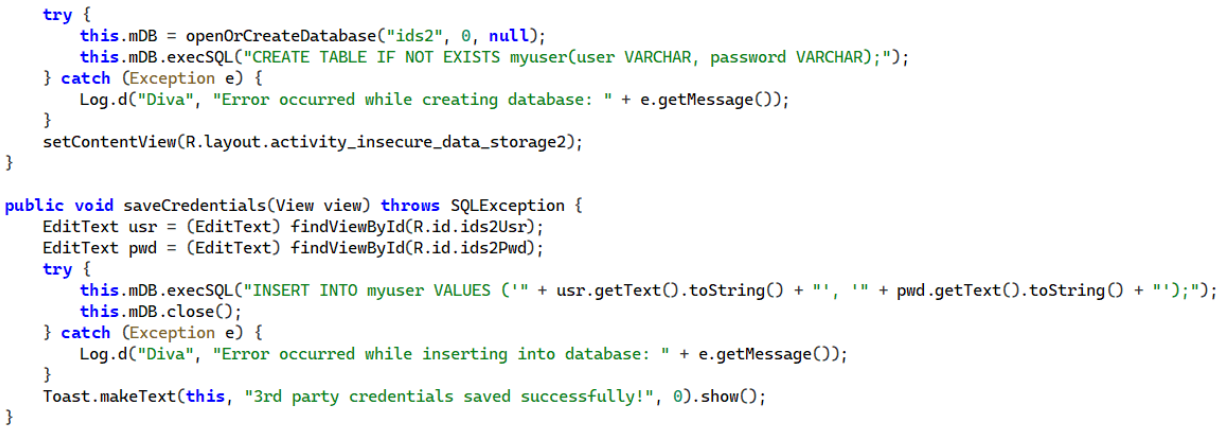
Insecure Data Storage – Part 2

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

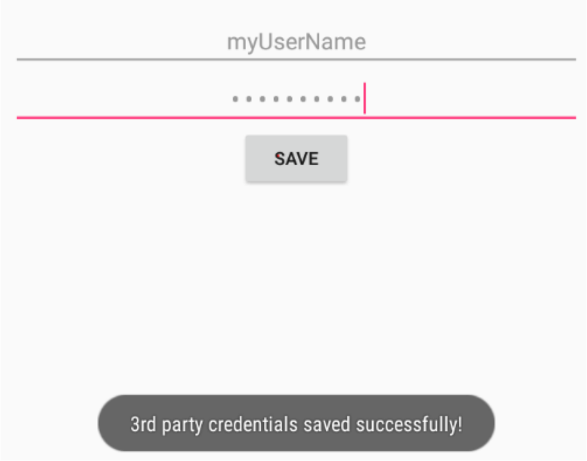
2. This is the vulnerable code:



```
        try {
            this.mDB = openOrCreateDatabase("ids2", 0, null);
            this.mDB.execSQL("CREATE TABLE IF NOT EXISTS myuser(user VARCHAR, password VARCHAR);");
        } catch (Exception e) {
            Log.d("Diva", "Error occurred while creating database: " + e.getMessage());
        }
        setContentView(R.layout.activity_insecure_data_storage2);
    }

    public void saveCredentials(View view) throws SQLException {
        EditText usr = (EditText) findViewById(R.id.ids2Usr);
        EditText pwd = (EditText) findViewById(R.id.ids2Pwd);
        try {
            this.mDB.execSQL("INSERT INTO myuser VALUES ('" + usr.getText().toString() + "', '" + pwd.getText().toString() + "');");
            this.mDB.close();
        } catch (Exception e) {
            Log.d("Diva", "Error occurred while inserting into database: " + e.getMessage());
        }
        Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
    }
```

3. The developer open database whose name is “**ids2**”, and create table named “**myuser**” and insert the username and password in database clearly without encryption. Let’s try to hack it.
4. I entered my data



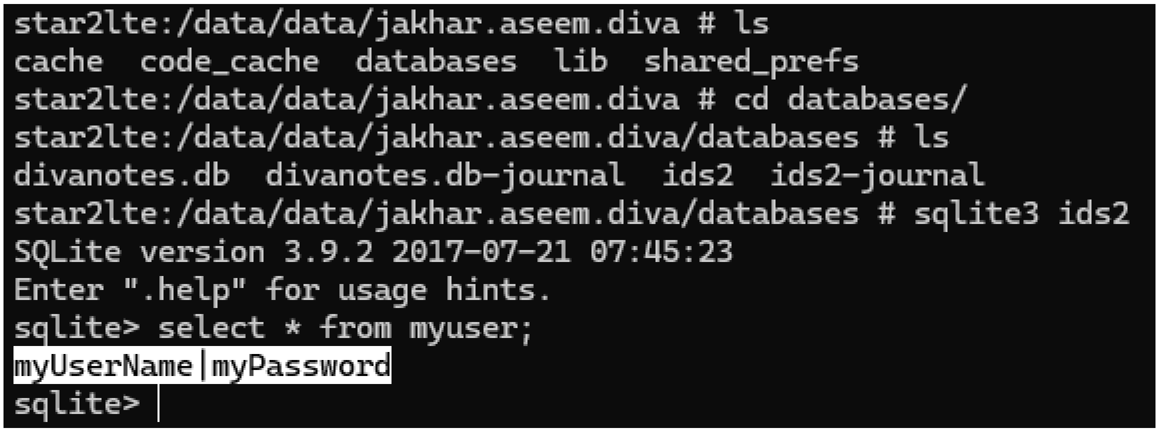
myUserName

••••••••••

3rd party credentials saved successfully!

Let’s go to adb shell.

5. Now, I know the database’s name and the table name. Can I read the stored data?



```
star2lte:/data/data/jakhar.aseem.diva # ls
cache  code_cache  databases  lib  shared_prefs
star2lte:/data/data/jakhar.aseem.diva # cd databases/
star2lte:/data/data/jakhar.aseem.diva/databases # ls
divanotes.db  divanotes.db-journal  ids2  ids2-journal
star2lte:/data/data/jakhar.aseem.diva/databases # sqlite3 ids2
SQLite version 3.9.2 2017-07-21 07:45:23
Enter ".help" for usage hints.
sqlite> select * from myuser;
myUserName|myPassword
sqlite>
```

Yeah, I read it successfully.