1.
```
root@Kali:~# nmap -Pn --script vuln 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-10 16:30 PST
Nmap scan report for 192.168.1.110
Host is up (0.0013s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp  open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.1
10
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.1.110:80/
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=
1462626880ade1ac87bd9c93a&id=92a4423d01
|
|     Path: http://192.168.1.110:80/index.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=
1462626880ade1ac87bd9c93a&id=92a4423d01
|
|     Path: http://192.168.1.110:80/about.html
|     Form id:
|_    Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=
1462626880ade1ac87bd9c93a&id=92a4423d01
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /wordpress/: Blog
|   /wordpress/wp-login.php: Wordpress login page.
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (
debian)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (
debian)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (d
ebian)'
|   /manual/: Potentially interesting folder
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.1
0 (debian)'
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp open  rpcbind
```

Flag 1.txt

2.
```
<!-- End footer Area -->
<!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
```

Command

```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <> (0 / 10)  0.00%  ETA: ??:??:?
 Brute Forcing Author IDs - Time: 00:00:00 <> (1 / 10) 10.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (2 / 10) 20.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (3 / 10) 30.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:01 <> (7 / 10) 70.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:01 <> (8 / 10) 80.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:01 <> (10 / 10) 100.00% Time: 00:00
:01

[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection
)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection
)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Wordpress Vulnerability

```
[+] http://192.168.1.110/wordpress/
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] http://192.168.1.110/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] http://192.168.1.110/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] http://192.168.1.110/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.17 identified (Latest, released on 2021-05-13).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.17'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.17'
```