

# XSS -- MUNA

## Contenido

Introducción .....	1
Registrar Aporte en Muna paso a paso. ....	1
Solución. ....	2
Prueba Final. ....	5
Verificación de Errores. ....	7

## *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.

## Aportar Libro

Ataque  || Defensa 

Título:

Autor:

Descripción:

Portada: (\*.jpg, \*.png)

 No file selected.

Archivo (URL):

(Escriba la dirección url del archivo \*.pdf)

 [\(Cancelar\)](#)

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.

```
root@kali: /var/log/apache2
File Actions Edit View Help
apache2 3869 www-data 4u IPv6 18330 0t0 TCP *:80 (LISTEN)
apache2 3870 www-data 4u IPv6 18330 0t0 TCP *:80 (LISTEN)
apache2 3872 www-data 4u IPv6 18330 0t0 TCP *:80 (LISTEN)
apache2 3873 www-data 4u IPv6 18330 0t0 TCP *:80 (LISTEN)
apache2 4534 www-data 4u IPv6 18330 0t0 TCP *:80 (LISTEN)
mariadb 5484 mysql 23u IPv4 21501 0t0 TCP 127.0.0.1:3306 (LISTEN)

(root@kali)-[/var/log/apache2]
# lsof -i -P -n
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
NetworkMa 503 root 26u IPv4 7316 0t0 UDP 192.168.1.18:68→192.168.1.1:67
firefox-e 2479 kali 52u IPv4 42993 0t0 TCP 192.168.1.18:58648→35.244.181.2
01:443 (ESTABLISHED)
firefox-e 2479 kali 57u IPv4 45283 0t0 TCP 192.168.1.18:50124→18.154.41.14
:443 (ESTABLISHED)
firefox-e 2479 kali 58u IPv4 42992 0t0 TCP 192.168.1.18:40214→34.149.100.2
09:443 (ESTABLISHED)
firefox-e 2479 kali 117u IPv4 15409 0t0 TCP 192.168.1.18:32790→34.107.243.9
3:443 (ESTABLISHED)
apache2 3865 root 4u IPv6 18330 0t0 TCP *:80 (LISTEN)
apache2 3868 www-data 4u IPv6 18330 0t0 TCP *:80 (LISTEN)
apache2 3869 www-data 4u IPv6 18330 0t0 TCP *:80 (LISTEN)
apache2 3870 www-data 4u IPv6 18330 0t0 TCP *:80 (LISTEN)
apache2 3872 www-data 4u IPv6 18330 0t0 TCP *:80 (LISTEN)
apache2 3873 www-data 4u IPv6 18330 0t0 TCP *:80 (LISTEN)
apache2 4534 www-data 4u IPv6 18330 0t0 TCP *:80 (LISTEN)
mariadb 5484 mysql 23u IPv4 21501 0t0 TCP 127.0.0.1:3306 (LISTEN)

(root@kali)-[/var/log/apache2]
#
```

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.

```
root@kali: /var/log/apache2

File Actions Edit View Help

[Thu Feb 08 07:17:41.826460 2024] [mpm_prefork:notice] [pid 3865] AH00163: Apache/2.4.58 (Debian) configured -- resuming normal operations
[Thu Feb 08 07:17:41.826506 2024] [core:notice] [pid 3865] AH00094: Command line: '/usr/sbin/apache2'
[Thu Feb 08 07:18:14.865126 2024] [php:error] [pid 3869] [client 127.0.0.1:33982] PHP Fatal error: Uncaught mysqli_sql_exception: Connection refused in /var/www/html/muna/conexion.inc:10\nStack trace:\n#0 /var/www/html/muna/conexion.inc(10): mysqli->__construct()\n#1 /var/www/html/muna/Usuario.class.php(13): conectar()\n#2 /var/www/html/muna/autenticar.php(8): Usuario->__construct()\n#3 {main}\n thrown in /var/www/html/muna/conexion.inc on line 10, referer: http://localhost/muna/
[Thu Feb 08 07:18:17.009680 2024] [php:error] [pid 3868] [client 127.0.0.1:33996] PHP Fatal error: Uncaught mysqli_sql_exception: Connection refused in /var/www/html/muna/conexion.inc:10\nStack trace:\n#0 /var/www/html/muna/conexion.inc(10): mysqli->__construct()\n#1 /var/www/html/muna/Usuario.class.php(13): conectar()\n#2 /var/www/html/muna/autenticar.php(8): Usuario->__construct()\n#3 {main}\n thrown in /var/www/html/muna/conexion.inc on line 10, referer: http://localhost/muna/
[Thu Feb 08 07:19:21.630251 2024] [php:error] [pid 3870] [client 127.0.0.1:55918] PHP Fatal error: Uncaught mysqli_sql_exception: Connection refused in /var/www/html/muna/conexion.inc:10\nStack trace:\n#0 /var/www/html/muna/conexion.inc(10): mysqli->__construct()\n#1 /var/www/html/muna/Usuario.class.php(13): conectar()\n#2 /var/www/html/muna/autenticar.php(8): Usuario->__construct()\n#3 {main}\n thrown in /var/www/html/muna/conexion.inc on line 10, referer: http://localhost/muna/
[Thu Feb 08 07:23:20.051070 2024] [php:warn] [pid 4534] [client 127.0.0.1:41282] PHP Warning: move_uploaded_file(portadas/dd.png): Failed to open stream: Permission denied in /var/www/html/muna/aportarController.php on line 29, referer: http://localhost/muna/aportar.php
[Thu Feb 08 07:23:20.053434 2024] [php:warn] [pid 4534] [client 127.0.0.1:41282] PHP Warning: move_uploaded_file(): Unable to move "/tmp/phpDmPc6N" to "portadas/dd.png" in /var/www/html/muna/aportarController.php on line 29, referer: http://localhost/muna/aportar.php
```

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

```
root@kali: /var/www/html/muna Muña
File Actions Edit View Help
total 164
-rwxrwxr-x 1 kali www-data 6749 Feb 7 07:37 aportarCifrado.php
-rwxrwxr-x 1 kali www-data 2223 Feb 7 07:37 aportarController.php
-rwxrwxr-x 1 kali www-data 3367 Feb 7 07:37 aportar.php
-rwxrwxr-x 1 kali www-data 675 Feb 7 07:37 autenticar.php
-rwxrwxr-x 1 kali www-data 1672 Feb 7 07:37 captcha.php
-rwxrwxr-x 1 kali www-data 4371 Feb 7 07:37 captcha.png
-rwxrwxr-x 1 kali www-data 334 Feb 7 07:51 conexion.inc
drwxrwxr-x 2 kali www-data 4096 Feb 7 07:37 css
drwxrwxr-x 2 kali www-data 4096 Feb 7 07:37 database
-rwxrwxr-x 1 kali www-data 3737 Feb 7 07:37 detalleLibro.php
-rwxrwxr-x 1 kali www-data 1872 Feb 7 07:37 Encriptar.class.php
-rwxrwxr-x 1 kali www-data 475 Feb 7 07:37 error.html
drwxrwxr-x 2 kali www-data 4096 Feb 7 07:37 fonts
-rwxrwxr-x 1 kali www-data 28805 Feb 7 07:37 icono.ico
drwxrwxr-x 2 kali www-data 4096 Feb 7 07:37 images
-rwxrwxr-x 1 kali www-data 4353 Feb 7 07:37 index.php
drwxrwxr-x 2 kali www-data 4096 Feb 7 07:37 js
-rwxrwxr-x 1 kali www-data 1803 Feb 7 07:37 Libro.class.php
-rwxrwxr-x 1 kali www-data 5605 Feb 7 07:37 libros.php
drwxrwxr-x 3 kali www-data 4096 Feb 7 07:37 nbproject
-rwxrwxr-x 1 kali www-data 2108 Feb 7 07:37 nuevoController.php
-rwxrwxr-x 1 kali www-data 2543 Feb 7 07:37 nuevo.php
-rwxrwxr-x 1 kali www-data 3427 Feb 7 07:37 perfil.php
drwxrwxr-x 2 kali www-data 4096 Feb 8 07:32 portadas
-rwxrwxr-x 1 kali www-data 231 Feb 7 07:37 README.md
-rwxrwxr-x 1 kali www-data 1275 Feb 7 07:37 Seguridad.class.php
drwxrwxr-x 2 kali www-data 4096 Feb 7 07:37 tutor
-rwxrwxr-x 1 kali www-data 2222 Feb 7 07:37 Usuario.class.php
-rwxrwxr-x 1 kali www-data 6314 Feb 7 07:37 Validacion.class.php
```

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.

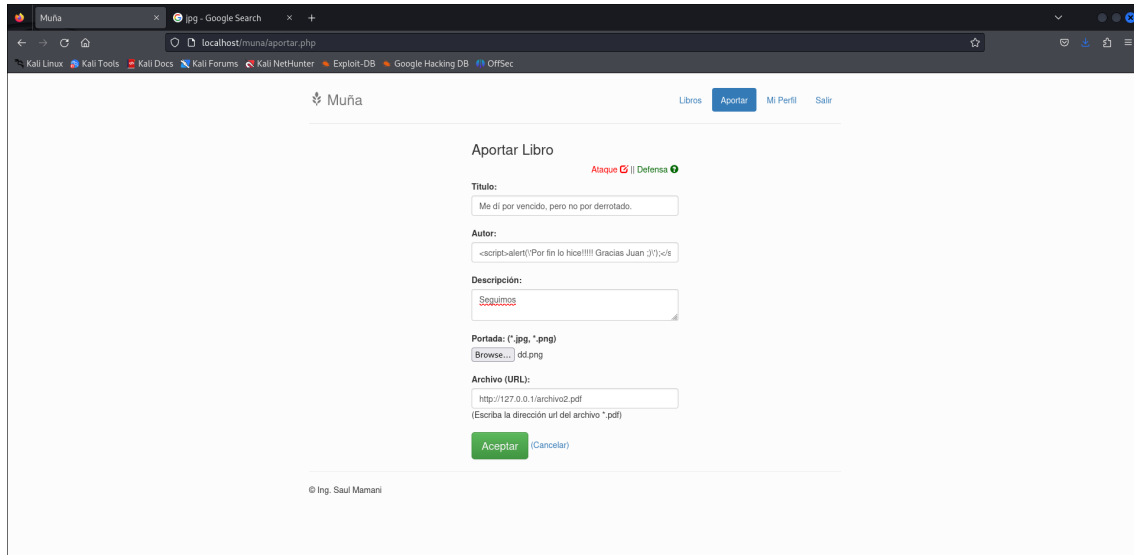
The screenshot shows a web browser window with the URL 'localhost/muna/aportar.php'. The page has a header with the 'Muña' logo and navigation links: 'Libros', 'Aportar' (highlighted), 'Mi Perfil', and 'Salir'. The main content area is titled 'Aportar Libro' and contains a form with the following fields: 'Titulo:', 'Autor:', 'Descripción:', 'Portada: (\* .jpg, \*.png)' with a 'Browse...' button, and 'Archivo (URL):' with a text input field containing 'http://'. Below the form are 'Aceptar' and '(Cancelar)' buttons. A status bar at the bottom indicates 'Ataque [X] | Defensa [X]'.

A partir de aquí rellenamos los diferentes apartados.

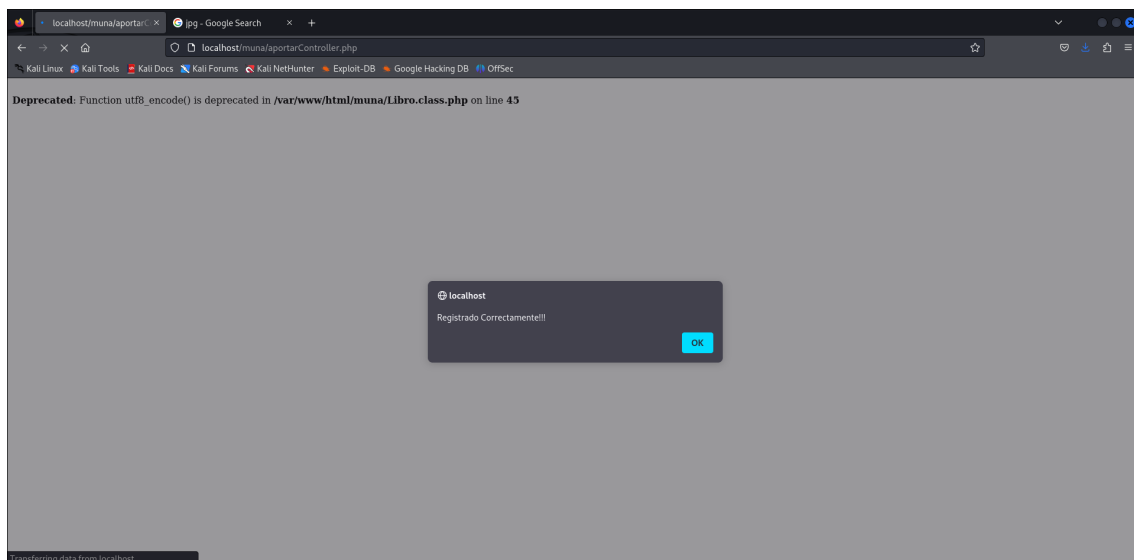
Joaquim Chagas Neto CCIEX 08/02/2024

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

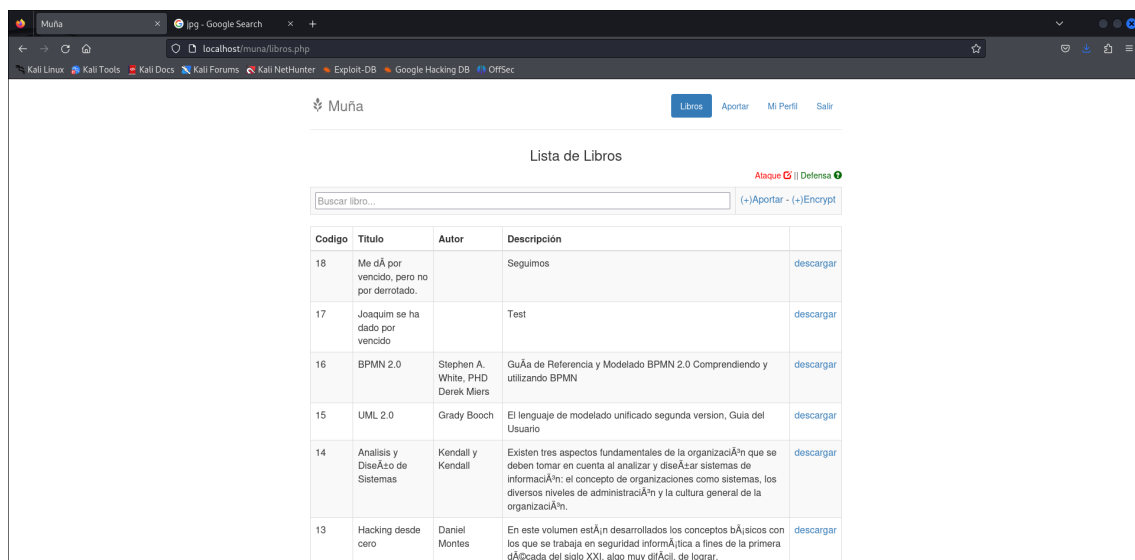
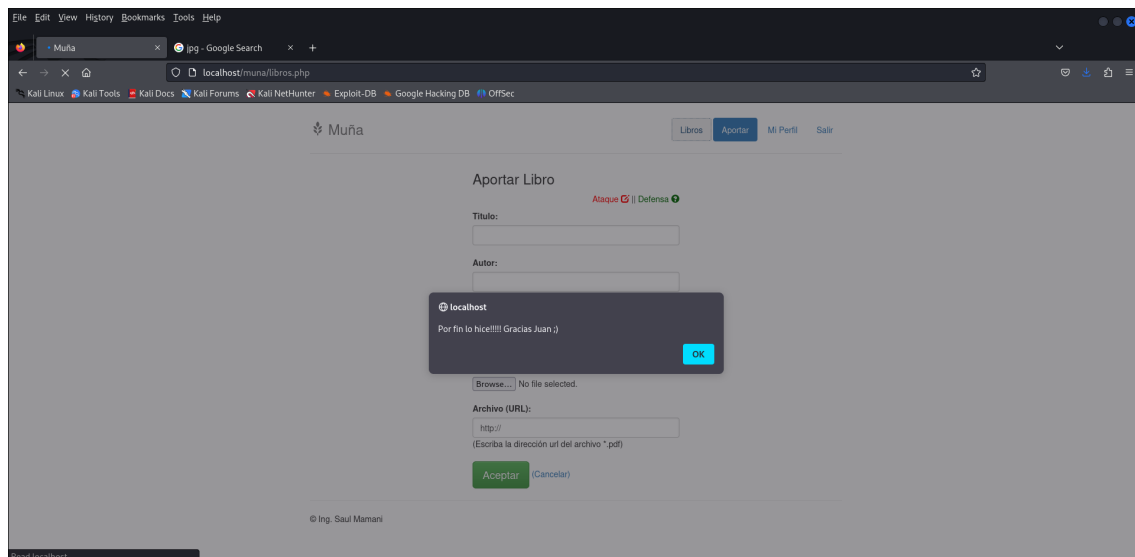
```
<script>alert('\Por fin lo hice!!!! Gracias Juan ;)\');</script>
```



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 clicar en la pestaña libros y nos saltará nuestro código XSS.



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

```
root@kali: /var/log/apache2 Muña
File Actions Edit View Help
1 /var/www/html/muna/Usuario.class.php(13): conectar()\n#2 /var/www/html/muna/autenticar.php(8): Usuario->__construct()\n#3 {main}\n thrown in /var/www/html/muna/conexion.inc on line 10, referer: http://localhost/muna/
[Thu Feb 08 07:18:17.009680 2024] [php:error] [pid 3868] [client 127.0.0.1:33996] PHP Fatal error: Uncaught mysqli_sql_exception: Connection refused in /var/www/html/muna/conexion.inc:10\nStack trace:\n#0 /var/www/html/muna/conexion.inc(10): mysqli->__construct()\n#1 /var/www/html/muna/Usuario.class.php(13): conectar()\n#2 /var/www/html/muna/autenticar.php(8): Usuario->__construct()\n#3 {main}\n thrown in /var/www/html/muna/conexion.inc on line 10, referer: http://localhost/muna/
[Thu Feb 08 07:19:21.630251 2024] [php:error] [pid 3870] [client 127.0.0.1:55918] PHP Fatal error: Uncaught mysqli_sql_exception: Connection refused in /var/www/html/muna/conexion.inc:10\nStack trace:\n#0 /var/www/html/muna/conexion.inc(10): mysqli->__construct()\n#1 /var/www/html/muna/Usuario.class.php(13): conectar()\n#2 /var/www/html/muna/autenticar.php(8): Usuario->__construct()\n#3 {main}\n thrown in /var/www/html/muna/conexion.inc on line 10, referer: http://localhost/muna/
[Thu Feb 08 07:23:20.051070 2024] [php:warn] [pid 4534] [client 127.0.0.1:41282] PHP Warning: move_uploaded_file(portadas/dd.png): Failed to open stream: Permission denied in /var/www/html/muna/aportarController.php on line 29, referer: http://localhost/muna/aportar.php
[Thu Feb 08 07:23:20.053434 2024] [php:warn] [pid 4534] [client 127.0.0.1:41282] PHP Warning: move_uploaded_file(): Unable to move "/tmp/phpDmPc6N" to "/portadas/dd.png" in /var/www/html/muna/aportarController.php on line 29, referer: http://localhost/muna/aportar.php

(root@kali)-[/var/log/apache2]
# date
Thu Feb 8 08:00:59 AM EST 2024

(root@kali)-[/var/log/apache2]
#
```

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.

```
root@kali: /var/log/apache2 Muña
File Actions Edit View Help
127.0.0.1 - - [08/Feb/2024:07:23:20 -0500] "POST /muna/aportarController.php HTTP/1.1" 200 658 "http://localhost/muna/aportar.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Feb/2024:07:23:28 -0500] "GET /muna/aportar.php HTTP/1.1" 200 1442 "http://localhost/muna/aportarController.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Feb/2024:07:32:17 -0500] "POST /muna/aportarController.php HTTP/1.1" 200 578 "http://localhost/muna/aportar.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Feb/2024:07:32:21 -0500] "GET /muna/aportar.php HTTP/1.1" 200 1441 "http://localhost/muna/aportarController.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Feb/2024:07:32:33 -0500] "GET /muna/libros.php HTTP/1.1" 200 2628 "http://localhost/muna/aportar.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Feb/2024:07:36:58 -0500] "GET /muna/aportar.php HTTP/1.1" 200 1442 "http://localhost/muna/libros.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Feb/2024:07:55:47 -0500] "POST /muna/aportarController.php HTTP/1.1" 200 578 "http://localhost/muna/aportar.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Feb/2024:07:55:56 -0500] "GET /muna/aportar.php HTTP/1.1" 200 1442 "http://localhost/muna/aportarController.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [08/Feb/2024:07:56:25 -0500] "GET /muna/libros.php HTTP/1.1" 200 2701 "http://localhost/muna/aportar.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"

(root@kali)-[/var/log/apache2]
#
```