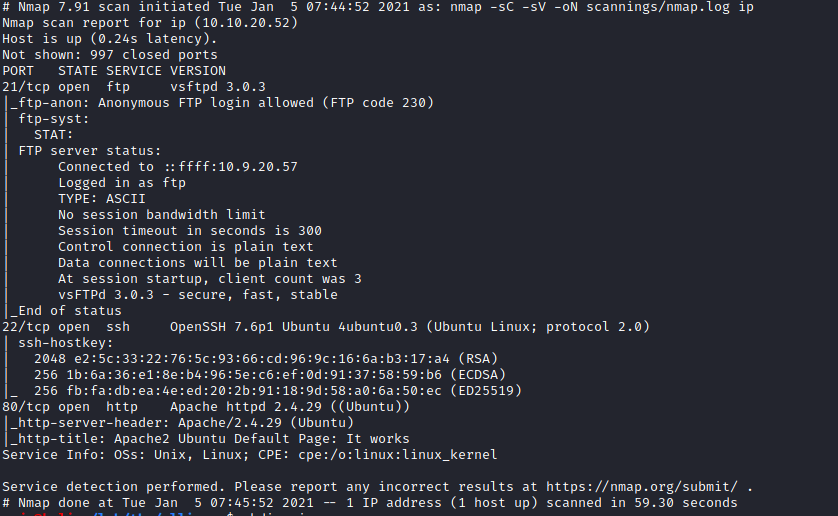
All In One

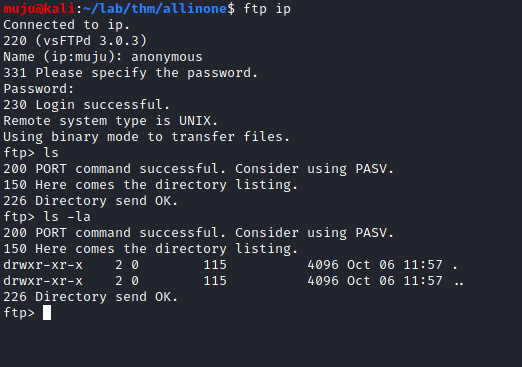
This is a fun box where we can find many ways where we can exploit let’s see how we can get the root into it let’s begin

SCANNING:-

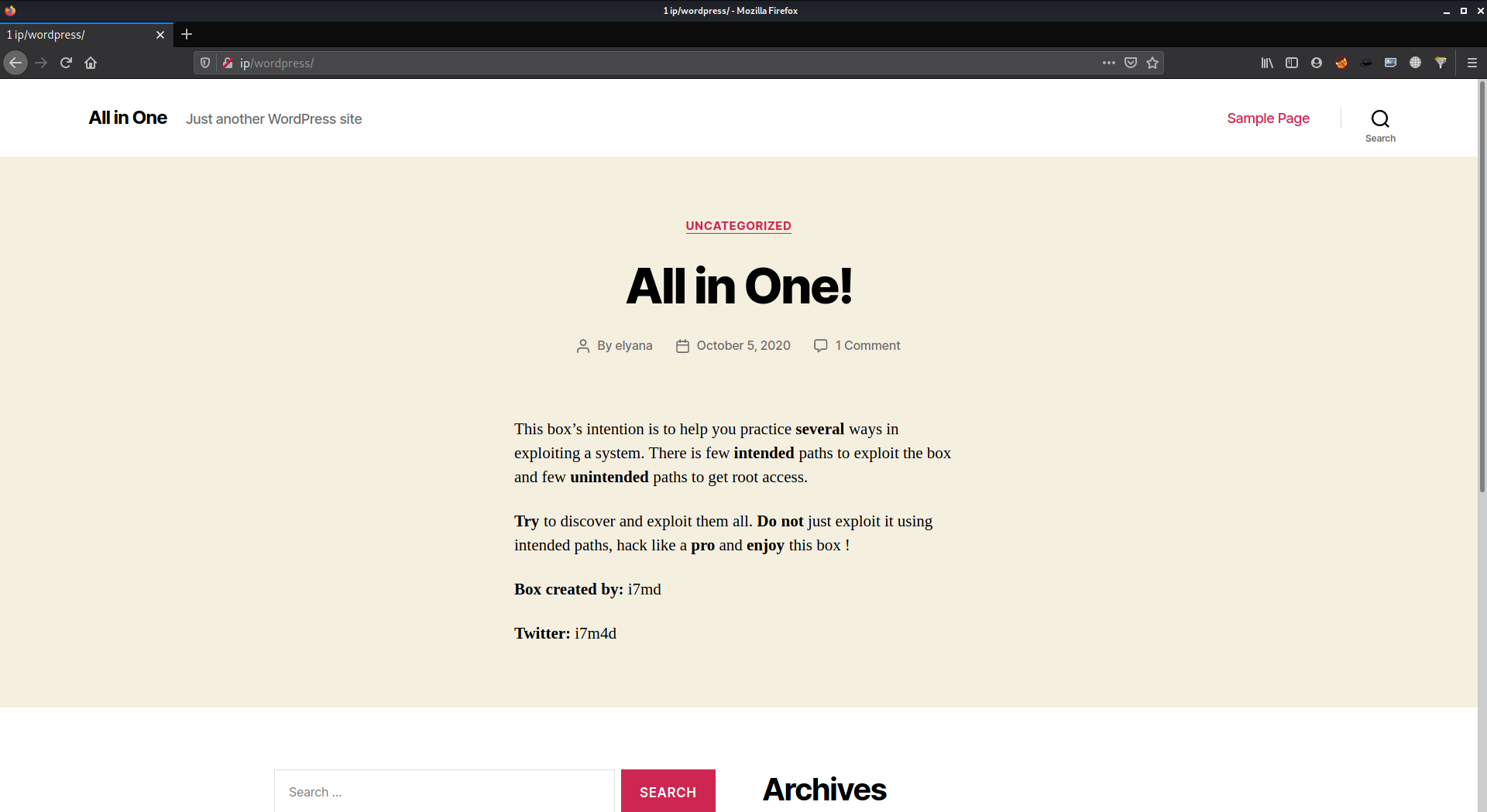
As we always do let’s start scanning the box for the open ports with Nmap gobuster for web directories and Nikto for common vulnerability



By looking at the results we there are three ports open FTP SSH and APACHE web server. We can also see that anonymous ftp logins are allowed let’s hope into FTP to find what’s present in it

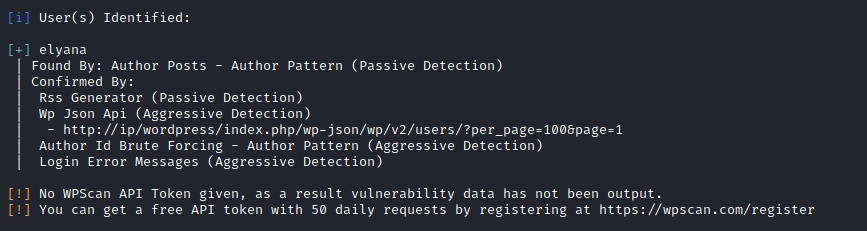


It seems to be the FTP is currently empty let’s check for the APACHE web server we ALL IN ONE page of WordPress it was also identified by the gobuster



ENUMERATING:-

Let’s start WordPress scanner and ENUMERATE users to find the user names for login into the WordPress to gain the access

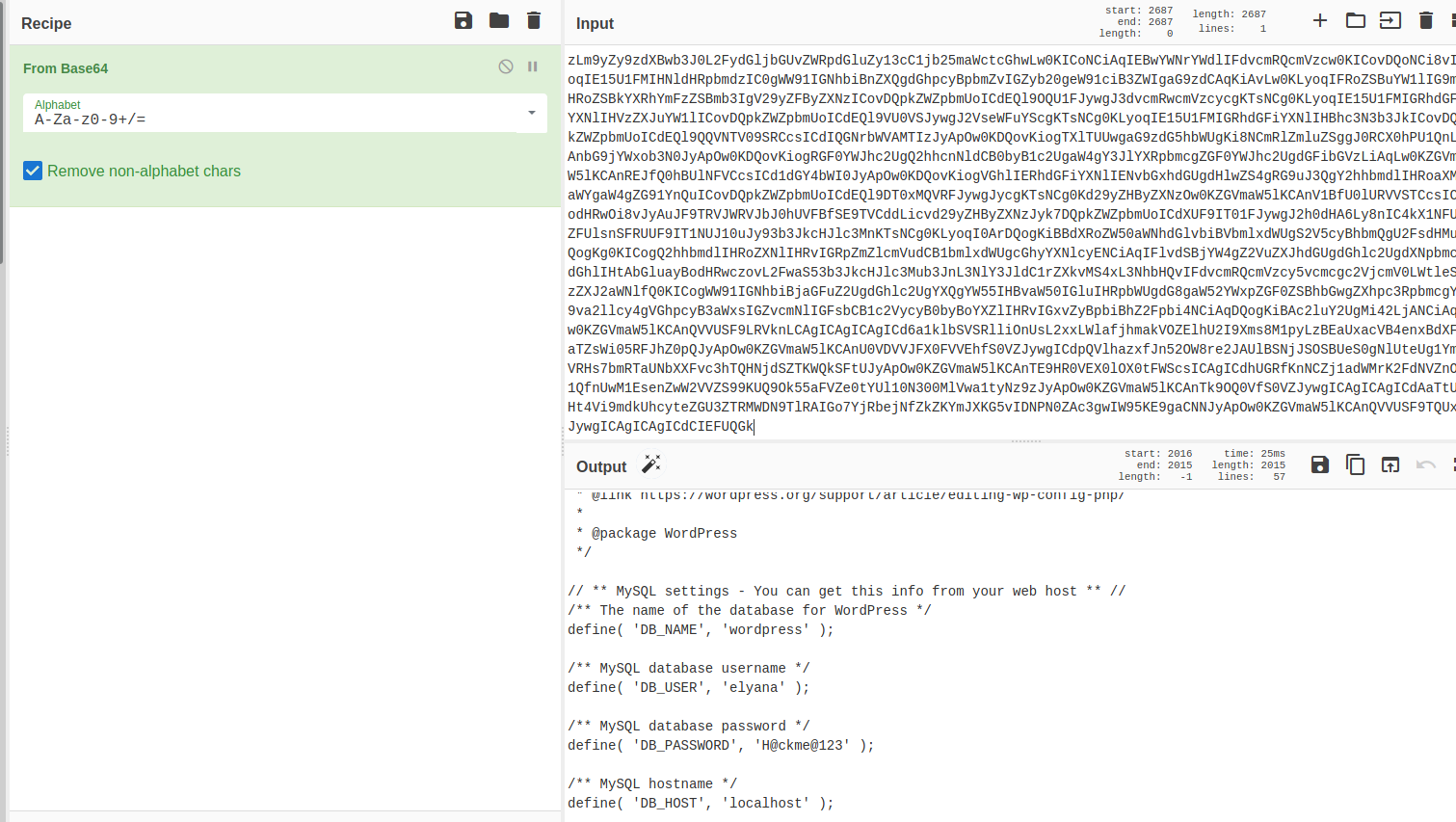


We got the username and need to escalate the passwd for login this we can do by using a vulnerability plugin installed in the WordPress which contains The File Inclusion vulnerability ( LFI ) allows an attacker to include a file

http://ip/wordpress/wp-content/plugins/mail-masta/inc/campaign/count\_of\_send.php?pl=php://filter/convert.base64-encode/resource=../../../../../wp-config.php

We are PHP filters for converting the code into the base64 format and by decrypting it we can able to see the code clearly in plain text

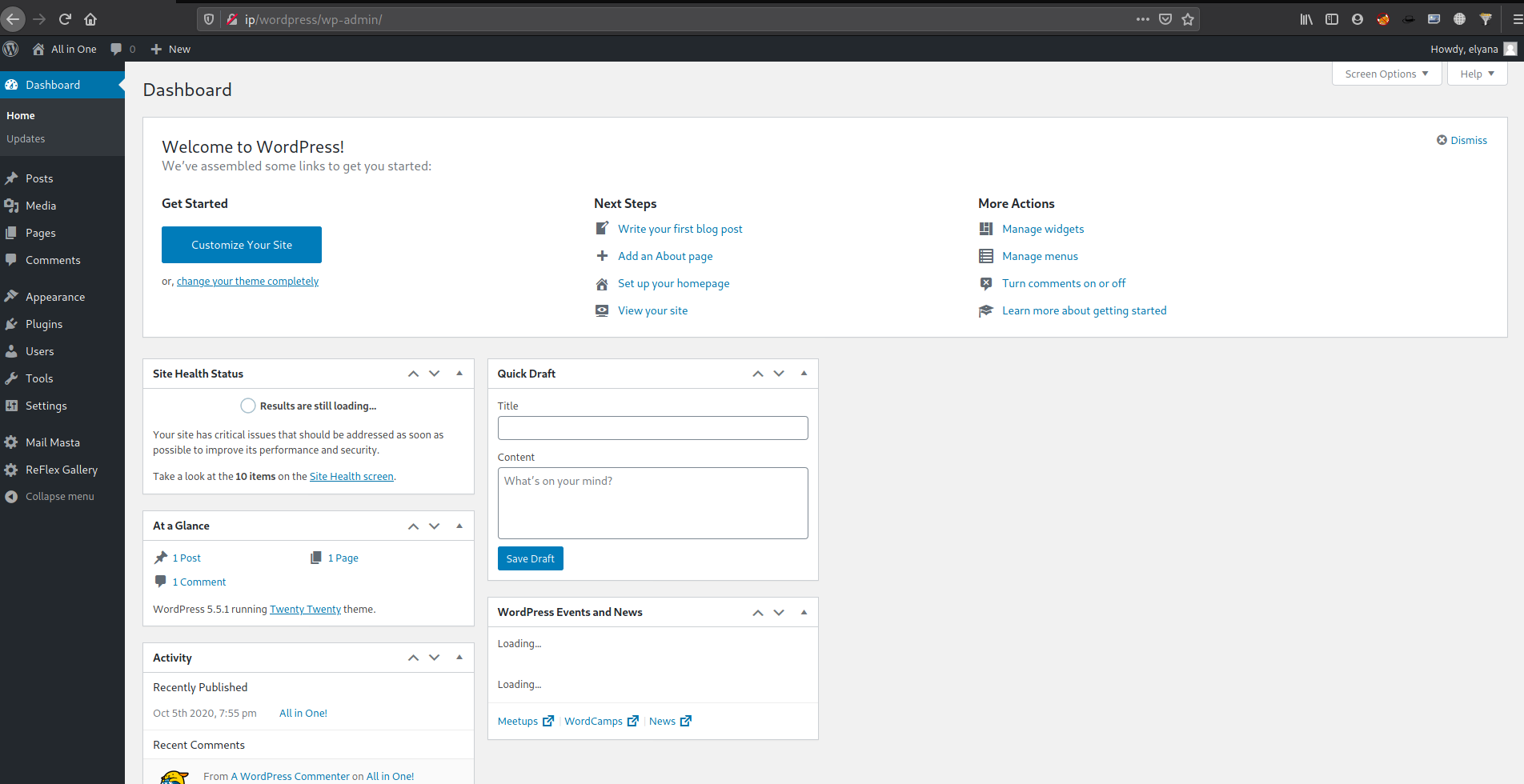
We can use the cyber chef for decrypting it is one of my favorite fools for encryption, encoding, compression, and data analysis.



As It was the easy box we have the same credentials for both database and WordPress

WORDPRESS:-

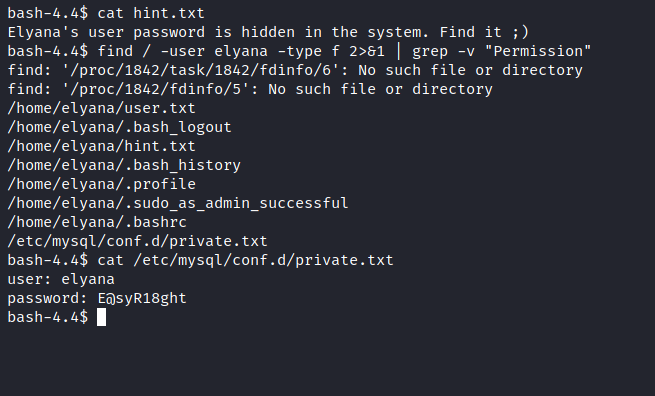
Let’s hope in into the WordPress and get a quick reverse shell from it



Am using my plugin for the reverse shell we can also use the website files to get the reverse shell once we got the shell and Navigate into the home directory we have a hint here saying that the password is saved in the box we need to find them

FIND:-

Am using find followed by the user and type as a file, sending an error message to null



ROOT ESCALATION:-

We got the credentials let’s escalate the user to root by knowing what permissions have been given to the user. We can use socat It can be used to break out from restricted environments by spawning an interactive system shell. Let’s break the restricted shell and BOOM we are ROOT

