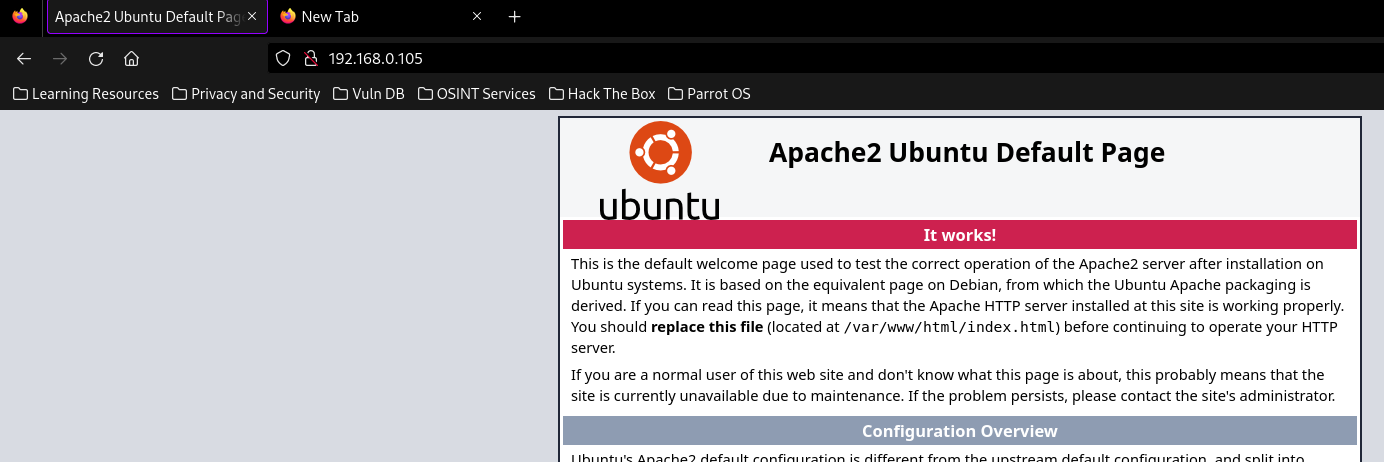
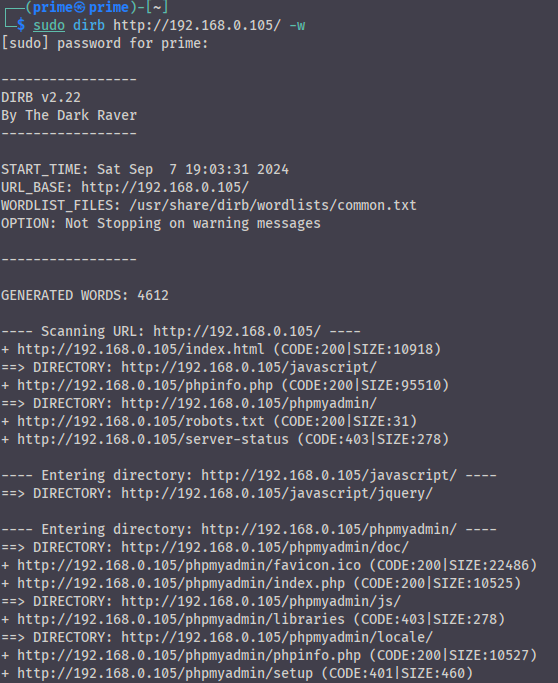
Callobes vulnerable machine



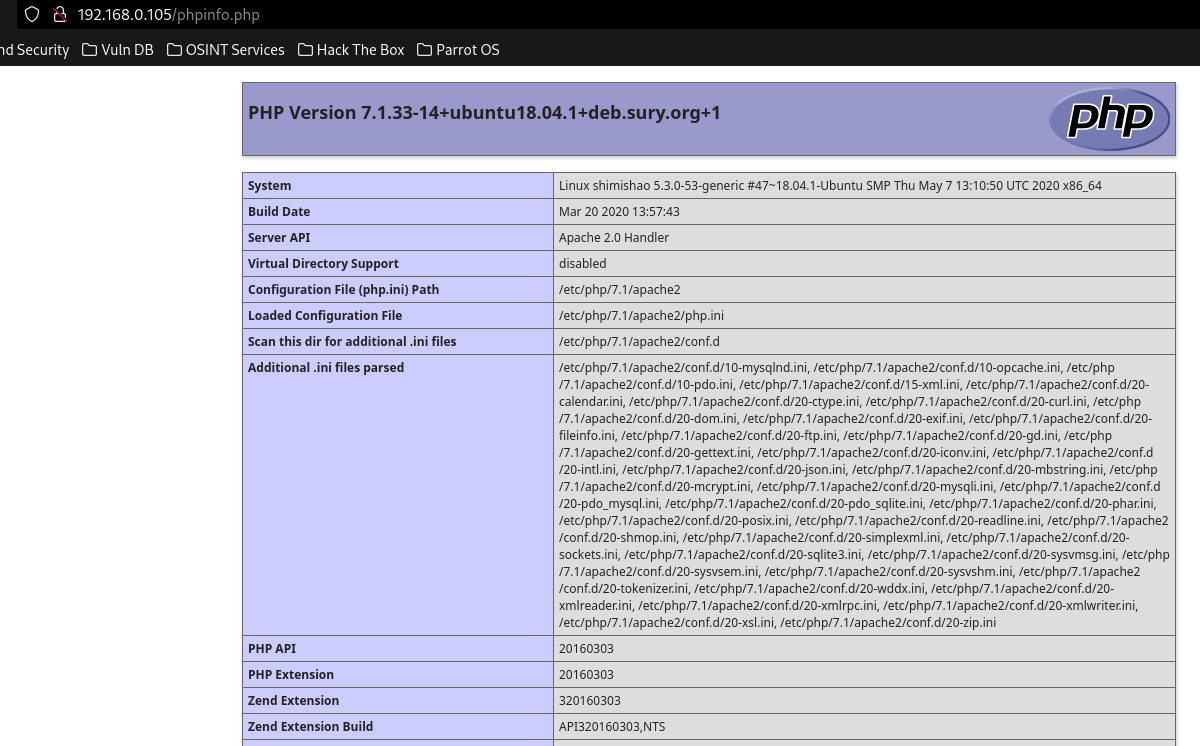
First of all, we need to perform directory scan



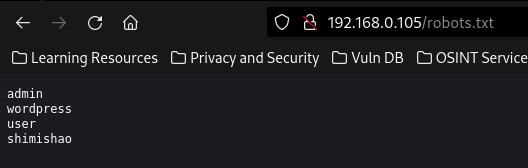
This command performs directory scan on our target system. It uses common.txt file for directory scan. Results:



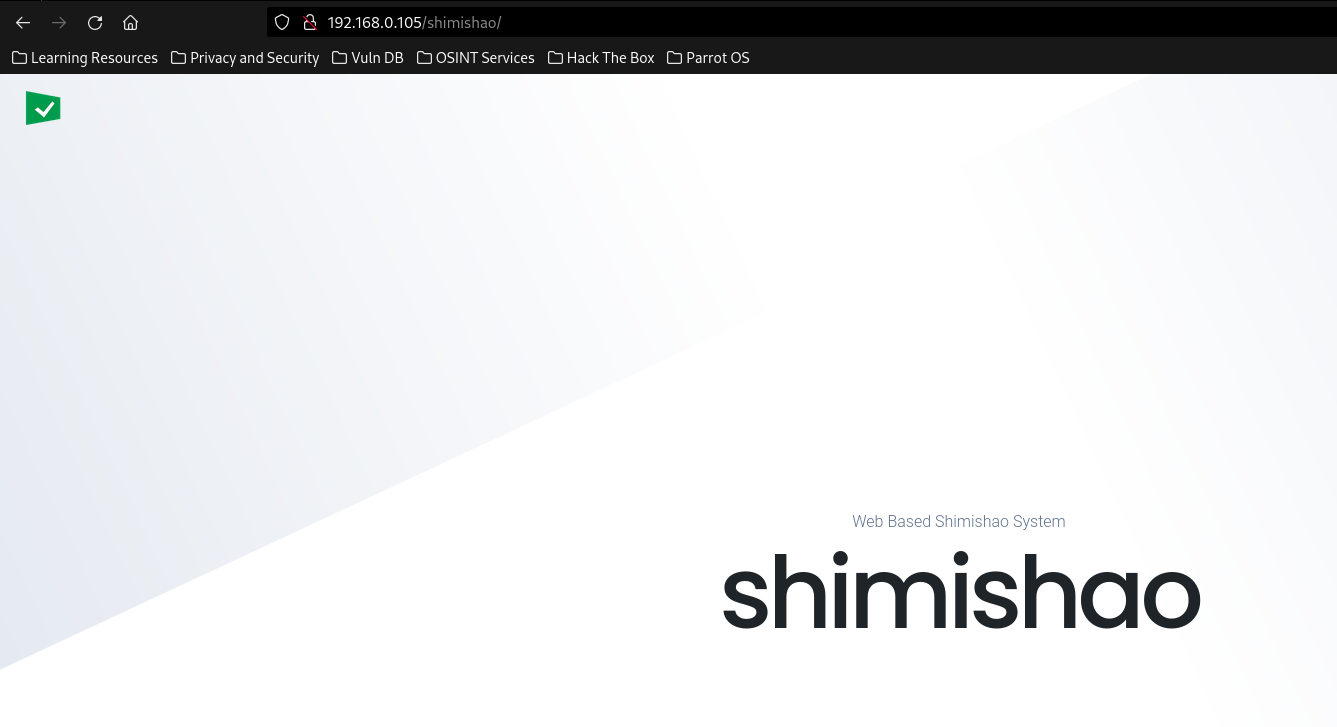
As you see, some critical paths are open, for example, phpinfo.php:



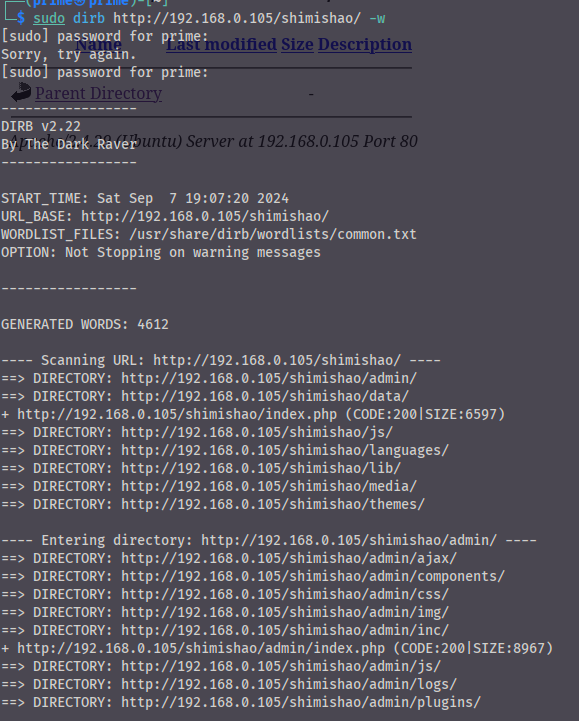
Take a look at this page. We can see PHP version (7.1.33-14), system version is also Linux and more and more sensitive data are revealed. With this data we can find vulnerabilities of versions.

Another file which is important for us is robots.txt. 

One of them only responds to 200 code. These are shimishao.



Lets make a directory scan and see which folders are open.

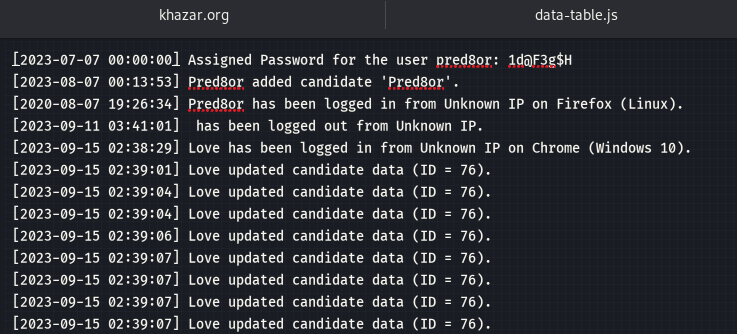


Except one of them, others are empty or not useful. That one of them is */admin/logs*.

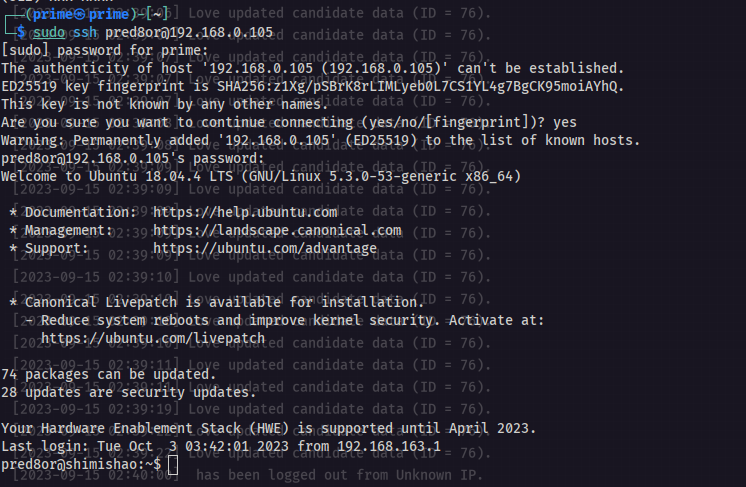
This folder contains the log of the admin user.



Download the file and look inside of it:



As you see, we have password of pred8or user. Check it with ssh connection.



Flag: (in user1.txt) ICSD{66d74978b307889bea234a4bc6570a36}

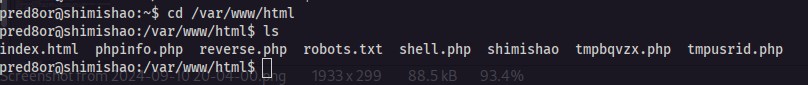
**THIS IS GREAT!!!**

**PrivEsc is coming!!!**

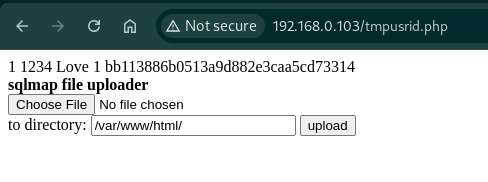
After this we make some steps to get the other flag.

First of all, let’s check wich files we can open or read in /var/www/html/ directory.

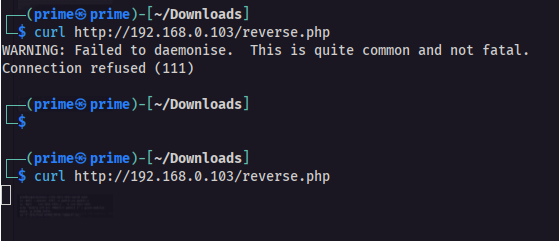
In this directory, we see these files:



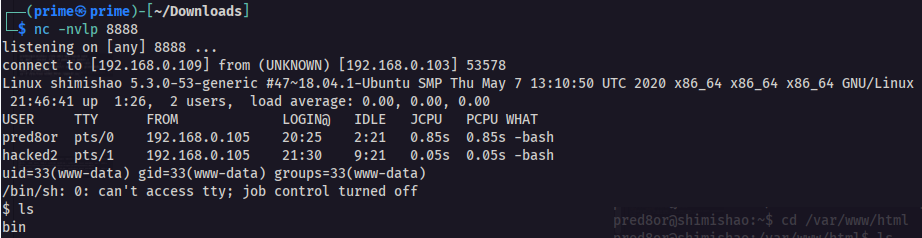
In here, we can see some files that we haven't seen before, tmpusrid.php, tmpbqvzx.php and shell.php. In this case we need only tmpusrid.php.



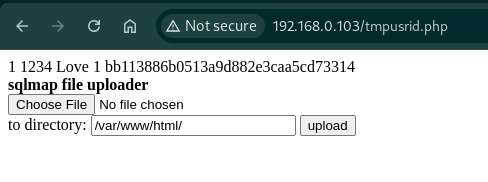
First of all, let’s check file upload. I created a reverse.php file and uploaded it to server and sent a request to it.



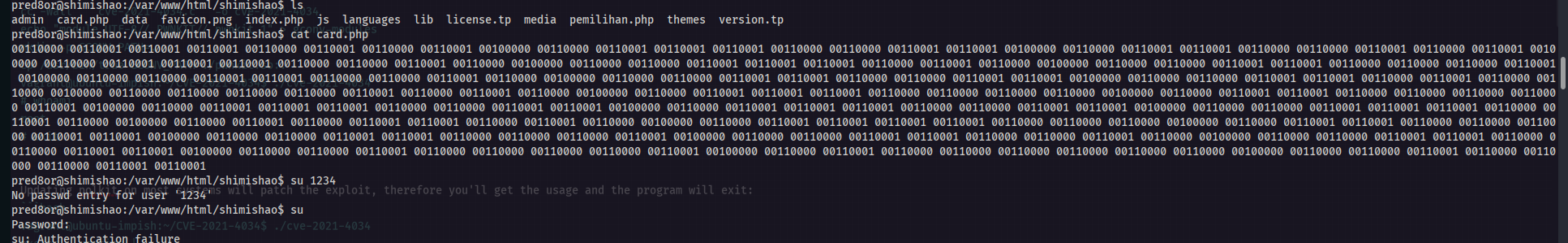
And created a listener too.



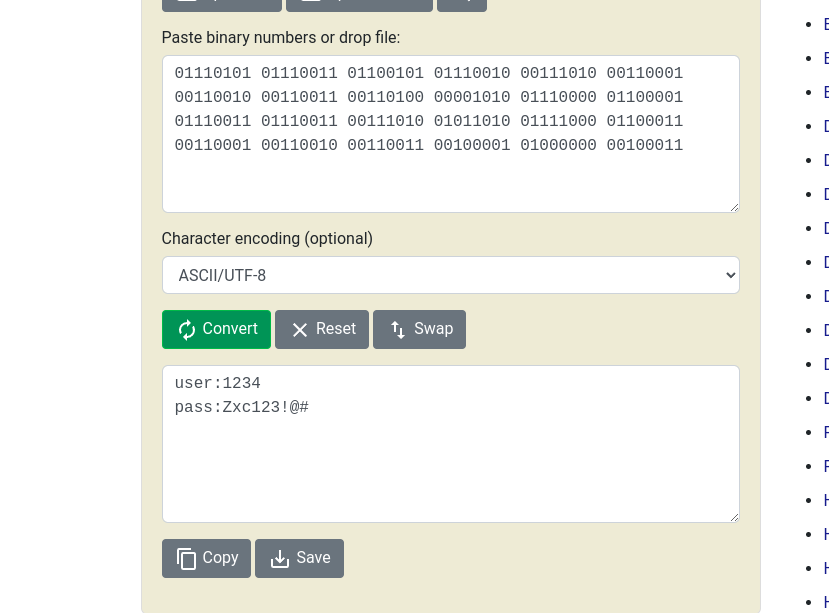
So I have access to system with this way too, but I want to move with pred8tor user via ssh because it has more privileges than www-data user.

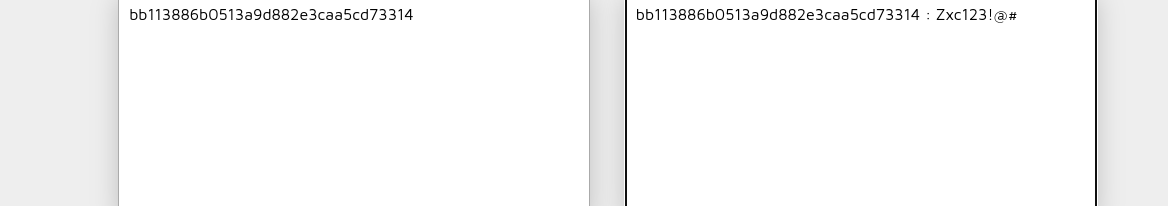
Before all of them, find out what is “1234” and “bb113886b0513a9d882e3caa5cd73314” in this photo. 

For understanding this, we need to look in to /var/www/html/shimishao folder. In this folder, there is a file named “card.php”. In this file:

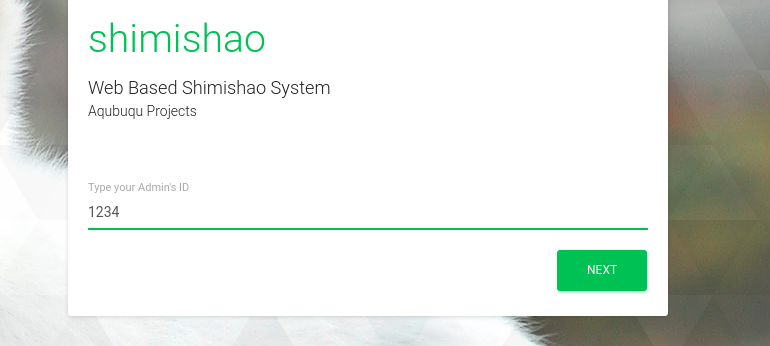


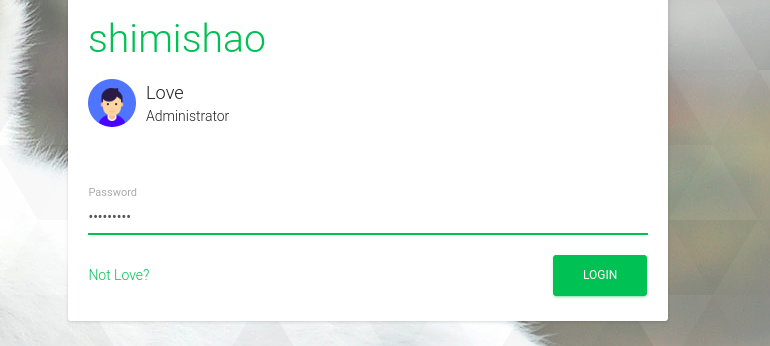
This is a binary text. Decrypt it two times. And boom:



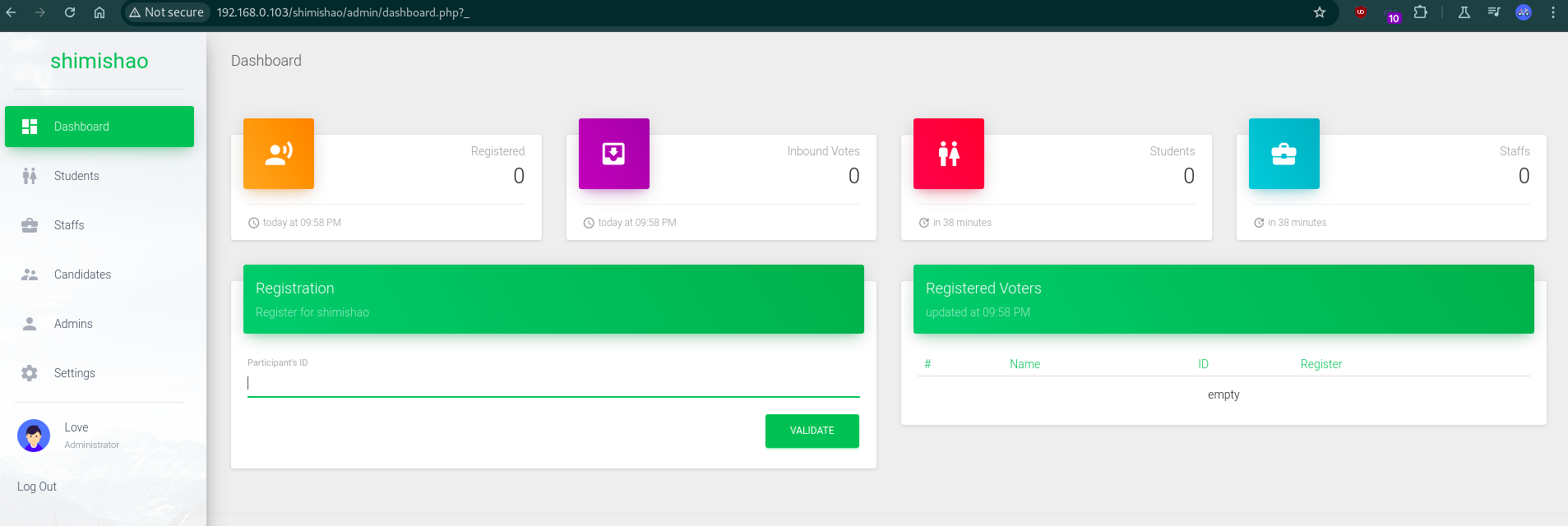
Our shimishao user is “1234” and password is “Zxc123!@#”. But what is that long text in previous images? It is MD5 hash of password. 

Let’s check user and password.

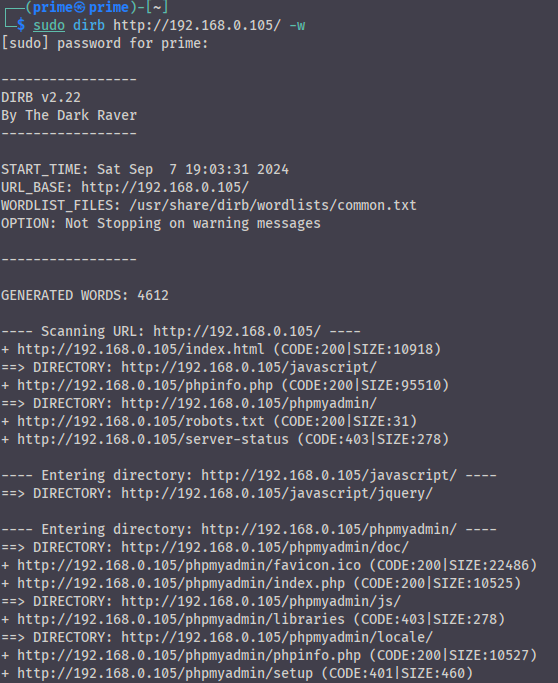




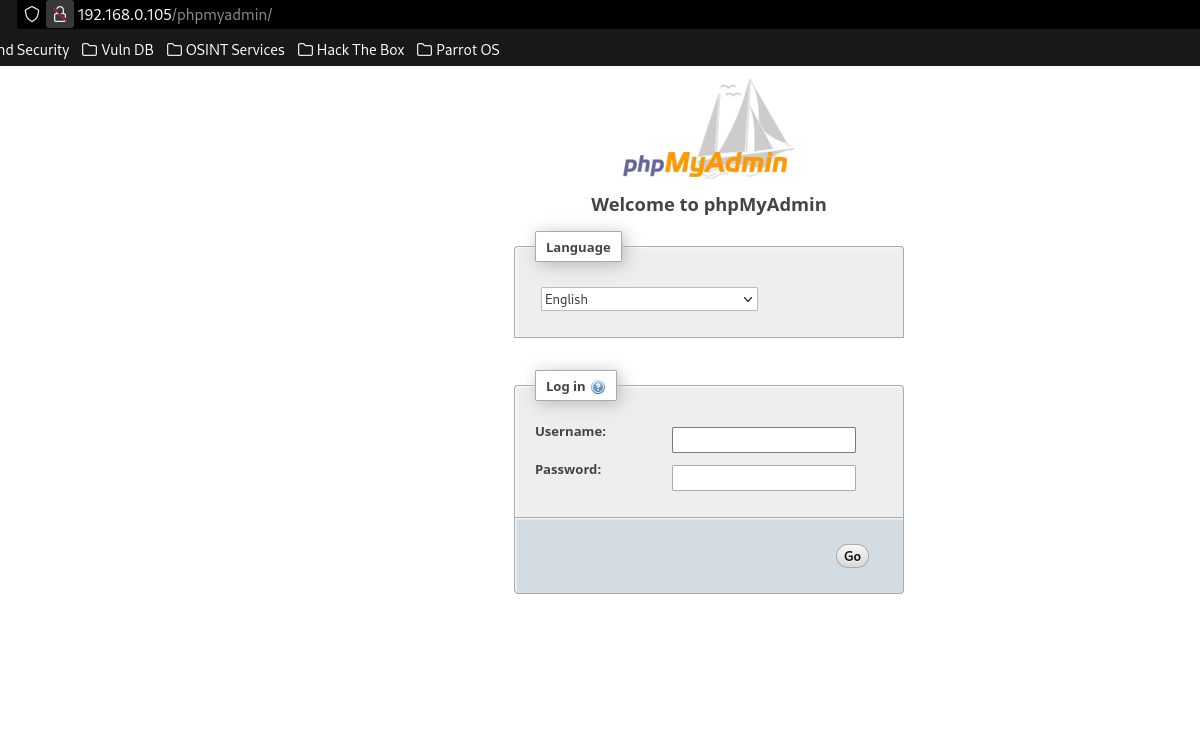
And we are admin now.

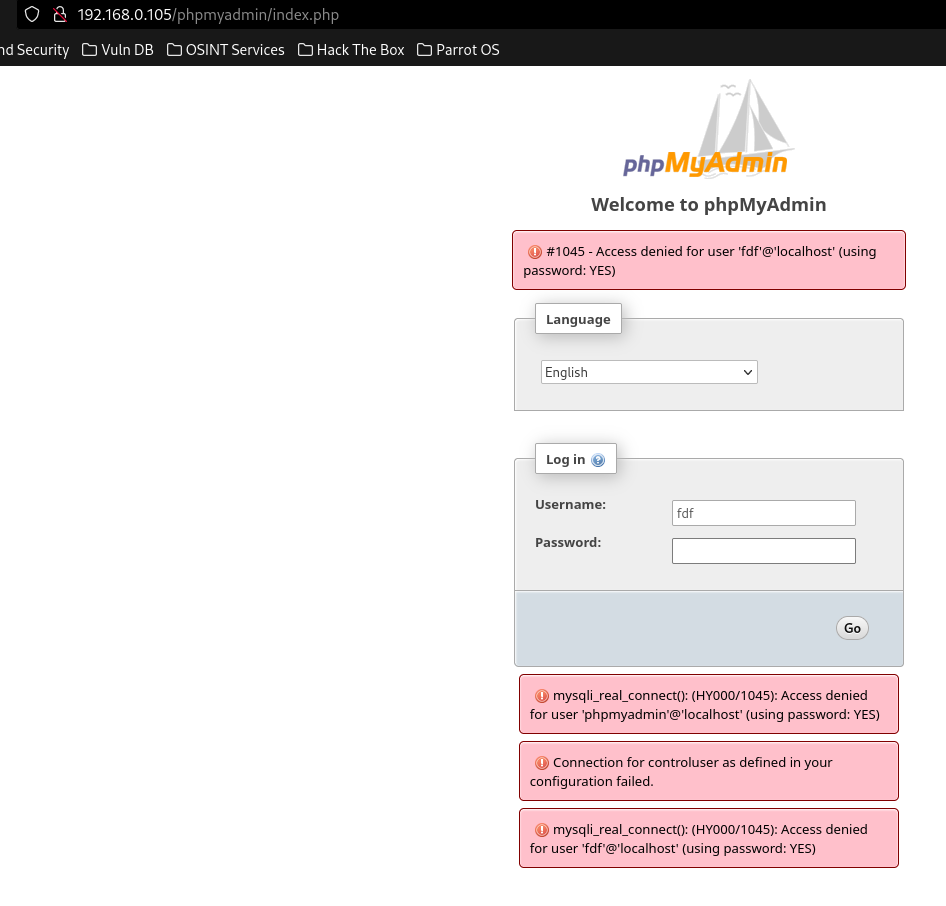
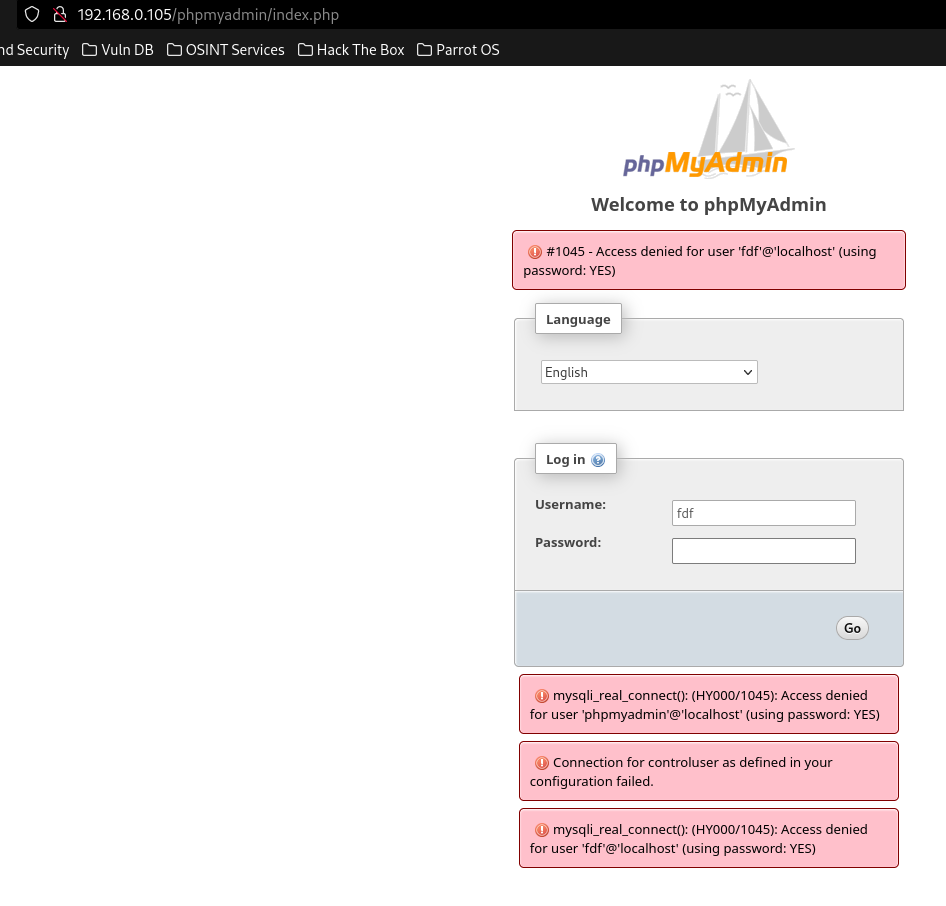


Let’s end web pentest

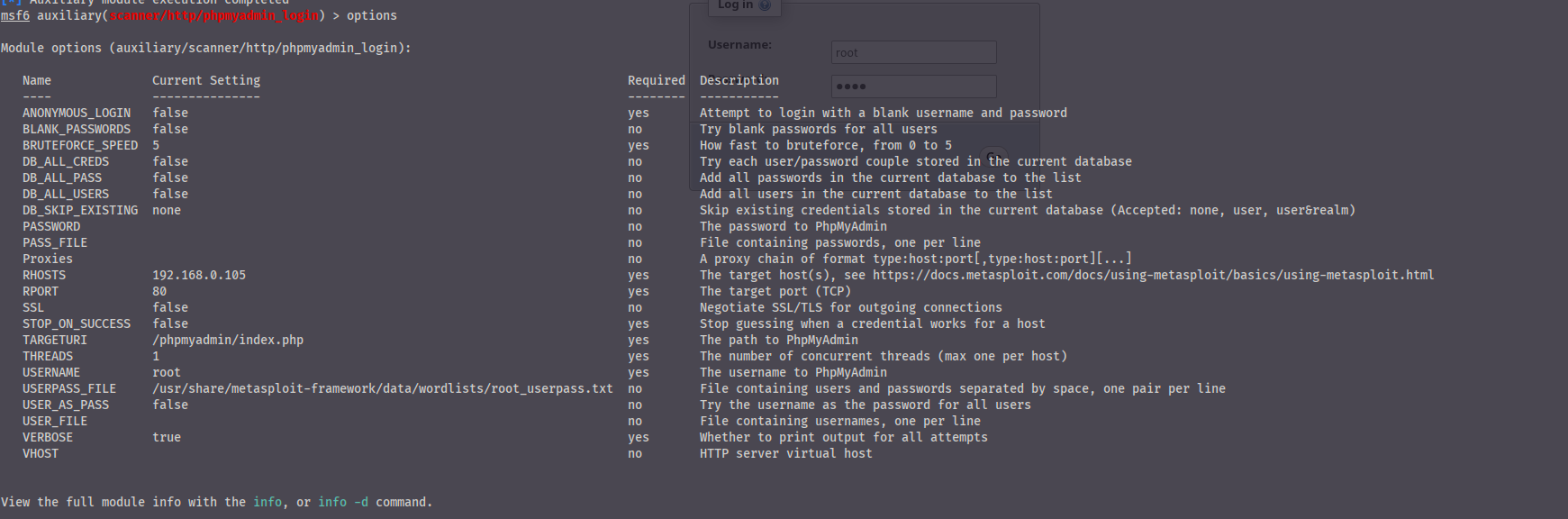
We are able to access the system. In this terminal we can perform PrivEsc but I want to look other dictionaries that dirb gives us

The target has /phpmyadmin/ directory. All of the 200 status codes forward us to /phpmyadmin/index.php.

If we try something as a username and password, we get these errors.



These errors are not important for us now.

In the Metasploit framework, an auxiliary module exists for performing bruteforce to phpmyadmin login. 

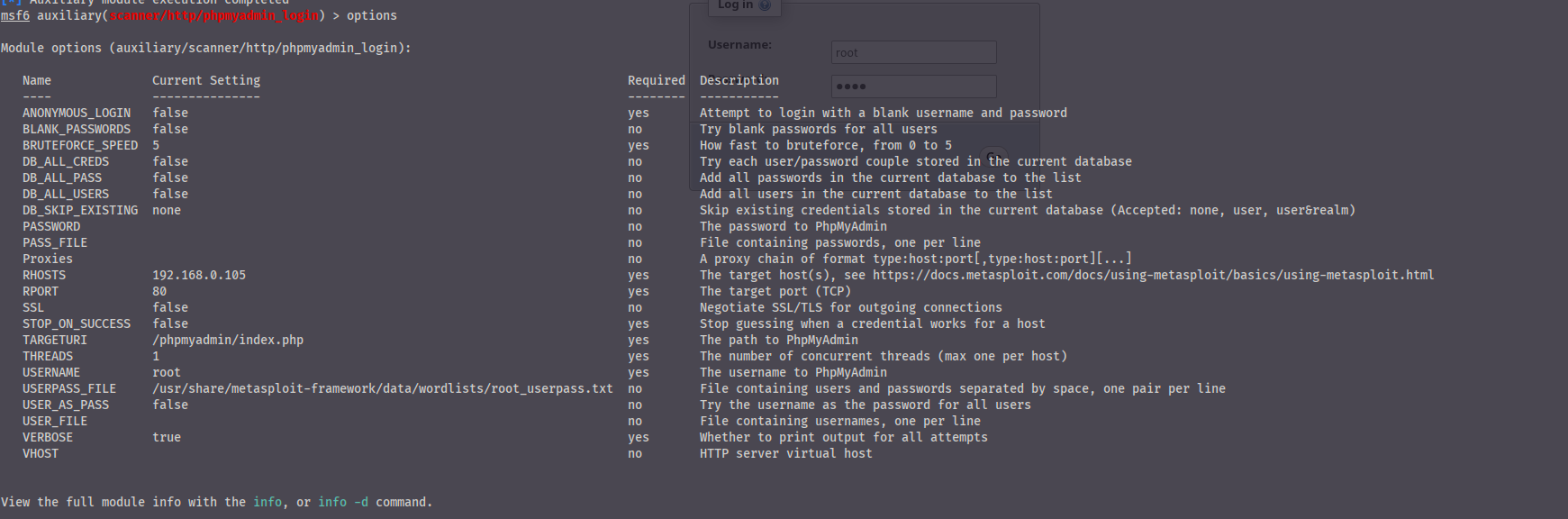
We can find it with the “search” command inside “msfconsole”. After selecting the module, we need to give the target host, path of phpmyadmin and userpass file or username file and password file separately. To set target host, path and userpass file

set RHOST 192.168.0.105

set PATH /phpmyadmin/index.php

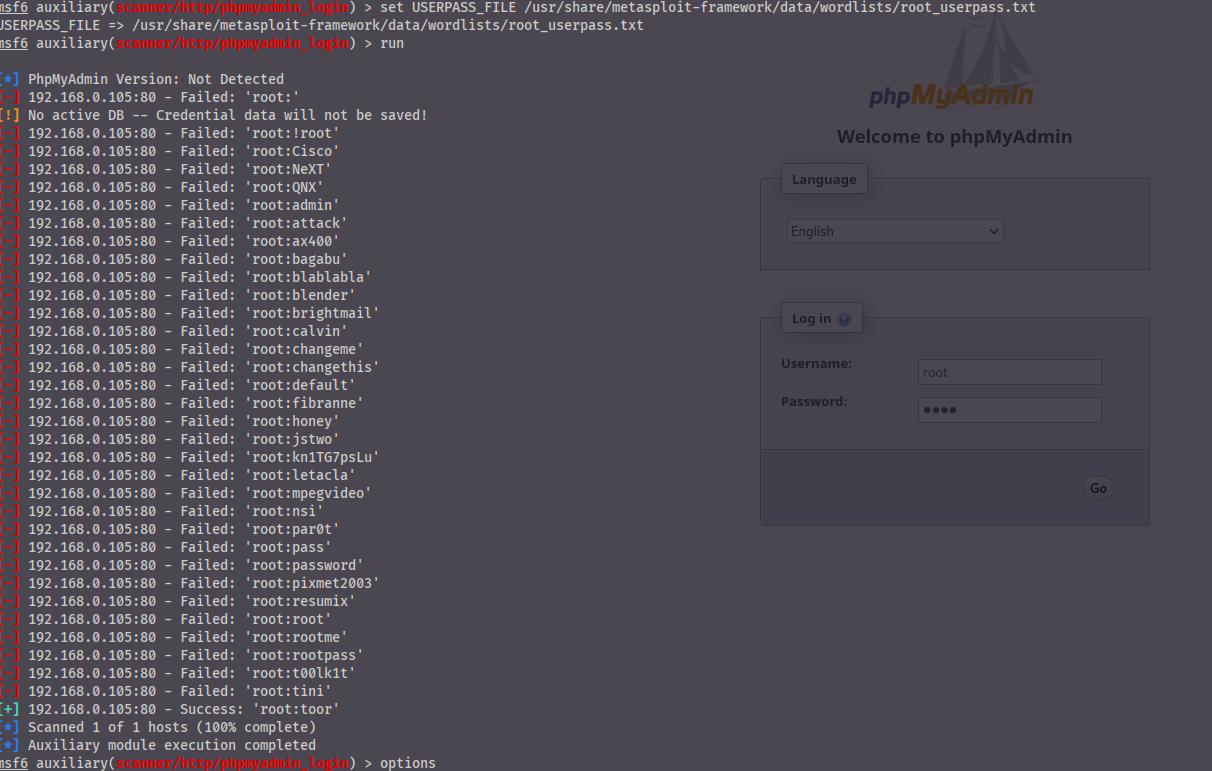
set USERPASS\_FILE /usr/share/metasploit-framework/data/wordlists/root\_userpass.txt

After setting all of these, we run the options command to see the info.



This module helps us to make a bruteforce attack to target the phpmyadmin system using root\_userpass.txt file. This file contains root user default passwords as “**username**:**password**” style. The module takes each line and separates it with “**:**”. Then puts username to username parameter and password to password parameter.

Then we can run the module with the “run” command. THe output will look like this.

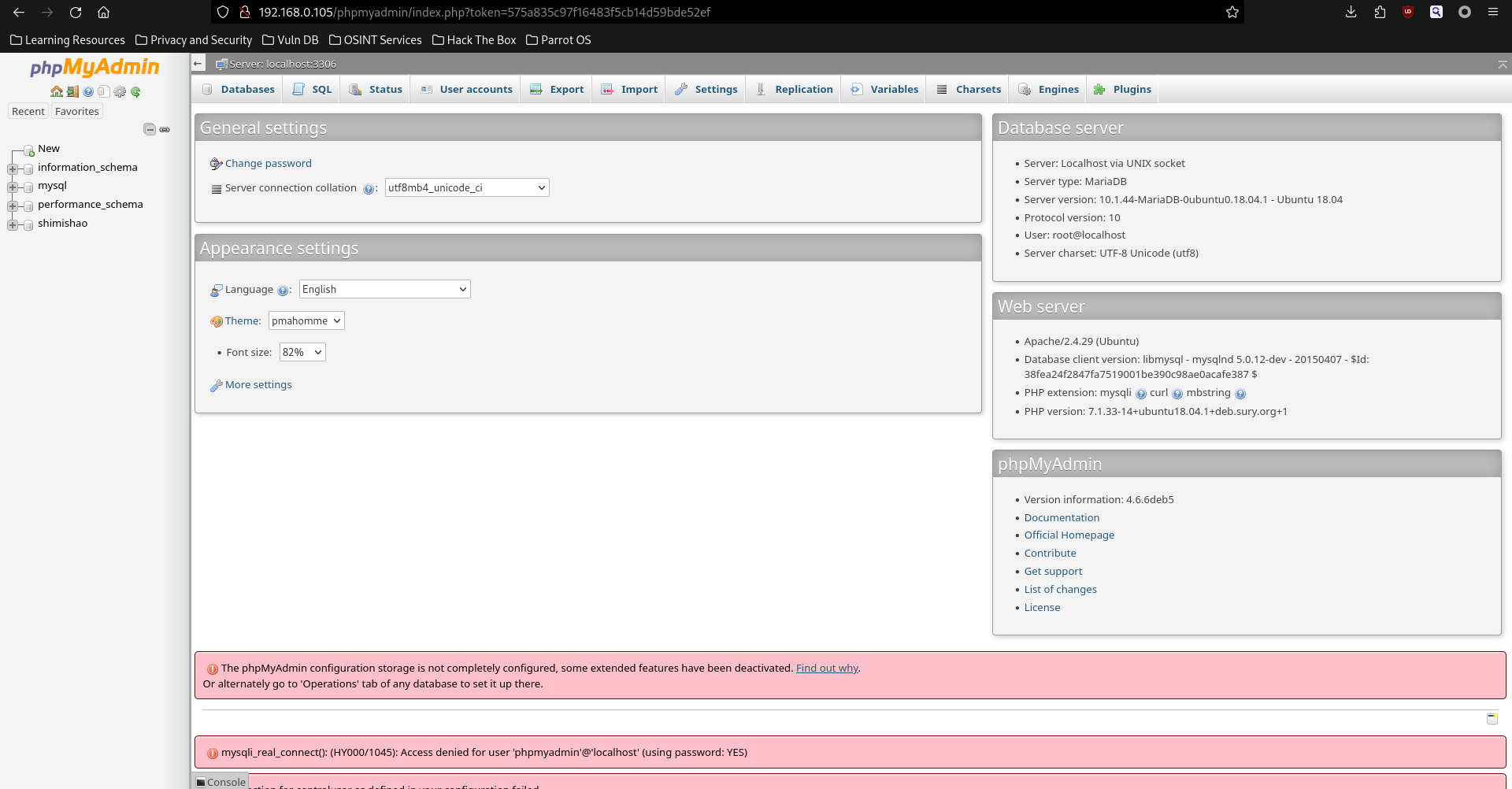


After several failures, we can see that the module is able to find username and password.

Then we can put parameter to in the target system and login to admin page

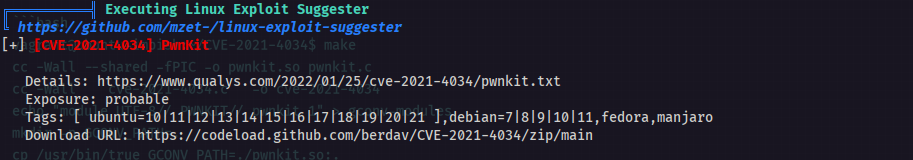


And kaboom!! We are able to see databases in our system.



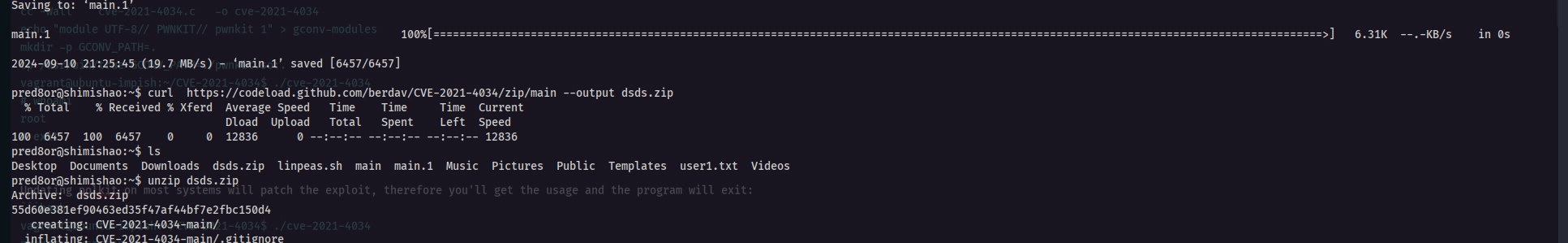
PrivEsc Part

If you remember, we have an open ssh port and pred8tor user. I use a tool named linepeass.sh for checking SUID and other things. In it’s output I see this.

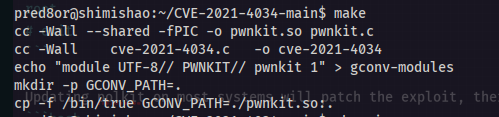


and decided to use this “PwnKit” tool.

First, I need to install this tool to the server. Secondly, we must build it with “make” command.



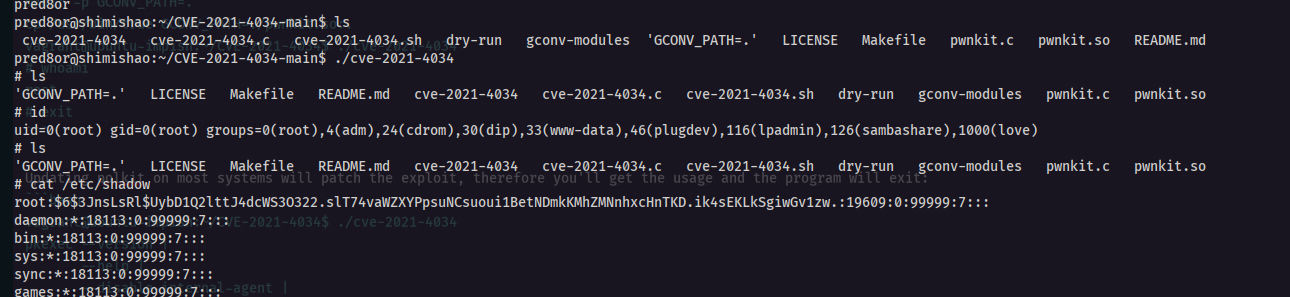
Second part:



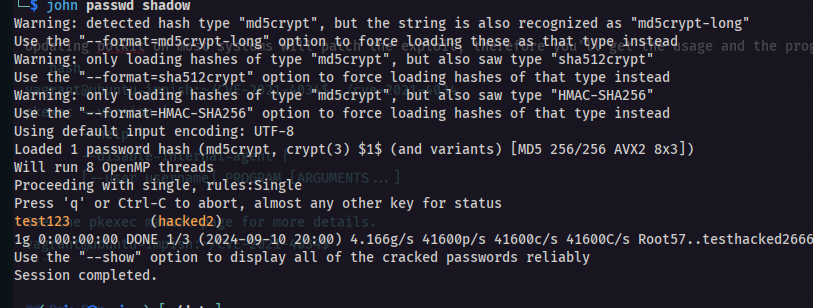
|

|

and



We are root now. After being root, i copied /etc/passwd and /etc/shadow because I am not fully root user. I have limitations. I copied those files to my computer and break password using “john”.



|

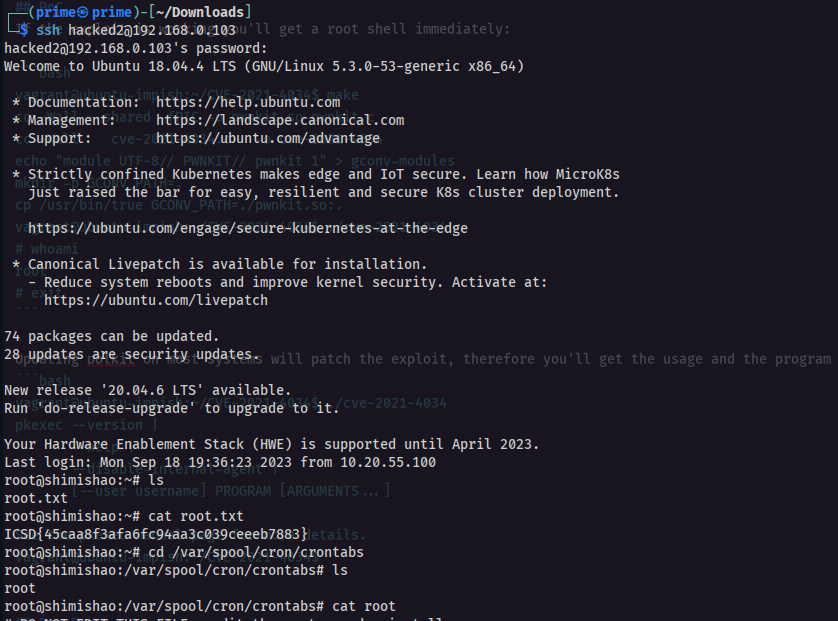
\

\

\

\

|

After this, I created a new ssh connection using password and username.

And root flag is **ICSD{45caa8f3afa6fc94aa3c039ceeeb7883}**