# Challenge 1: Gain Access to a Remote

Reporting my Methods and Findings bellow (Could not solve the question):  
Starting the VM was a challenge since it was giving a driver problem it required some MediaTek wifi 6 driver. And my laptop as intel driver. So from some online googling I got to know that Mediatek drivers are in Asus and ROG Laptops. So I borrowed Asus laptop from my friend which got me started on to the process.   
  
I Logged in to the guest user and searched for localhost to get me to the website to be exploited. I found login and signup page and thought of it to be the final website to be exploited (I did not know about the note app yet).

I made a random account from signup and then logged in to the account from which I got to know that there is actually a dataset being created behind it. And since website databases are ofcourse confidential, it occurred to me that if I managed to get access of database somehow then that would somehow lead me to root access. Further I tried to inspect all the php and js code base of all 3 pages (login, signup, note app) I could not find any ambiguity in the code (since it was mentioned that vulnerability as been added).

Js script was refering to api/notes path so I tried look for all the files present in the hosting. I searched for localhost/api where I found 2 founders (note and user). I opened all files within those 2 folders but could not find a thing in there.

Since I wanted to tap into the database, I made a random try to enter by searching for localhost/database which showed me 2 sql files and I thought this was it. I opened seed.sql where I found Piyush bhai and email [piyush@saic.com](mailto:piyush@saic.com) also I found a very long password and thought that to be an encrypted password. I tried some stuff on it but lead to nothing. Similarly I opened schema.sql where it was instructed to create users table with all relevant fields. But I had to find the table so I dropped that also after sometime.

Then I moved on to examining php files for frontend of the note app where I found a comment saying that “create a link to /admin page if $role is admin” right above the add note button so I thought this could be a clue and searched for localhost/admin page but it redirected me to homepage of note app.

I read about admin role in js and php and also about myphpadmin but could not find a thing and that’s where I stopped on this question since I do not know web development or php or js so I thought that I am wasting time trying to do something I do not know.

I made my last and illegal try now. I do know that doing this was illegal for the test.

From the website it was evident that Piyush bhaiya had not made all this website for a test. I figured it to be a template from github somewhere. I surfaced the web and actually found the github page from where this whole template was picked. And then I started comparing the php code line by line.

Turns out the admin comment was not there in the original code which made me sure that yes it is the right vulnerability but since I do not know php or web dev, I could not host that github code on my own so find some loose ends. That’s where I stopped for all.