

---

## Insecure Logging

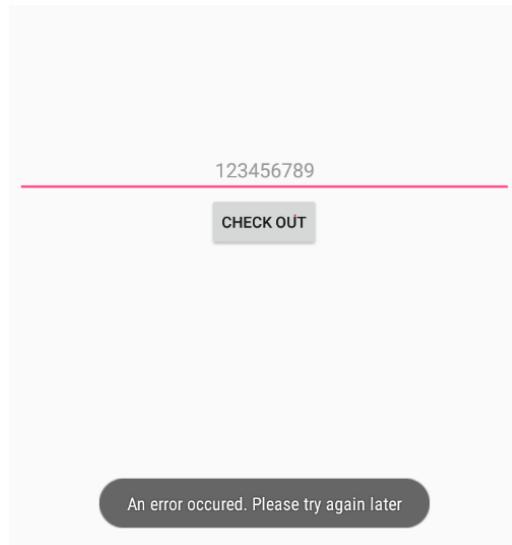
---

1. The objective of this lab is to find out what is being logged where/how and the vulnerable code.
2. After decompilation of the apk file, I get the code of this lab.

```
public void checkout(View view) {
    EditText cctxt = (EditText) findViewById(R.id.ccText);
    try {
        processCC(cctxt.getText().toString());
    } catch (RuntimeException e) {
        Log.e("diva-log", "Error while processing transaction with credit card: " + cctxt.getText().toString());
        Toast.makeText(this, "An error occurred. Please try again later", 0).show();
    }
}

private void processCC(String ccstr) {
    RuntimeException e = new RuntimeException();
    throw e;
}
```

3. The main issue is that the credit card number logged in plain text. So, if anyone can read the logs, he will be able to read the credit card number easily. Let's try to read it from logs.
4. I entered the credit card number in the application.



5. Let's observe the logs.

```
star2lte:/ # logcat | grep 'diva'
11-14 17:14:41.509 2175 W PackageManager: Not granting permission android.permission.WRITE_EXTERNAL_STORAGE to package jakhar.aseem.diva because it was previously installed without
11-14 17:14:41.509 2175 W PackageManager: Not granting permission android.permission.READ_EXTERNAL_STORAGE to package jakhar.aseem.diva because it was previously installed without
11-14 17:14:41.663 2175 2215 W PackageManager: Not granting permission android.permission.WRITE_EXTERNAL_STORAGE to package jakhar.aseem.diva because it was previously installed without
11-14 17:14:41.663 2175 2215 W PackageManager: Not granting permission android.permission.READ_EXTERNAL_STORAGE to package jakhar.aseem.diva because it was previously installed without
11-14 17:14:48.760 2175 2683 I ActivityManager: START u0 {act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] flg=0x10200000 cmp=jakhar.aseem.diva/.MainActivity bnds=[244,529][360,724] (has extras)} from uid 1000 on display 0
11-14 17:14:48.787 2175 2674 I ActivityManager: Start proc 3173:jakhar.aseem.diva/u0a47 for activity jakhar.aseem.diva/.MainActivity
11-14 17:54:05.681 2175 2185 I ActivityManager: START u0 {cmp=jakhar.aseem.diva/.LogActivity} from uid 10047 on display 0
11-14 17:54:10.710 3173 3173 E diva-log: Error while processing transaction with credit card: 123
11-14 17:54:59.618 3173 3173 E diva-log: Error while processing transaction with credit card: 123456
11-14 18:53:54.264 2175 2364 I ActivityManager: START u0 {cmp=jakhar.aseem.diva/.InsecureDataStorage1Activity} from uid 10047 on display 0
11-14 19:42:45.039 2175 2683 I ActivityManager: START u0 {act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] flg=0x10200000 cmp=jakhar.aseem.diva/.MainActivity bnds=[244,529][360,724] (has extras)} from uid 1000 on display 0
11-14 19:45:05.498 2175 2323 I ActivityManager: START u0 {cmp=jakhar.aseem.diva/.InsecureDataStorage1Activity} from uid 10047 on display 0
11-14 19:45:05.582 2175 2196 I ActivityManager: Displayed jakhar.aseem.diva/.InsecureDataStorage1Activity: +81ms (total +2m21s516ms)
11-14 19:51:31.847 2175 3034 I ActivityManager: START u0 {cmp=jakhar.aseem.diva/.LogActivity} from uid 10047 on display 0
11-14 19:51:31.907 2175 2196 I ActivityManager: Displayed jakhar.aseem.diva/.LogActivity: +57ms
11-14 19:55:51.624 3173 3173 E diva-log: Error while processing transaction with credit card: 123456789
```

## 6. I already get the credit card number from logs.