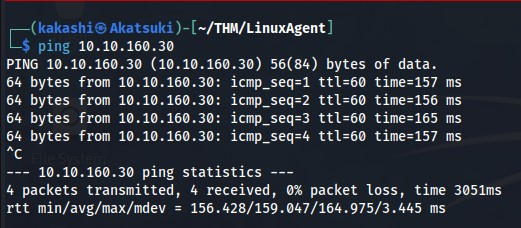
CTF Writeups

TryHackMe

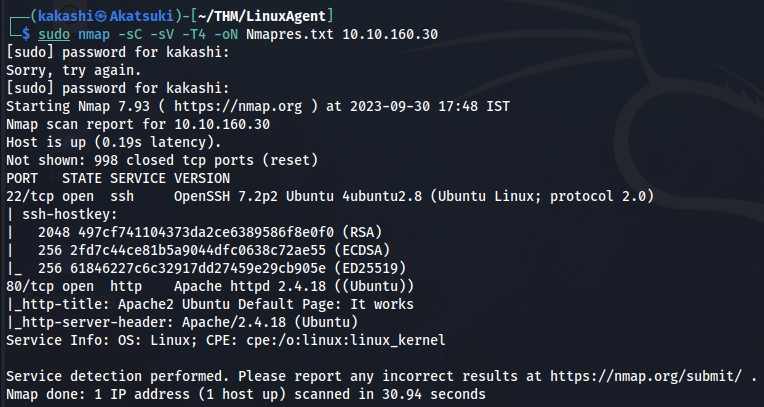
LazyAdmin

Machine IP: **10.10.160.30**

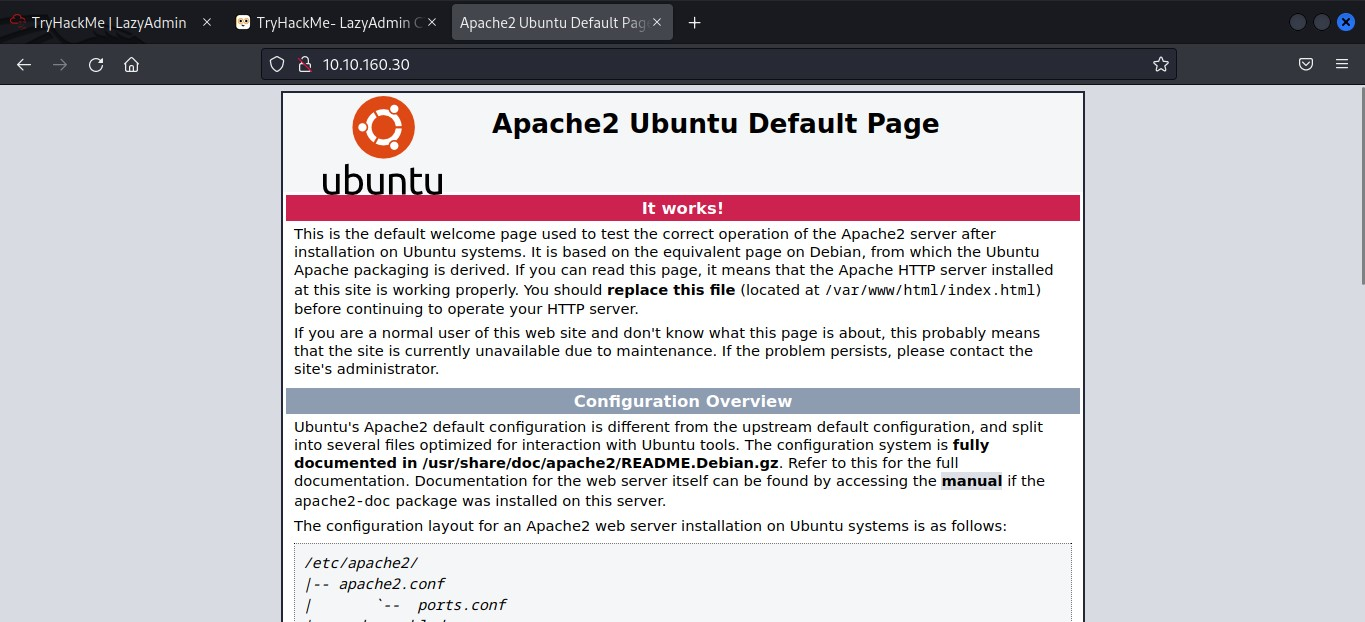
Let’s check whether Target Machine is Reachable or not using **ping** command.



Our Target Host is Reachable and let’s check for any open ports using the **nmap** command.

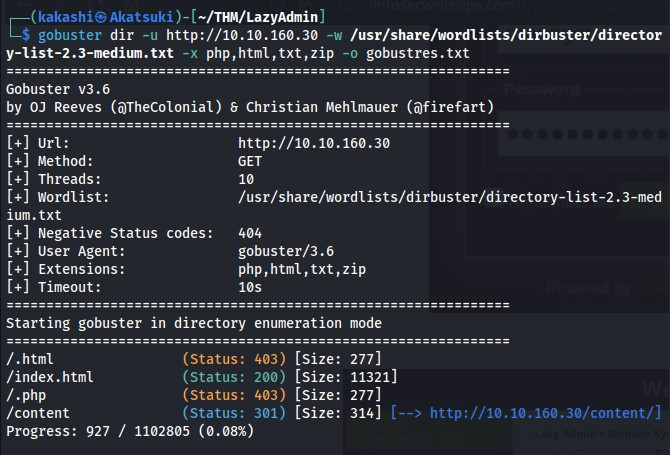


We Found that port **22 (SSH)** and **80 (HTTP)** is open, For ssh we need username and password, The Only Available as for now is Port 80, Lets check the website.

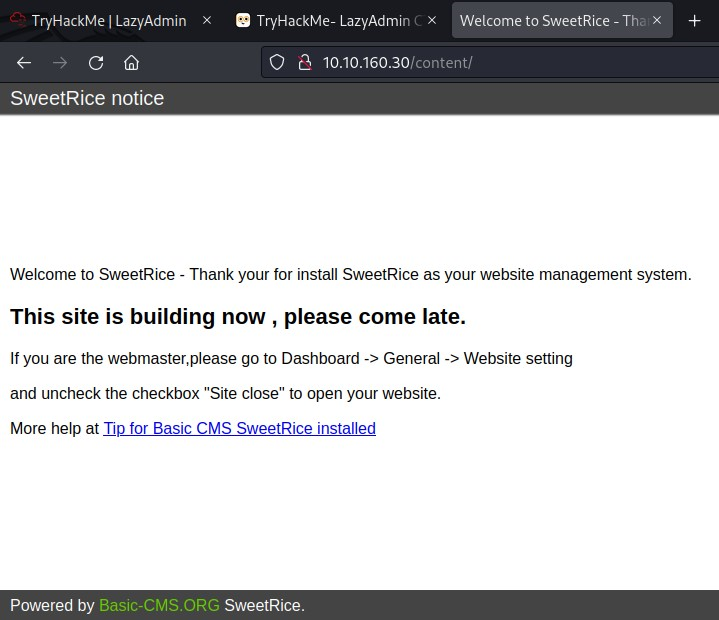


We Found out that it is a default apache web server page and there is not much useful information in it.

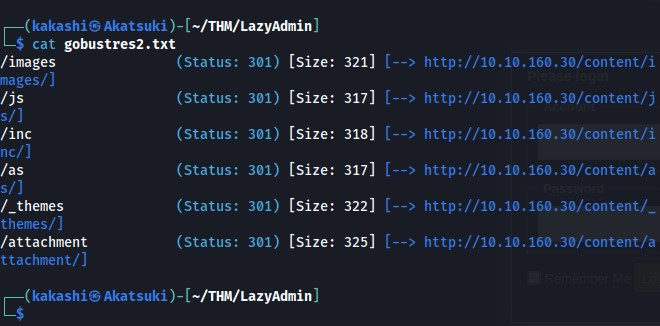
Lets using Directory Fuzzing tool **gobuster** to find any hidden directories in the web server.



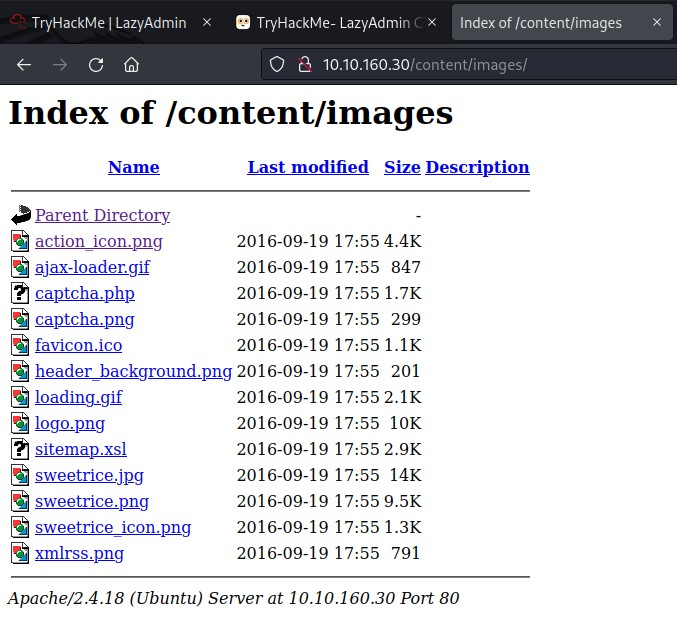
We found an interesting directory named **./content**, Lets check the content in it.

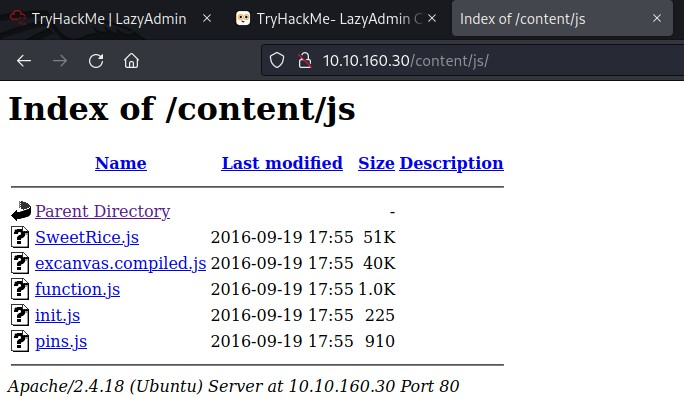


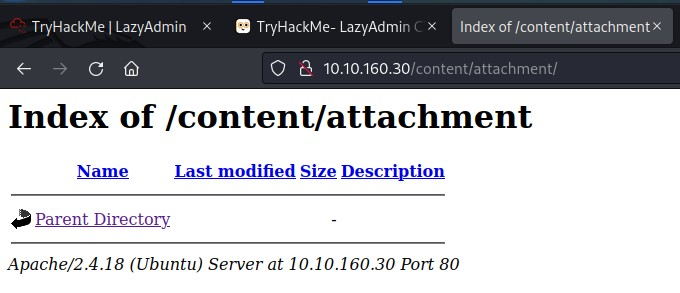
It is a sweetrice CMS website and there is not much information, again we use fuzzing tool to check whether any hidden directories are there in the /content.

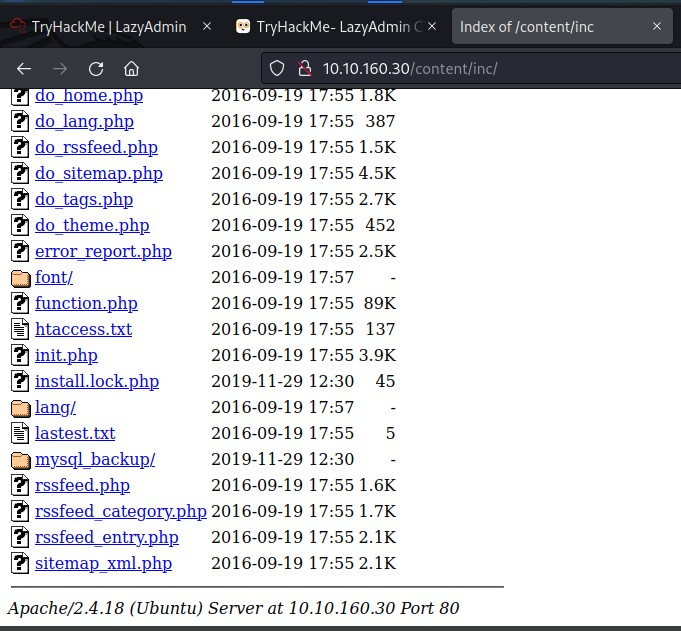
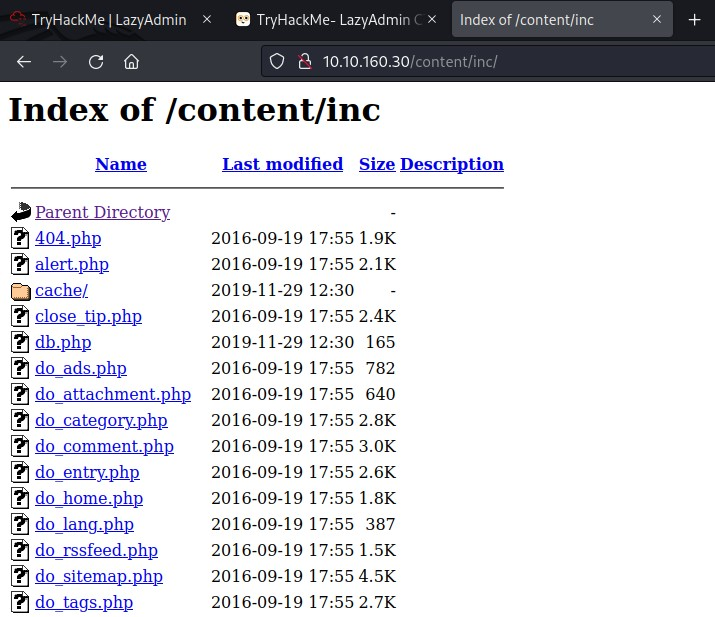


Let’s check the directories one by one to find any useful information.

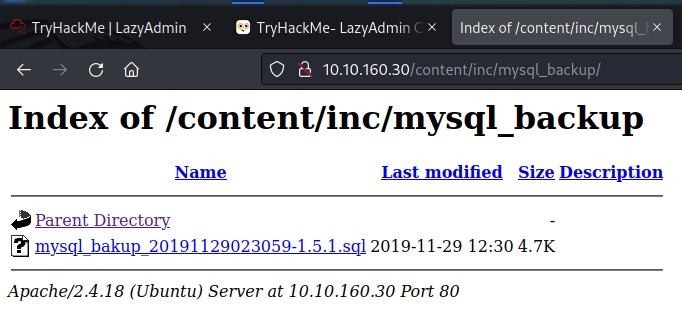




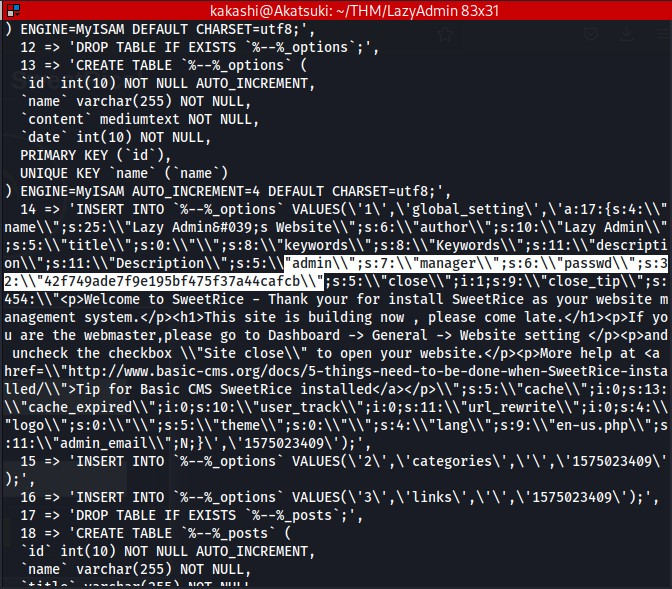




In the Above **/inc** directory we found a folder mysql\_backup which could be useful for us, Lets inspect that.



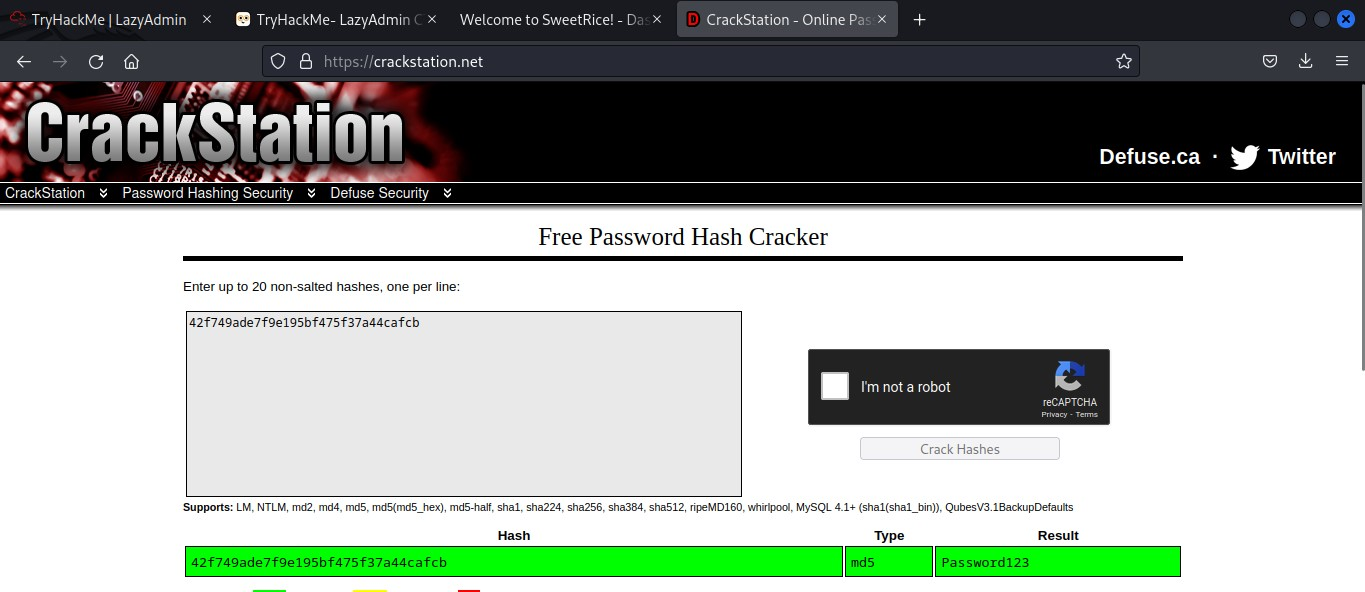
Let’s Download the file and analyze the content in it.



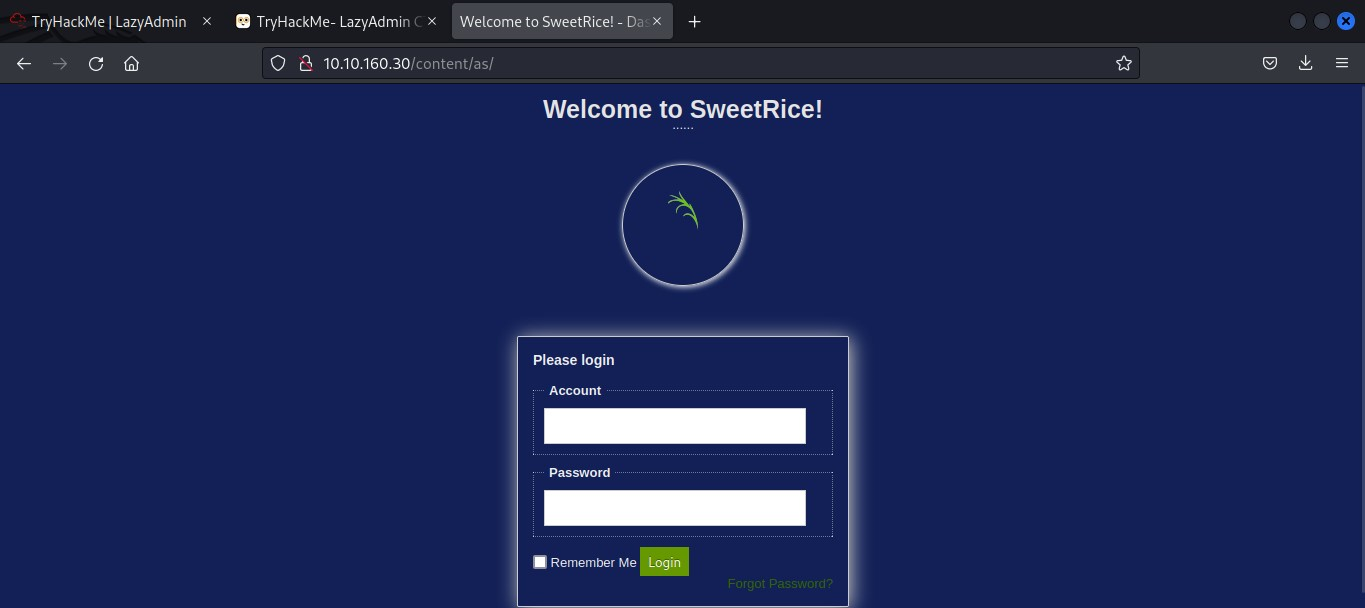
We found the following credentials from the sql\_backup file.

Username : **manager**

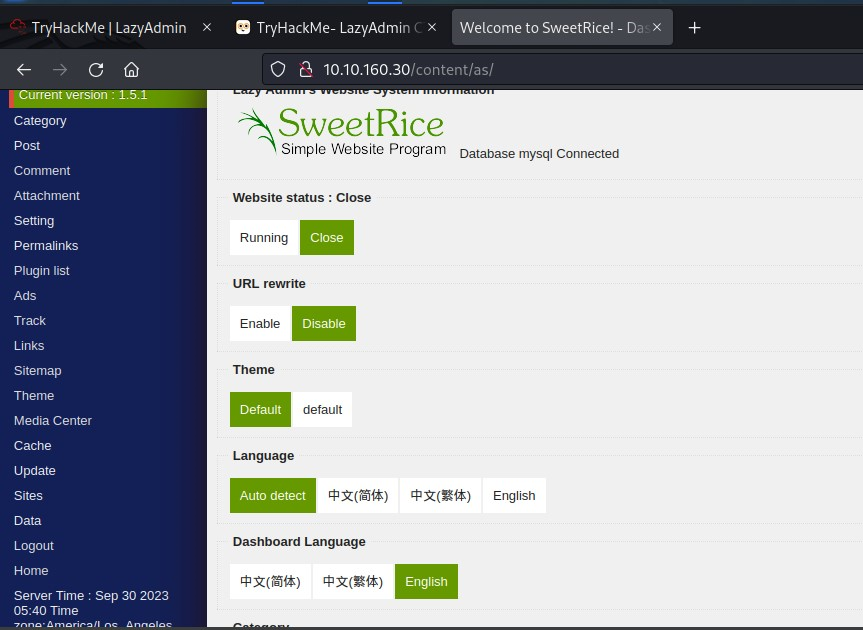
Password : **42f749ade7f9e175bf475f37a44cafcb (Password123) Cracked using crackstation.com**

****

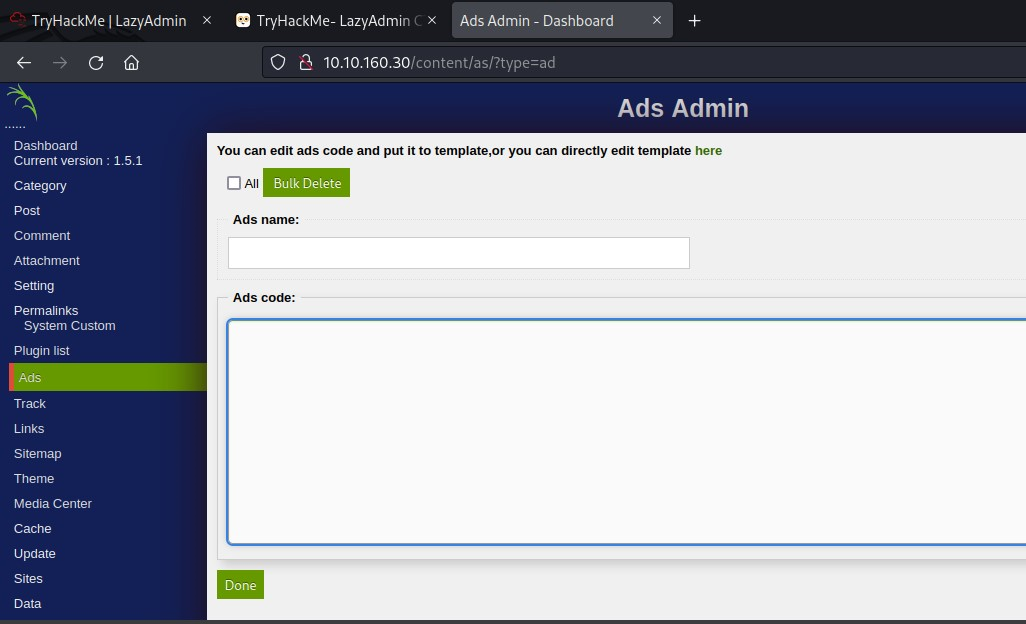
The Credentials can be useful.

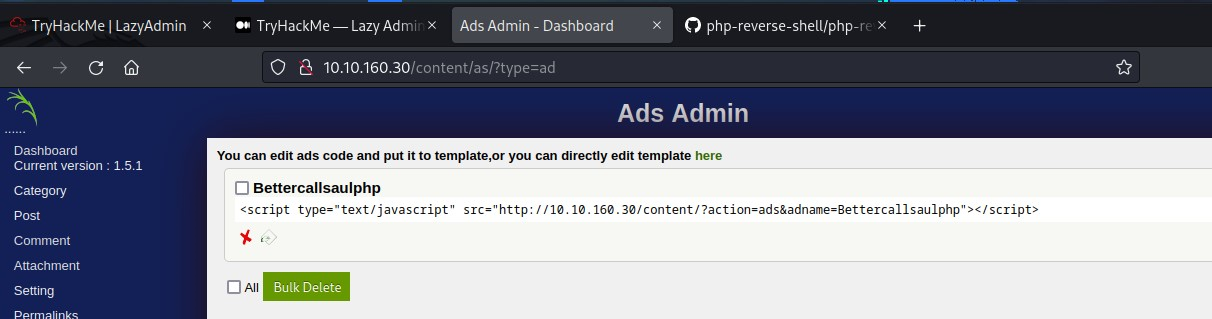


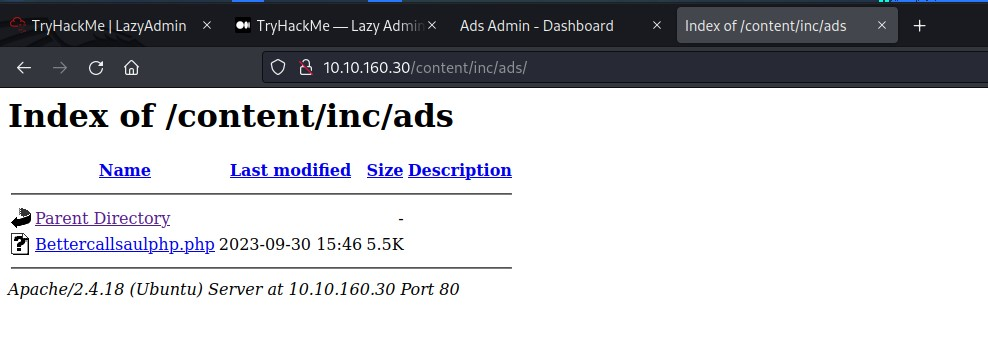
We found a login page in the **/as** directory, Lets try the credentials we found in the sql\_backup file to login into page.



While analyzing the page we can exploit the page with many ways, like file upload vulnerability and many more, We found a interesting section **Ads** where we can write a html page or anything and post it as AD. We can use this column to upload our **php\_reverse\_shell (PentestMonkey)** and Upload it.

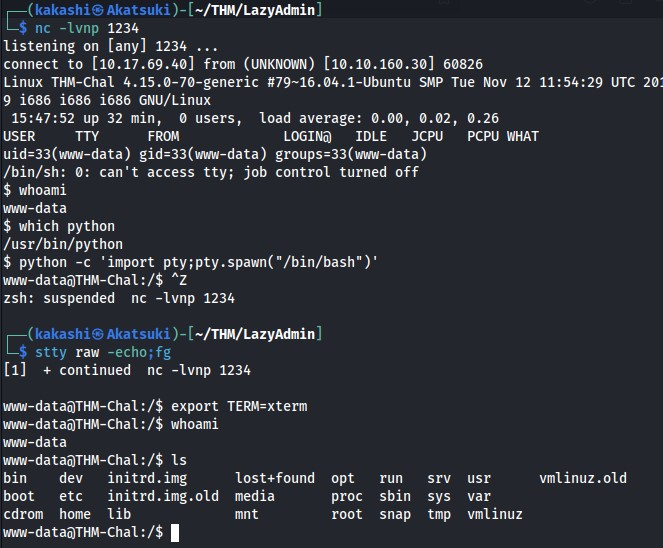


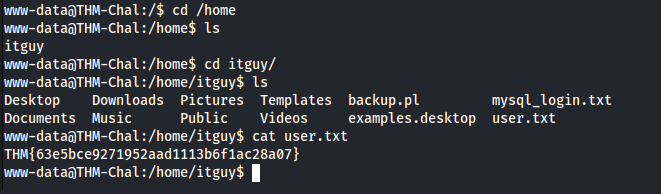




Just Click the payload we have uploaded to get a reverse shell.

Our php\_reverse\_shell is uploaded. Lets open a other terminal and listen to the incoming traffic using netcat.

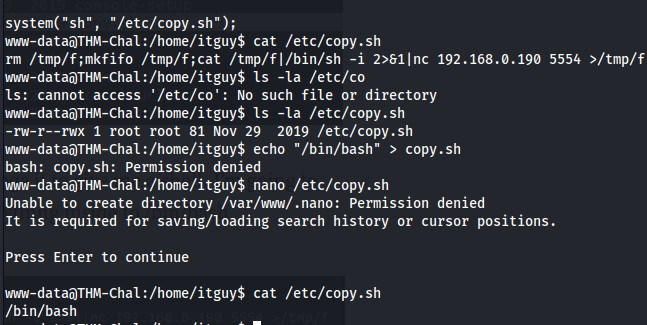


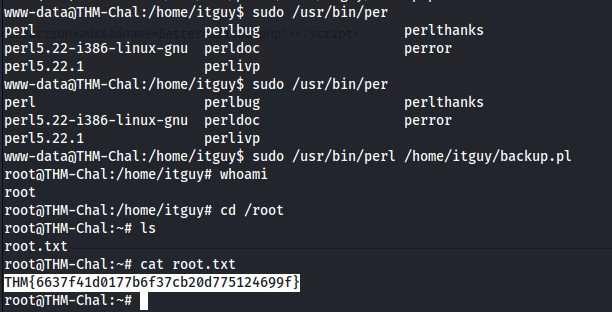


We Found the uer flag.

We need to Find the root flag, To do that we need to Elevate or Escalate Privilege to root.

Lets check the Privilege Status of the user. What we have analyzed is user can run perl as a sudo without password and access to the backup.pl and we have also checked that we can edit the backup.pl and also the copy.sh in the /etc directory. Let’s Analyze the content in the copy.sh file and rewrite the entire copy.sh into /bin/bash to spawn a shell and running perl as root we get a root shell.





We found the root flag.