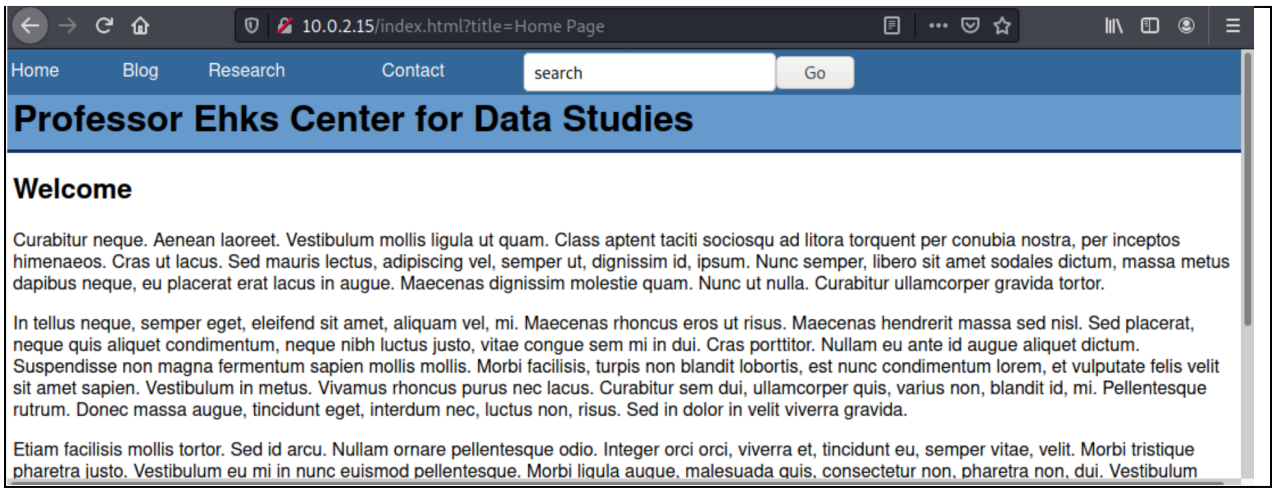
LAMPSecurity: CTF4

We start with nmap scan .
We run the following command : nmap -A 10.0.2.1-254

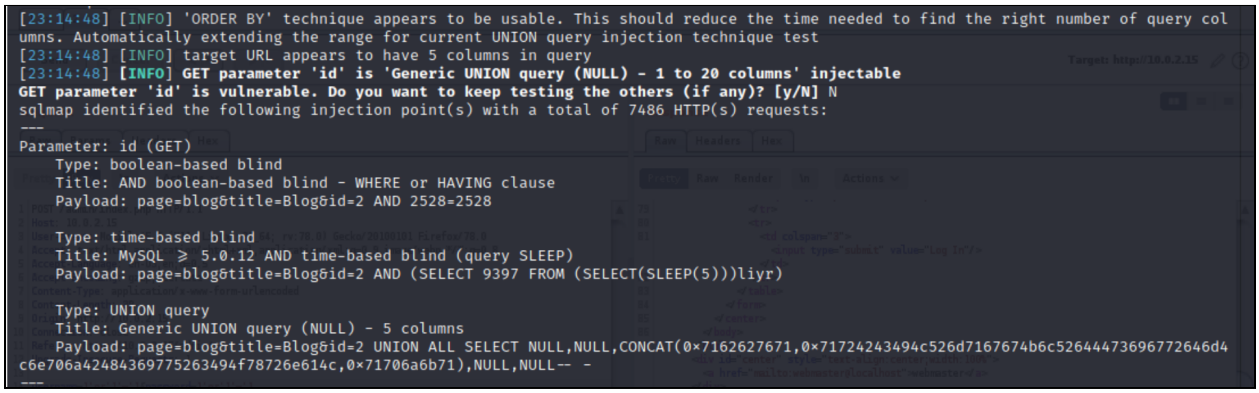
After finding the IP, type it on firefox to get the following website.

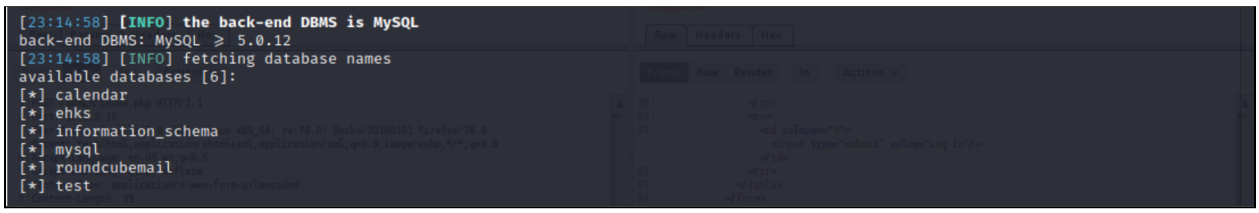


After surfing through the website I found a SQL injection is possible in the following url in id parameter upon injecting a single quote (‘).
http://10.0.2.15/index.html?page=blog&title=Blog&id=2

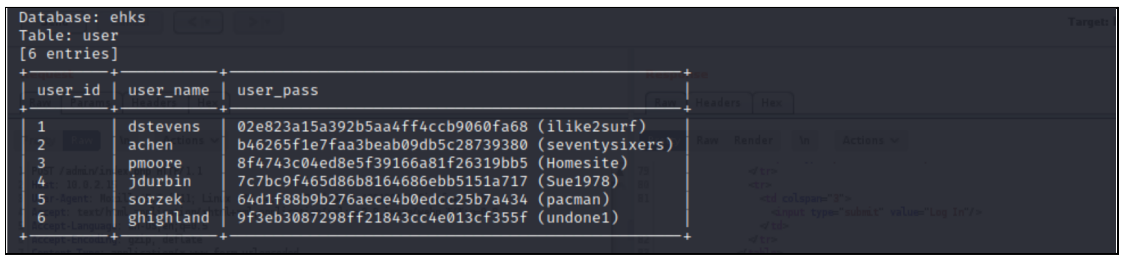
I decided to run sqlmap on the request. So I refreshed the page and intercepted it using burpsuite. Copied the request into a text file.

Next I ran the following sqlmap command on the terminal.
sqlmap -r filename.txt --level=3 --risk=2 --dbs





Got all databases available.Next step is to find information about tables from ehks database (since the website belongs to Professor Ehks) using the following command.
sqlmap -r filename.txt -D ehks --tables --dump --batch



We see that we got 3 tables and also the contents of the 3 tables.
The content from user table contains the username and password. From the nmap scan , it is known that ssh port 22 is open.
So we would try to get in using the above credentials through ssh using following command.

ssh achen@10.0.2.15

It displayed the following error :
Unable to negotiate with 10.0.2.15 port 22: no matching key exchange method found. Their offer:
diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

Its solution would be to use :
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 achen@10.0.2.15

We type the password : seventysixers
And we are in.
Next we try getting root and a sudo su command sufficed.