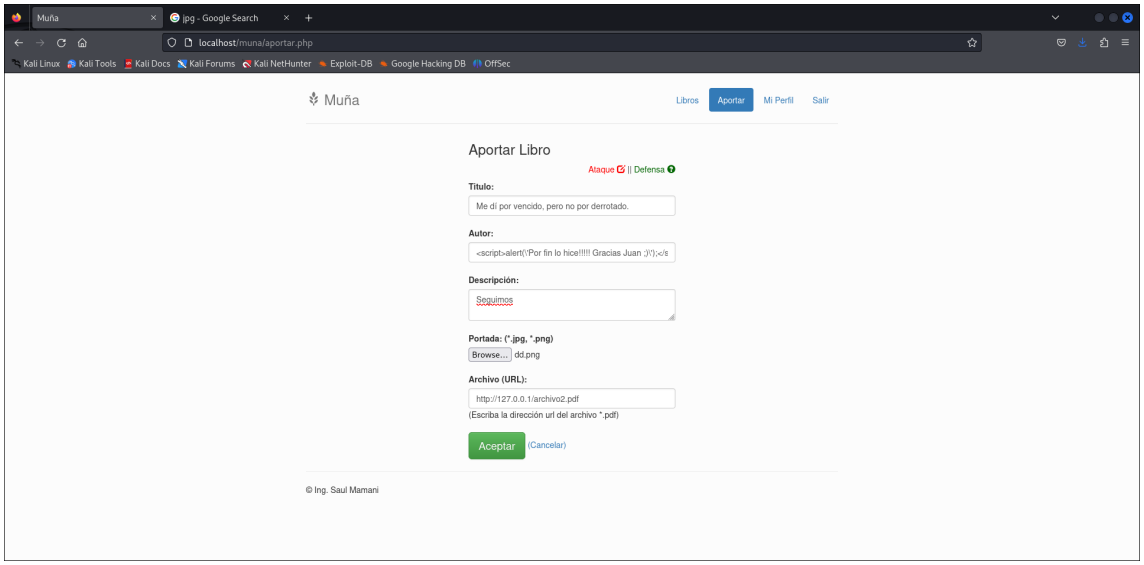


A partir de aquí rellenamos los diferentes apartados.

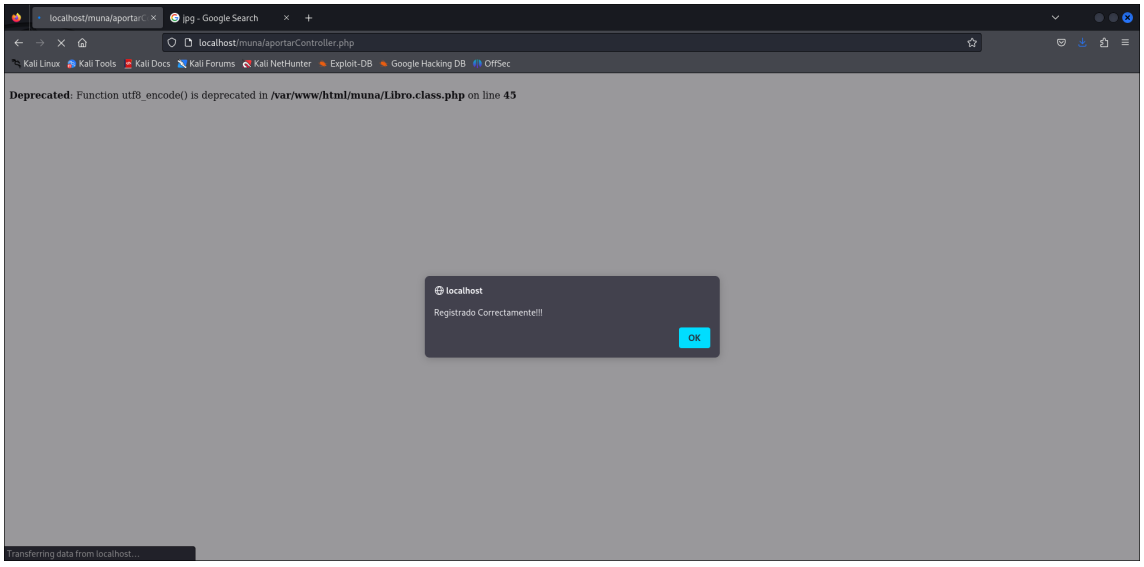
Joaquim Chagas Neto CCIEX 08/02/2024

Como estoy intentando hacer un XSS en esta página en el apartado Autor escribiremos nuestro código XSS:

<script>alert(\'Por fin lo hice!!!!! Gracias Juan ;)\');</script>

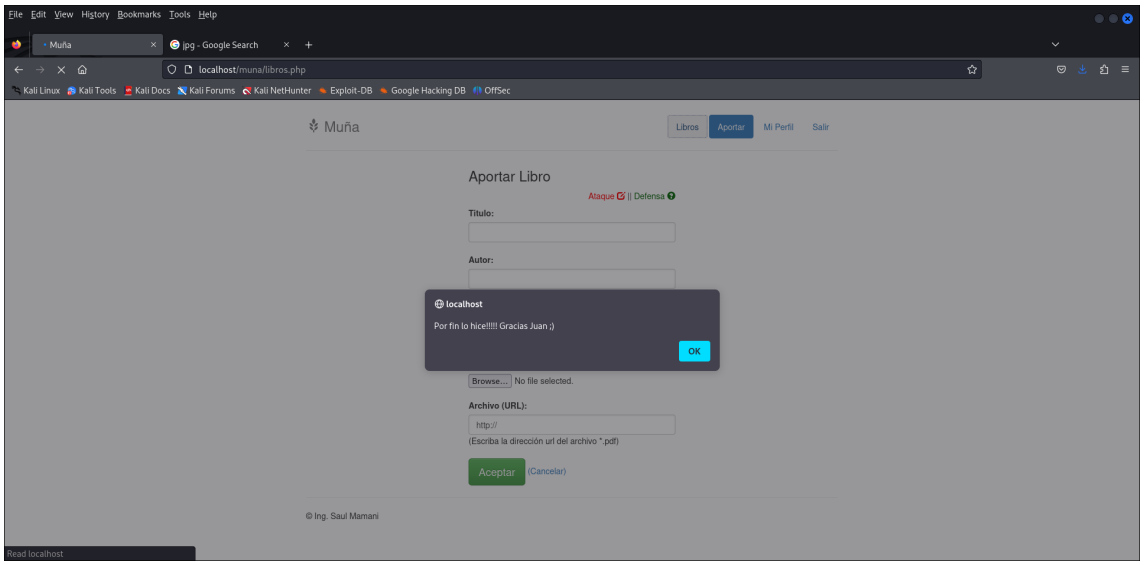


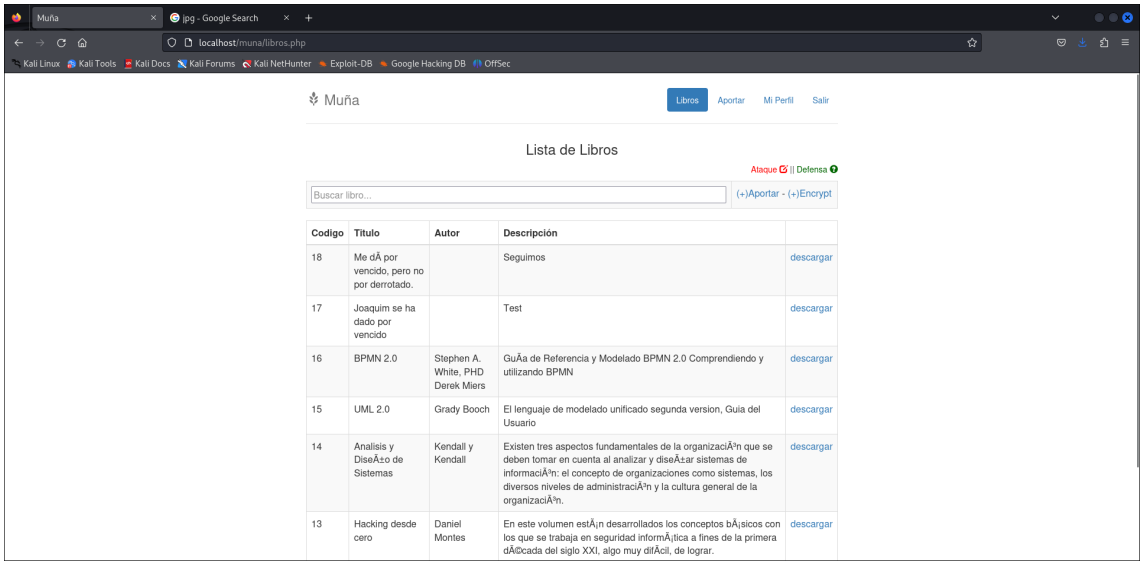
Y le damos a aceptar.



Observamos que se ha registrado correctamente, pero no vemos nuestro XSS, ¿Dónde estará? Para saber si lo hemos hecho bien o no tendremos que clickear en la pestaña libros y nos saltará nuestro código XSS.

Joaquim Chagas Neto CCIEX 08/02/2024



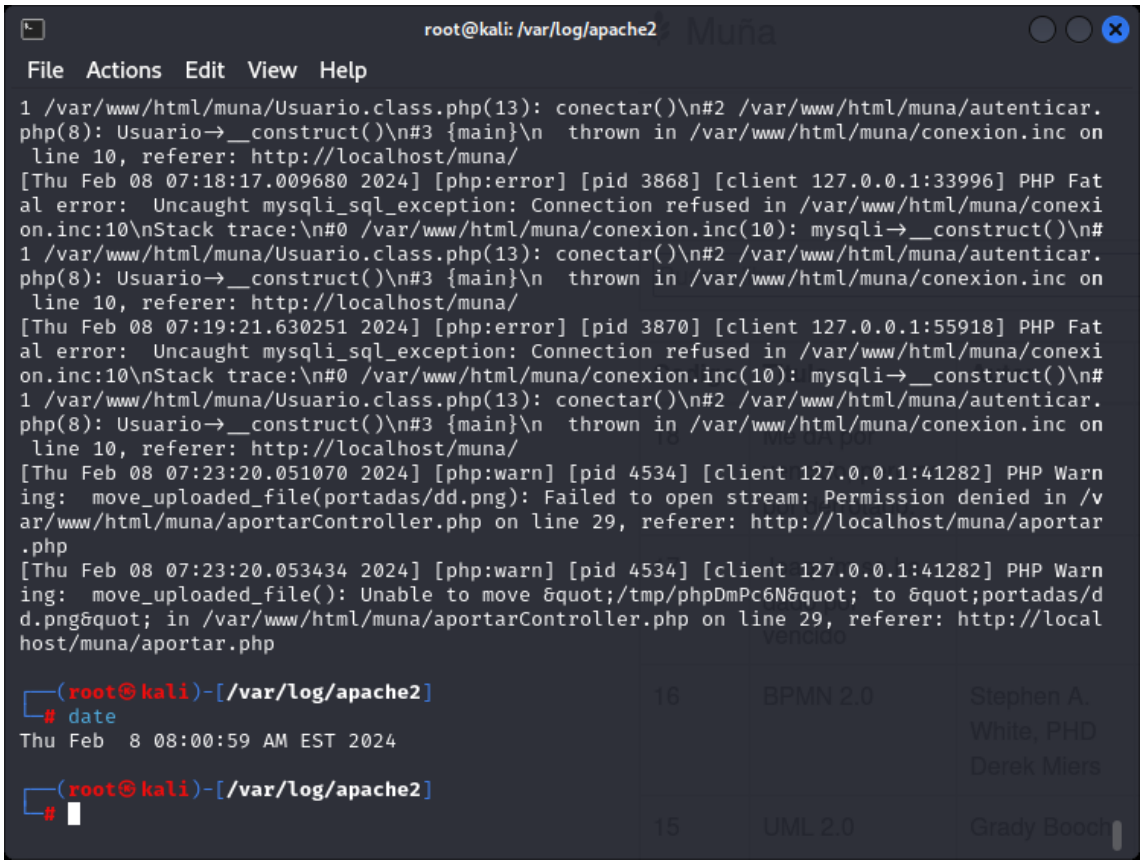


Se ha subido nuestro libro con nuestro código.

Verificación de Errores.

Nos vamos a nuestra carpeta de logs en apache (cd /var/logs/apache2) y hacemos un cat error.log. para ver si se produjo algún error mientras subimos el libro.

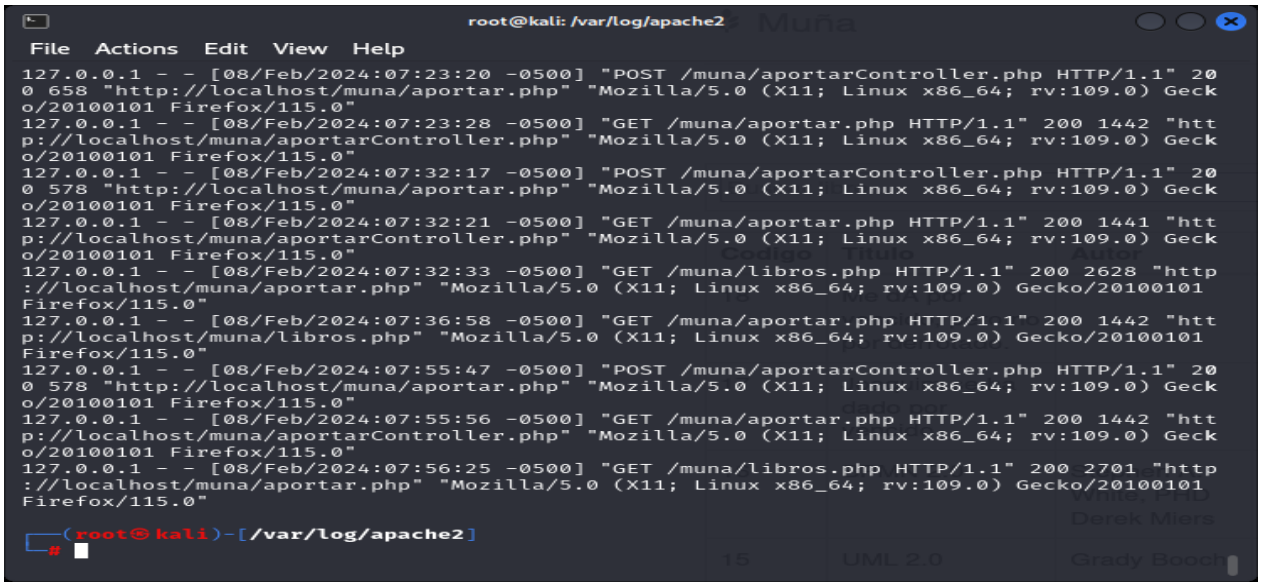
Joaquim Chagas Neto CCIEX 08/02/2024



El último error que hemos tenido fue el que no nos dejaba subir el archivo antes de realizar todos los pasos anteriores a las 7:23 horas.

Si nos vamos al archivo Access.log, observamos que se produjo un GET /muna/libros.php con código 200 en http://localhost/muna/aportar.php.

Esto indica que se subió el archivo sin problemas.



Joaquim Chagas Neto CCIEX 08/02/2024