This is the ctf LazyAdmins on tryhackme.

Search for directories with gobuster
We find a variety of directories.
One is **/content** which contains a placeholder page revealing the management system and sweetrice.
Then we make another search with gobuster on /content and find even more directiories.
We find some pages such as /inc which leads to a directory and file listing.
We also find a /content/index.php which leads to a login page
From this we can do a username and password cracking for the forms with hydra.
We find a username mitch with the password secret.
From here we can login and get a dashboard.
When looking through we see multiple places to upload files and also write html code which provides multiple possibilities of entry.
We choose the ads page where we can upload code and note down the version 1.5.1 which according to exploit-db for sweetrice has a sscf/php code execution vulnerability. For this we can see that the cve provides html code.
Then we can paste this html into the ads html and change the url in the cves html code to match the page. You also need to copy and paste a php reverse shell into the html code and provide your ip and port.
Then we provide a name for the “ad” and then activate it on the page.
Now we listen with netcat from our terminal and navigate to where we placed the html code and it should execute.
Now we have a shell, however not a root shell.
We get the user flag and then run sudo -l to see what can be run as sudo.
We see a perl file which can be run as sudo but with the specific file path.
The perl file seems to already contain a reverse shell which we either can modify to connect back to our machine, or just make it directly spawn a shell which when ran with sudo spawns a root shell.
So we just do echo “/bin/bash” > copy.sh
Now we can do sudo /usr/bin/perl /home/itguy/backup.pl
This will spawn a root shell and we're not root and can get the root flag!