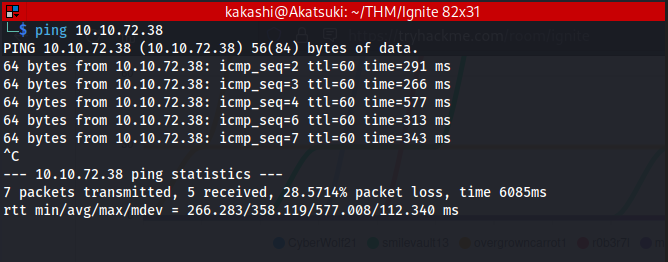
CTF Writeups

Try Hack Me

Ignite

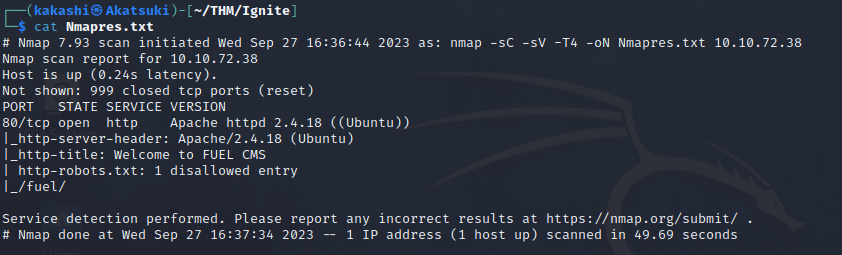
Machine IP: 10.10.72.38

Checking the Connectivity of the Target Machine:

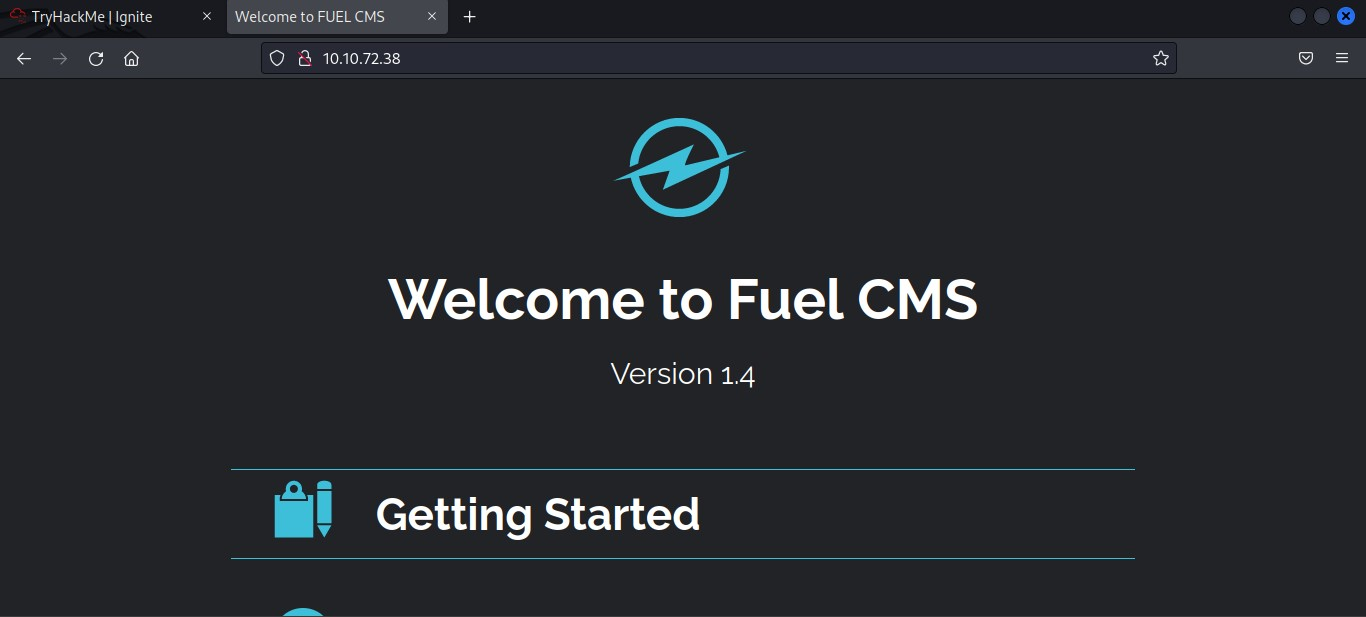


The Target Machine is up and we are gonna check for the open ports on the target machine using nmap tool:

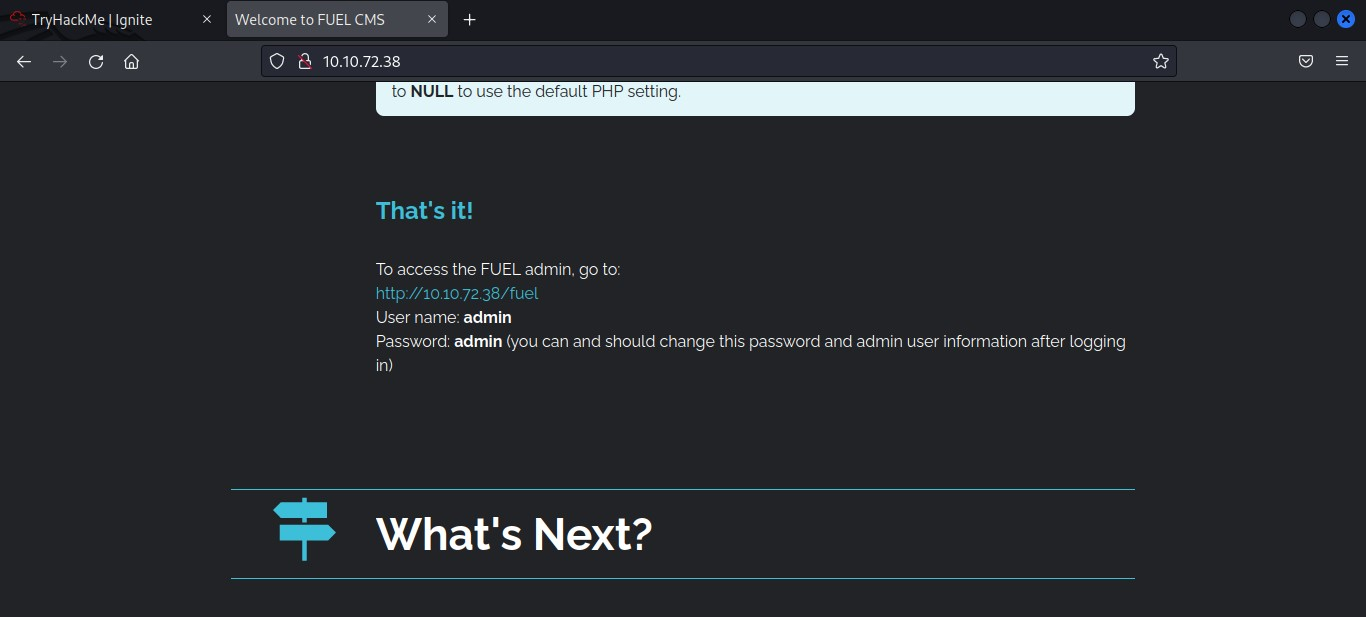
**sudo nmap -sV -sC -T4 -oN Nmapres.txt 10.10.72.38**

****

We Found only port 80 is open, Try visit the webpage in the browser,



While Surfing through the Mainpage of the Fuel CMS website we found a credentials for the fuel dashboard page,

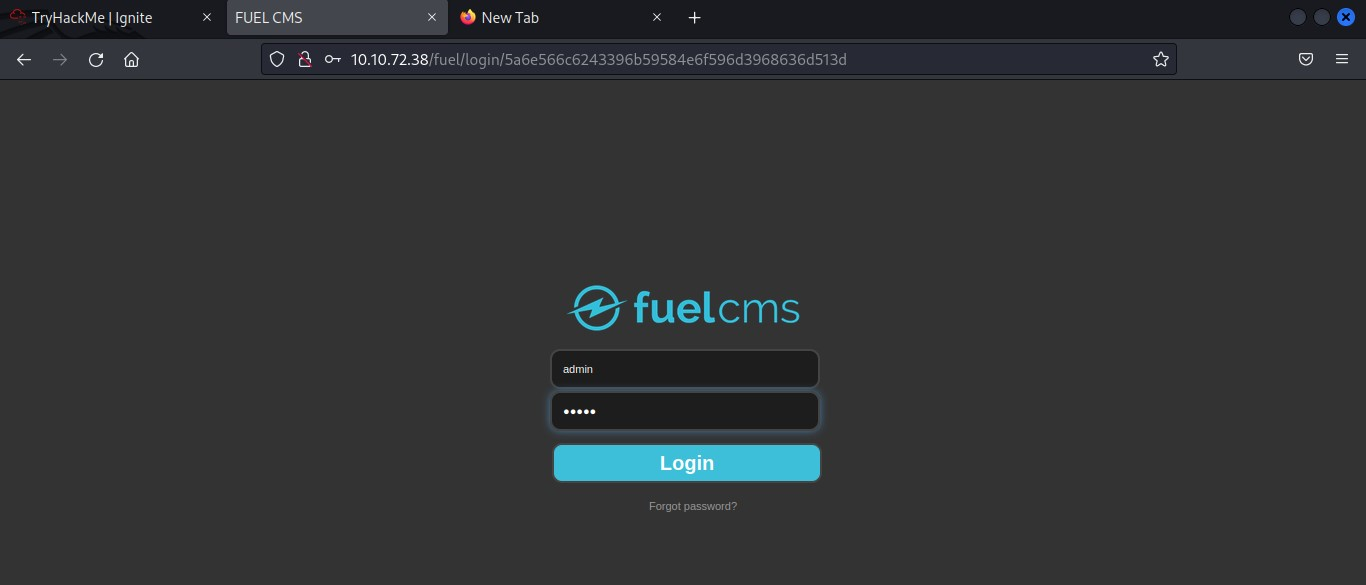


Navigate Through the Dashboard Page,

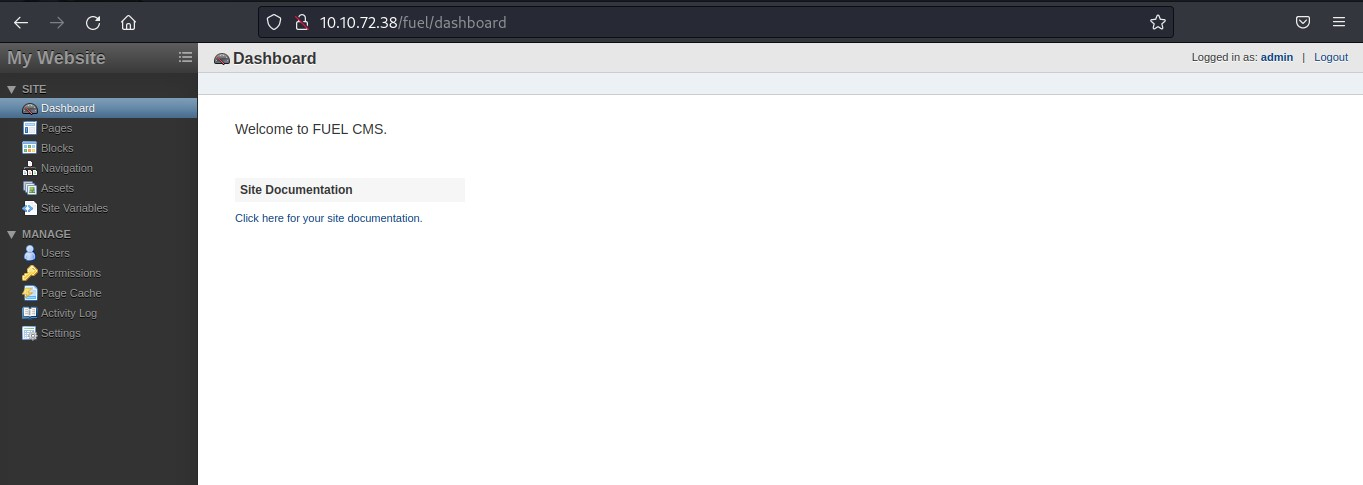
Fuel CMS Admin Credentials,

Username: **admin**

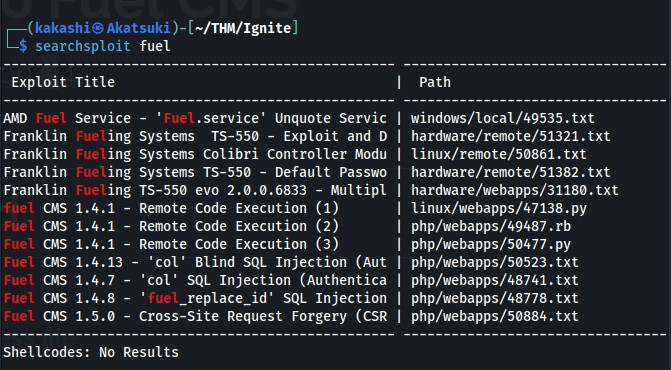
Password: **admin**



We got the Admin Dashboard Panel,



Since there is no useful information in the admin dashboard and in the website, Try Searchsploit to check whether there is any vulnerability related to Fuel CMS.



From the Fuel CMS Mainpage we found that its version is 1.4, That version of Fuel CMS is vulnerable to Remote Code Execution.

Clone the Python code from the Above searchsploit result to the current Directory.

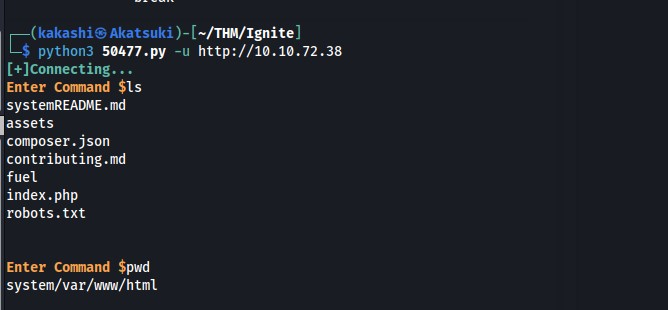
To Clone the Code to the Local Directory Use the below code:

**searchsploit -m php/webapps/50477.py**  
-m flag means mirror

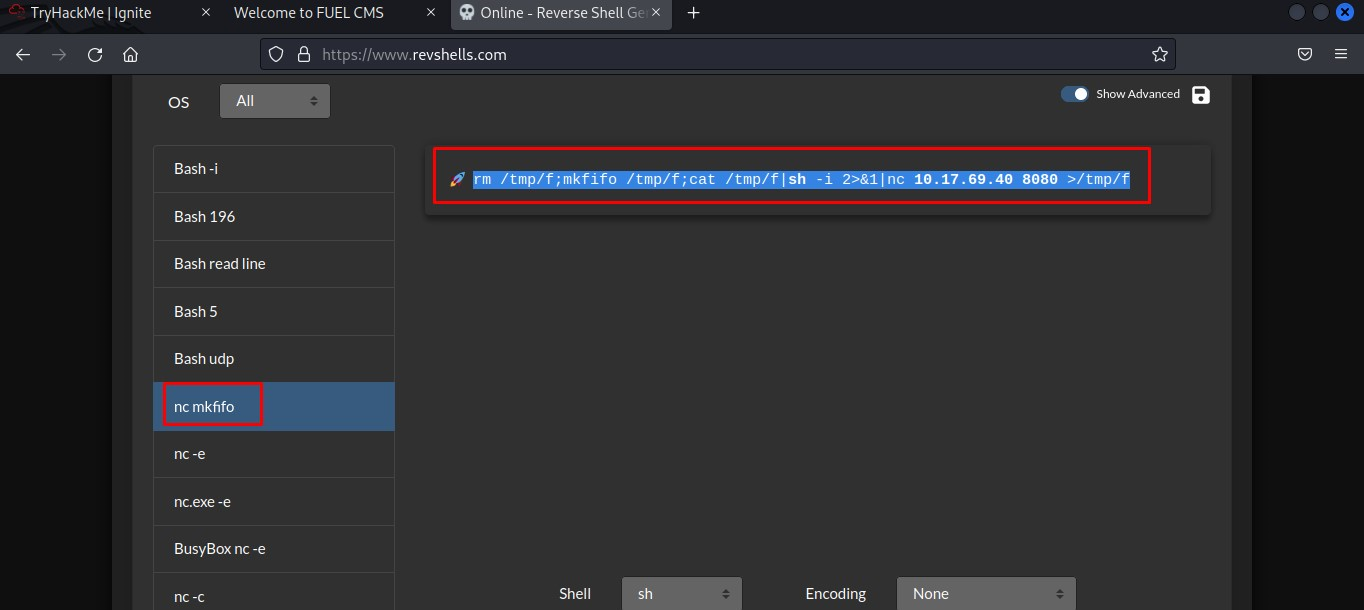
Analysis the Python code,.



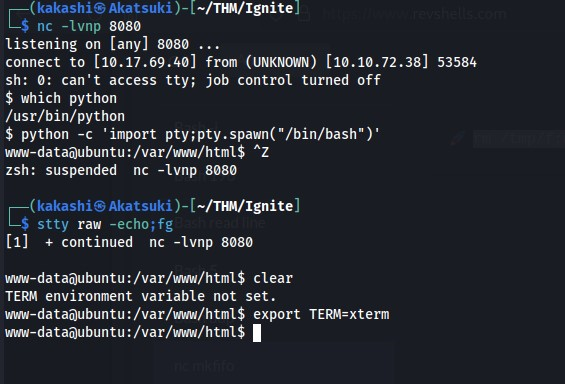
This Python Code does not require any listening port or ip address in its code, we need to directly run the python code along with specifying the ip addr of the Target machine.



We are able to run bash commands in the shell spawned in the above, So we can use netcat to gain shell, Try revshells.com to generate code for gaining the shell.

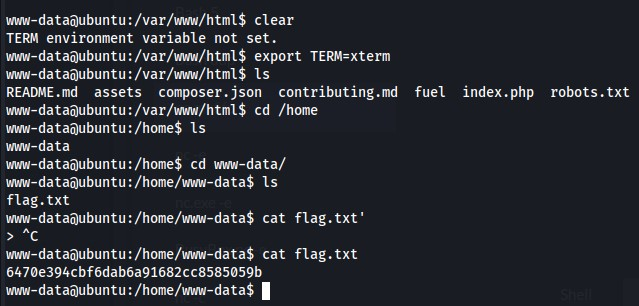


By executing the above nc shell code we are able to spawn a dedicated shell using netcat.



We have gained shell and made it stable with the above code.

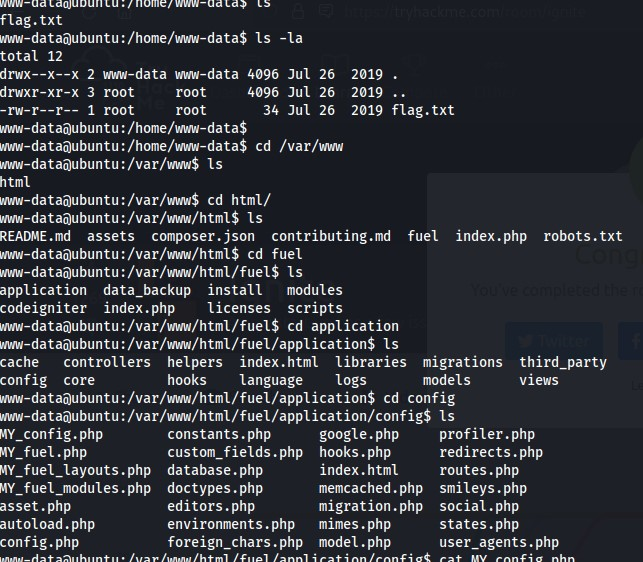
Now Surf through the file system to find the flags.



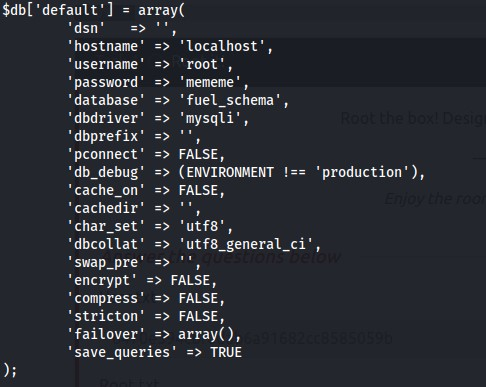
We have found one flag, To find the other flag that is root flag we need to Escalate to the root accout. Since Sudo -l does not work and www-data does not have password, We need to find the password for the root account, The only way to find the password of the root account is to completely analyze the file system.

Since Fuel CMS is a Database we need to find the database file that contains the credential of the users.

The Database file is found at the below directory.



While analyzing the **database.php** file,

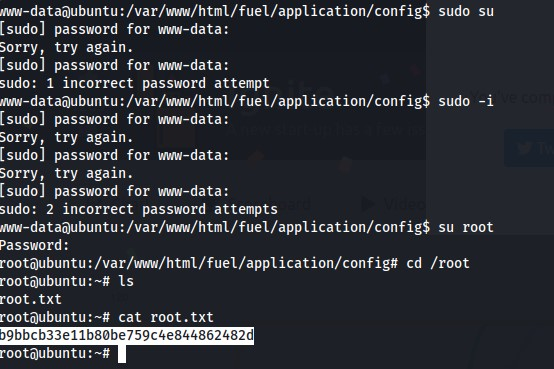


We found the password for the user root, the credentials are,

Username: **root**

Password: **mememe**

Since these credentials are for the database, there might be a chance to use the same credentials for the web server also, Lets give a try.



Bingo, We found the root flag.