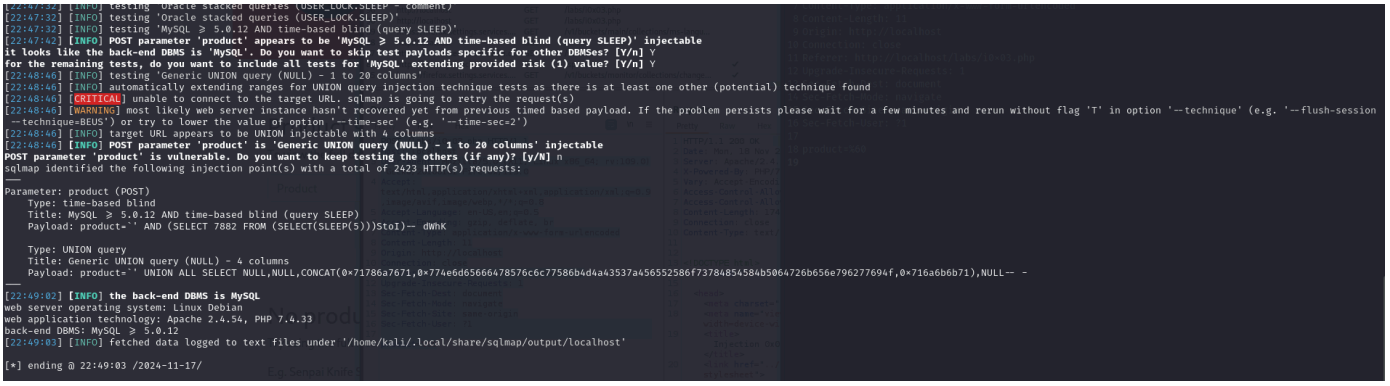
04 - SQL Injection - Capstone

Here we are at the capstone project. Lets see if we can hack it. Or if we are a hack.

After going through the application, there is not much attack surface in this case, we have the main page, and the page that display the items with details.

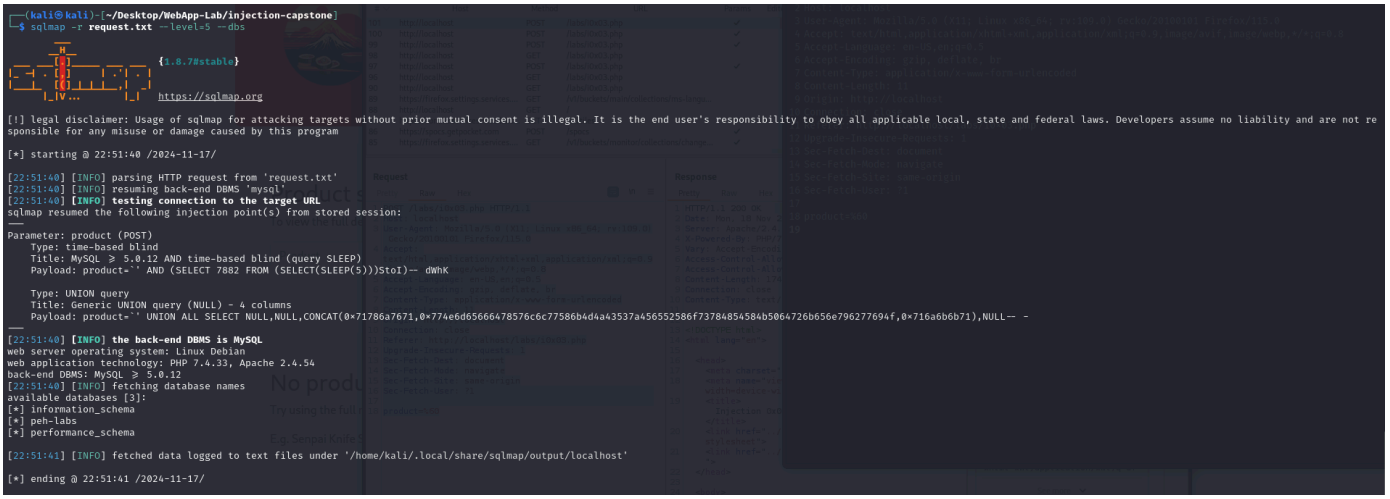
Lets run:

"#sqlmap -r request.txt --level=5"

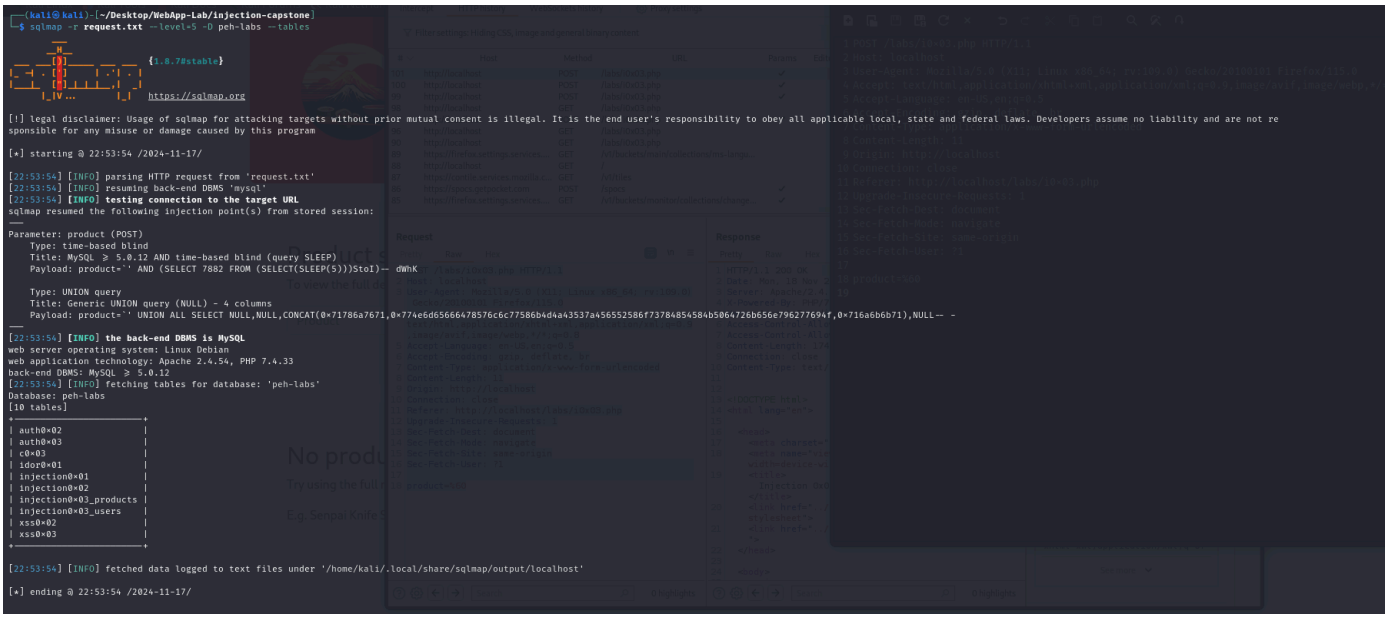


It is vulnerable. We can see the payload. Lets have sql do everything.

--dbs

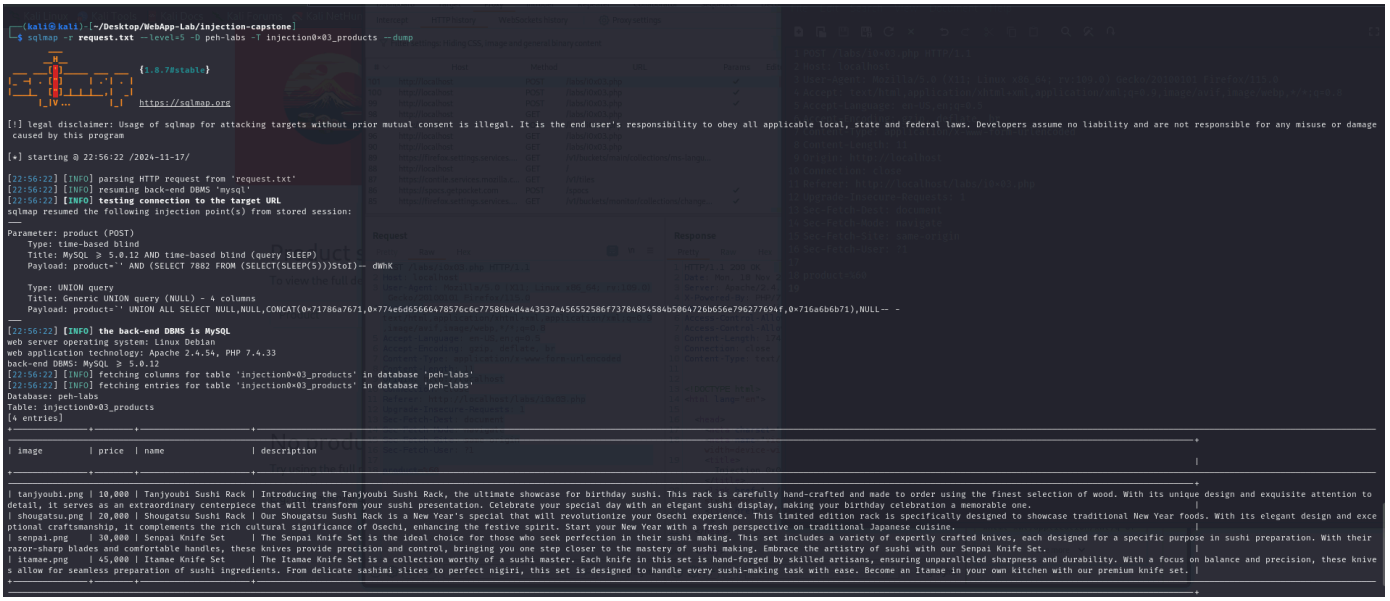


--tables

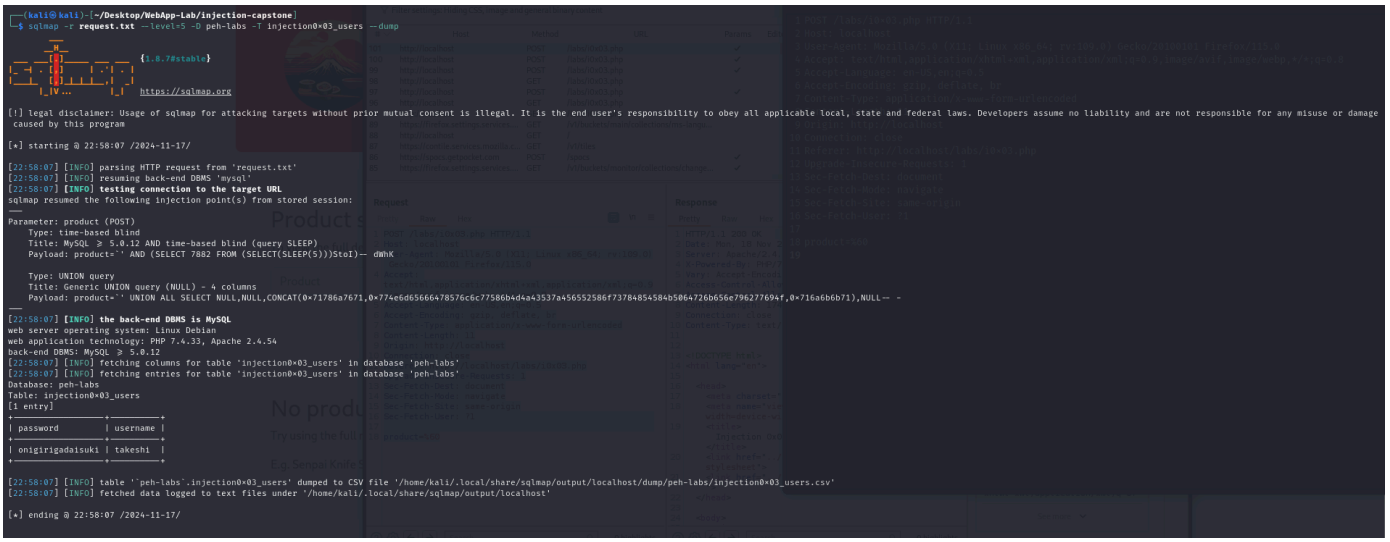


Now, we can dump whatever there is in those 2.

"#sqlmap -r request.txt --level=5 -D peh-labs -T injection0x03_products --dump"



Now, we do it for the other table.



And, we have the password, and username.

We can try initial access. But, as this is being hosted in my machine, we know it wont work as this username is not an user in our machine/server.

Our instructor, Alex, goes through the exploitation manually. I am not going to be documenting that.

Take aways: Check if the tool you are using offers this idea "if this succeeds, then do this" type of thing. We can see the sqlmap has this idea behind it. We first check if it is vulnerable, then we enumerate the database, and dump what we want.