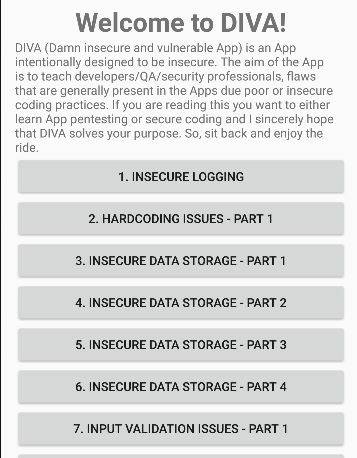
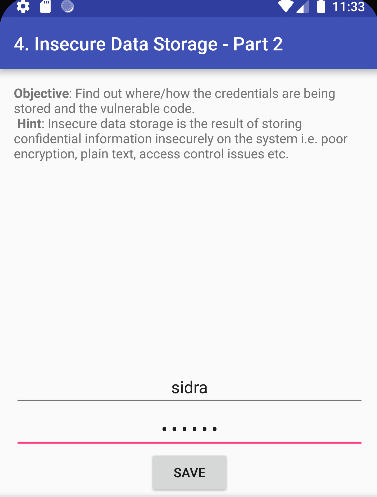
Insecure Data Storage Part – 2

Navigate to the DIVA application on the android emulator and go to Insecure Data Storage part -2



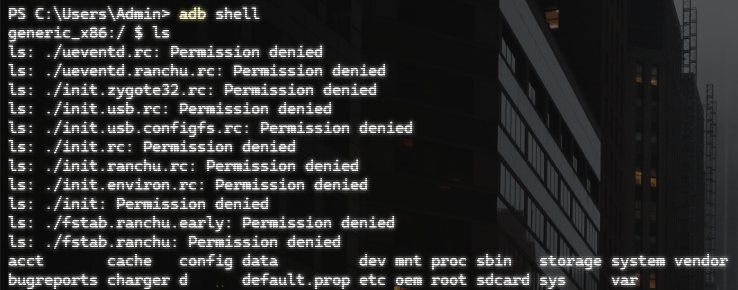
We see this interface, let’s write our credentials in this case it is user: sidra, password:qwerty



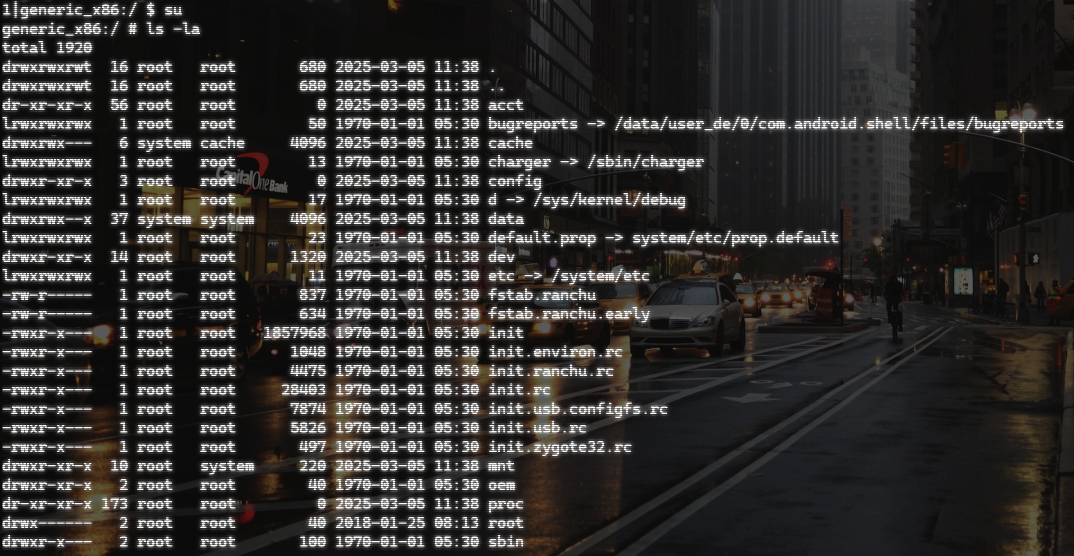
We see a message that the credentials are saved



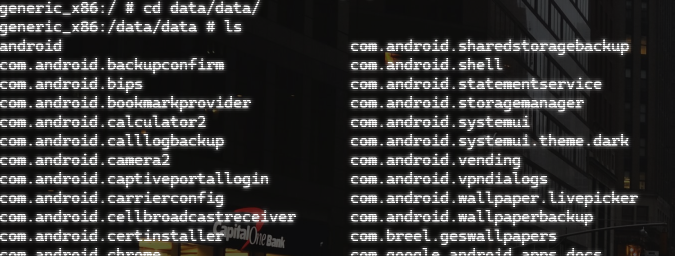
We then connect the emulator to adb shell



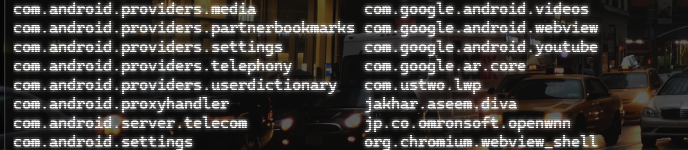
And get root privileges using ‘su’ command



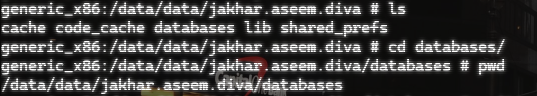
We then navigate to data/data/ folder and list the directories



Navigate to ‘jakahar.aseem.diva’ folder



List the folders in this directory, we find the databases here, navigate to databases, print the current working directory path using ‘pwd’ and copy this path



Exit the shell and enter adb root to give phone’s root access to adb and pull the path that we initially copied to the desktop. List the directories in this pulled folder, we see a folder called ids2.



We can read this folder and see that the credentials that we entered in the emulator is saved here in plaintext, hence, exploiting insecure database storage vulnerability.

