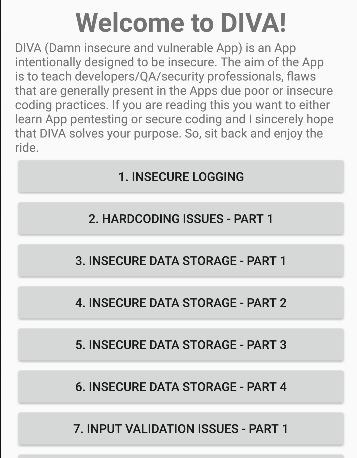
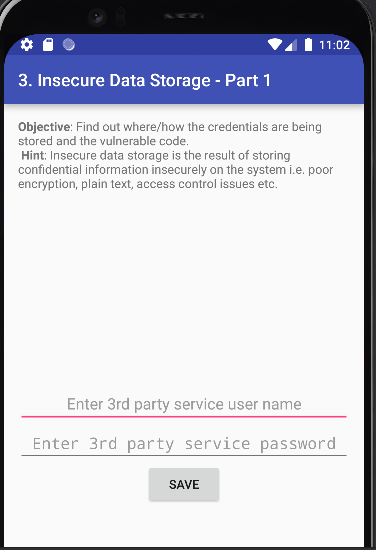
Insecure Data Storage Part – 1

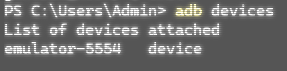
Navigate to DIVA application and go to Insecure Data storage part -1



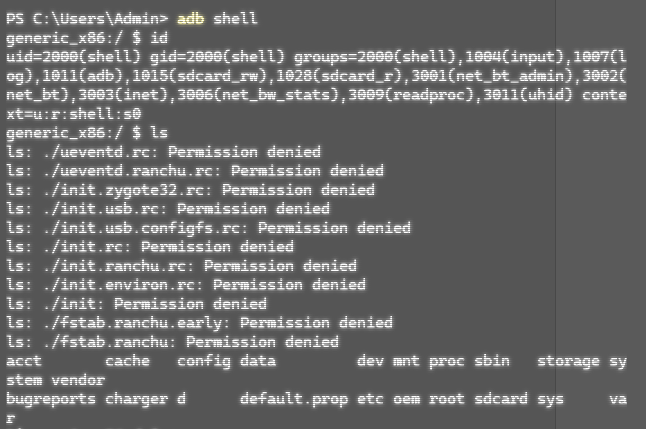
We see this interface



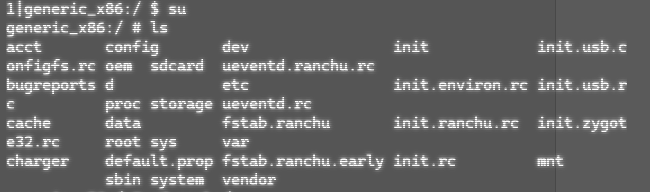
Lets check if our virtual emulator is connected to adb, we see that is connected



We then connect the device to adb shell



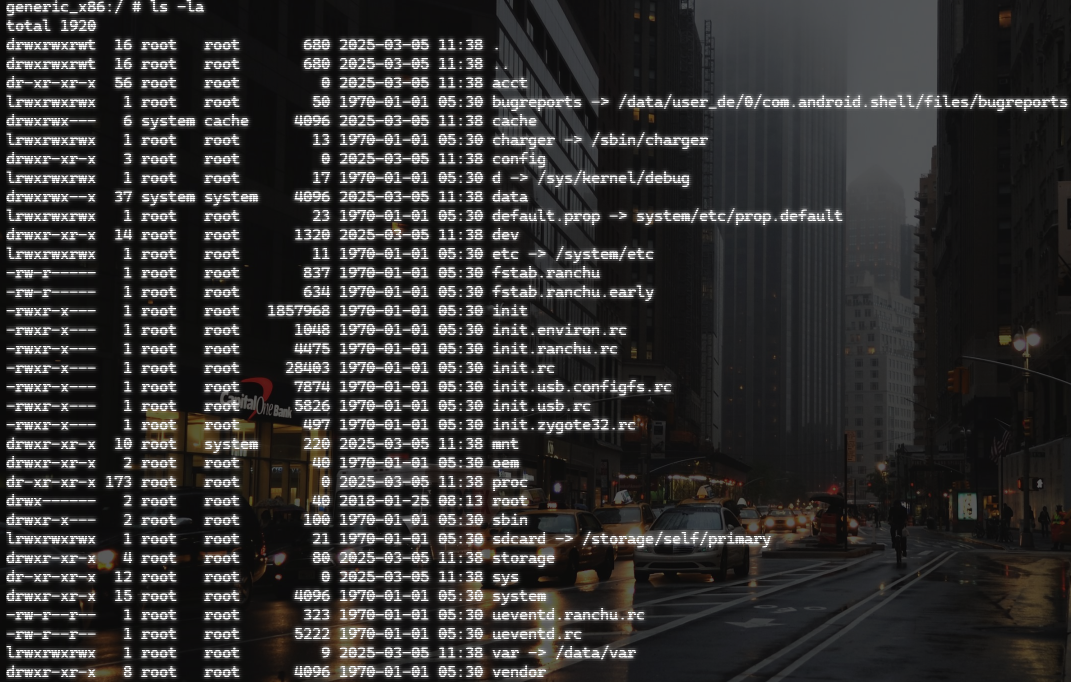
We notice that the privileges are not escalated, to get root privileges we can use ‘su’ command.



Now if we check the current privilege it will show root



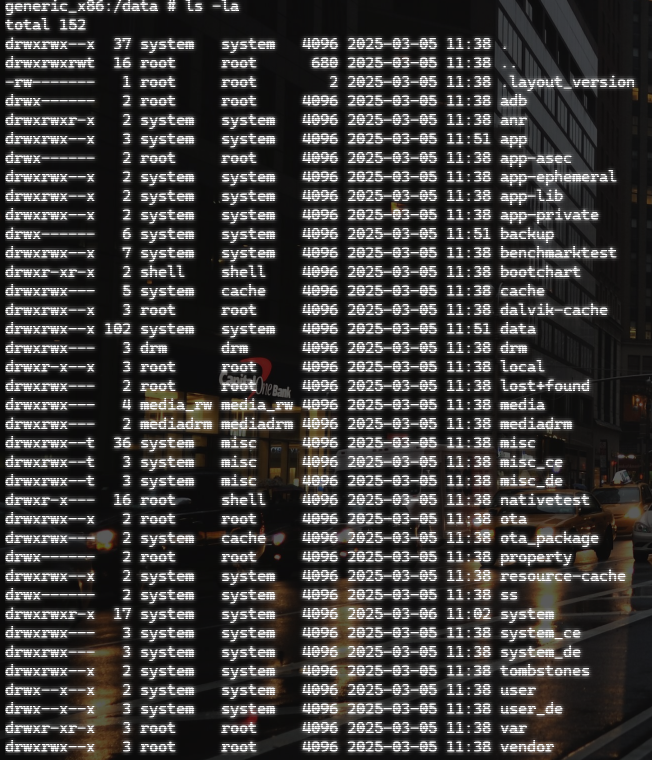
We can then go ahead and check the directories in root access



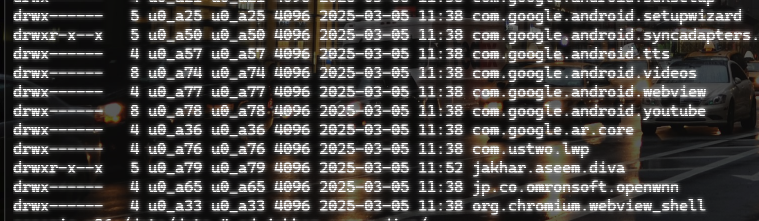
We see that there is a data folder



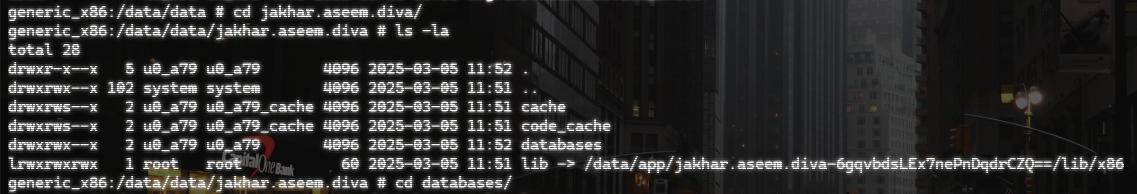
We can go ahead and list the files in data folder



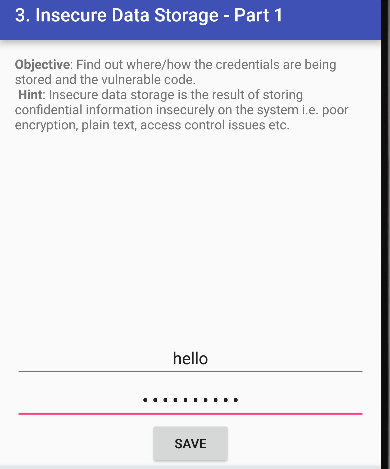
There is a ‘jakhar.aseem.diva’ folder in data, let’s go to that folder



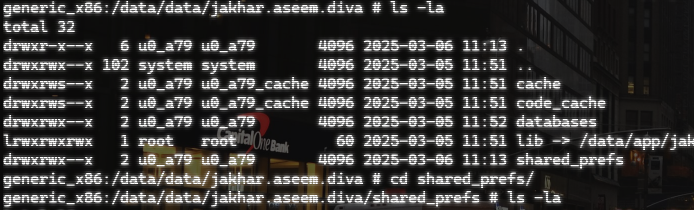
On listing the contents of the folder we see a directory for databases



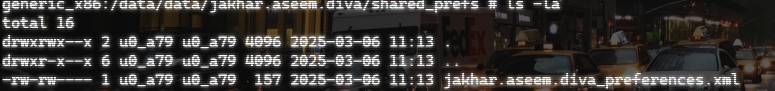
Let’s go back to our emulator and type random credentials in the interface



After this we can see a new folder in ‘jakhar.aseem.diva’ folder called ‘ shared\_prefs’



When we go to shared\_prefs, we see that there is an xml folder



On reading this xml folder we can see the credentials that we have entered, hence, exploiting the insecure data storage vulnerability.

