DAMN VULNERABLE BANK(DVBA SETUP GUIDE)

Author : Rengoku

INTRODUCTION :

The setup will have 4 process

1. Building the app backend
2. Building the app frontend
3. Bypass Root + Ssl Pin + Frida
4. Decrypt Parameter Value

A.) BUILDING THE APP BACKEND

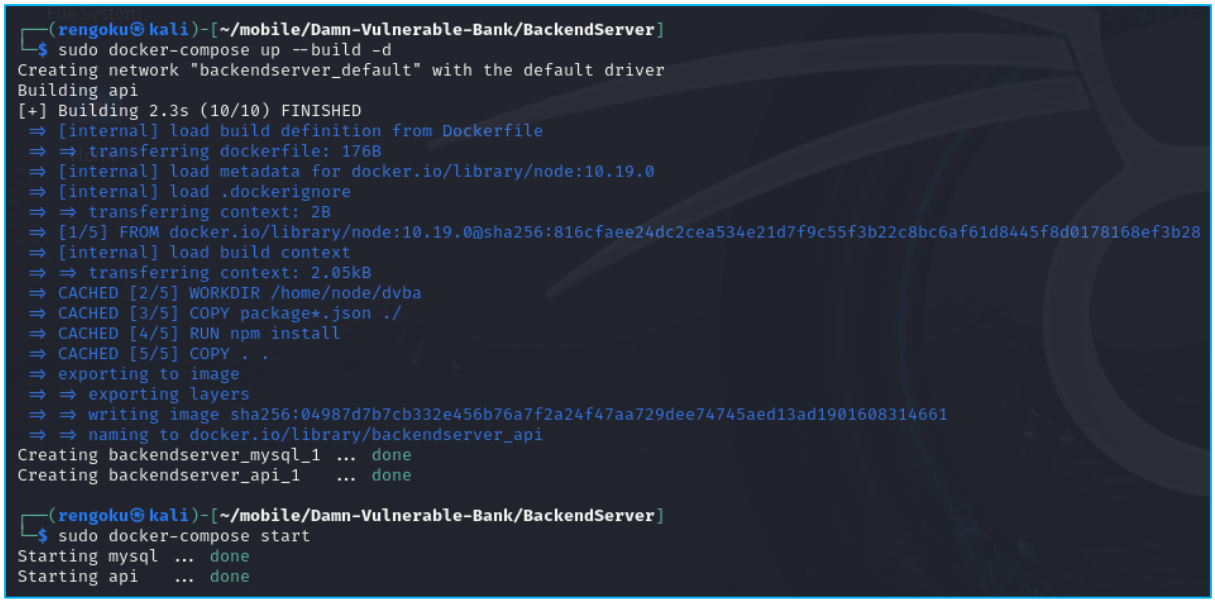

Figure 1.1 building the app backend

1. Download the DVBA repository and go to the backend directory which is BackendServer
2. Build the backend using docker with command “sudo docker-compose up --build -d”
3. In the figure 1.1 above. Shown I have already build the backend server. So to start the server just use commands. “sudo docker-compose start”
4. COPY the backend IP which is on the eth0 network interface
5. DONE ! you have successfully build the backend

B.) BUILDING THE APP FRONTEND

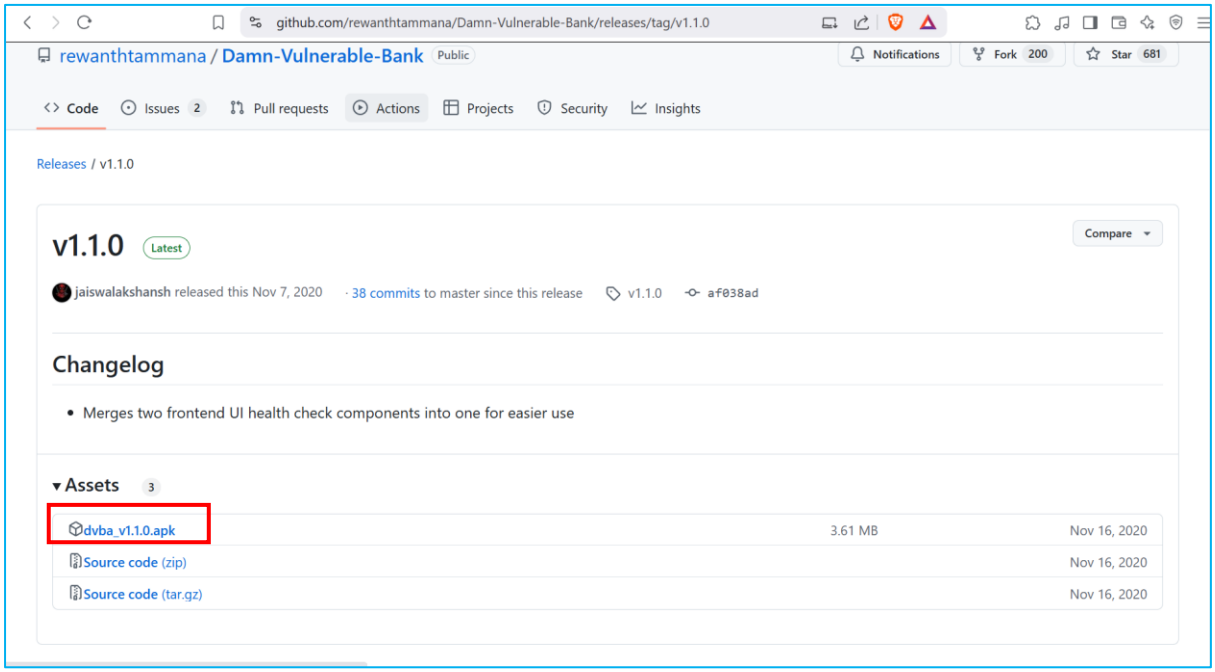

Figure 1.2 DVBA APK

1. Download the DVBA apk on your mobile device that want to be pentest.
2. Install The APP
3. To connect Front End with backend. At the server API section on the app insert below "http://BACKENDIP:3000". Check Health and go to sign up page.
4. If connection successful. You can create user account ! if failed. It will say something went wrong.
5. DONE !

C.) BYPASS ROOT DETECTION + SSL PINNING + FRIDA DETECTION

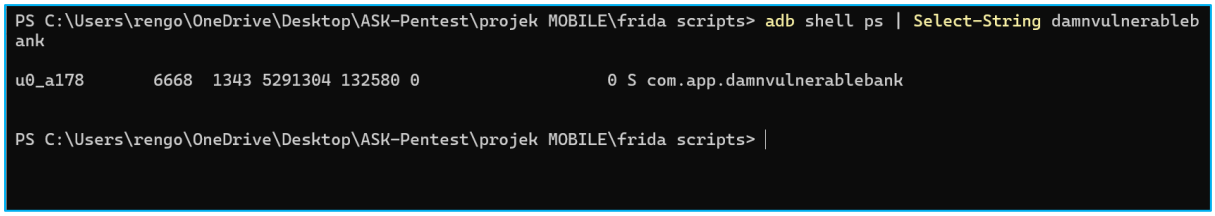

Figure 1.3 Find DVBA Process ID

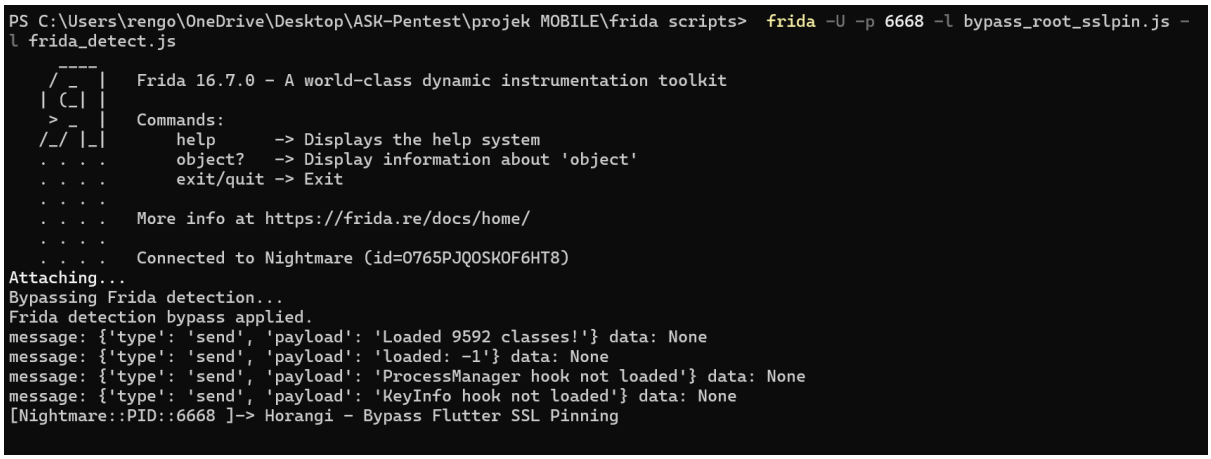

Figure 1.4 Inject Frida Scripts

1. Open Powershell
2. Run the commands “adb shell ps | Select-String damnvulnerablebank”
3. The process ID is 6668
4. Using The commands frida -U -p 6668 -l bypass_root_sslpin.js -l frida_detect.js You can bypass the app
5. ‘-p’ 6668 is the process ID and ‘-l’ is the script used
6. IF BYPASS FAILED. You won’t be able to open the app at all

D.) DECRYPT PARAMETER VALUE

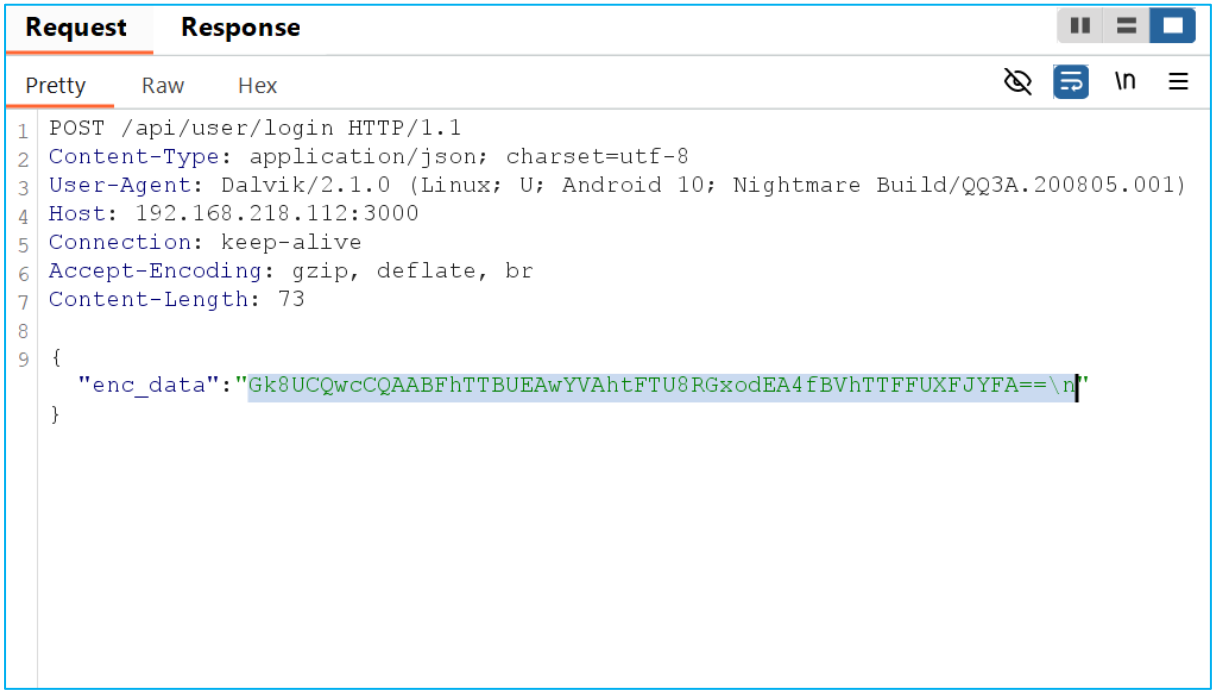

Figure 1.5 The App Encrypted Parameter Value

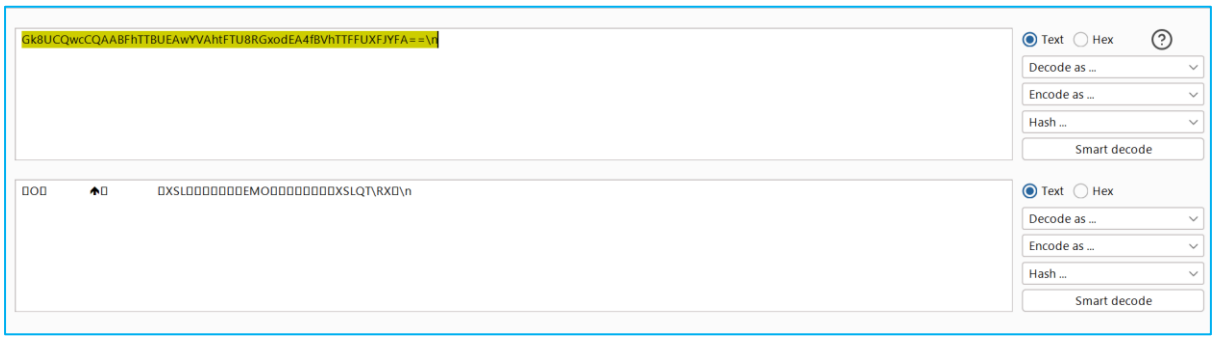

Figure 1.6 Decrypted using normal BASE64 Decoder

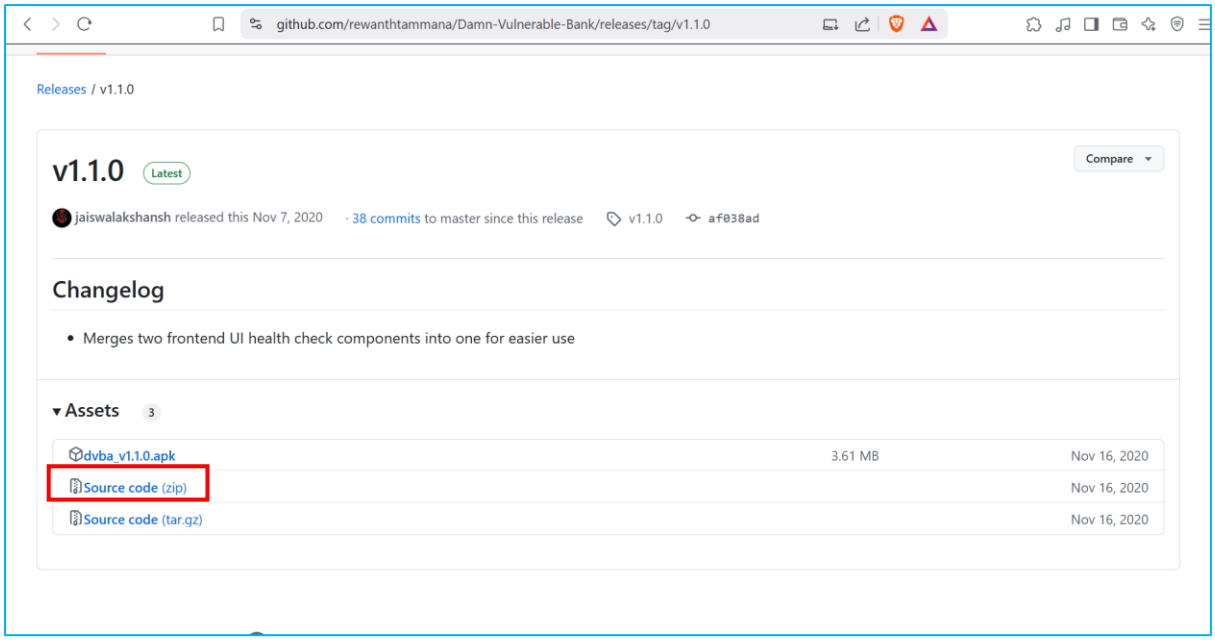

Figure 1.7 APP Source Code

```
PS C:\Users\rengo\OneDrive\Desktop\ASK-Pentest\projek MOBILE\frida scripts> python decryptEncrypt.py
Choose an option:
1. Encrypt text
2. Decrypt text
Enter choice (1/2): 2
Enter Base64-encoded text to decrypt: Gk8AGQoBEg8ZPhQcAwUEH0NAS19VUllDBw==\n

Decrypted text:
 {"account_number":"1234"}
PS C:\Users\rengo\OneDrive\Desktop\ASK-Pentest\projek MOBILE\frida scripts>
```

Figure 1.8 Decrypted Parameter Value

1. To Decrypt this first we must understand how it works. First read the backend Code of the app to understand it . The directory is in here **"\Damn-Vulnerable-Bank-1.1.0\Damn-Vulnerable-Bank-1.1.0\DamnVulnerableBank\app\src\main\java\com\app\damnvulnerablebank/EncryptDecrypt.java"** .
2. Everytime you want to alter the value of the parameter use the python script I have provided.

FINDINGS

Figure 1.9 Error Based SQL Injection