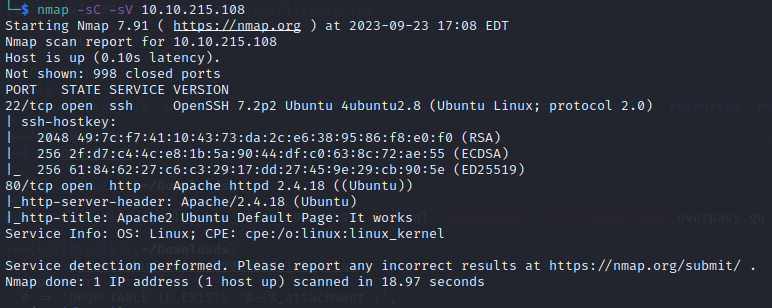
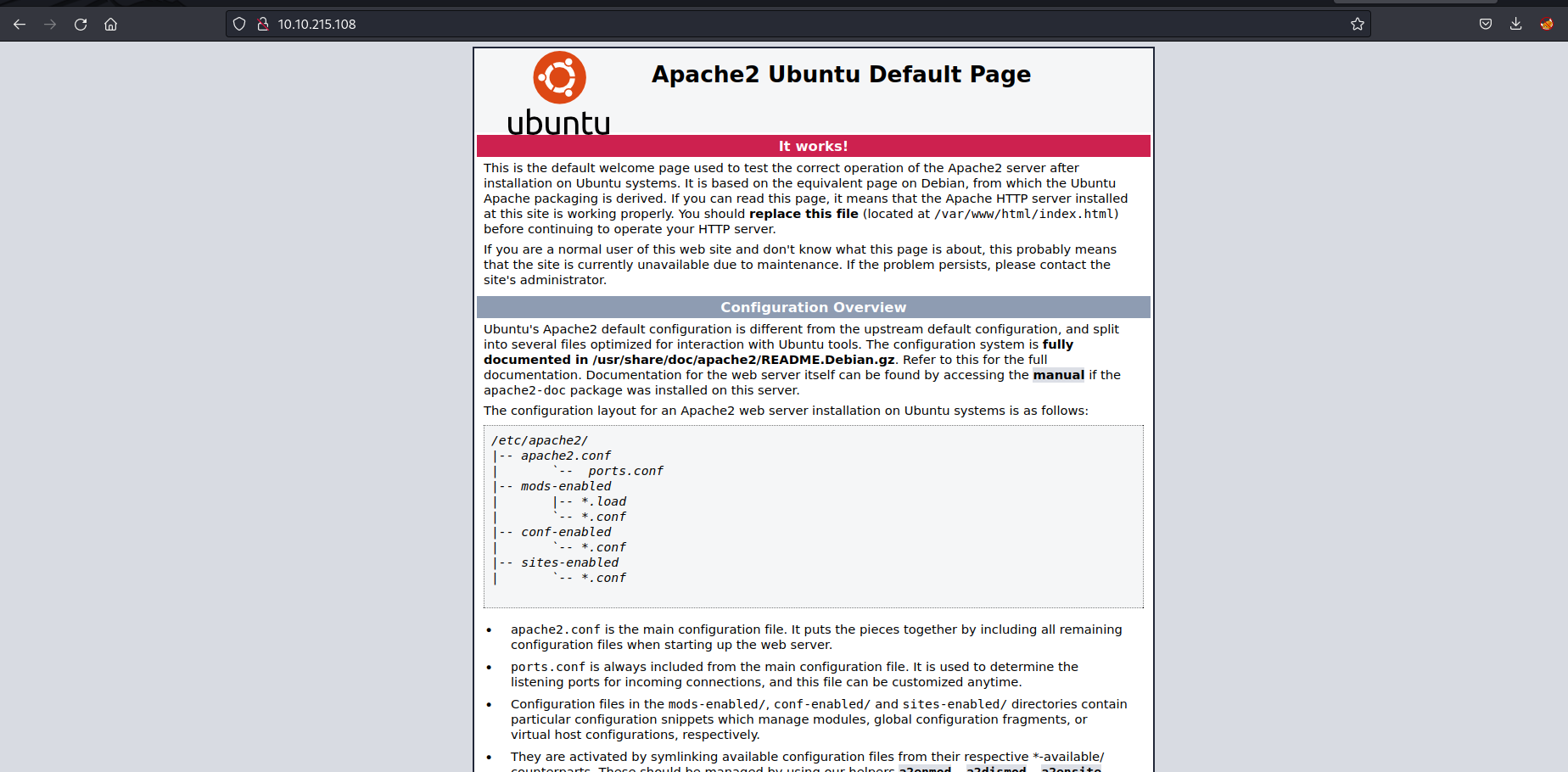
**Enumeration**

1. Nmap -sC -sV (machine ip)

We get:

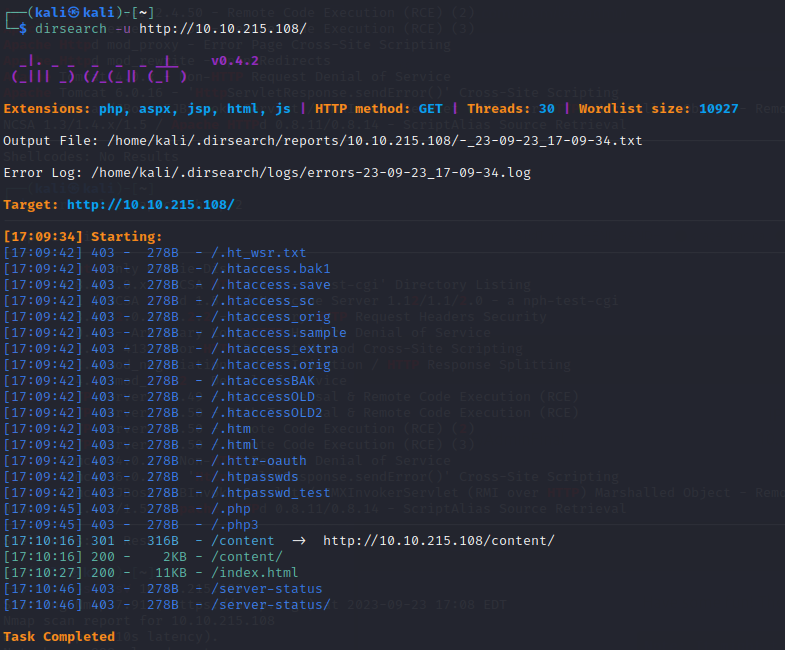


Here we see that there’s an SSH open on port 22 as well as an http website. Let’s check there!

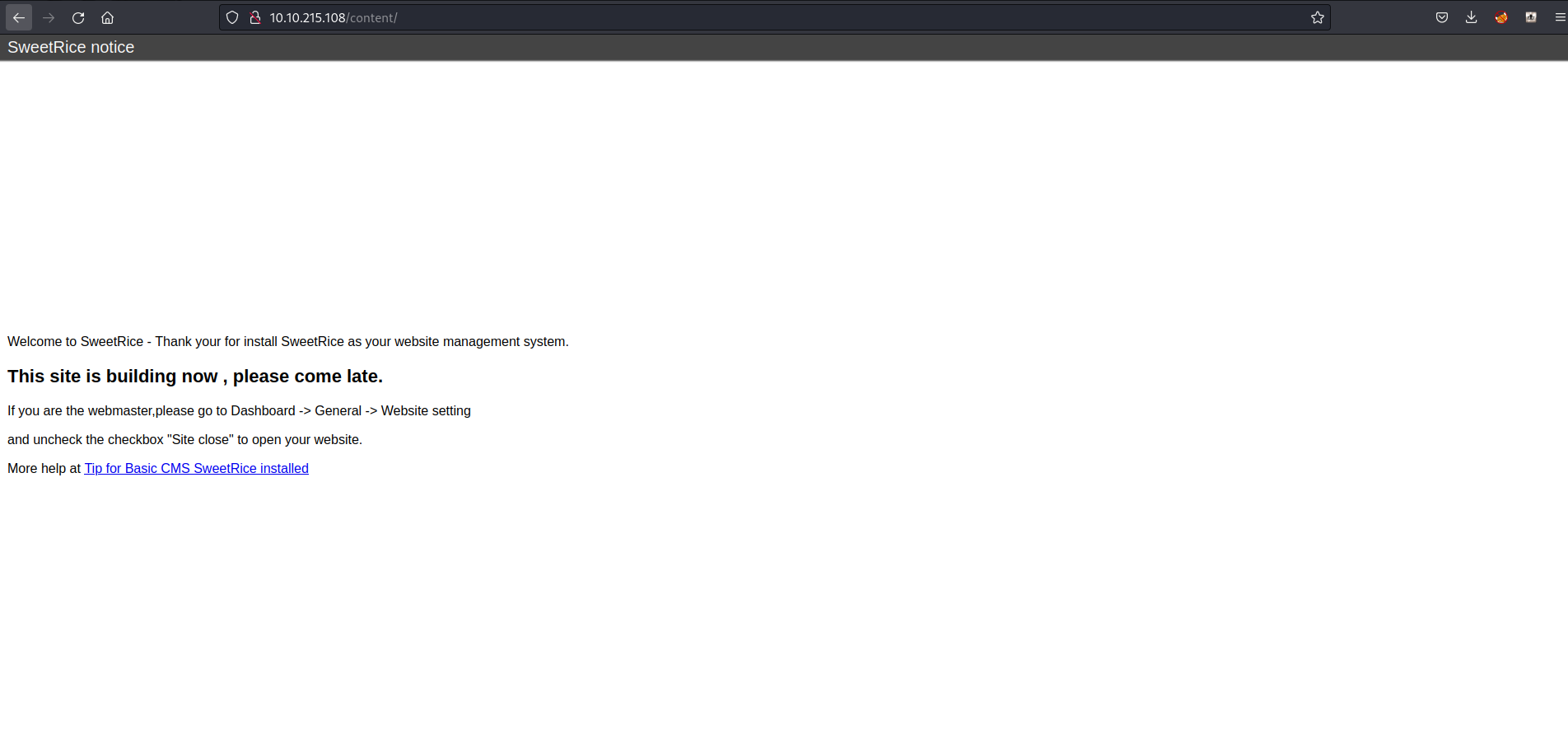


Looks like it’s an Apache2 website. Let’s find out if there are any subdirectories here!

1. dirsearch -u <http://(machine> ip)/

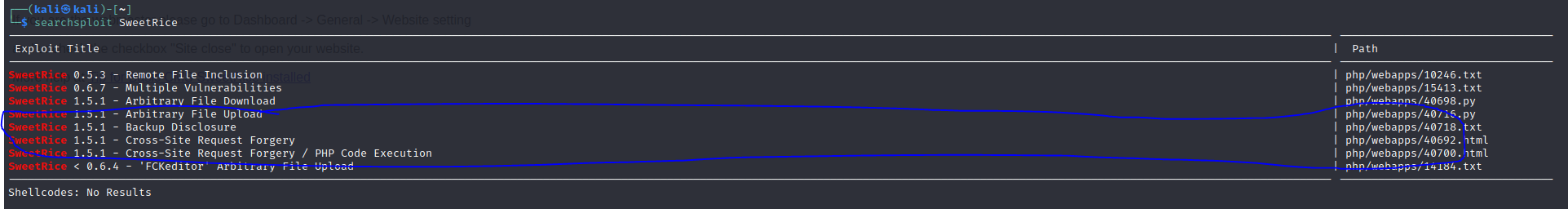


As we can see, there’s an interesting subdirectory here called /content/. Let’s check it out.



Looks like this website is made from SweetRice. No idea what the version is but let’s find if there are any vulnerabilities we can exploit here with searchsploit?

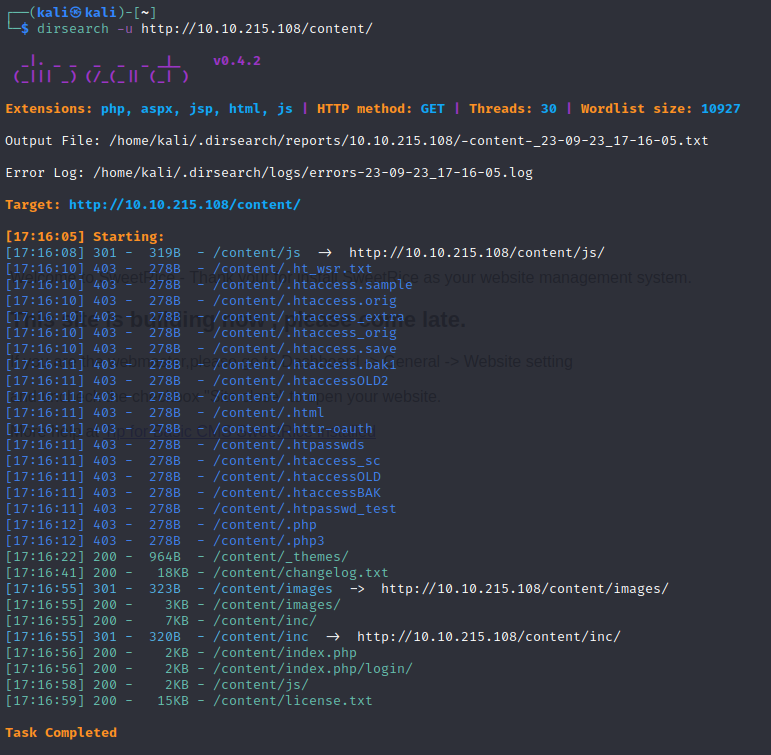
1. searchsploit sweetrice



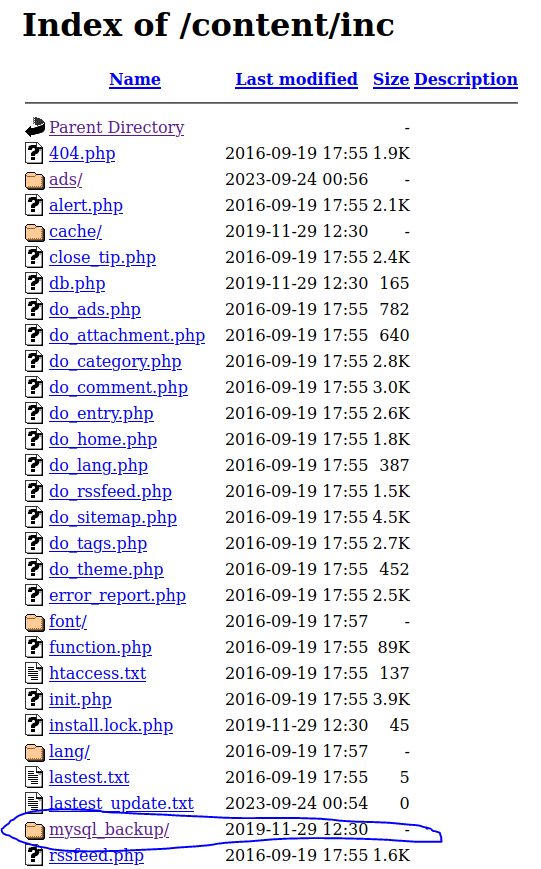
Looks like we can upload files onto this website with Arbitrary file upload. And with the backup disclosure, we can even find credentials through here.

But that can’t be all for contents can it? Let’s see if there’s anything more hiding behind it with another dirsearch.

1. direarch -u <http://(machine> ip)/content/



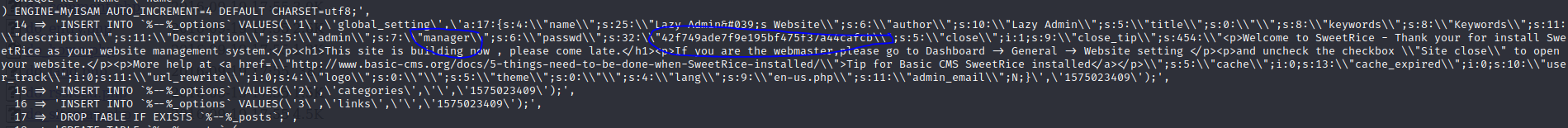
Looks like there were! Looks like there’s a login page, let’s keep that noted. Images probably won’t be too helpful. But there seems to be stuff inside the /inc/ directory, let’s see what’s inside.

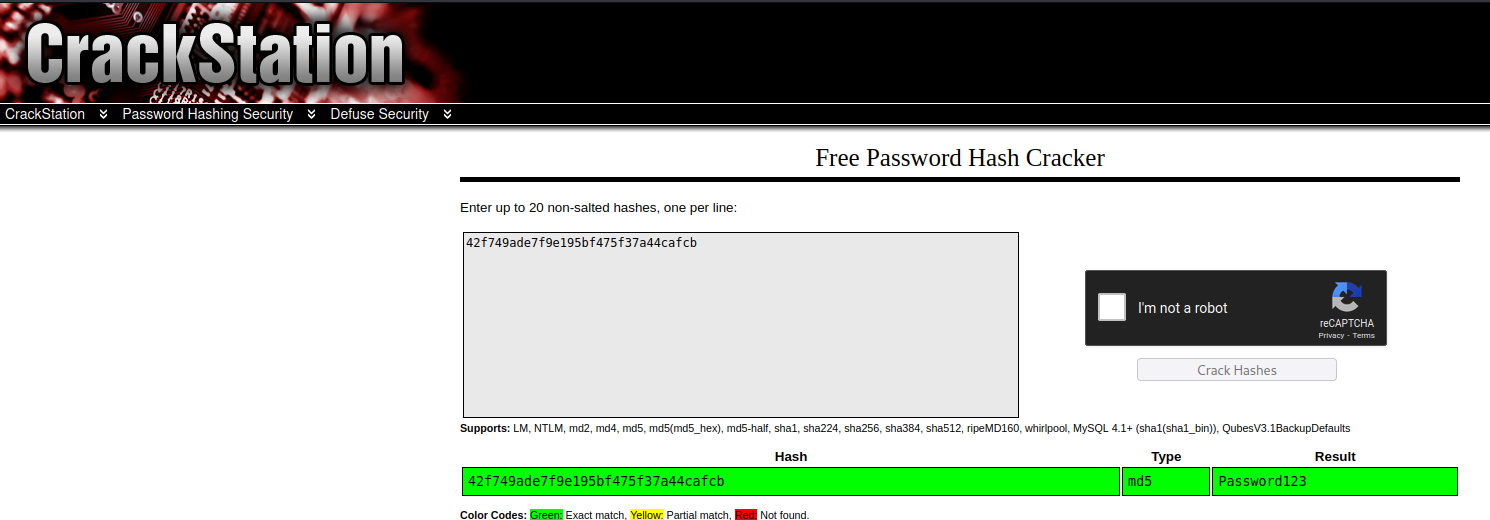


That sure is a lot. But this mysql backup sounds important. Let’s check it out!

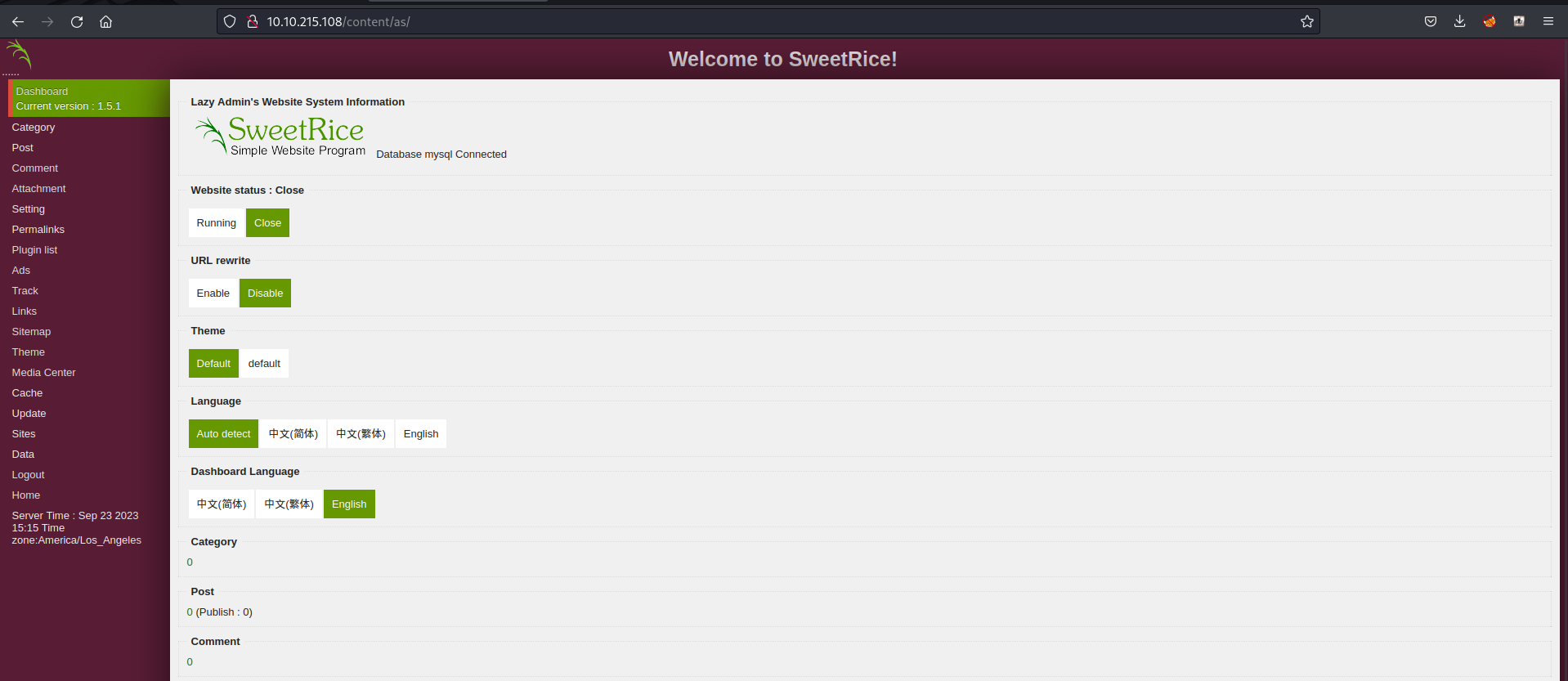
**Exploitation**

1. cat mysql\_bakup\_20191129023059-1.5.1.sql



This may look like a lot of code. But we don’t need to read all of that. What’s important are what’s circled here. It seems that the admin account is username “manager” while the password seems to be hashed out! Let’s decrypt this password. 

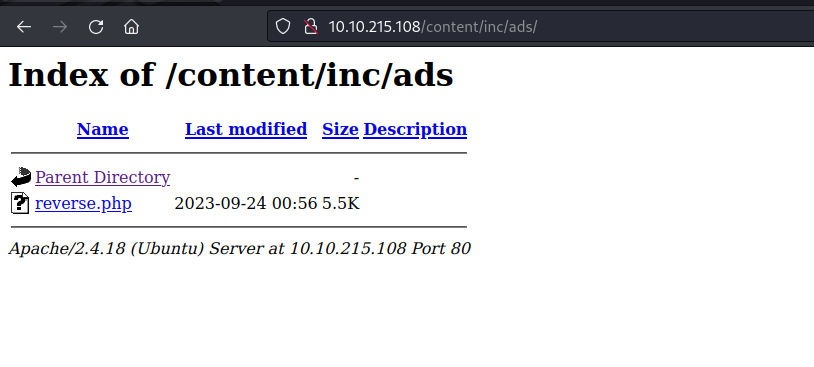
As we can see, it seems it was md5 encrypted. Now that we’ve got the password, we can now login to the website through /content/as



Now we’re inside the dashboard! Now remember we can upload files, so let’s upload a reverse shell here through the ads page. Here I used https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php Just need to change the ip to the VPN’s ip and the port to whatever port that’s available. Here I used port 4444.

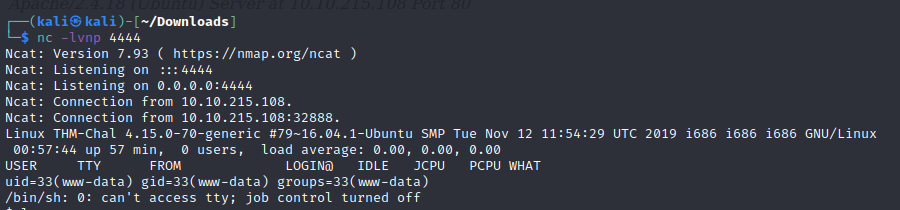
In the ads page, we just name it reverse or reverse\_shell. Something that will let us recognize it’s our file. Then we just copy-paste the reverse shell into the “ads” code.

Once that’s done, we should be able to see it in contents/inc/ads/ directory.

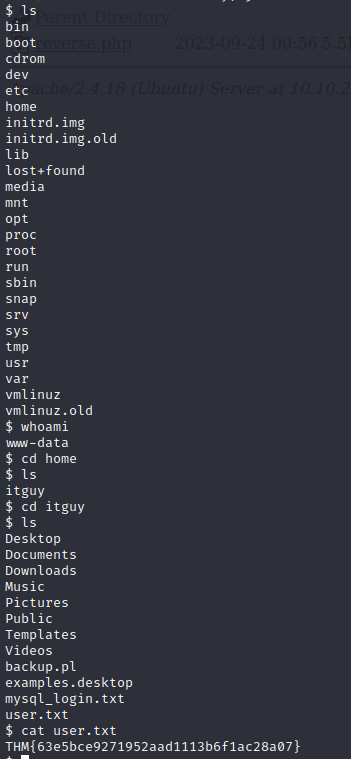


Now we just need to get a listening port up and once that’s up, we click on the reverse.php file here!

1. nc -lvnp 4444 (or whatever port number you put in the reverse shell)



Looks like we’ve ssh’d in! Now let’s just look around for files that stand out here.

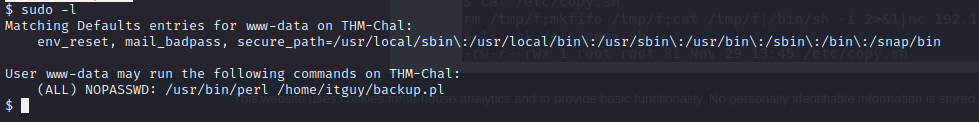


And here, we’ve got our first flag! Great!

**Privilege Escalation**

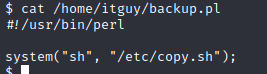
Now we’re not done yet, now we’ve got to get our root privileges. Let’s see what permissions we have for now:

1. sudo -l



We can run these two commands. Let’s try them out.

1. cat /home/itguy/backup.pl





Looks like this file already has a reverse shell inside for some reason. Let’s see what we can do with it

1. ls -la /etc/copy.sh



Looks like we can write in it! Unfortunately it seems we can’t nano or vim. So let’s try and copy this command! We’ll do this by first copy pasting this code into a text editor, and then change our listening port, then echo that into the copy.sh file.

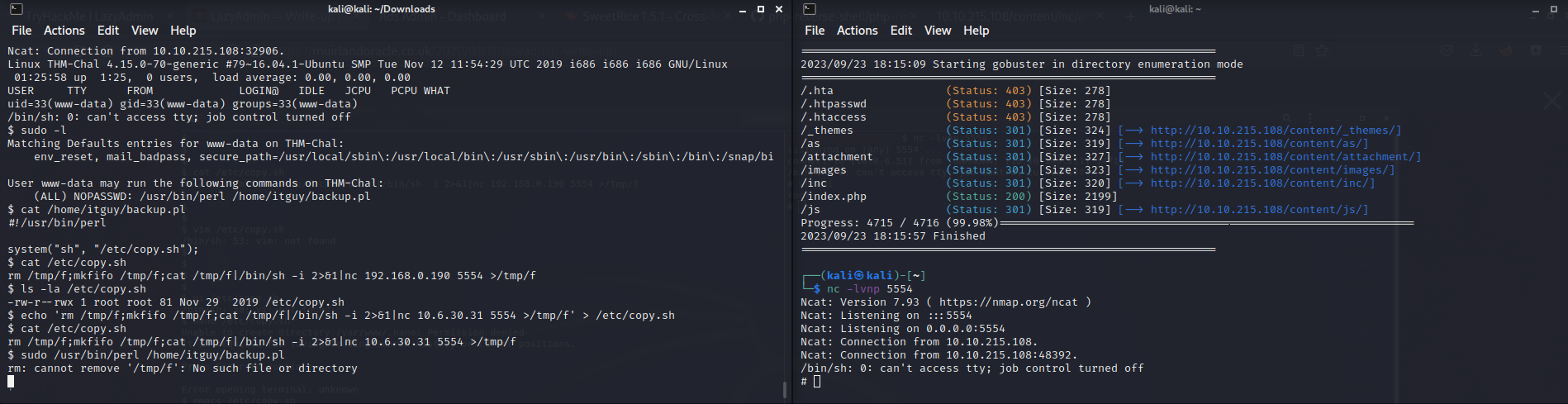


As we can see, now the listening port is 5554 but the ip is now our computer’s ip (the vpn ip). Let’s run the listening port now in our main terminal!

1. Nc -lvnp 5554

Now that the listening ports on, remember those commands we were allowed to run as the itguy user? Let’s use them now!

1. Sudo /usr/bin/perl /home/itguy/backup.pl



It worked! Let’s make sure we’re root now.



Now we just search around and we should get the flag!