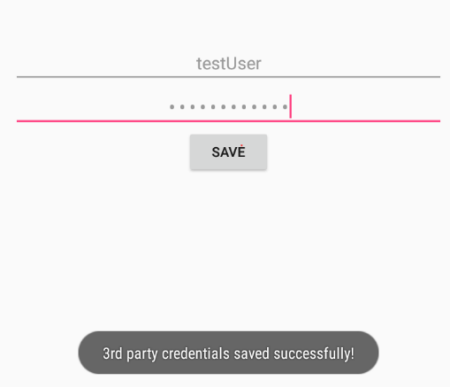
Insecure Data Storage – Part 1

1. Lab objective is to find where/how the credentials are being stored and the vulnerable code.
2. I decompiled the apk file and get start to review the code of the targeted activity. I noticed the credentials stored in shared preferences in plain text without any encryption.

```
public void saveCredentials(View view) {
    SharedPreferences spref = PreferenceManager.getDefaultSharedPreferences(this);
    SharedPreferences.Editor spedit = spref.edit();
    EditText usr = (EditText) findViewById(R.id.ids1Usr);
    EditText pwd = (EditText) findViewById(R.id.ids1Pwd);
    spedit.putString("user", usr.getText().toString());
    spedit.putString("password", pwd.getText().toString());
    spedit.commit();
    Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
}
```

3. I entered dummy credentials and navigated to the files of the application, and I found a new file created named "**shared_prefs**". When I open it, I found file xml file named "**jakhar.aseem.diva_preferences.xml**". I read it and Finally I get the credentials that I entered it before.




```
star2lte:/data/data/jakhar.aseem.diva # ls
cache  code_cache  databases  lib  shared_prefs
star2lte:/data/data/jakhar.aseem.diva # cd shared_prefs/
star2lte:/data/data/jakhar.aseem.diva/shared_prefs # ls
jakhar.aseem.diva_preferences.xml
star2lte:/data/data/jakhar.aseem.diva/shared_prefs # cat jakhar.aseem.diva_preferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="user">testUser</string>
    <string name="password">testPassword</string>
</map>
star2lte:/data/data/jakhar.aseem.diva/shared_prefs #
C:\Users\alita\Desktop>
```