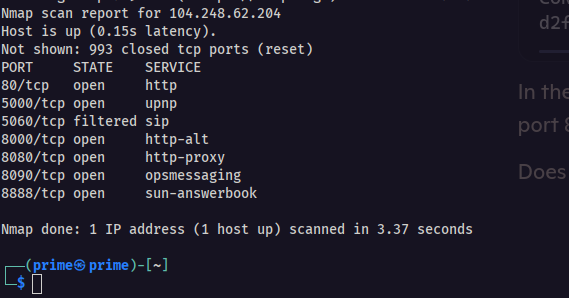
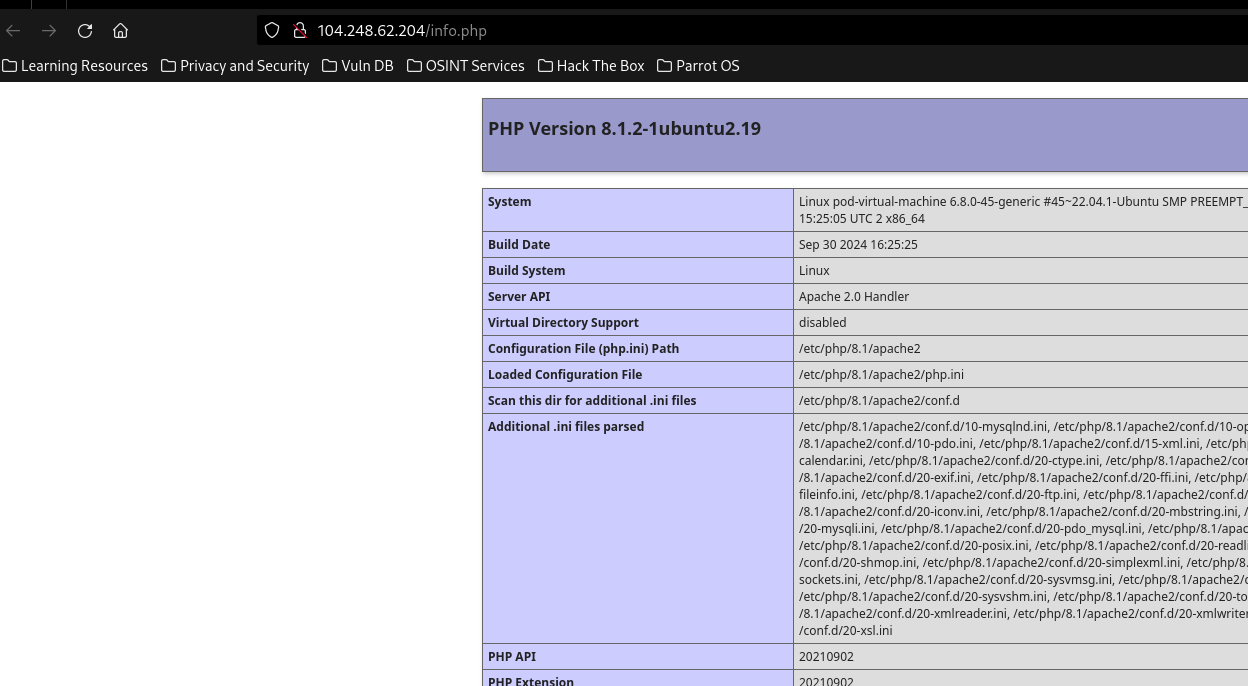
PoD machine walkthrough

First, perform a port scan with nmap.

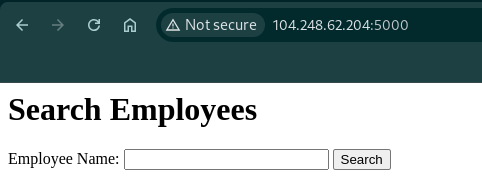


If you perform a directory scan, you can only see this file.

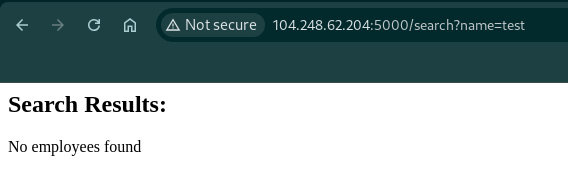
Sensitive Data Exposure



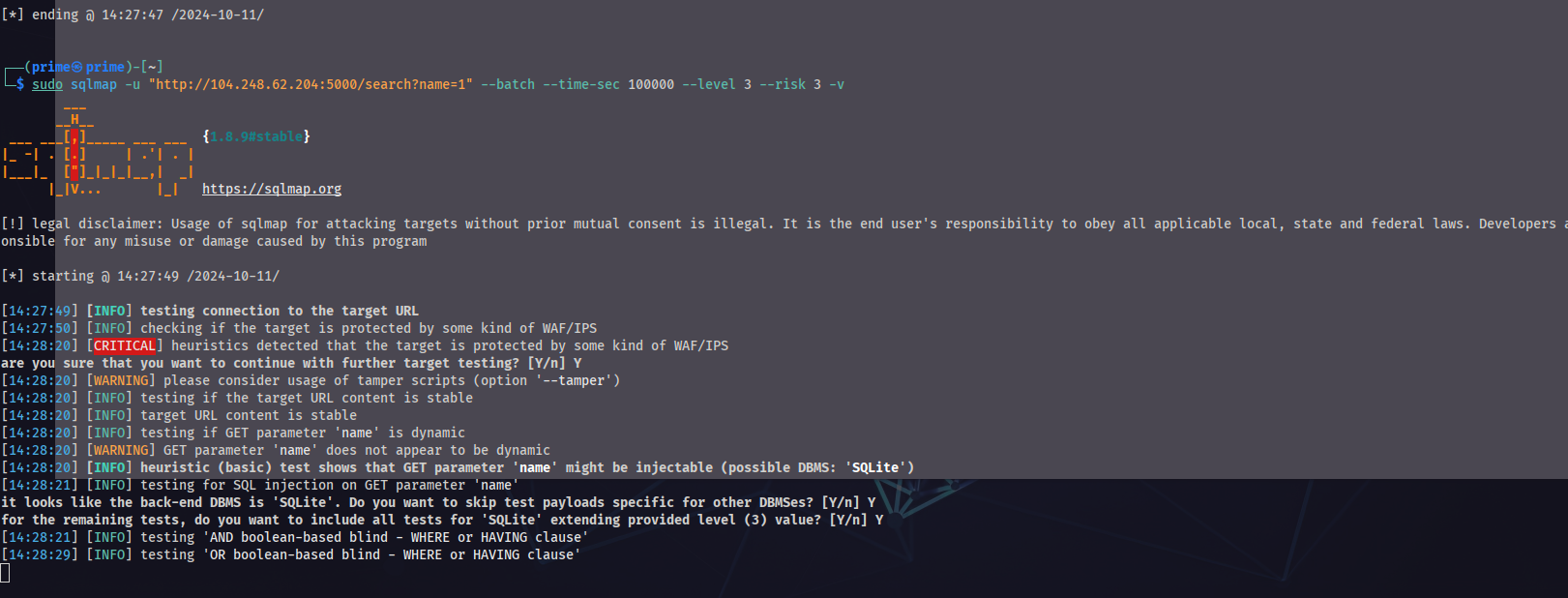
As you see, we have 7 open ports. 80 is a normal Apache2 server. Except for the 5000th port, we cannot see anything. In 5000 port, we see this



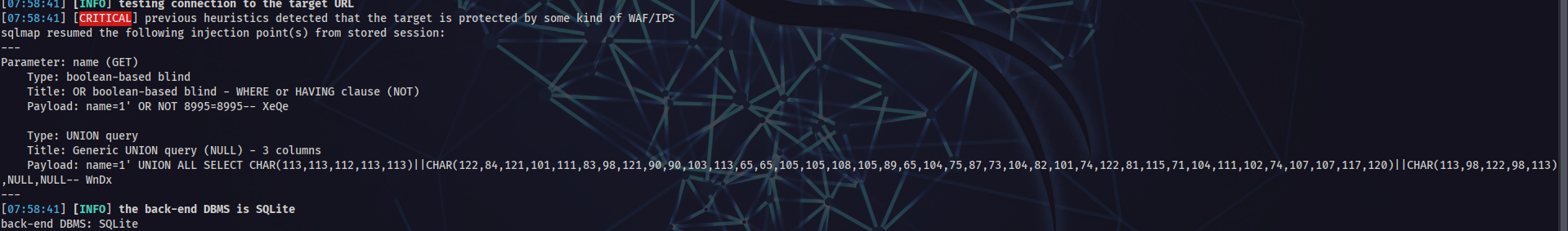
This is a searching site and it sends data with the GET method.

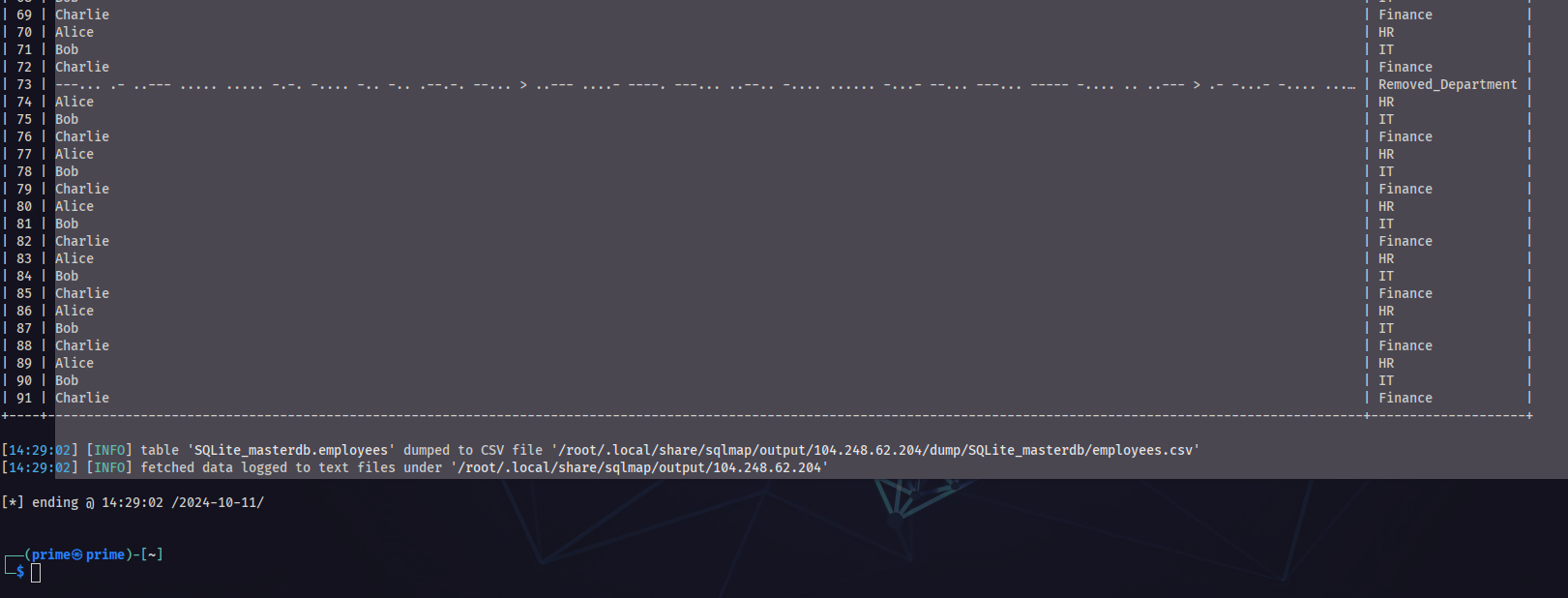


Here I made a scan with the sqlmap tool.

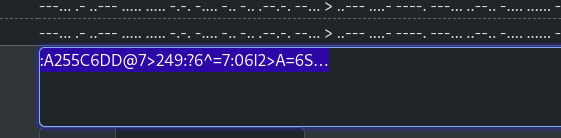


And we find a SQLi in this path

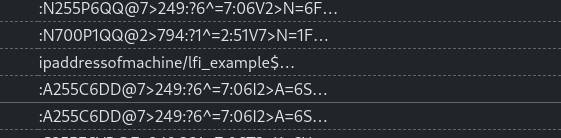
We dumped the database and found this text



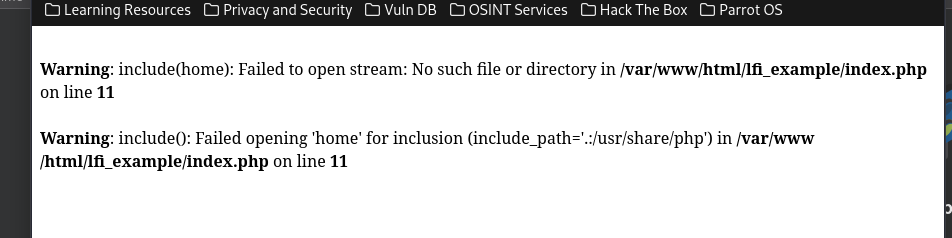
---... .- ..--- ..... ..... -.-. -.... -.. -.. .--.-. --... > ..--- ....- ----. ---... ..--.. -.... ...... -...- --... ---... ----- -.... .. ..--- > .- -...- -.... ...…

Converted this to normal text 

And decoded one time again.



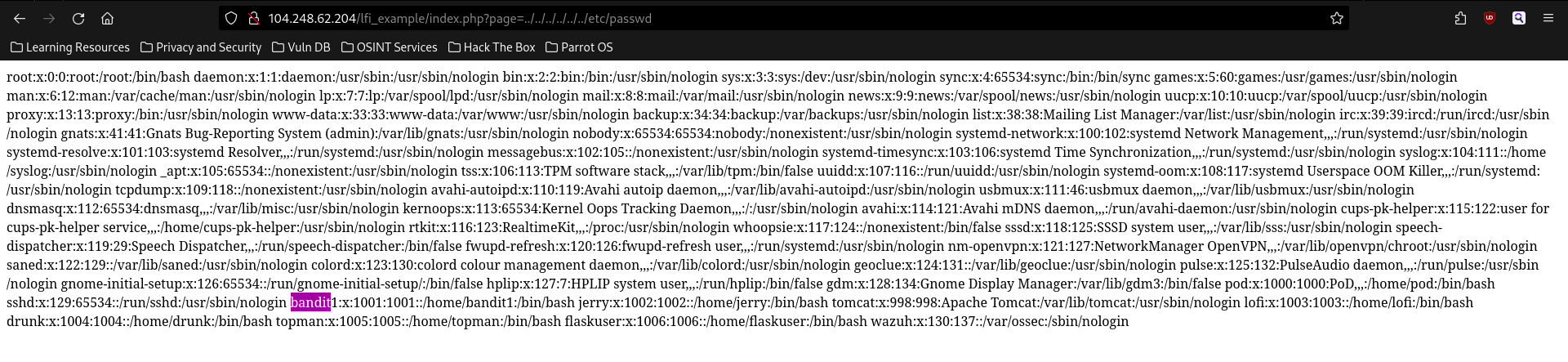
This is our 2nd web vulnerability’s path. When we go to the



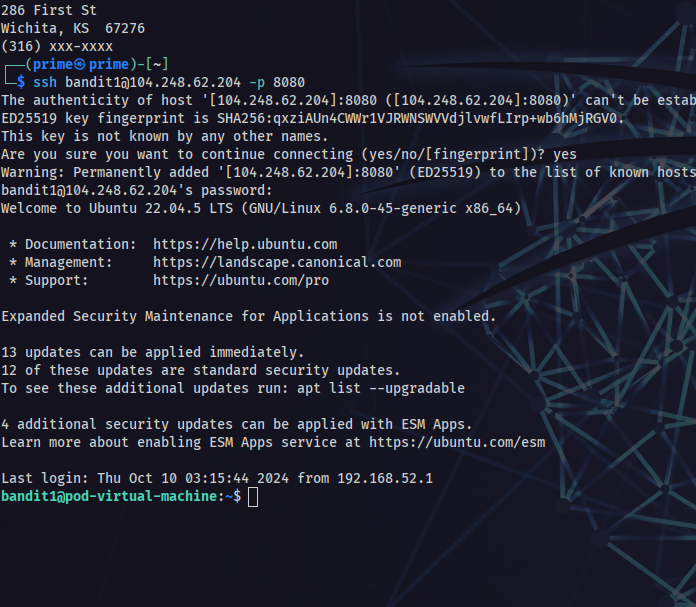
If you analyze error, you can see that index.php tries to include some php page. This means we can also do it.

http://<IP>/lfi\_example/index.php?page=../../../../../../etc/passwd

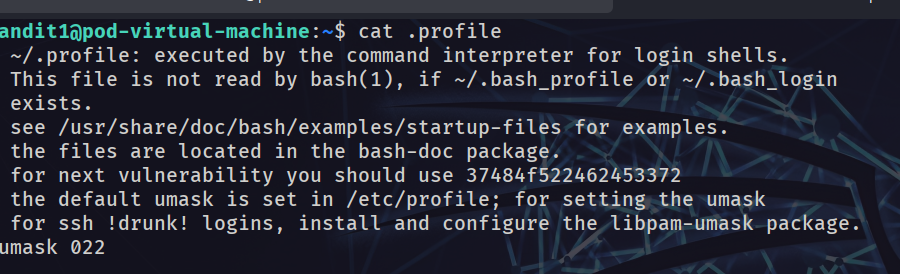
This is our payload and result is



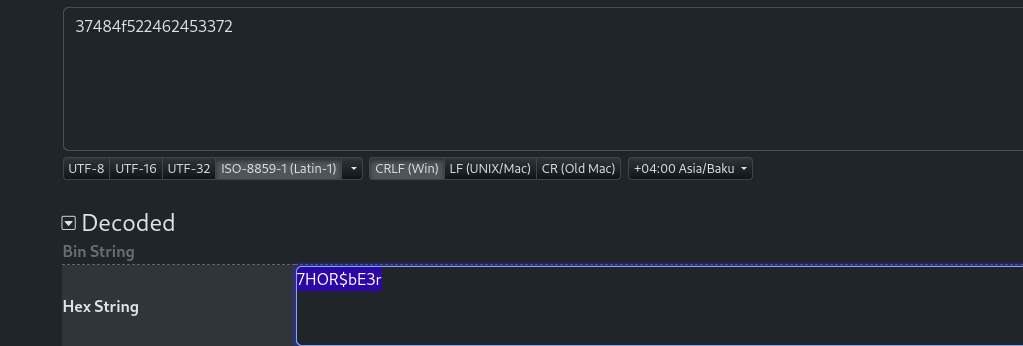
We found the user and we connected with bandit1:bandit1 username and password via SSH.



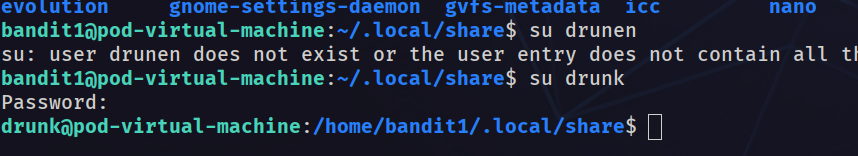
Open the .profile file and you will see the line that does not belong there.

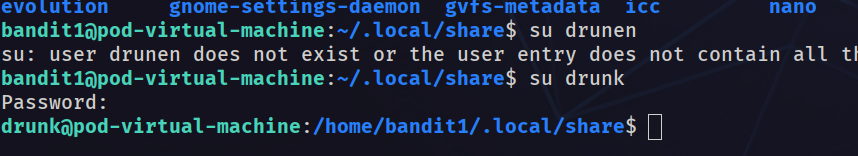


Decode it

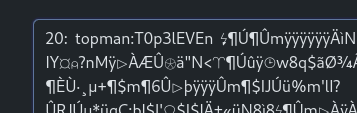


This is the password of “drunk” user.

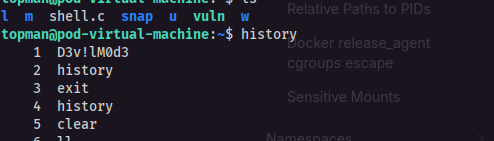
  
In “drunk” home directory, you can see Friends.jpg. We can download the image with “scp” command.

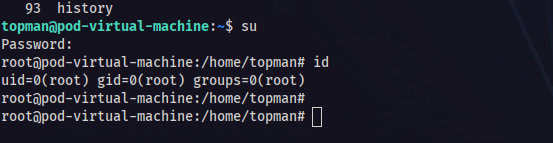


In here, used our server for getting image from server. Then I uploaded it to [this site](https://stylesuxx.github.io/steganography/) and result is..



We have the password of the topman user. In topman, if you look at the history. you will see the password of root user.





And this is end of walkthrough