**Activities access**

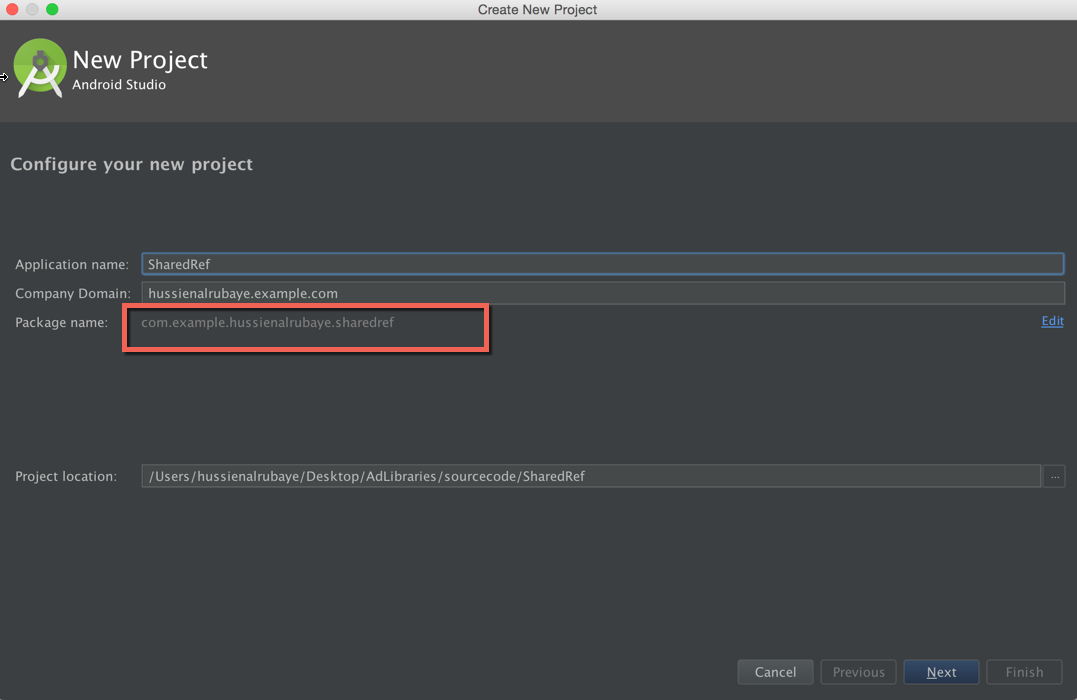
Description:

Android Activities navigation works as same as the website works. In web base applications all pages are public , that is mean if we know name of any page like “home.html” or”contact.html” we could open that page by write it name after the website domain name like <http://host/home.html>. In android we could do same thing, we could navigate to any activity using “am” package commands, this is important point in security. For example; if we develop bank app that has two activities first activity for login and second activity for making transactions the user has to login to do transactions.

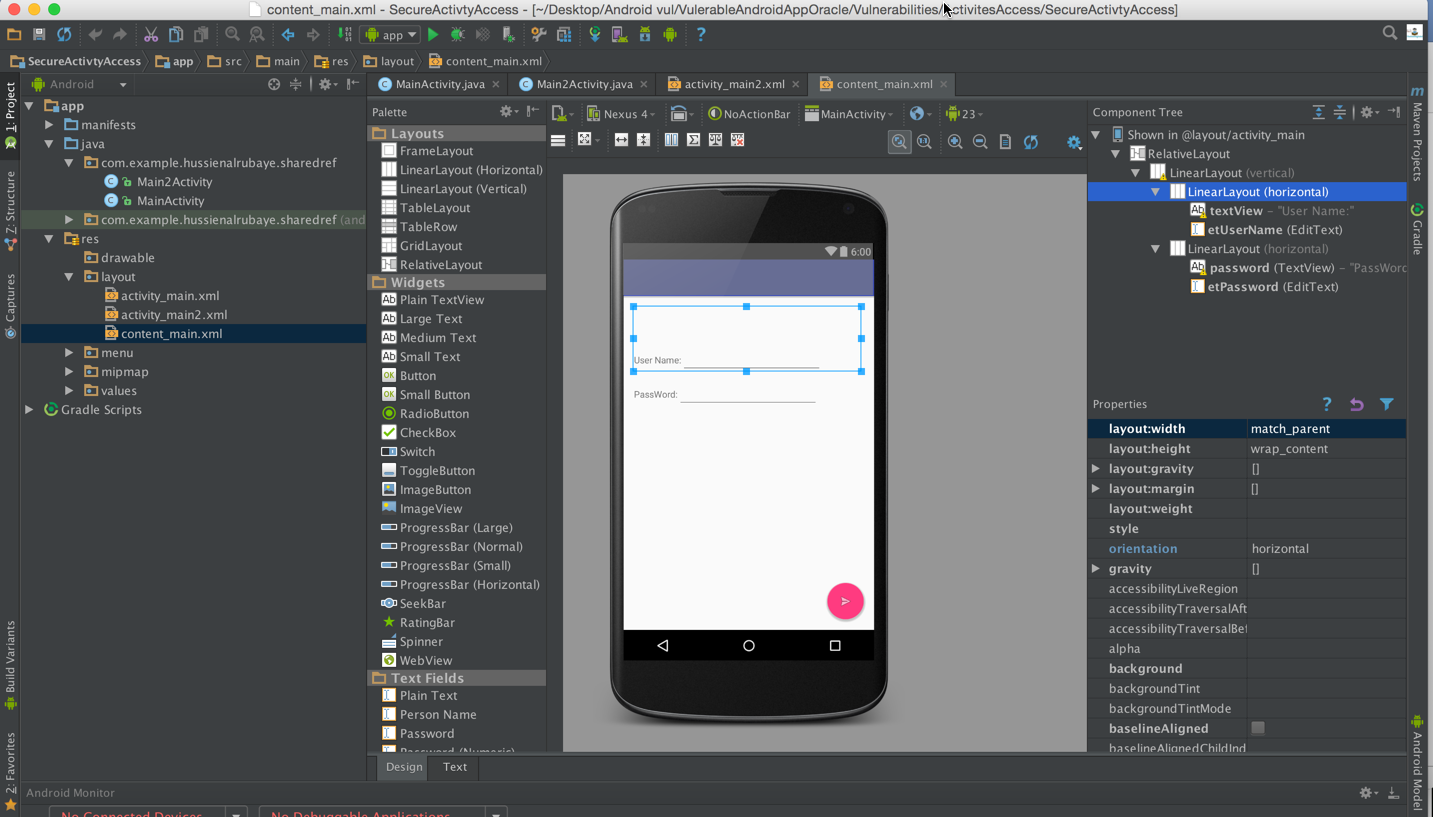
The security weak point here is that by using “am” package commands, hackers could navigate to transactions activity without login, that when we will try to prove in this document. Then we will discus how to protect our self from this Threads.

**Steps to build the secure app (SecureActivtyAccess):** we will create simple app that ask user to enter his user name equal “admin” and password equal “admin”, if the login credentials is correct, he will pass to the second page for change password, then we will show how hacker access to change password without login , then we will secure this point.

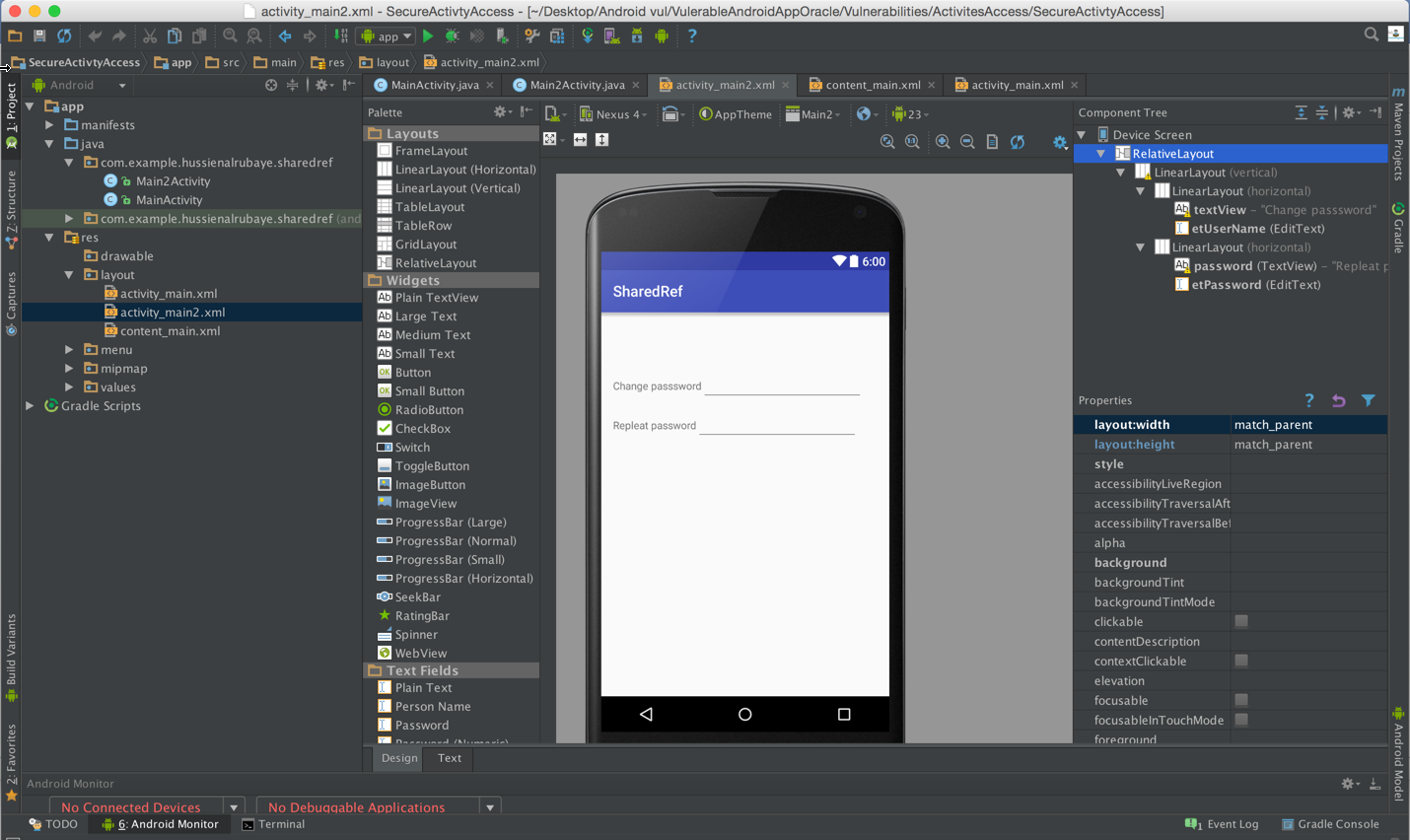
1. Open new project with name “**SecureActivtyAccess**”, save the package name, we will need next



1. add some objects ( TextView, EditText, Button) and make the app like this, see the name of every tool in the right.



1. And add new Activity named **Activity2main.java** for change password. Whiteout write code for change password.



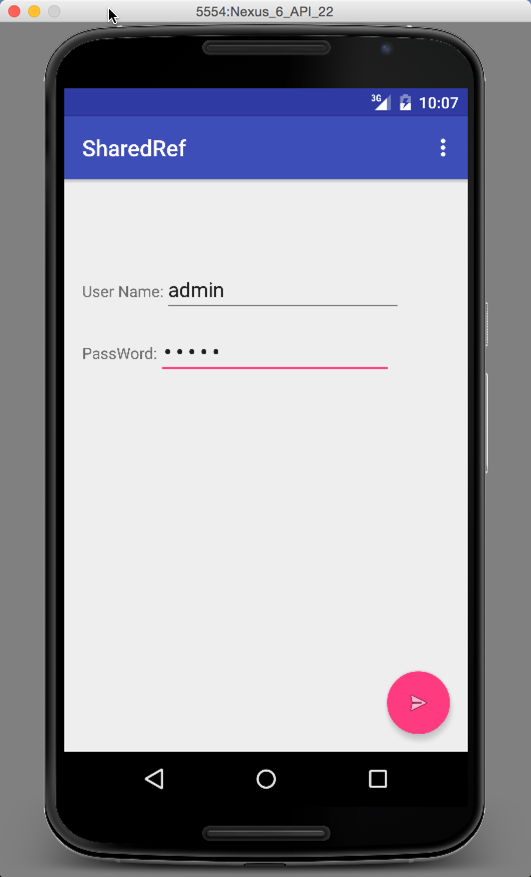
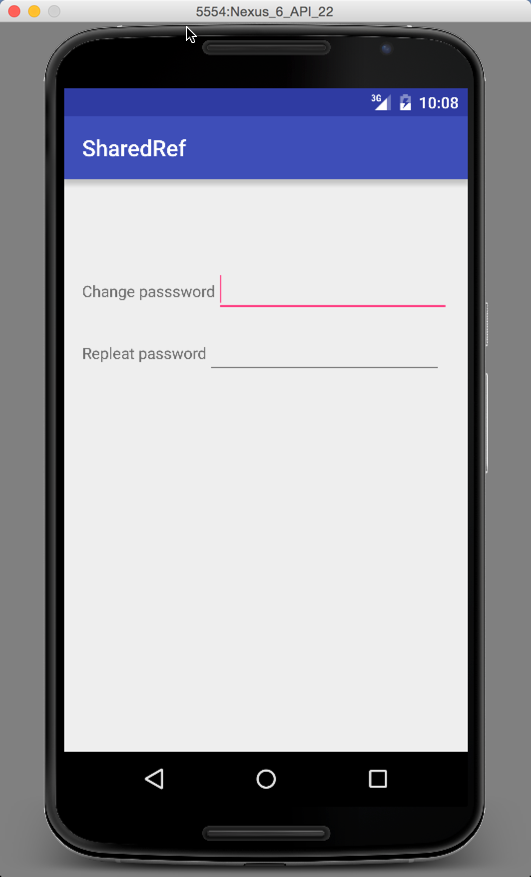
1. Update MainActivty.Java to be like this

|  |
| --- |
| Java |
| public class MainActivity extends AppCompatActivity {  // key for user name  public final String UserName = "admin";  // key for password  public final String Password = "admin";  // shared references instance to access to virtual file  SharedPreferences sharedpreferences;  // input text name  EditText etUserName;  // input text password  EditText etPassword;  @Override  protected void onCreate(Bundle savedInstanceState) {  super.onCreate(savedInstanceState);  setContentView(R.layout.*activity\_main*);  Toolbar toolbar = (Toolbar) findViewById(R.id.*toolbar*);  setSupportActionBar(toolbar);  // initialize user name instance with the real input in xml  etUserName=(EditText)findViewById(R.id.*etUserName*);  // initialize password instance with the real input in xml  etPassword=(EditText)findViewById(R.id.*etPassword*);  // // initialize shared references  FloatingActionButton fab = (FloatingActionButton) findViewById(R.id.*fab*);  // listen to floating button when click  fab.setOnClickListener(new View.OnClickListener() {  @Override  public void onClick(View view) {   if(UserName.equals(etUserName.getText().toString()) && Password.equals(etPassword.getText().toString()))  //display message saved  {  Toast.*makeText*(MainActivity.this, "Data is Saved", Toast.*LENGTH\_LONG*).show();  Intent intent = new Intent(getApplicationContext(), Main2Activity.class);   startActivity(intent);  }  }  });}  } |

1. Update Main2Activty.java to be like this

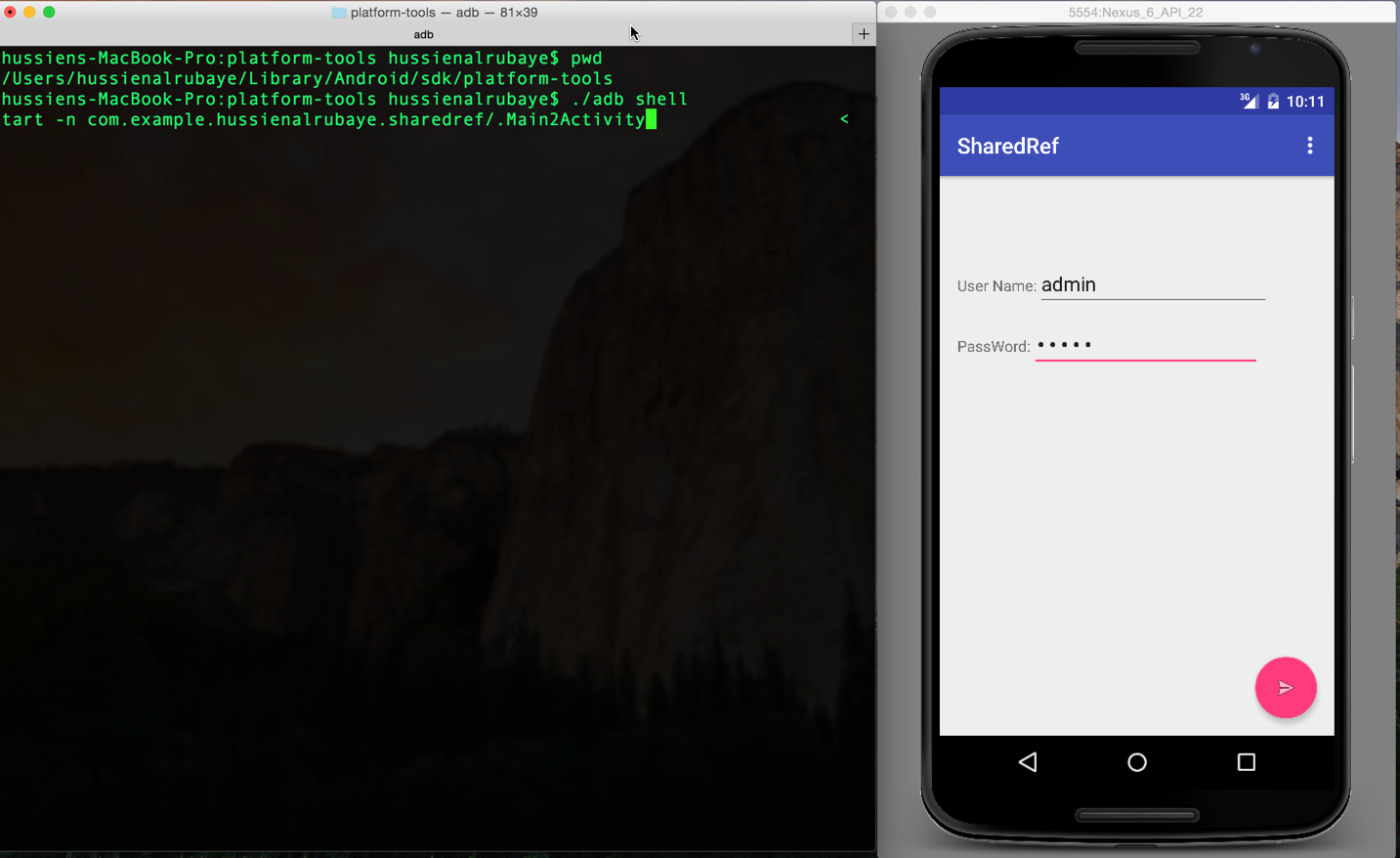
|  |
| --- |
| Java |
| public class Main2Activity extends AppCompatActivity {   @Override  protected void onCreate(Bundle savedInstanceState) {  super.onCreate(savedInstanceState);  setContentView(R.layout.*activity\_main2*);  Bundle b=getIntent().getExtras();   } } |

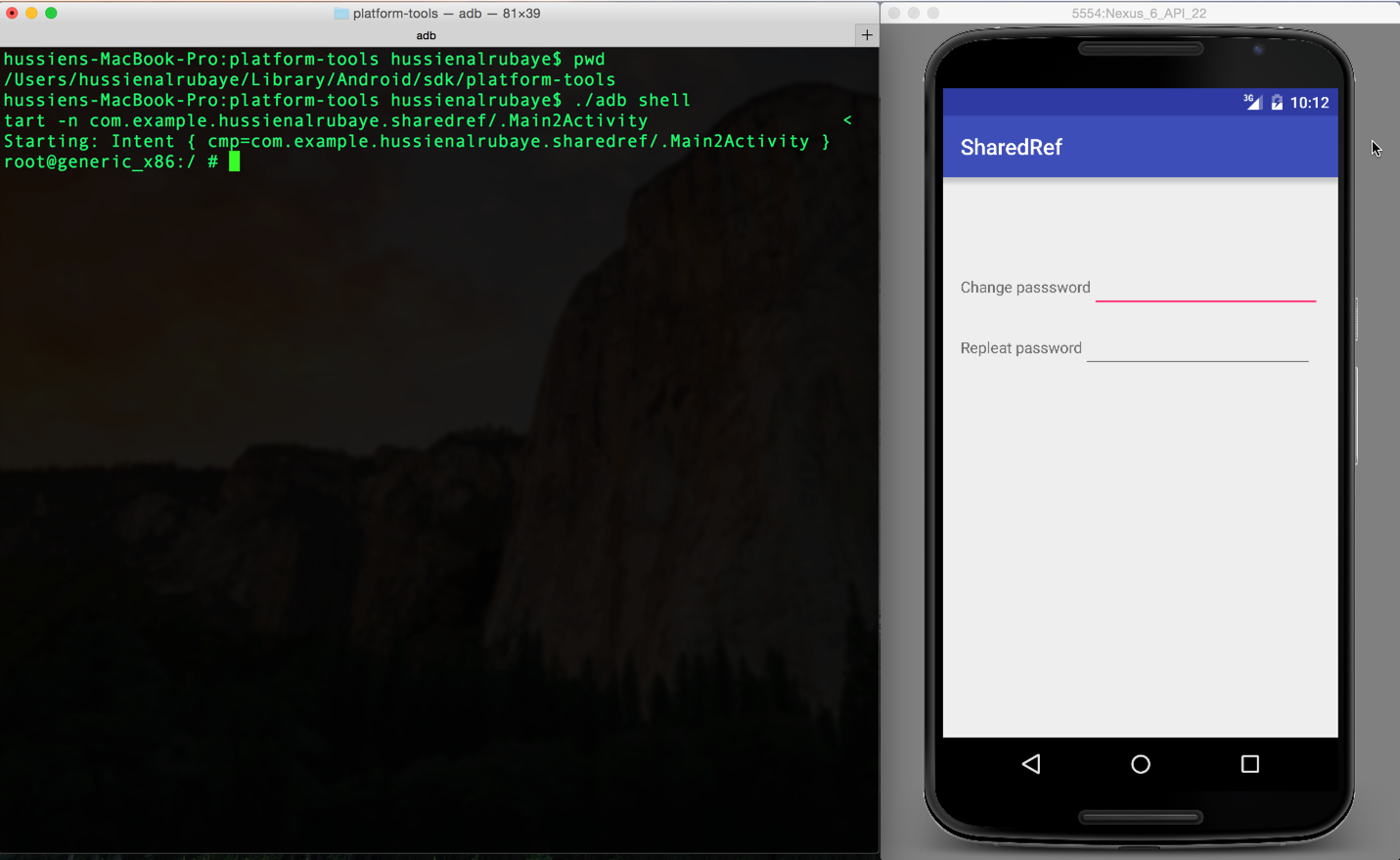
**Example of Run the app and register with admin user name and password**

**Steps to hacker app:** To hacker this app and access to change password activity without login**,** Just Run terminal from Android Platform-tools folder to run **adb commands** and execute this commands

* **./adb shell**
* **am start –n PackageName/.ActivityName**





As you see we access to change password without login

**Fix This Problem**

To fix this problem we will send key associate with value over the intent to change password activity. Then in the second activity, we will read the key and make sure from the value if correct we open the activity otherwise we will dismiss the activity. So when we run “am” command without key to open Main2Activity it will not open.

We will start update the classes

1. Update MainActivty.Java to be like this

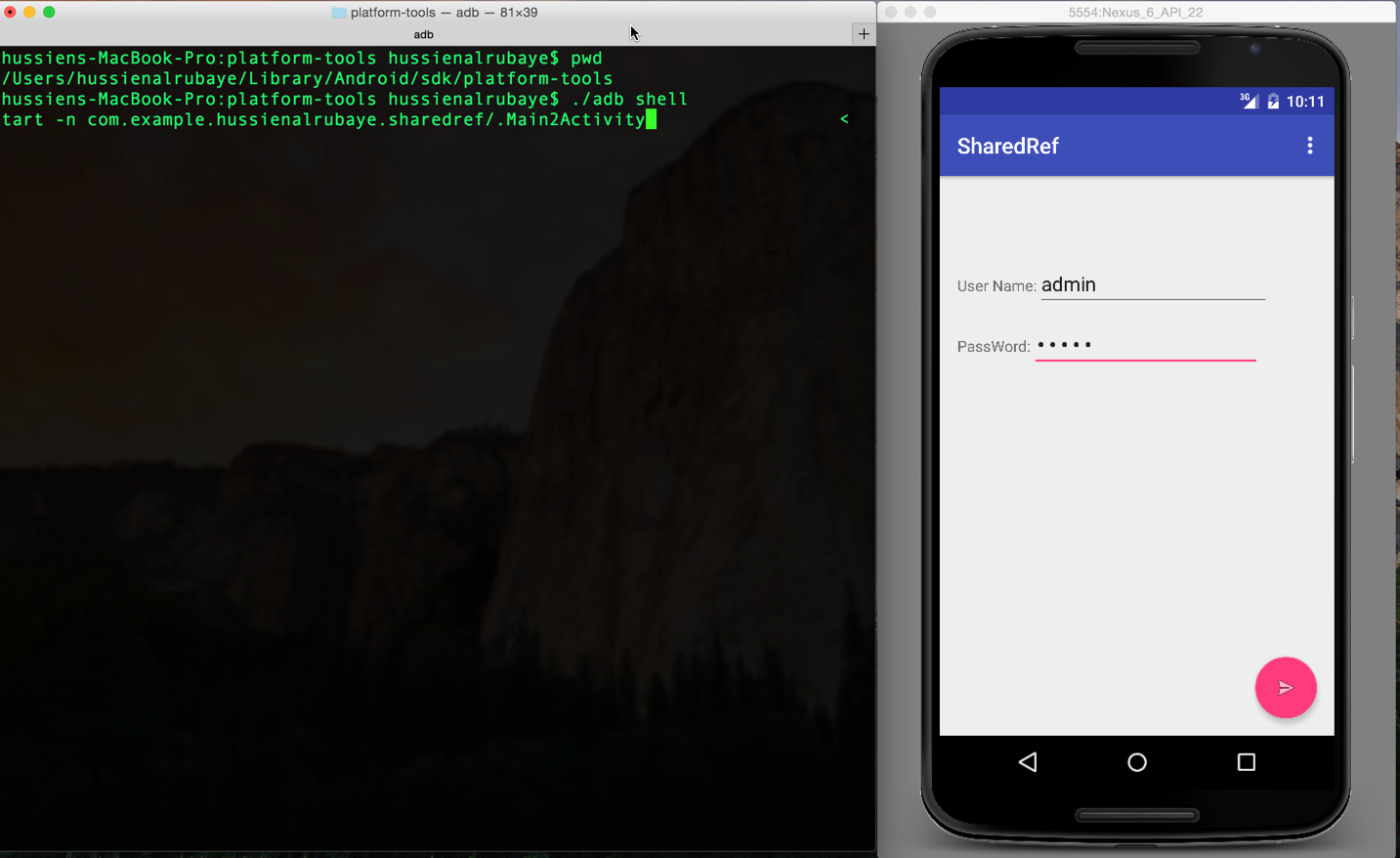
|  |
| --- |
| Java |
| public class MainActivity extends AppCompatActivity {  // key for user name  public final String UserName = "admin";  // key for password  public final String Password = "admin";  // shared references instance to access to virtual file  SharedPreferences sharedpreferences;  // input text name  EditText etUserName;  // input text password  EditText etPassword;  @Override  protected void onCreate(Bundle savedInstanceState) {  super.onCreate(savedInstanceState);  setContentView(R.layout.*activity\_main*);  Toolbar toolbar = (Toolbar) findViewById(R.id.*toolbar*);  setSupportActionBar(toolbar);  // initialize user name instance with the real input in xml  etUserName=(EditText)findViewById(R.id.*etUserName*);  // initialize password instance with the real input in xml  etPassword=(EditText)findViewById(R.id.*etPassword*);  // // initialize shared references  FloatingActionButton fab = (FloatingActionButton) findViewById(R.id.*fab*);  // listen to floating button when click  fab.setOnClickListener(new View.OnClickListener() {  @Override  public void onClick(View view) {   if(UserName.equals(etUserName.getText().toString()) && Password.equals(etPassword.getText().toString()))  //display message saved  {  Toast.*makeText*(MainActivity.this, "Data is Saved", Toast.*LENGTH\_LONG*).show();  Intent intent = new Intent(getApplicationContext(), Main2Activity.class);  intent.putExtra("key", 3433);  startActivity(intent);  }   }  });  }  } |

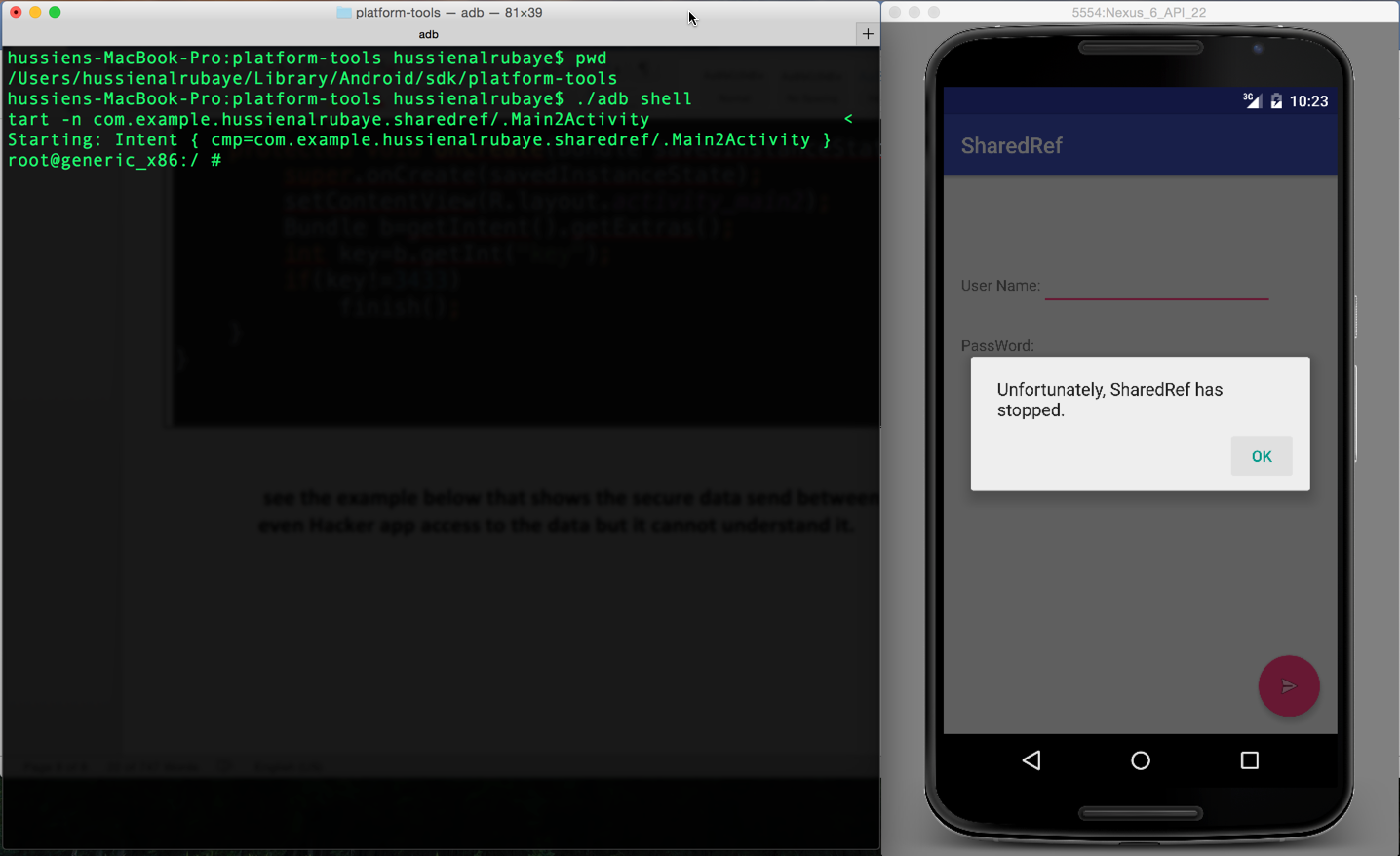
1. Update Main2Activty.java to be like this

|  |
| --- |
| Java |
| public class Main2Activity extends AppCompatActivity {   @Override  protected void onCreate(Bundle savedInstanceState) {  super.onCreate(savedInstanceState);  setContentView(R.layout.*activity\_main2*);  Bundle b=getIntent().getExtras();  int key=b.getInt("key");  if(key!=3433)  finish();  } } |

**When we the hacker run the command again, he we could not access to change password page**

* **./adb shell**
* **am start –n Packaname/.ActivityName**



****