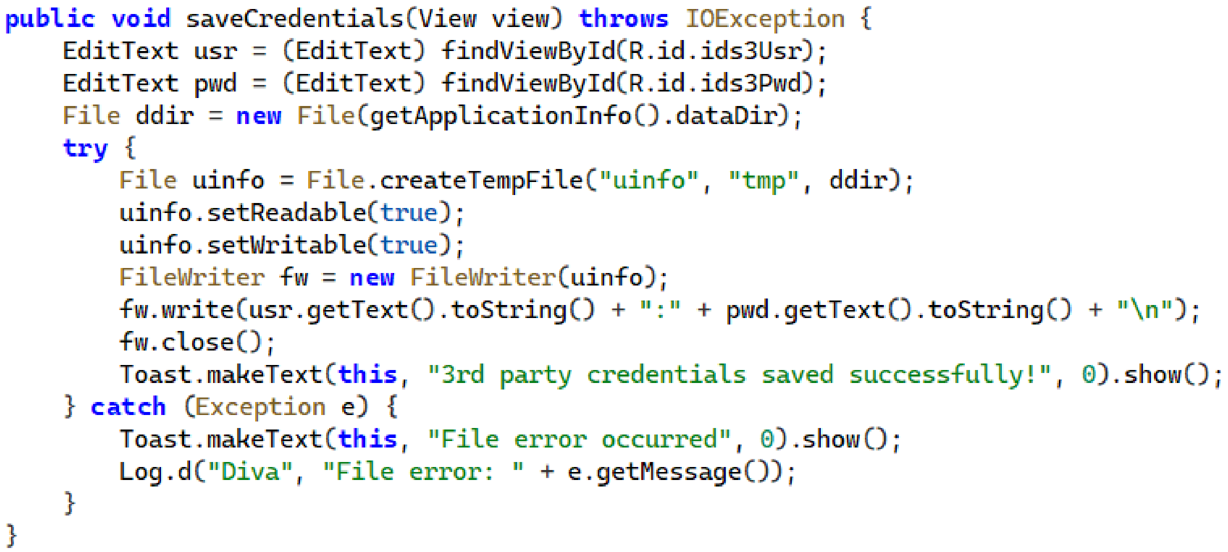
Insecure Data Storage – Part 3

1. The objective is to find where/how the credentials are being stored and the vulnerable code.
2. This is the code:



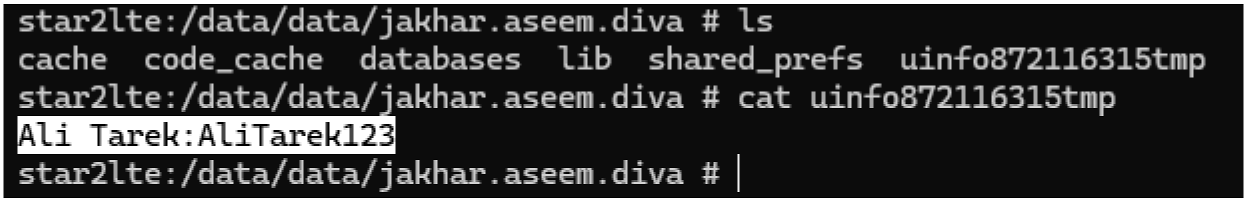
```java
public void saveCredentials(View view) throws IOException {
    EditText usr = (EditText) findViewById(R.id.ids3Usr);
    EditText pwd = (EditText) findViewById(R.id.ids3Pwd);
    File ddir = new File(getApplicationInfo().dataDir);
    try {
        File uinfo = File.createTempFile("uinfo", "tmp", ddir);
        uinfo.setReadable(true);
        uinfo.setWritable(true);
        FileWriter fw = new FileWriter(uinfo);
        fw.write(usr.getText().toString() + ":" + pwd.getText().toString() + "\n");
        fw.close();
        Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
    } catch (Exception e) {
        Toast.makeText(this, "File error occurred", 0).show();
        Log.d("Diva", "File error: " + e.getMessage());
    }
}
```

   Let’s break it down.

   The developer gets the application file’s directory, then create a new file named “**uinfo**” and make it readable and writable. Then, he stored the user info in plain text in the new file.

3. I will enter my username and password and try to access it from adb shell.

   I found new file created named “**uinfo872116315tmp**” when I read it, I found my username and password.



```
star2lte:/data/data/jakhar.aseem.diva # ls
cache   code_cache   databases   lib   shared_prefs   uinfo872116315tmp
star2lte:/data/data/jakhar.aseem.diva # cat uinfo872116315tmp
Ali Tarek:AliTarek123
star2lte:/data/data/jakhar.aseem.diva #
```