

National Forensic Sciences University

School of Cyber security and Digital Forensics



Subject: CTMSCS S2 P3 Android Security

(TA-II Assignment)

Submitted to: Mr. Digvijay Singh Rathod and Mr. Jay Teraiya

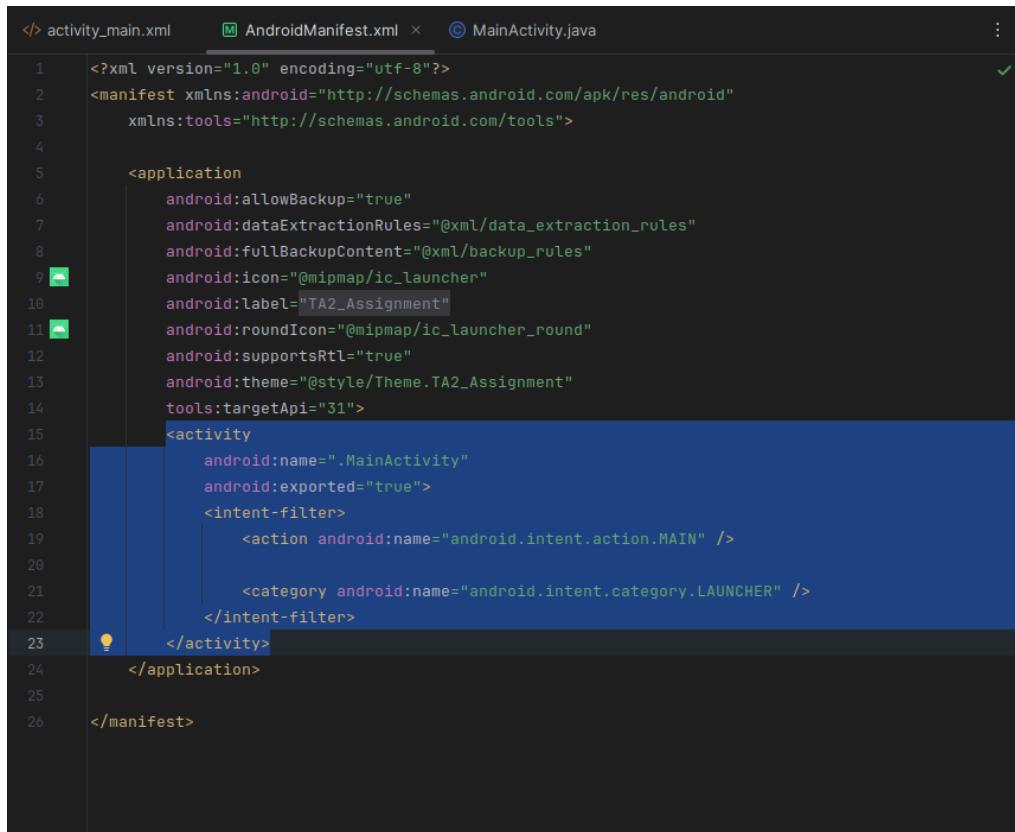
Submitted by: Disha Sharma (240103002014)

Submission Date: 06/04/2025

INDEX

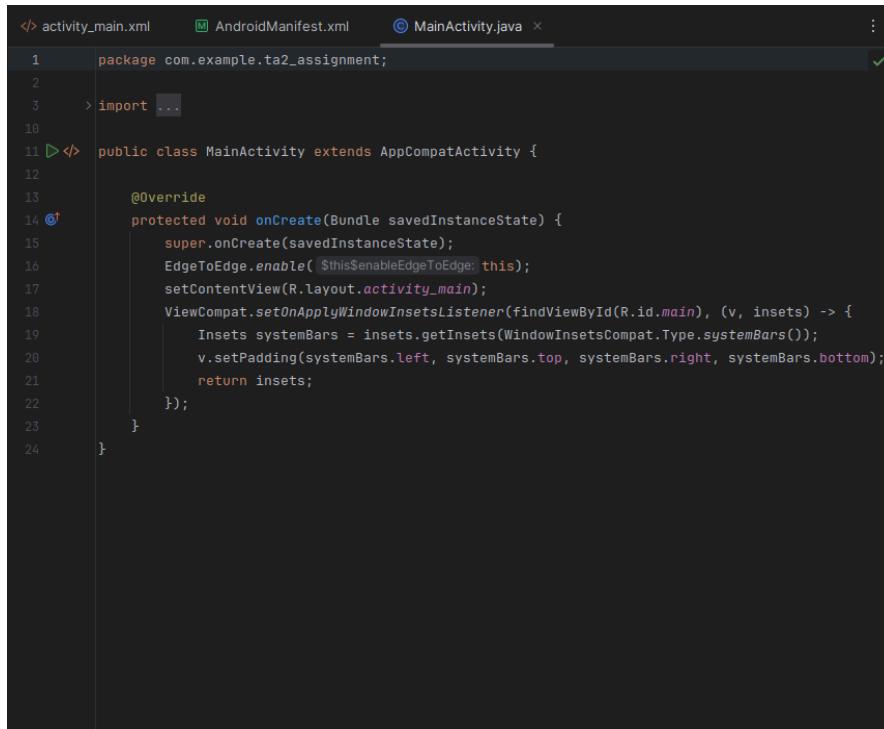
1. Android Studio and AVD
2. Android Debug Bridge Commands
3. DIVA Vulnerable Application
4. Reverse Engineering
5. Request Interception
6. Insecure Bank2 Application
7. GoatDroid Practical
8. Open GApps
9. Security Auditing using Drozer
10. Analysis using MobSF and FRIDA
11. OWASP Security Shepherd

Demonstration of Android Application Framework component such as Activity and android manifest file etc. using Android Studio.



```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools">

    <application
        android:allowBackup="true"
        android:dataExtractionRules="@xml/data_extraction_rules"
        android:fullBackupContent="@xml/backup_rules"
        android:icon="@mipmap/ic_launcher"
        android:label="@string/app_name"
        android:roundIcon="@mipmap/ic_launcher_round"
        android:supportsRtl="true"
        android:theme="@style/Theme.TA2_Assignment"
        tools:targetApi="31">
        <activity
            android:name=".MainActivity"
            android:exported="true">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```



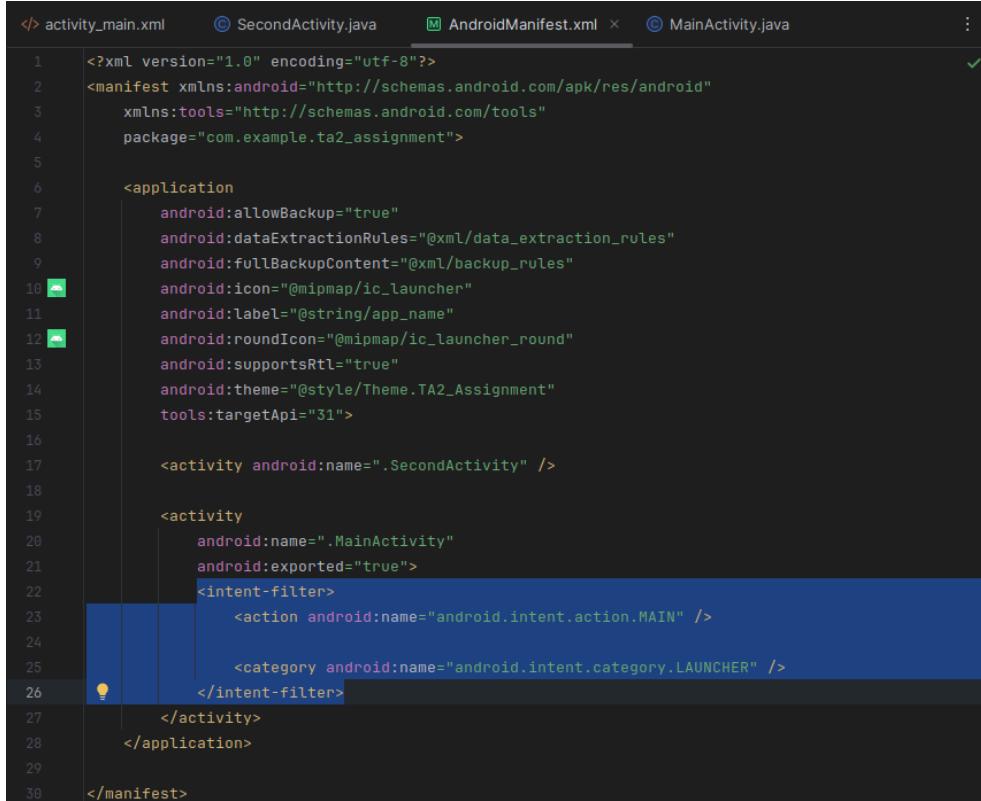
```
package com.example.ta2_assignment;

import ...

public class MainActivity extends AppCompatActivity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        EdgeToEdge.enable($this$enableEdgeToEdge: this);
        setContentView(R.layout.activity_main);
        ViewCompat.setOnApplyWindowInsetsListener(findViewById(R.id.main), (v, insets) -> {
            Insets systemBars = insets.getInsets(WindowInsetsCompat.Type.systemBars());
            v.setPadding(systemBars.left, systemBars.top, systemBars.right, systemBars.bottom);
            return insets;
        });
    }
}
```

Demonstration of Android Intent and Intent Filter

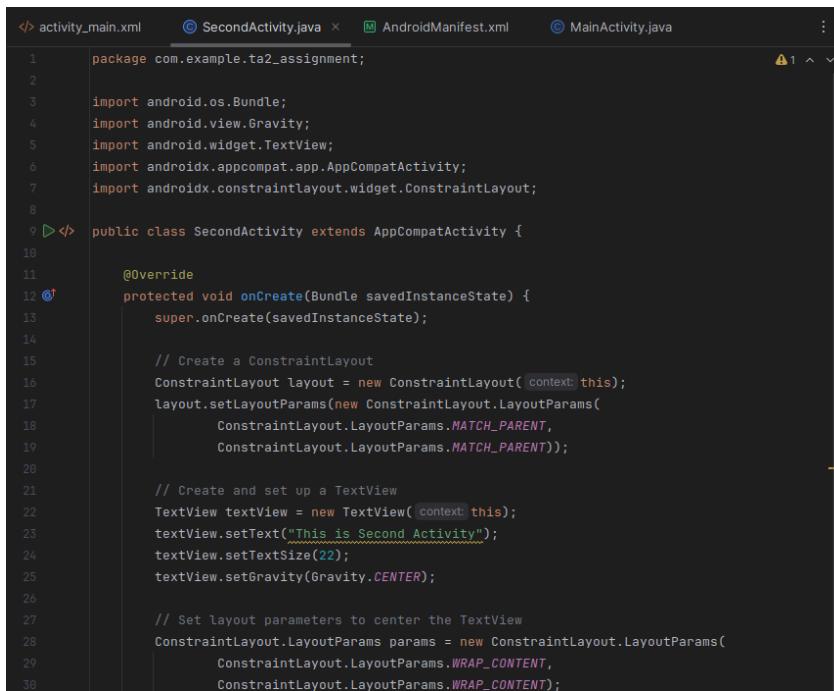


```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools"
    package="com.example.ta2_assignment">

    <application
        android:allowBackup="true"
        android:dataExtractionRules="@xml/data_extraction_rules"
        android:fullBackupContent="@xml/backup_rules"
        android:icon="@mipmap/ic_launcher"
        android:label="@string/app_name"
        android:roundIcon="@mipmap/ic_launcher_round"
        android:supportsRtl="true"
        android:theme="@style/Theme.TA2_Assignment"
        tools:targetApi="31">

        <activity android:name=".SecondActivity" />

        <activity
            android:name=".MainActivity"
            android:exported="true">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```



```
package com.example.ta2_assignment;

import android.os.Bundle;
import android.view.Gravity;
import android.widget.TextView;
import androidx.appcompat.app.AppCompatActivity;
import androidx.constraintlayout.widget.ConstraintLayout;

public class SecondActivity extends AppCompatActivity {

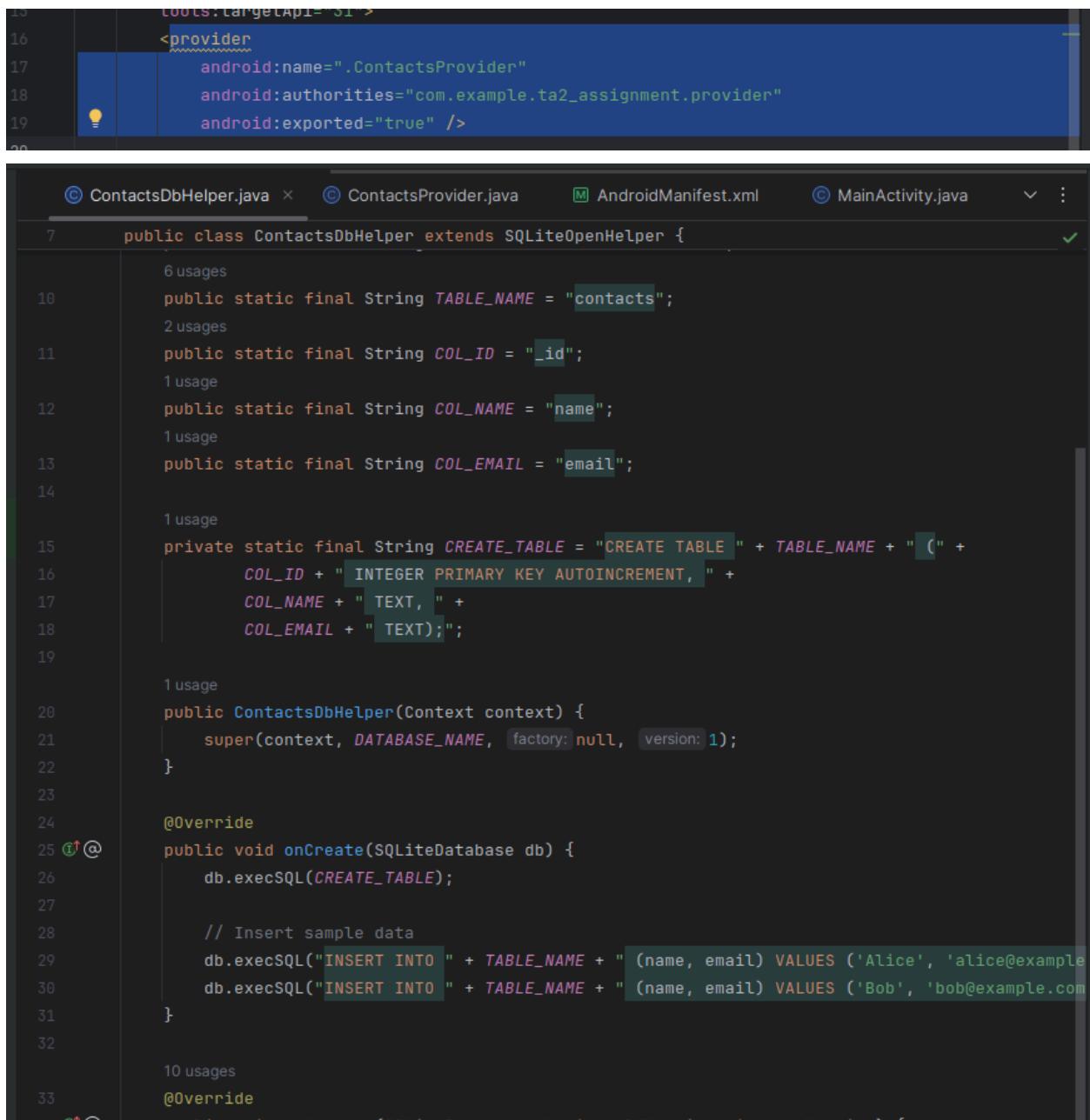
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);

        // Create a ConstraintLayout
        ConstraintLayout layout = new ConstraintLayout(context);
        layout.setLayoutParams(new ConstraintLayout.LayoutParams(
            ConstraintLayout.LayoutParams.MATCH_PARENT,
            ConstraintLayout.LayoutParams.MATCH_PARENT));

        // Create and set up a TextView
        TextView textView = new TextView(context);
        textView.setText("This is Second Activity");
        textView.setTextSize(22);
        textView.setGravity(Gravity.CENTER);

        // Set layout parameters to center the TextView
        ConstraintLayout.LayoutParams params = new ConstraintLayout.LayoutParams(
            ConstraintLayout.LayoutParams.WRAP_CONTENT,
            ConstraintLayout.LayoutParams.WRAP_CONTENT);
```

Demonstration of Android Content Provider



The screenshot shows the Android Studio interface with several tabs at the top: ContactsDbHelper.java, ContactsProvider.java, AndroidManifest.xml, MainActivity.java, and others. The ContactsDbHelper.java tab is active, displaying Java code for a SQLiteOpenHelper subclass. The code defines constants for table names and column IDs, and implements the onCreate() method to create the table and insert sample data. The AndroidManifest.xml tab shows a provider element with the name ".ContactsProvider", authorities "com.example.ta2_assignment.provider", and exported set to true.

```
15     tools:targetApi="31" >
16     <provider
17         android:name=".ContactsProvider"
18         android:authorities="com.example.ta2_assignment.provider"
19         android:exported="true" />
20
21
22
23
24
25  @Override
26  public void onCreate(SQLiteDatabase db) {
27      db.execSQL(CREATE_TABLE);
28
29      // Insert sample data
30      db.execSQL("INSERT INTO " + TABLE_NAME + " (name, email) VALUES ('Alice', 'alice@example.com')");
31      db.execSQL("INSERT INTO " + TABLE_NAME + " (name, email) VALUES ('Bob', 'bob@example.com')");
32  }
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
687
688
689
689
690
691
692
693
694
695
696
697
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
717
718
719
719
720
721
722
723
724
725
726
727
727
728
729
729
730
731
732
733
734
735
736
737
737
738
739
739
740
741
742
743
744
745
746
747
747
748
749
749
750
751
752
753
754
755
756
757
757
758
759
759
760
761
762
763
764
765
766
767
767
768
769
769
770
771
772
773
774
775
776
777
777
778
779
779
780
781
782
783
784
785
786
787
787
788
789
789
790
791
792
793
794
795
796
797
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
817
818
819
819
820
821
822
823
824
825
826
827
827
828
829
829
830
831
832
833
834
835
836
837
837
838
839
839
840
841
842
843
844
845
846
847
847
848
849
849
850
851
852
853
854
855
856
857
857
858
859
859
860
861
862
863
864
865
866
867
867
868
869
869
870
871
872
873
874
875
876
877
877
878
879
879
880
881
882
883
884
885
886
887
887
888
889
889
890
891
892
893
894
895
896
897
897
898
899
899
900
901
902
903
904
905
906
907
907
908
909
909
910
911
912
913
914
915
916
916
917
918
918
919
920
921
922
923
924
925
926
926
927
928
928
929
930
931
932
933
934
935
936
937
937
938
939
939
940
941
942
943
944
945
946
946
947
948
948
949
950
951
952
953
954
955
956
956
957
958
958
959
960
961
962
963
964
965
965
966
967
967
968
969
969
970
971
972
973
974
975
976
976
977
978
978
979
980
981
982
983
984
985
985
986
987
987
988
989
989
990
991
992
993
994
995
995
996
997
997
998
999
999
1000
1000
1001
1001
1002
1002
1003
1003
1004
1004
1005
1005
1006
1006
1007
1007
1008
1008
1009
1009
1010
1010
1011
1011
1012
1012
1013
1013
1014
1014
1015
1015
1016
1016
1017
1017
1018
1018
1019
1019
1020
1020
1021
1021
1022
1022
1023
1023
1024
1024
1025
1025
1026
1026
1027
1027
1028
1028
1029
1029
1030
1030
1031
1031
1032
1032
1033
1033
1034
1034
1035
1035
1036
1036
1037
1037
1038
1038
1039
1039
1040
1040
1041
1041
1042
1042
1043
1043
1044
1044
1045
1045
1046
1046
1047
1047
1048
1048
1049
1049
1050
1050
1051
1051
1052
1052
1053
1053
1054
1054
1055
1055
1056
1056
1057
1057
1058
1058
1059
1059
1060
1060
1061
1061
1062
1062
1063
1063
1064
1064
1065
1065
1066
1066
1067
1067
1068
1068
1069
1069
1070
1070
1071
1071
1072
1072
1073
1073
1074
1074
1075
1075
1076
1076
1077
1077
1078
1078
1079
1079
1080
1080
1081
1081
1082
1082
1083
1083
1084
1084
1085
1085
1086
1086
1087
1087
1088
1088
1089
1089
1090
1090
1091
1091
1092
1092
1093
1093
1094
1094
1095
1095
1096
1096
1097
1097
1098
1098
1099
1099
1100
1100
1101
1101
1102
1102
1103
1103
1104
1104
1105
1105
1106
1106
1107
1107
1108
1108
1109
1109
1110
1110
1111
1111
1112
1112
1113
1113
1114
1114
1115
1115
1116
1116
1117
1117
1118
1118
1119
1119
1120
1120
1121
1121
1122
1122
1123
1123
1124
1124
1125
1125
1126
1126
1127
1127
1128
1128
1129
1129
1130
1130
1131
1131
1132
1132
1133
1133
1134
1134
1135
1135
1136
1136
1137
1137
1138
1138
1139
1139
1140
1140
1141
1141
1142
1142
1143
1143
1144
1144
1145
1145
1146
1146
1147
1147
1148
1148
1149
1149
1150
1150
1151
1151
1152
1152
1153
1153
1154
1154
1155
1155
1156
1156
1157
1157
1158
1158
1159
1159
1160
1160
1161
1161
1162
1162
1163
1163
1164
1164
1165
1165
1166
1166
1167
1167
1168
1168
1169
1169
1170
1170
1171
1171
1172
1172
1173
1173
1174
1174
1175
1175
1176
1176
1177
1177
1178
1178
1179
1179
1180
1180
1181
1181
1182
1182
1183
1183
1184
1184
1185
1185
1186
1186
1187
1187
1188
1188
1189
1189
1190
1190
1191
1191
1192
1192
1193
1193
1194
1194
1195
1195
1196
1196
1197
1197
1198
1198
1199
1199
1200
1200
1201
1201
1202
1202
1203
1203
1204
1204
1205
1205
1206
1206
1207
1207
1208
1208
1209
1209
1210
1210
1211
1211
1212
1212
1213
1213
1214
1214
1215
1215
1216
1216
1217
1217
1218
1218
1219
1219
1220
1220
1221
1221
1222
1222
1223
1223
1224
1224
1225
1225
1226
1226
1227
1227
1228
1228
1229
1229
1230
1230
1231
1231
1232
1232
1233
1233
1234
1234
1235
1235
1236
1236
1237
1237
1238
1238
1239
1239
1240
1240
1241
1241
1242
1242
1243
1243
1244
1244
1245
1245
1246
1246
1247
1247
1248
1248
1249
1249
1250
1250
1251
1251
1252
1252
1253
1253
1254
1254
1255
1255
1256
1256
1257
1257
1258
1258
1259
1259
1260
1260
1261
1261
1262
1262
1263
1263
1264
1264
1265
1265
1266
1266
1267
1267
1268
1268
1269
1269
1270
1270
1271
1271
1272
1272
1273
1273
1274
1274
1275
1275
1276
1276
1277
1277
1278
1278
1279
1279
1280
1280
1281
1281
1282
1282
1283
1283
1284
1284
1285
1285
1286
1286
1287
1287
1288
1288
1289
1289
1290
1290
1291
1291
1292
1292
1293
1293
1294
1294
1295
1295
1296
1296
1297
1297
1298
1298
1299
1299
1300
1300
1301
1301
1302
1302
1303
1303
1304
1304
1305
1305
1306
1306
1307
1307
1308
1308
1309
1309
1310
1310
1311
1311
1312
1312
1313
1313
1314
1314
1315
1315
1316
1316
1317
1317
1318
1318
1319
1319
1320
1320
1321
1321
1322
1322
1323
1323
1324
1324
1325
1325
1326
1326
1327
1327
1328
1328
1329
1329
1330
1330
1331
1331
1332
1332
1333
1333
1334
1334
1335
1335
1336
1336
1337
1337
1338
1338
1339
1339
1340
1340
1341
1341
1342
1342
1343
1343
1344
1344
1345
1345
1346
1346
1347
1347
1348
1348
1349
1349
1350
1350
1351
1351
1352
1352
1353
1353
1354
1354
1355
1355
1356
1356
1357
1357
1358
1358
1359
1359
1360
1360
1361
1361
1362
1362
1363
1363
1364
1364
1365
1365
1366
1366
1367
1367
1368
1368
1369
1369
1370
1370
1371
1371
1372
1372
1373
1373
1374
1374
1375
1375
1376
1376
1377
1377
1378
1378
1379
1379
1380
1380
1381
1381
1382
1382
1383
1383
1384
1384
1385
1385
1386
1386
1387
1387
1388
1388
1389
1389
1390
1390
1391
1391
1392
1392
1393
1393
1394
1394
1395
1395
1396
1396
1397
1397
1398
1398
1399
1399
1400
1400
1401
1401
1402
1402
1403
1403
1404
1404
1405
1405
1406
1406
1407
1407
1408
1408
1409
1409
1410
1410
1411
1411
1412
1412
1413
1413
1414
1414
1415
1415
1416
1416
1417
1417
1418
1418
1419
1419
1420
1420
1421
1421
1422
1422
1423
1423
1424
1424
1425
1425
1426
1426
1427
1427
1428
1428
1429
1429
1430
1430
1431
1431
1432
1432
1433
1433
1434
1434
1435
1435
1436
1436
1437
1437
1438
1438
1439
1439
1440
1440
1441
1441
1442
1442
1443
1443
1444
1444
1445
1445
1446
1446
1447
1447
1448
1448
1449
1449
1450
1450
1451
1451
1452
1452
1453
1453
1454
1454
1455
1455
1456
1456
1457
1457
1458
1458
1459
1459
1460
1460
1461
1461
1462
1462
1463
1463
1464
1464
1465
1465
1466
1466
1467
1467
1468
1468
1469
1469
1470
1470
1471
1471
1472
1472
1473
1473
1474
1474
1475
1475
1476
1476
1477
1477
1478
1478
1479
1479
1480
1480
1481
1481
1482
1482
1483
1483
1484
1484
1485
1485
1486
1486
1487
1487
1488
1488
1489
1489
1490
1490
1491
1491
1492
1492
1493
1493
1494
1494
1495
1495
1496
1496
1497
1497
1498
1498
1499
1499
1500
1500
1501
1501
1502
1502
1503
1503
1504
1504
1505
1505
1506
1506
1507
1507
1508
1508
1509
1509
1510
1510
1511
1511
1512
1512
1513
1513
1514
1514
1515
1515
1516
1516
1517
1517
1518
1518
1519
1519
1520
1520
1521
1521
1522
1522
1523
1523
1524
1524
1525
1525
1526
1526
1527
1527
1528
1528
1529
1529
1530
1530
1531
1531
1532
1532
1533
1533
1534
1534
1535
1535
1536
1536
1537
1537
1538
1538
1539
1539
1540
1540
1541
1541
1542
1542
1543
1543
1544
1544
1545
1545
1546
1546
1547
1547
1548
1548
1549
1549
1550
1550
1551
1551
1552
1552
1553
1553
1554
1554
1555
1555
1556
1556
1557
1557
1558
1558
1559
1559
1560
1560
1561
1561
1562
1562
1563
1563
1564
1564
1565
1565
1566
1566
1567
1567
1568
1568
1569
1569
1570
1570
1571
1571
1572
1572
1573
1573
1574
1574
1575
1575
1576
1576
1577
1577
1578
1578
1579
1579
1580
1580
1581
1581
1582
1582
1583
1583
1584
1584
1585
1585
1586
1586
1587
1587
1588
1588
1589
1589
1590
1590
1591
1591
1592
1592
1593
1593
1594
1594
1595
1595
1596
1596
1597
1597
1598
1598
1599
1599
1600
1600
1601
1601
1602
1602
1603
1603
1604
1604
1605
1605
1606
1606
1607
1607
1608
1608
1609
1609
1610
1610
1611
1611
1612
1612
1613
1613
1614
1614
1615
1615
1616
1616
1617
1617
1618
1618
1619
1619
1620
1620
1621
1621
1622
1622
1623
1623
1624
1624
1625
1625
1626
1626
1627
1627
1628
1628
1629
1629
1630
1630
1631
1631
1632
1632
1633
1633
1634
1634
1635
1635
1636
1636
1637
1637
1638
1638
1639
1639
1640
1640
1641
1641
1642
1642
1643
1643
1644
1644
1645
1645
1646
1646
1647
1647
1648
1648
1649
1649
1650
1650
1651
1651
1652
1652
1653
1653
1654
1654
1655
1655
1656
1656
1657
1657
1658
1658
1659
1659
1660
1660
1661
1661
1662
1662
1663
1663
1664
1664
1665
1665
1666
1666
1667
1667
1668
1668
1669
1669
1670
1670
1671
1671
1672
1672
1673
1673
1674
1674
1675
1675
1676
1676
1677
1677
1678
1678
1679
1679
1680
1680
1681
1681
1682
1682
1683
1683
1684
1684
1685
1685
1686
1686
1687
1687
1688
1688
1689
1689
1690
169
```

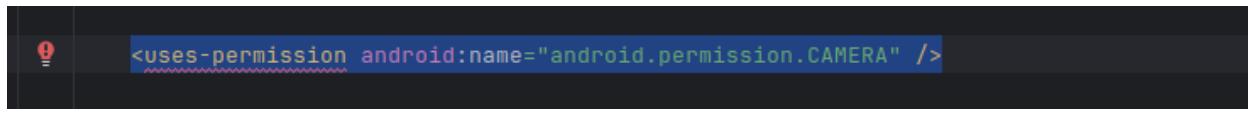
Demonstration of Android Broadcast Receiver

```
<receiver android:name=".MyBroadcastReceiver">
    <intent-filter>
        <action android:name="com.example.ta2_assignment.ACTION_CUSTOM_BROADCAST" />
    </intent-filter>
</receiver>
```

The screenshot shows a code editor interface with several tabs at the top: MyBroadcastReceiver.java (selected), ContactsProvider.java, AndroidManifest.xml, and MainActivity.java. The main pane displays the Java code for MyBroadcastReceiver:

```
1 package com.example.ta2_assignment;
2
3 import android.content.BroadcastReceiver;
4 import android.content.Context;
5 import android.content.Intent;
6 import android.widget.Toast;
7
8 public class MyBroadcastReceiver extends BroadcastReceiver {
9
10     @Override
11     public void onReceive(Context context, Intent intent) {
12         // Action matched, show a Toast
13         Toast.makeText(context, "Broadcast Received!", Toast.LENGTH_SHORT).show();
14     }
15 }
16
```

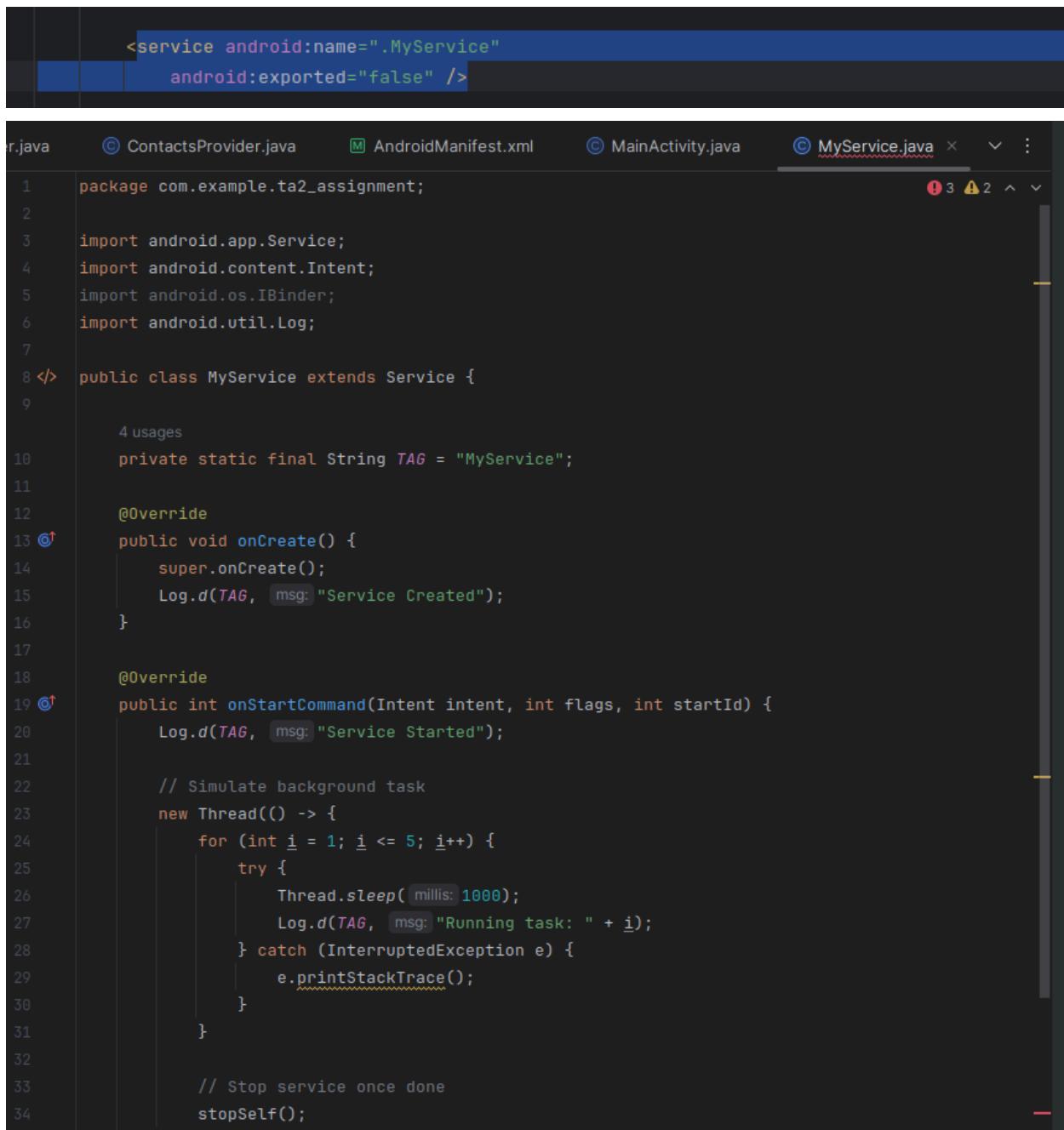
Demonstration of Android Security Permission Model



The screenshot shows the Android Studio interface with the code editor open. The tabs at the top indicate the files being edited: MyBroadcastReceiver.java, ContactsProvider.java, AndroidManifest.xml, and MainActivity.java. The MainActivity.java file is currently active.

```
1 package com.example.ta2_assignment;
2
3 import android.Manifest;
4 import android.content.pm.PackageManager;
5 import android.os.Bundle;
6 import android.widget.Button;
7 import android.widget.Toast;
8 import androidx.annotation.NonNull;
9 import androidx.appcompat.app.AppCompatActivity;
10 import androidx.core.app.ActivityCompat;
11 import androidx.core.content.ContextCompat;
12 import androidx.constraintlayout.widget.ConstraintLayout;
13
14 public class MainActivity extends AppCompatActivity {
15
16     private static final int REQUEST_CAMERA_PERMISSION = 100;
17
18     @Override
19     protected void onCreate(Bundle savedInstanceState) {
20         super.onCreate(savedInstanceState);
21
22         // Create layout and button programmatically
23     }
24 }
```

Demonstration of Android Services



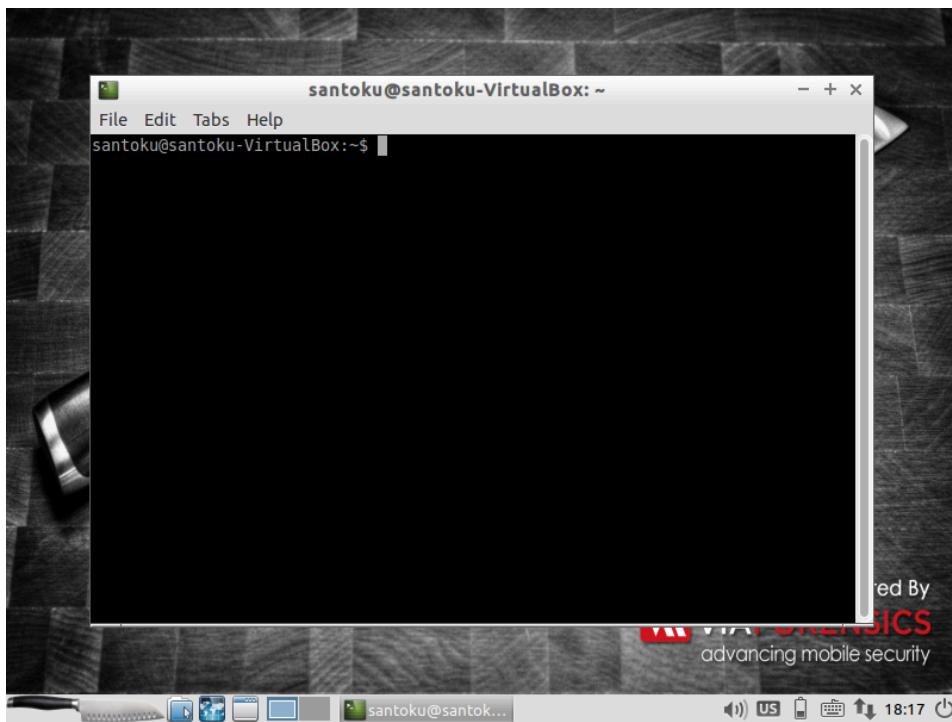
The screenshot shows a development environment with two tabs open: `AndroidManifest.xml` and `MyService.java`. The `AndroidManifest.xml` tab displays the XML configuration for the service:

```
<service android:name=".MyService"
        android:exported="false" />
```

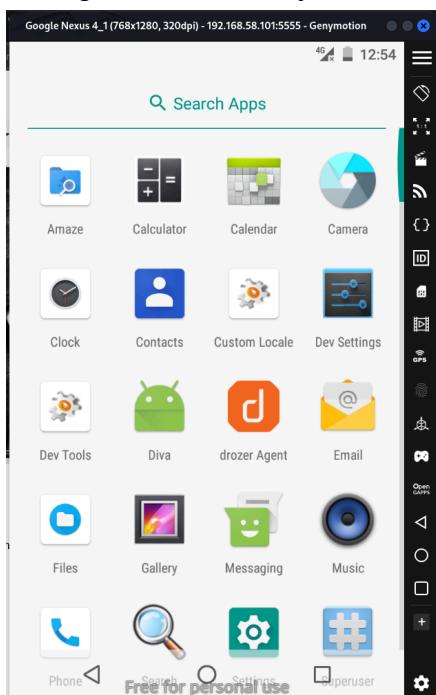
The `MyService.java` tab shows the Java code for the service implementation:

```
1 package com.example.ta2_assignment;
2
3 import android.app.Service;
4 import android.content.Intent;
5 import android.os.IBinder;
6 import android.util.Log;
7
8 public class MyService extends Service {
9
10    private static final String TAG = "MyService";
11
12    @Override
13    public void onCreate() {
14        super.onCreate();
15        Log.d(TAG, msg: "Service Created");
16    }
17
18    @Override
19    public int onStartCommand(Intent intent, int flags, int startId) {
20        Log.d(TAG, msg: "Service Started");
21
22        // Simulate background task
23        new Thread(() -> {
24            for (int i = 1; i <= 5; i++) {
25                try {
26                    Thread.sleep(millis: 1000);
27                    Log.d(TAG, msg: "Running task: " + i);
28                } catch (InterruptedException e) {
29                    e.printStackTrace();
30                }
31            }
32
33            // Stop service once done
34            stopSelf();
35        });
36    }
37}
```

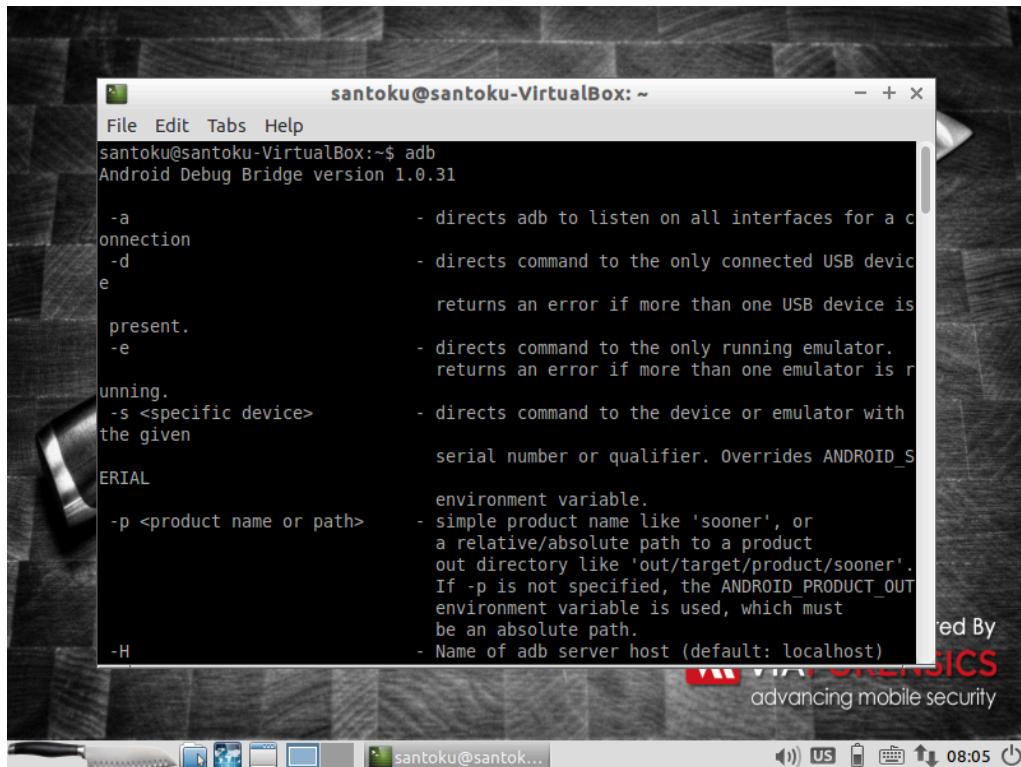
Configuration of Santoku OS



Configuration of Genymotion

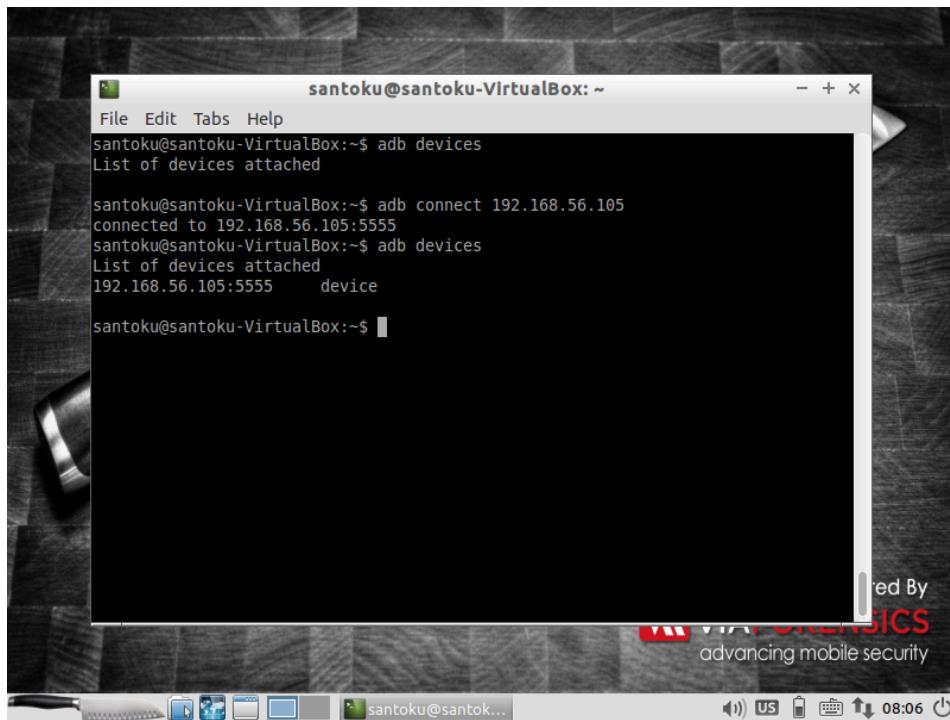


Demonstration of ADB commands



```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ adb
Android Debug Bridge version 1.0.31

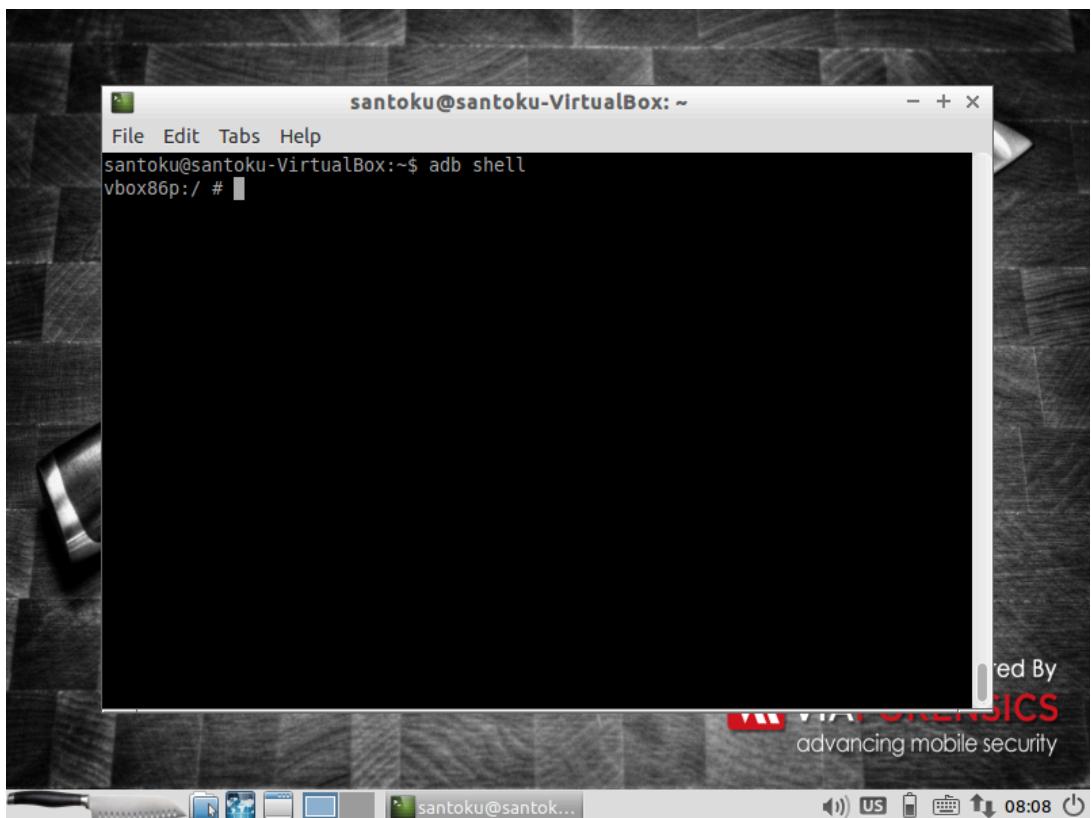
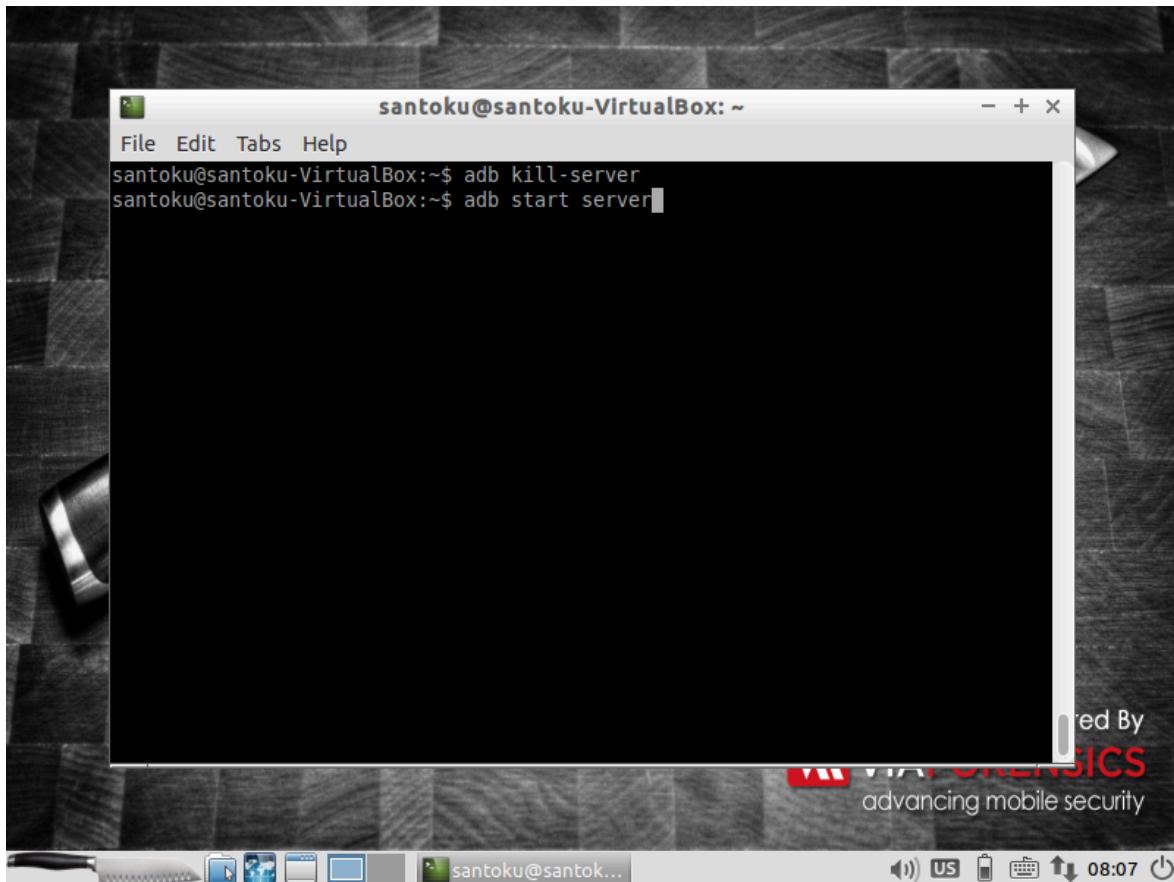
-a          - directs adb to listen on all interfaces for a connection
-d          - directs command to the only connected USB device
-e          - returns an error if more than one USB device is present.
-e          - directs command to the only running emulator. Returns an error if more than one emulator is running.
-s <specific device> - directs command to the device or emulator with the given serial number or qualifier. Overrides ANDROID_SERIAL environment variable.
-p <product name or path> - simple product name like 'sooner', or a relative/absolute path to a product out directory like 'out/target/product/sooner'. If -p is not specified, the ANDROID_PRODUCT_OUT environment variable is used, which must be an absolute path.
-H          - Name of adb server host (default: localhost)
```



```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ adb devices
List of devices attached

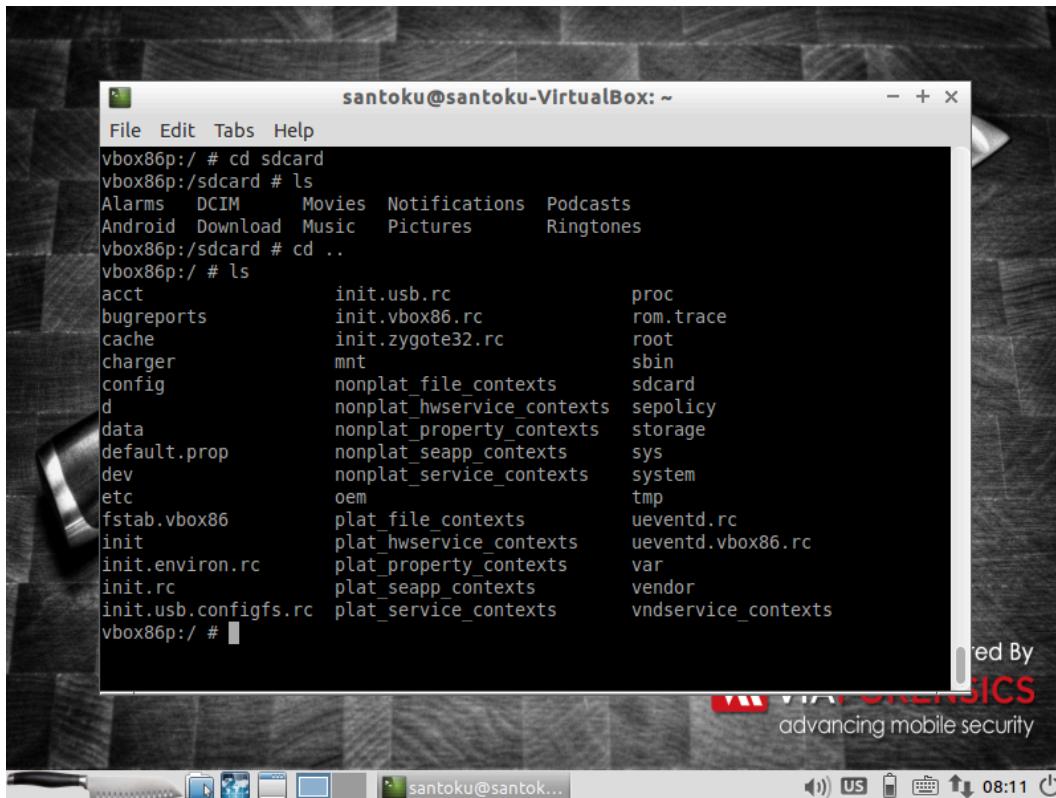
santoku@santoku-VirtualBox:~$ adb connect 192.168.56.105
connected to 192.168.56.105:5555
santoku@santoku-VirtualBox:~$ adb devices
List of devices attached
192.168.56.105:5555    device

santoku@santoku-VirtualBox:~$
```

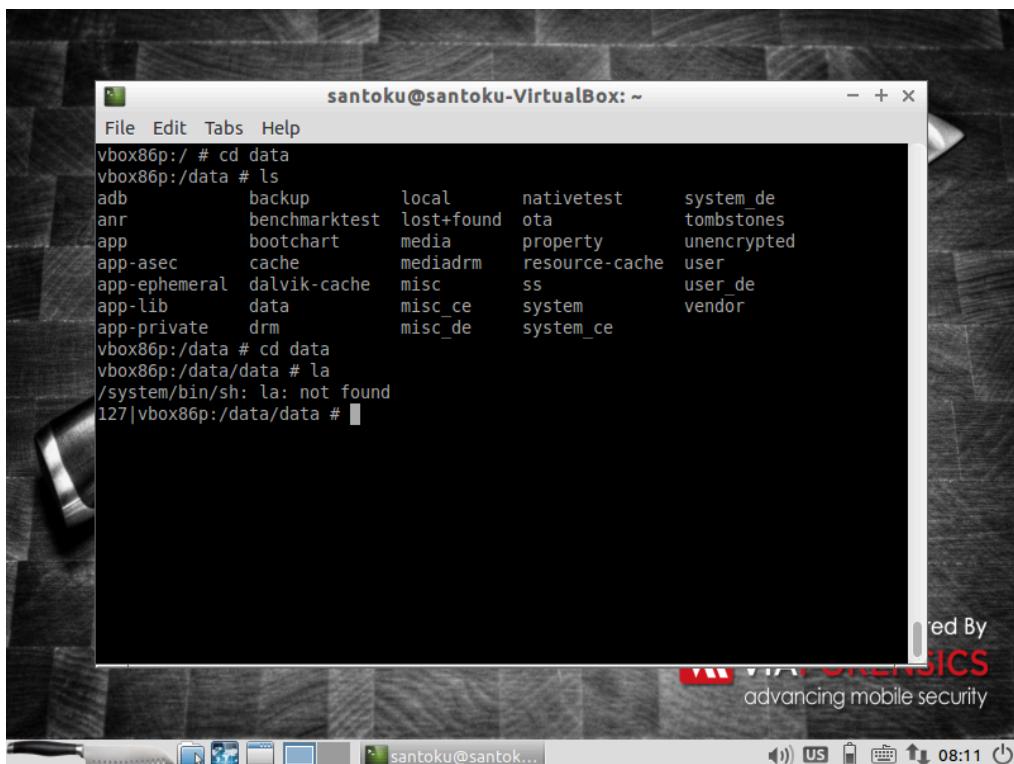


```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ adb shell
vbox86p:/ # ls
acct           init.usb.rc          proc
bugreports     init.vbox86.rc       rom.trace
cache          init.zygote32.rc    root
charger        mnt
config         nonplat_file_contexts
d              nonplat_hwservice_contexts
data           nonplat_property_contexts
default.prop   nonplat_seapp_contexts
dev            nonplat_service_contexts
etc            oem
fstab.vbox86   plat_file_contexts
init           plat_hwservice_contexts
init.environ.rc  plat_property_contexts
init.rc        plat_seapp_contexts
init.usb.configfs.rc  plat_service_contexts
vbox86p:/ #
```

```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
external/speex 53fd3aa39d4bcb2023b38728f2960eb2bf14f362
external/spirv-llvm 60a7eaee1fc4dda9c90ab21ab91c8c9e7ccce3a2
external/sqlite 98ae87b7357d961c2fc98584204863bdcab922b
external/squashfs-tools 8c214c801b59ca22b66a0f5cbb3c61af39311fc3
external/strace 5270d443a29a8e82fcc697bb13aa08328dce913c
external/stressapptest ea469443e9c2cd1fda87188df2b1ffe0e30656b2
external/svox 68406cc3de6a2f0aea279c23bd4d8a836757ba0b
external/swiftshader c4da9210b76c9b130217218ed7d5b31ceb0eec3
external/syslinux 76d05dc695b06c4e987bb8078f78032441e1430c
external/tagsoup 9c02d9f506855965ec513685788890dfc856a5bc
external/tcpdump 60AAF97844d4c21b8618fd50046e036c5f78ebe0
external/testng 2d09ec828c313edd6f9f5021c9b166854d742521
external/timezonepicker-support 99e91a76fd74bad10266623d67cdb98d011f709e
external/tinyalsa 5c97d4873d068790cc9b4fed4808fe2935f9b21
external/tinycompress 3d913d4ac8ded0f75c48dac2ffac60fd51c6a2b4
external/tinyxml 973b9695a088751f06967715c1a9fb4f6d73a05
external/tinyxml2 57ad9c9edf5f99f5d7fa5aeac6bee840254c6153
external/toolchain-utils 3690e025de8daaed03c4acb02d2b054e5c4c0dd5
external/toybox e99fefea29bbd83f9fb3e7bb4b280733ae3695450
external/tpm2 204257160b290c4b6e8849b668810bccb3c9da45
external/tremolo 006fe9a16bacdb4aa7bb582a125a998c6b1dd4ac
external/unicode eccbd5dcdb02b3d90ff769df285381e1bb54f788
external/universal-tween-engine 75d2d4e1d27ca8ccf0fd7dc4456b0a3dcf509dd2
external/v8 922f352287cb099020e33cca3b826ada6fd0efd6
```



```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
vbox86p:/ # cd sdcard
vbox86p:/sdcard # ls
Alarms DCIM Movies Notifications Podcasts
Android Download Music Pictures Ringtones
vbox86p:/sdcard # cd ..
vbox86p:/ # ls
acct           init.usb.rc          proc
bugreports     init.vbox86.rc       rom.trace
cache          init.zygote32.rc    root
charger        mnt                 sbin
config         nonplat_file_contexts sepolicy
d              nonplat_hwservice_contexts storage
data           nonplat_property_contexts sys
default.prop   nonplat_seapp_contexts system
dev            nonplat_service_contexts tmp
etc            oem                 ueventd.rc
fstab.vbox86   plat_file_contexts ueventd.vbox86.rc
init           plat_hwservice_contexts var
init.environ.rc plat_property_contexts vendor
init.rc        plat_seapp_contexts vndservice_contexts
init.usb.configfs.rc plat_service_contexts
vbox86p:/ #
```



```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
vbox86p:/ # cd data
vbox86p:/data # ls
adb      backup    local    nativetest    system de
anr      benchmarktest lost+found  ota      tombstones
app      bootchart   media    property     unencrypted
app-asec cache     mediadrm  resource-cache user
app-ephemeral dalvik-cache misc    ss        user_de
app-lib  data      misc_ce   system     vendor
app-private drm      misc_de   system_ce
vbox86p:/data # cd data
vbox86p:/data/data # la
/system/bin/sh: la: not found
127|vbox86p:/data/data #
```

santoku@santoku-VirtualBox: ~

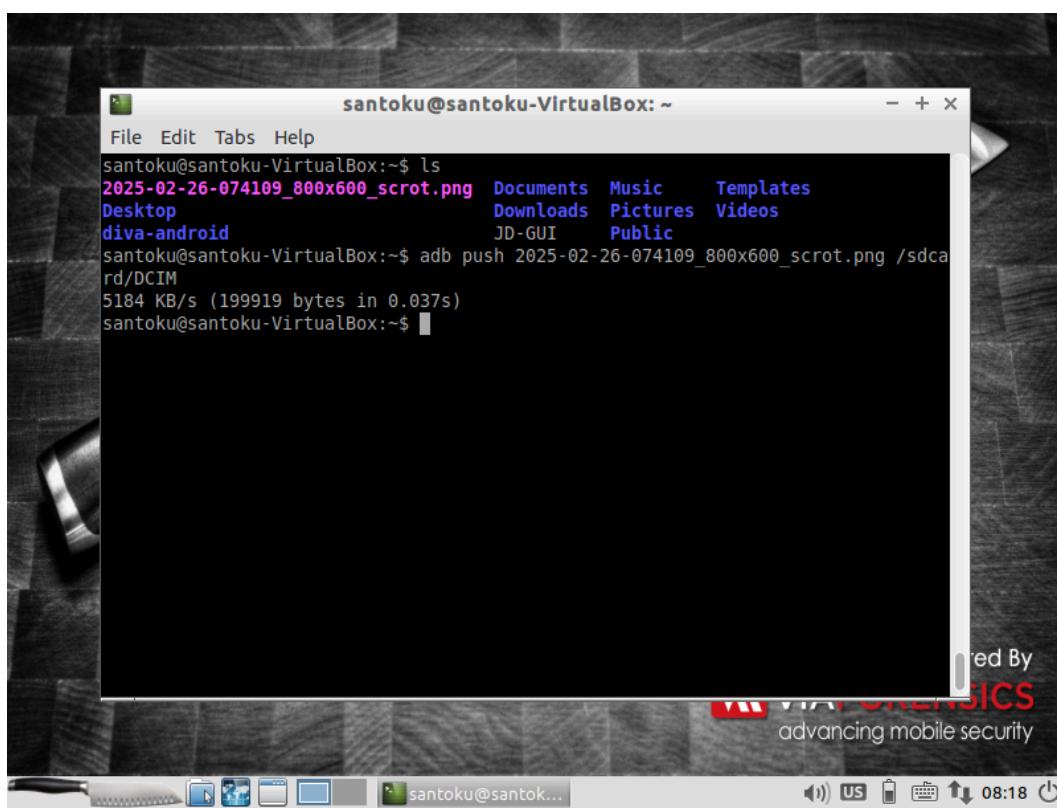
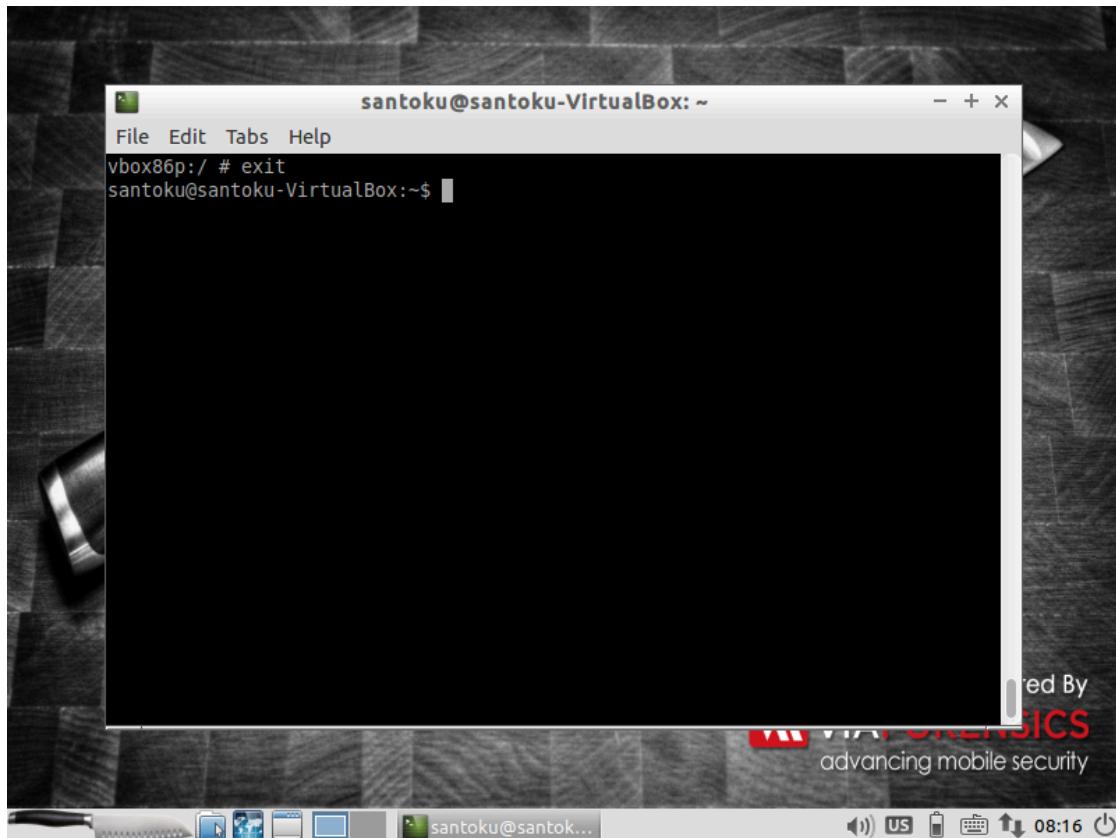
```
File Edit Tabs Help
com.android.providers.contacts
com.android.providers.downloads
com.android.providers.downloads.ui
com.android.providers.media
com.android.providers.settings
com.android.providers.telephony
com.android.providers.userdictionary
com.android.provision
com.android.proxyhandler
com.android.quicksearchbox
com.android.server.telecom
com.android.settings
com.android.sharedstoragebackup
com.android.shell
com.android.smspush
com.android.statementservice
com.android.storagemanager
com.android.systemui
com.android.vpndialogs
com.android.wallpaper.livepicker
com.android.wallpaperbackup
com.android.wallpapercropper
com.android.wallpaperpicker
com.android.webview
```

Advancing mobile security

santoku@santoku-VirtualBox: ~

```
vbox86p:/data/data # cd
vbox86p:/ # ps
USER          PID   PPID      VSZ      RSS WCHAN          ADDR S NAME
root        1945     244    5600    2900 sigsuspend  f2d12bb9 S sh
root        1978   1945    6992    2492 0           f1debbb9 R ps
vbox86p:/ #
```

Advancing mobile security



```
santoku@santoku-VirtualBox:~$ ls
2025-02-26-074109_800x600_scrot.png  Documents  Music    Templates
Desktop                  Downloads  Pictures  Videos
diva-android              JD-GUI    Public

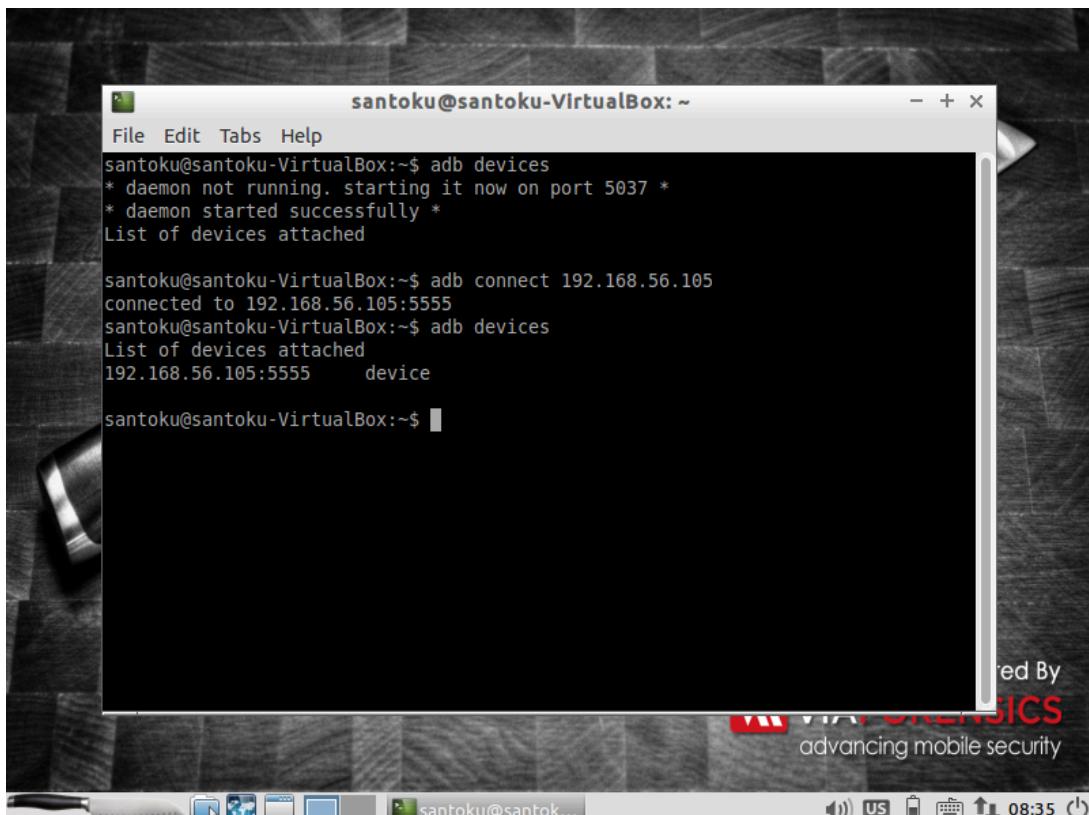
santoku@santoku-VirtualBox:~$ adb push 2025-02-26-074109_800x600_scrot.png /sdcard/DCIM
5184 KB/s (199919 bytes in 0.037s)
santoku@santoku-VirtualBox:~$ adb shell
vbox86p:/ # cd sdcard/DCIM
vbox86p:/sdcard/DCIM # ls
2025-02-26-074109_800x600_scrot.png
vbox86p:/sdcard/DCIM #
```

```
KB, data=131KB
02-26 02:51:29.703 2002 2144 D : HostConnection::get() New Host Connection established 0xe2f27190, pid 2002, tid 2144
02-26 02:51:29.705 477 2146 D local_opengl: Sending id 29 to host
02-26 02:51:29.706 2002 2144 D : HostComposition ext ANDROID_EMU_host_composition v1 ANDROID_EMU_host_composition_v2 ANDROID_EMU_async_unmap_buffer ANDROID_EMU_sync_buffer_data GL_OES_EGL_image_external_essl3 GL_OES_vertex_array_object GL_KHR_texture_compression_astc_ldr ANDROID_EMU_host_side_tracing ANDROID_EMU_async_frame_commands ANDROID_EMU_gles max version 3_1
02-26 02:51:29.713 2002 2144 D EGL_emulation: eglCreateContext: 0xe2f05180: maj 3 min 1 rcv 4
02-26 02:51:29.841 2002 2144 I GLRootView: onSurfaceChanged: 768x1136, gl10: com.google.android.gles.jni.GLImpl@325c6cb
02-26 02:51:29.848 2002 2144 I GLRootView: layout content pane 768x1136 (compensation 0)
02-26 02:51:29.939 513 543 I ActivityManager: Displayed com.android.gallery3d/app.GalleryActivity: +364ms
02-26 02:51:29.986 1064 1241 E eglCodecCommon: goldfish_dma_create_region: could not obtain fd to device! fd -1 errno=2
02-26 02:51:32.783 225 261 W genymotion_audio: Not supplying enough data to HAL, expected position 2430831 , only wrote 2278080
02-26 02:51:33.354 513 513 W WindowManager: removeWindowToken: Attempted to remove non-existing token: android.os.Binder@c83e632
```

```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
02-26 02:52:07.931 D/RIL      ( 239): onRequest: SIGNAL_STRENGTH
02-26 02:52:07.931 D/AT-RIL   ( 239): AT> AT+CSQ
02-26 02:52:07.931 D/AT-BSB   ( 498): AT< AT+CSQ
02-26 02:52:07.931 D/AT-BSB   ( 498): AT> +CSQ: 12,4,90,120,80,120,4,90,100,10,3
0,7,200
OK-26 02:52:07.931 D/AT-BSB   ( 498):
02-26 02:52:07.931 D/AT-RIL   ( 239): AT< +CSQ: 12,4,90,120,80,120,4,90,100,10,3
0,7,200
02-26 02:52:07.931 D/AT-RIL   ( 239): AT< OK
02-26 02:52:07.932 D/RILJ     ( 734): [3949]< SIGNAL_STRENGTH SignalStrength: 12
4 90 120 80 120 4 90 100 10 30 7 0 -402225288 cdma [SUB0]
02-26 02:52:27.934 D/RILJ     ( 734): [3949]> SIGNAL_STRENGTH [SUB0]
02-26 02:52:27.934 D/RIL     ( 239): onRequest: SIGNAL_STRENGTH
02-26 02:52:27.934 D/AT-RIL   ( 239): AT> AT+CSQ
02-26 02:52:27.934 D/AT-BSB   ( 498): AT< AT+CSQ
02-26 02:52:27.935 D/AT-BSB   ( 498): AT> +CSQ: 12,4,90,120,80,120,4,90,100,10,3
0,7,200
OK-26 02:52:27.935 D/AT-BSB   ( 498):
02-26 02:52:27.935 D/AT-RIL   ( 239): AT< +CSQ: 12,4,90,120,80,120,4,90,100,10,3
0,7,200
02-26 02:52:27.935 D/AT-RIL   ( 239): AT< OK
02-26 02:52:27.935 D/RILJ     ( 734): [3949]< SIGNAL_STRENGTH SignalStrength: 12
4 90 120 80 120 4 90 100 10 30 7 0 -402225288 cdma [SUB0]
```

```
santoku@santoku-VirtualBox: ~/Downloads
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ ls
2025-02-26-074109_800x600_screenshot.png  Documents  Music    Templates
Desktop                           Downloads  Pictures  Videos
diva-android                         JD-GUI    Public
santoku@santoku-VirtualBox:~$ cd Downloads
santoku@santoku-VirtualBox:~/Downloads$ ls
diva-beta.apk
santoku@santoku-VirtualBox:~/Downloads$ adb install diva-beta.apk
5283 KB/s (1502294 bytes in 0.277s)
Failure [INSTALL_FAILED_ALREADY_EXISTS: Attempt to re-install jakhar.aseem.diva
without first uninstalling.]
santoku@santoku-VirtualBox:~/Downloads$
```

Demonstration of Android Boot Process using ADB



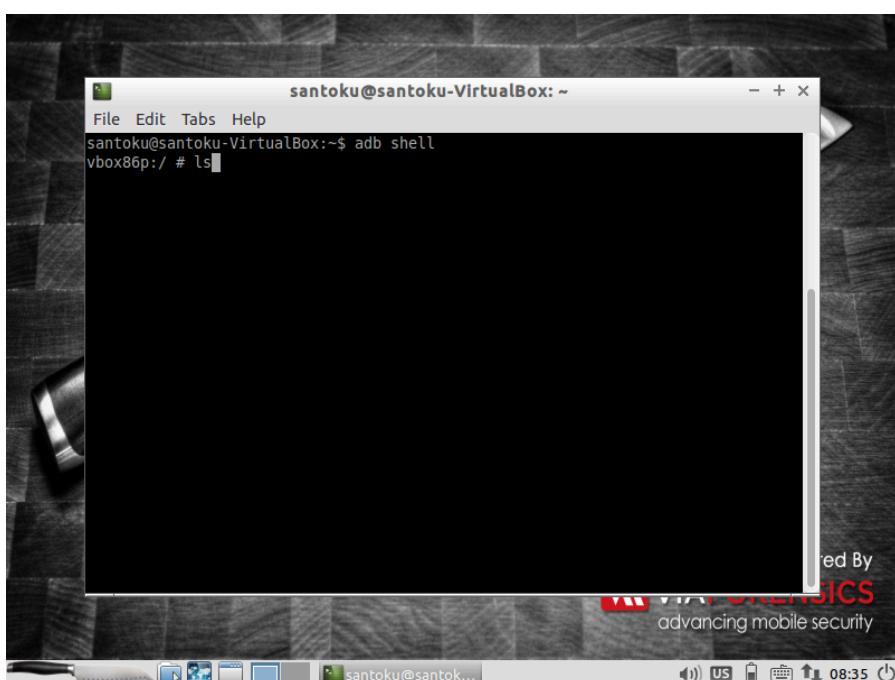
santoku@santoku-VirtualBox: ~

```
santoku@santoku-VirtualBox:~$ adb devices
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
List of devices attached

santoku@santoku-VirtualBox:~$ adb connect 192.168.56.105
connected to 192.168.56.105:5555
santoku@santoku-VirtualBox:~$ adb devices
List of devices attached
192.168.56.105:5555    device

santoku@santoku-VirtualBox:~$
```

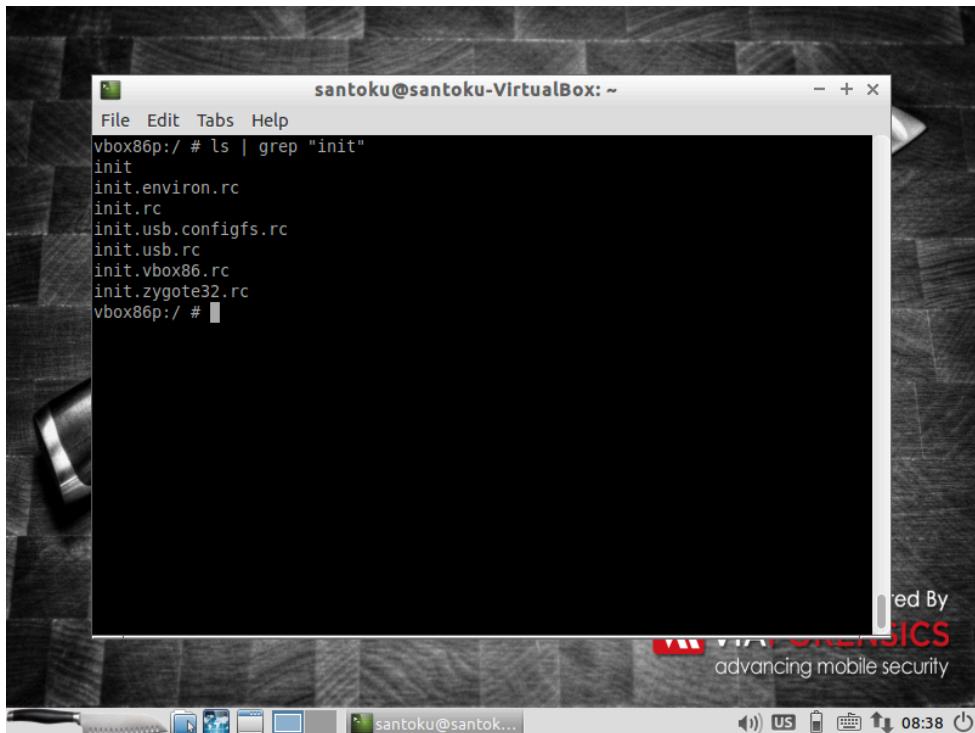
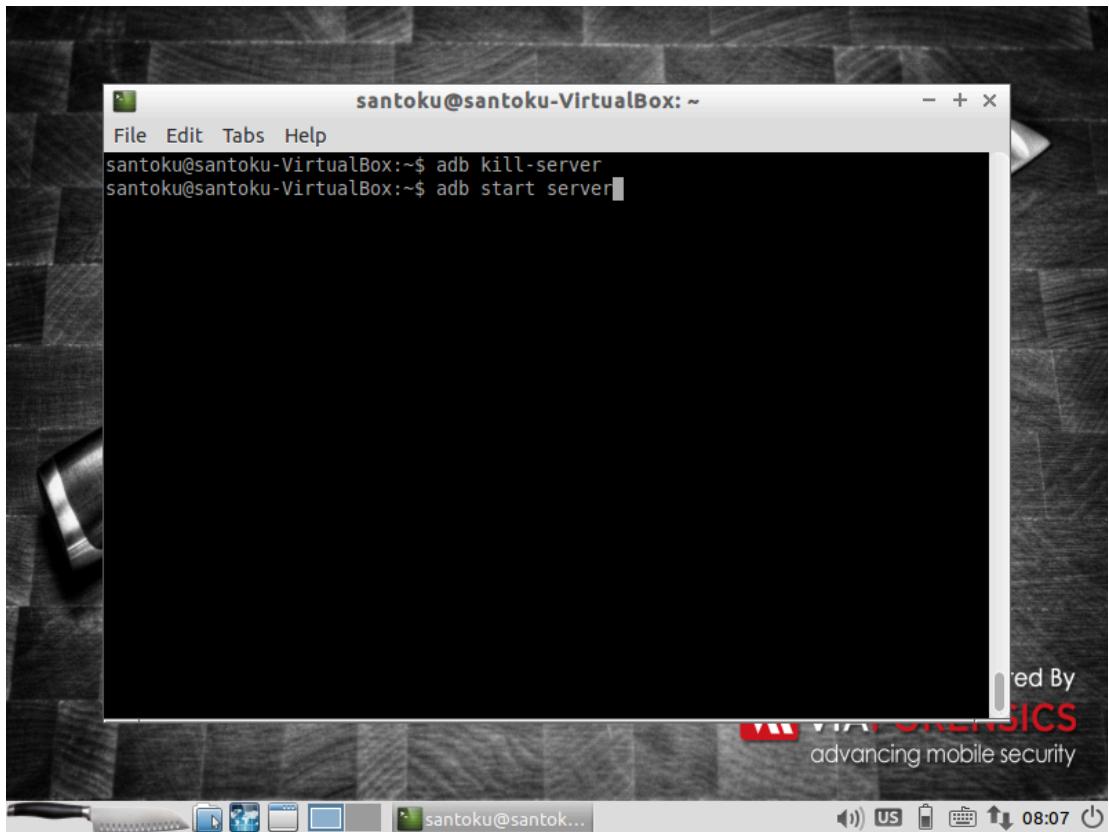
The screenshot shows a terminal window titled "santoku@santoku-VirtualBox: ~". The user runs "adb devices" which outputs that the daemon is not running and starts it on port 5037, confirming successful startup. Then, "adb connect 192.168.56.105" is run, connecting to the device at 192.168.56.105:5555. Finally, "adb devices" is run again, showing the device is now connected.



santoku@santoku-VirtualBox: ~

```
santoku@santoku-VirtualBox:~$ adb shell
vbox86p:/ # ls
```

The screenshot shows a terminal window titled "santoku@santoku-VirtualBox: ~". The user runs "adb shell", which connects them to the Android device's shell. They then run "ls" to list the contents of the current directory, which is "/".



```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
Segmentation fault
139|vbox86p:/ # cat init.rc
# Copyright (C) 2012 The Android Open Source Project
#
# IMPORTANT: Do not create world writable files or directories.
# This is a common source of Android security bugs.
#

import /init.environ.rc
import /init.usb.rc
import /init.${ro.hardware}.rc
import /init.usb.configfs.rc
import /init.${ro.zygote}.rc

on early-init
    # Set init and its forked children's oom_adj.
    write /proc/1/oom_score_adj -1000

    # Disable sysrq from keyboard
    write /proc/sys/kernel/sysrq 0

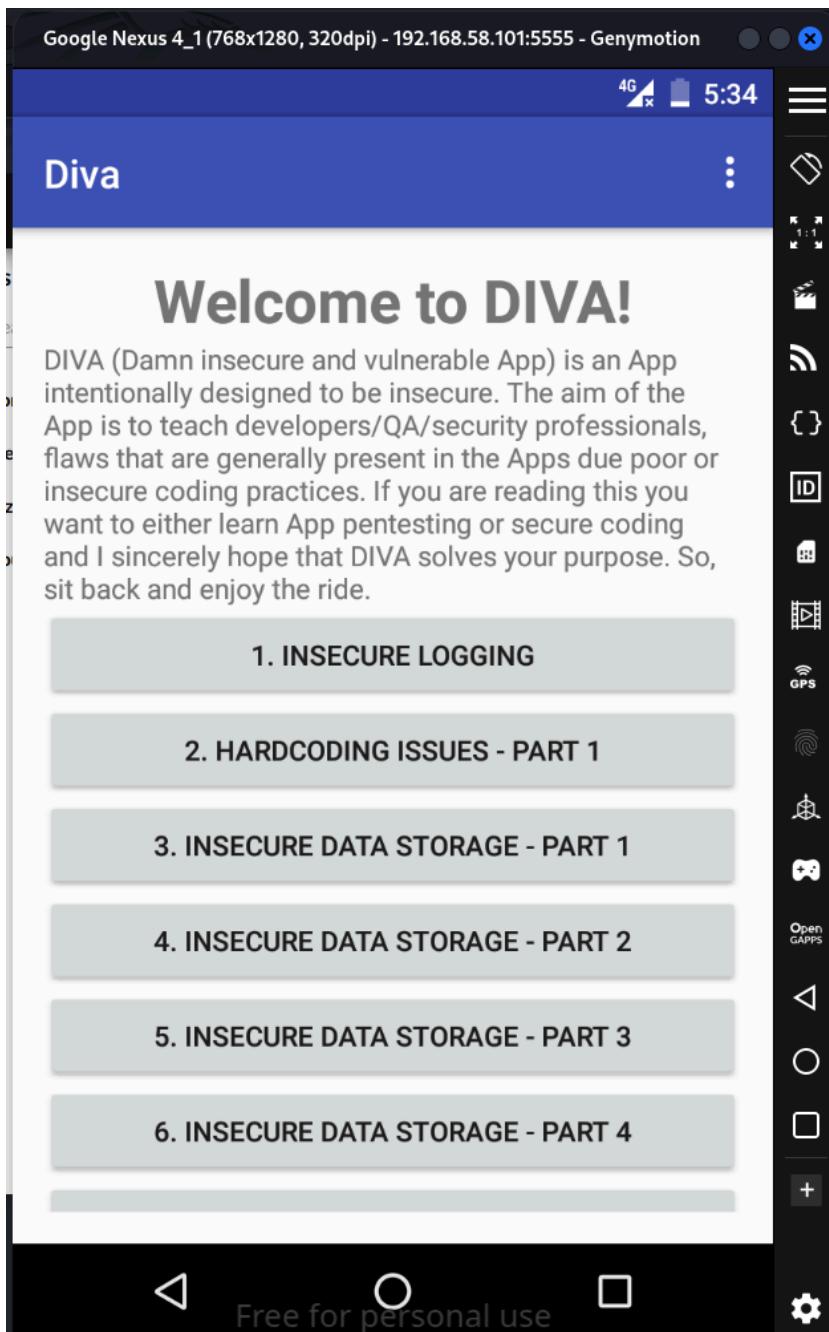
    # Set the security context of /adb_keys if present.
    restorecon /adb_keys

red By
[REDACTED] CRASHICS
advancing mobile security

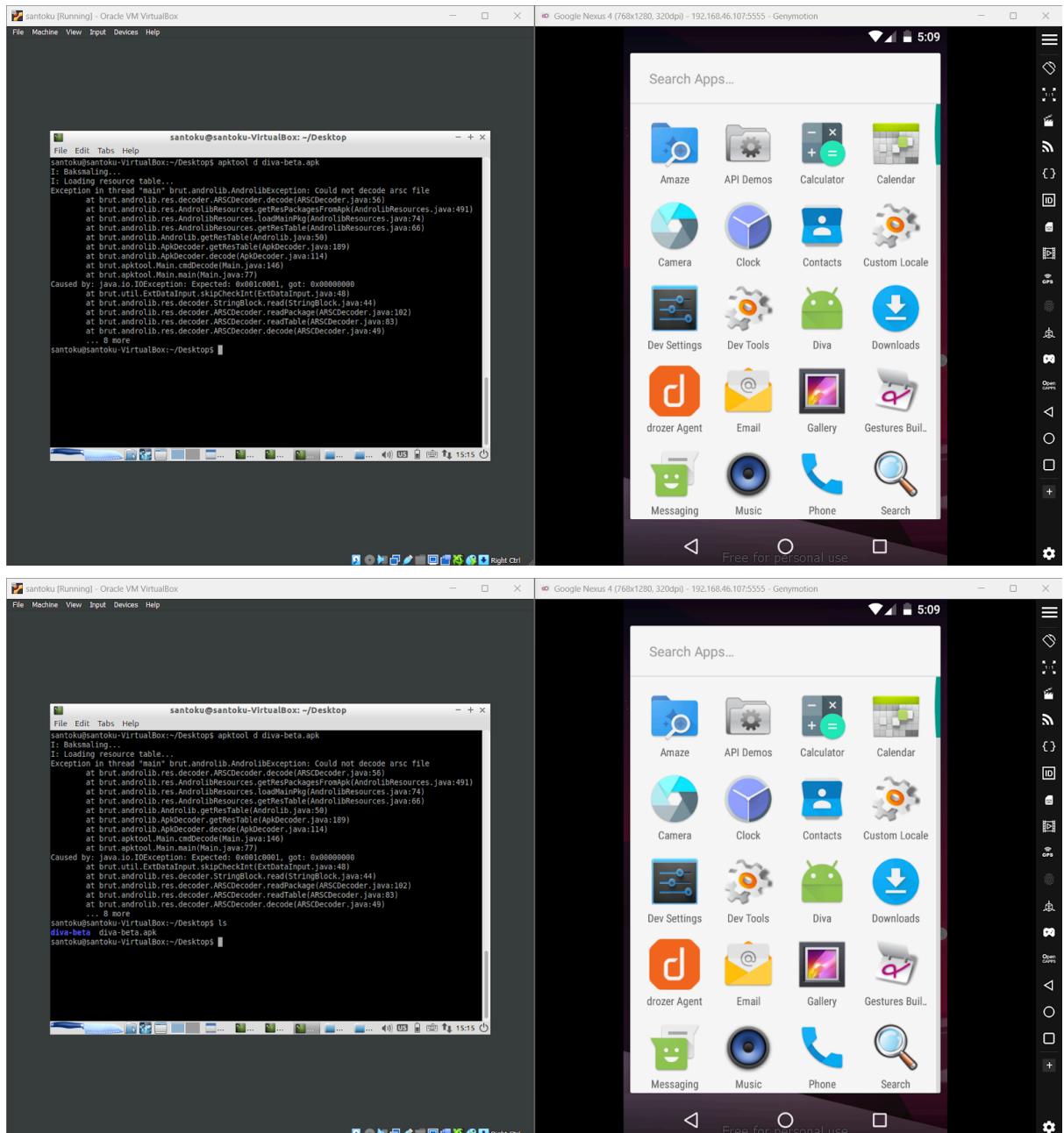
santoku@santoku... 08:39
```

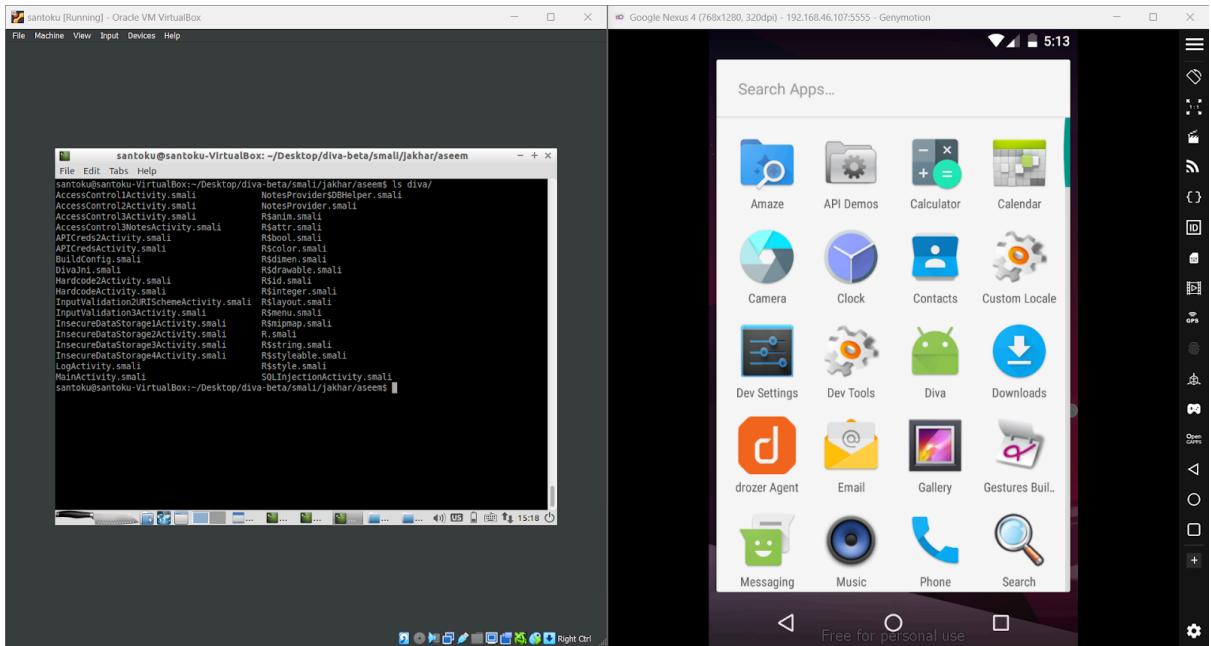
```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
vbox86p:/ # ps -ef | grep "zygote"
root      223      1  0 03:02:55 ?    00:00:00 zygote
webview_zygote 693      1  0 03:02:59 ?    00:00:00 webview zygote32
root     1834   1789  0 03:08:52 pts/1 00:00:00 grep zygote
vbox86p:/ #
```

Configuration of DIVA

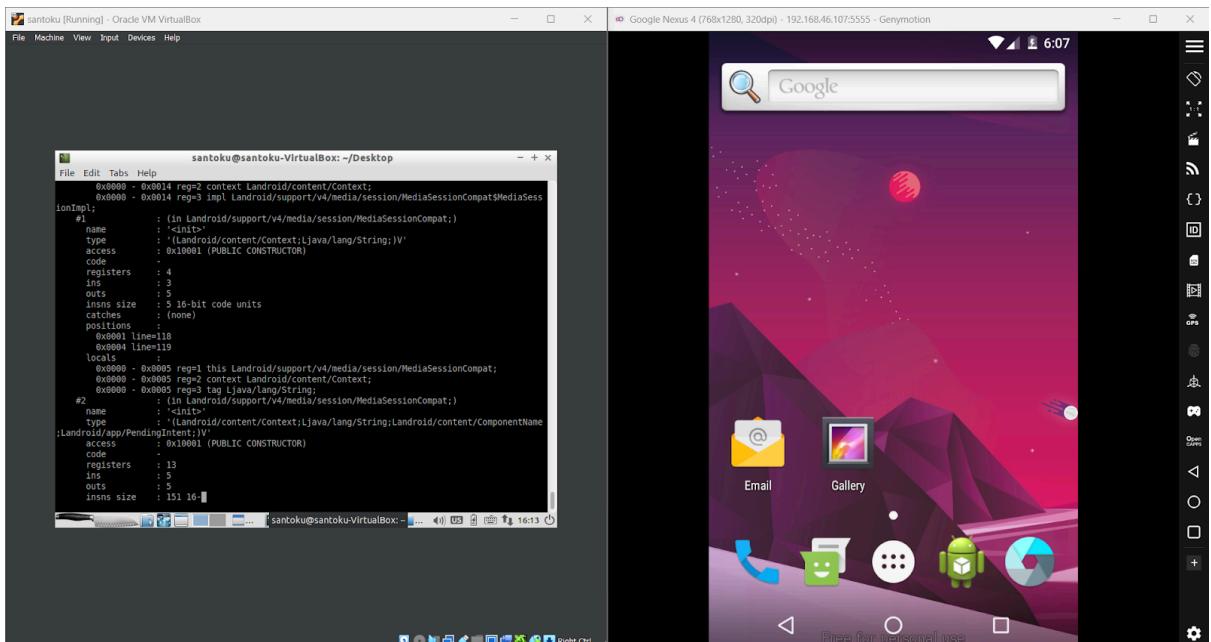
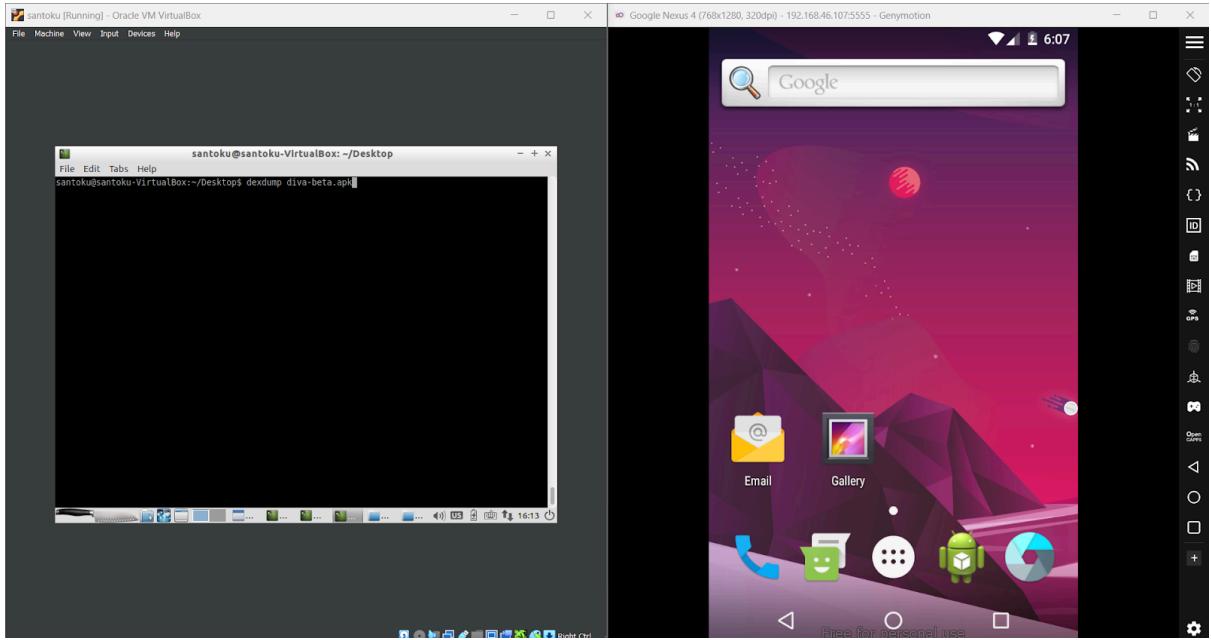


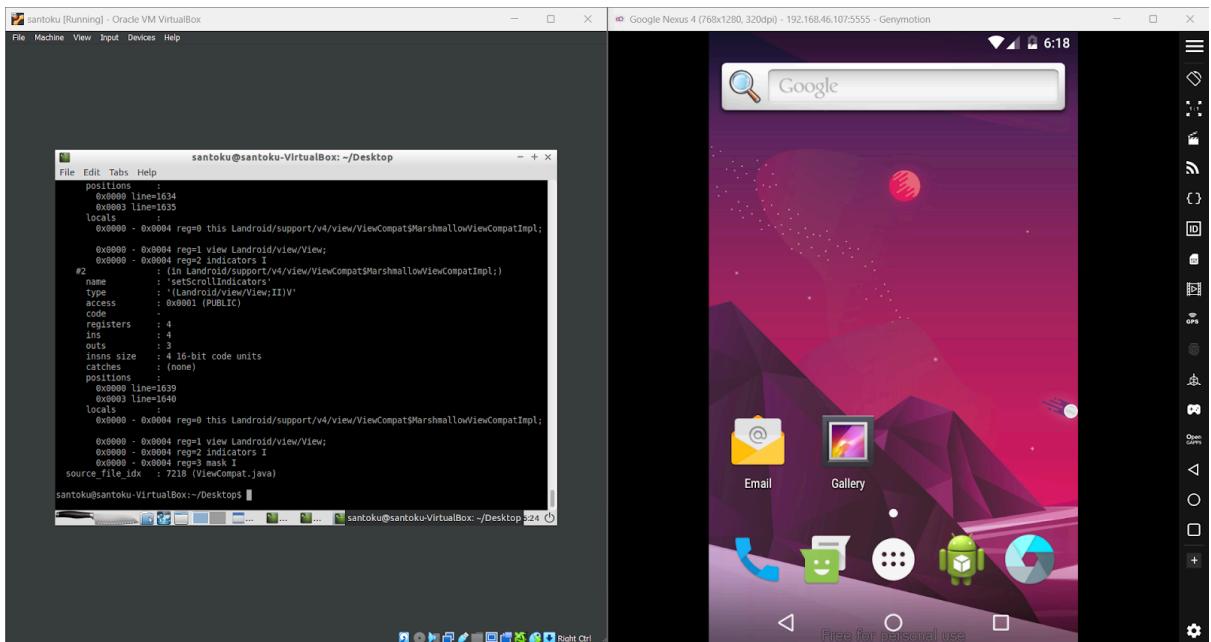
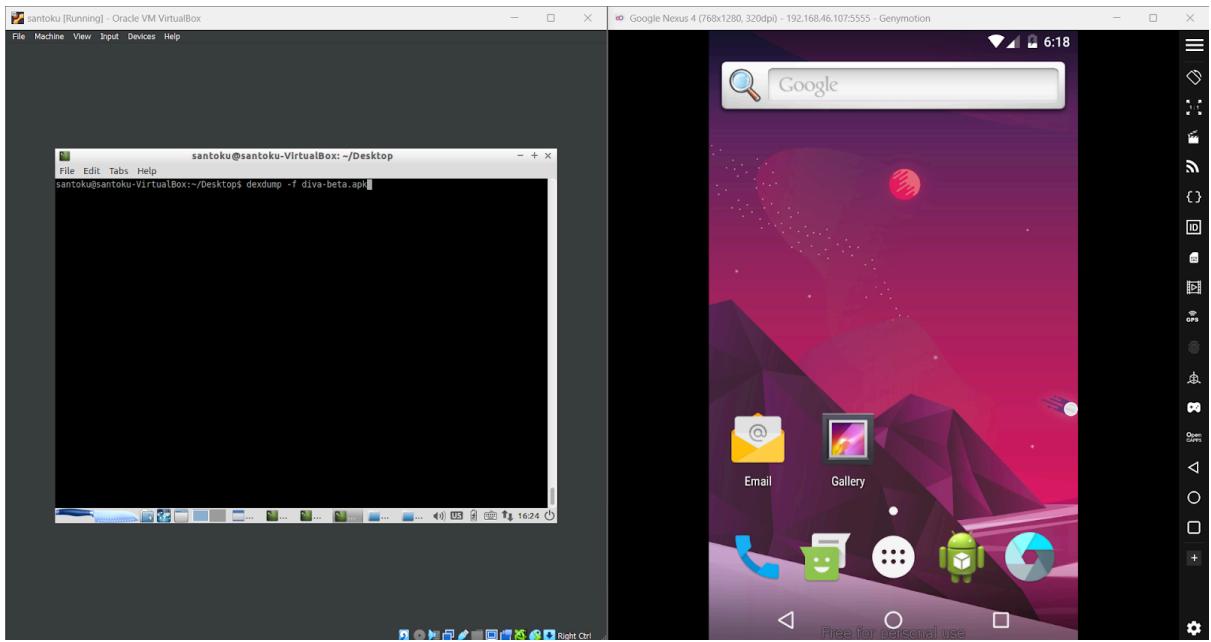
Reverse Engineering using APKTools

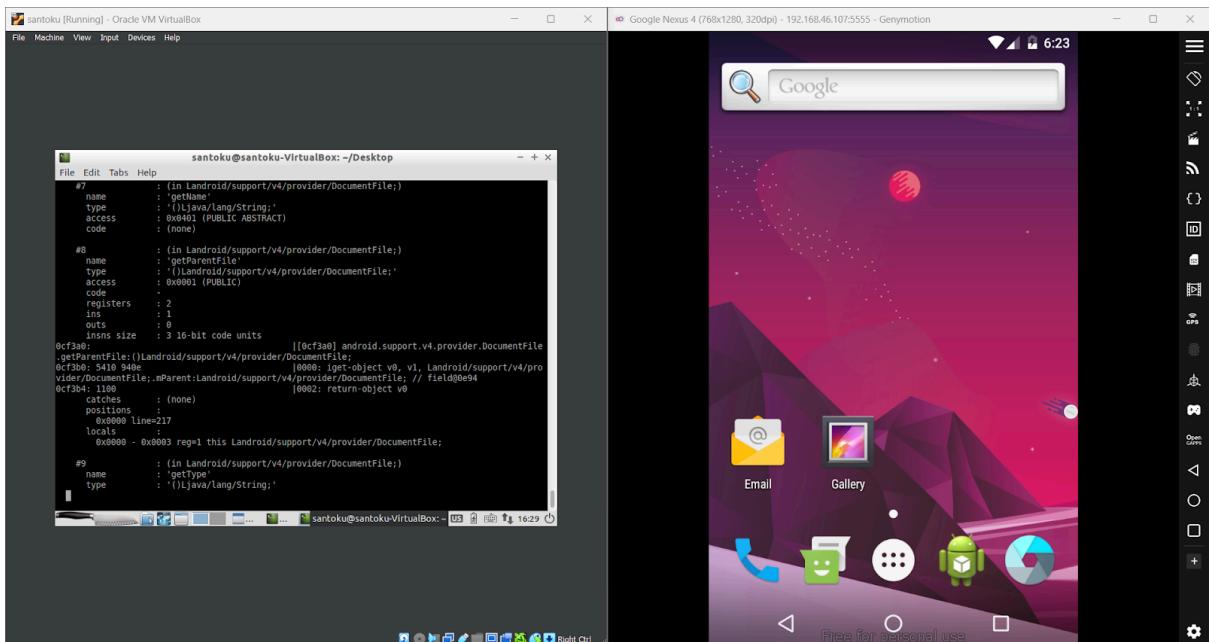
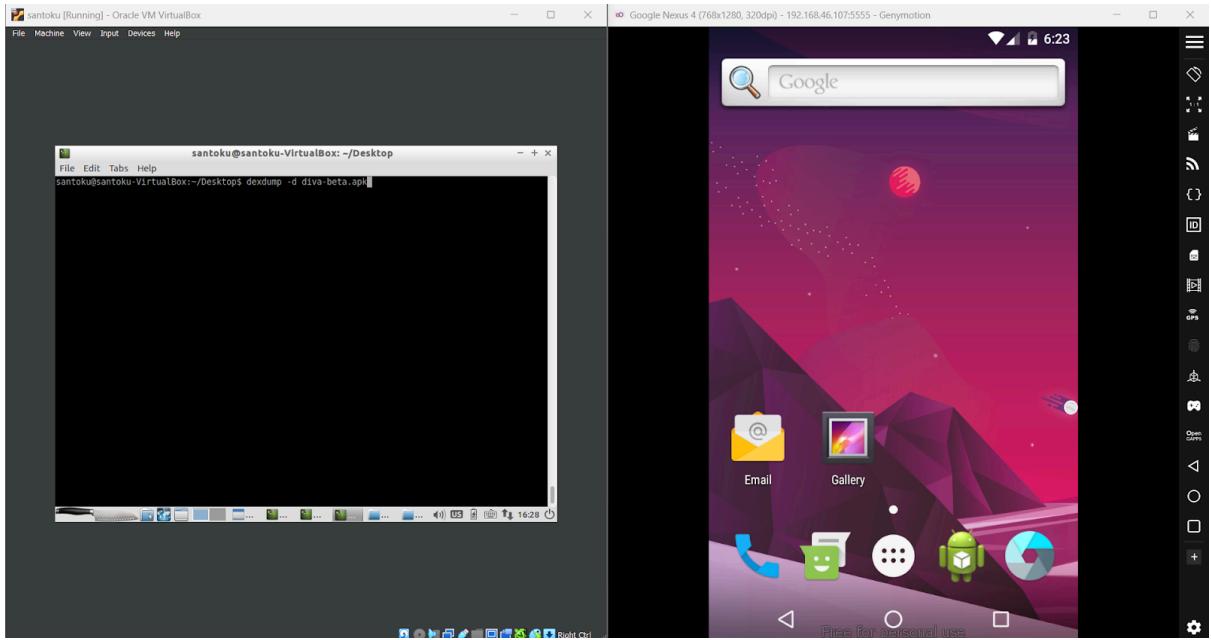




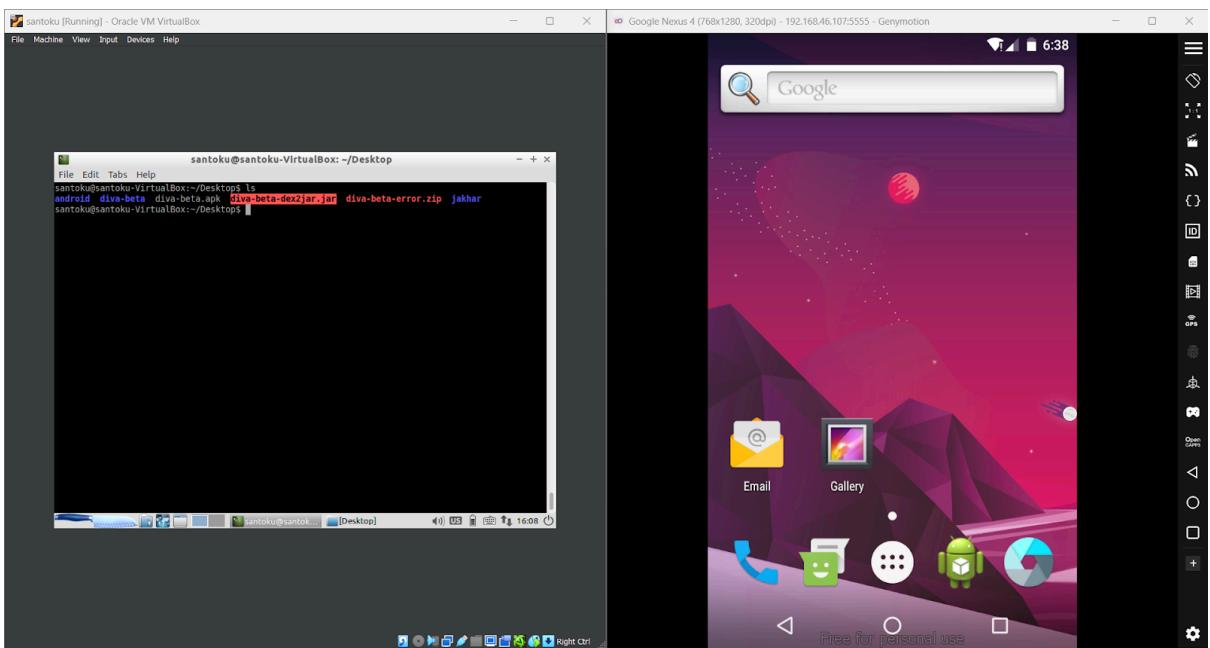
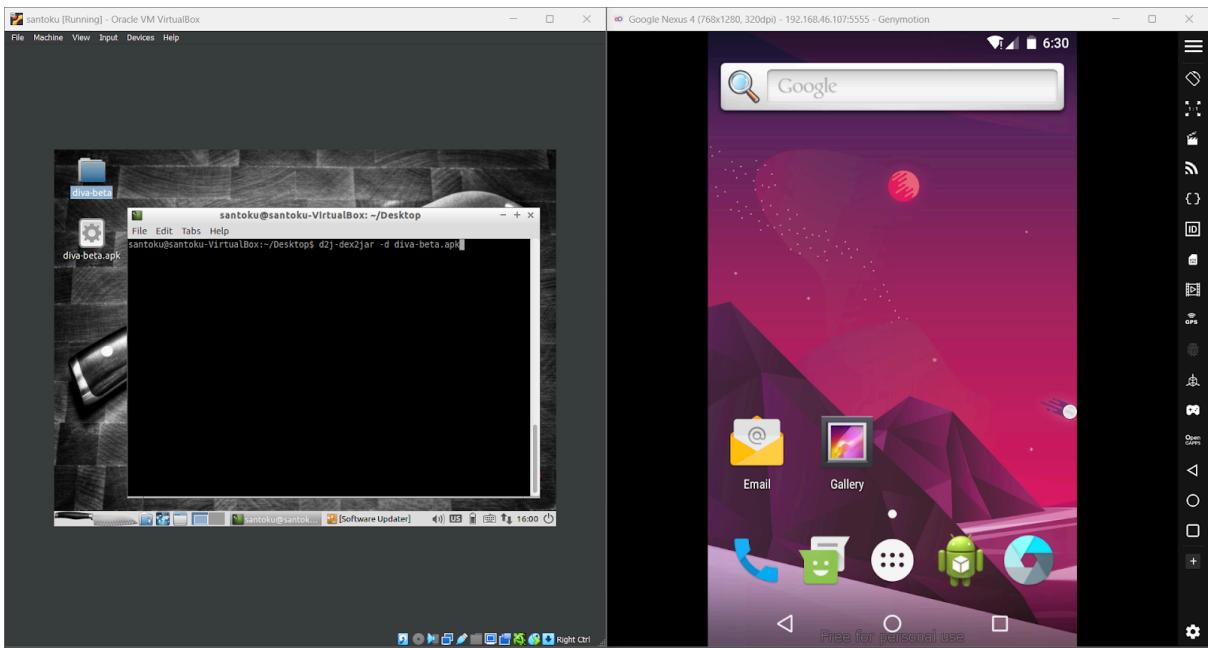
Reverse Engineering using Haxdump Dex Dump and d2j

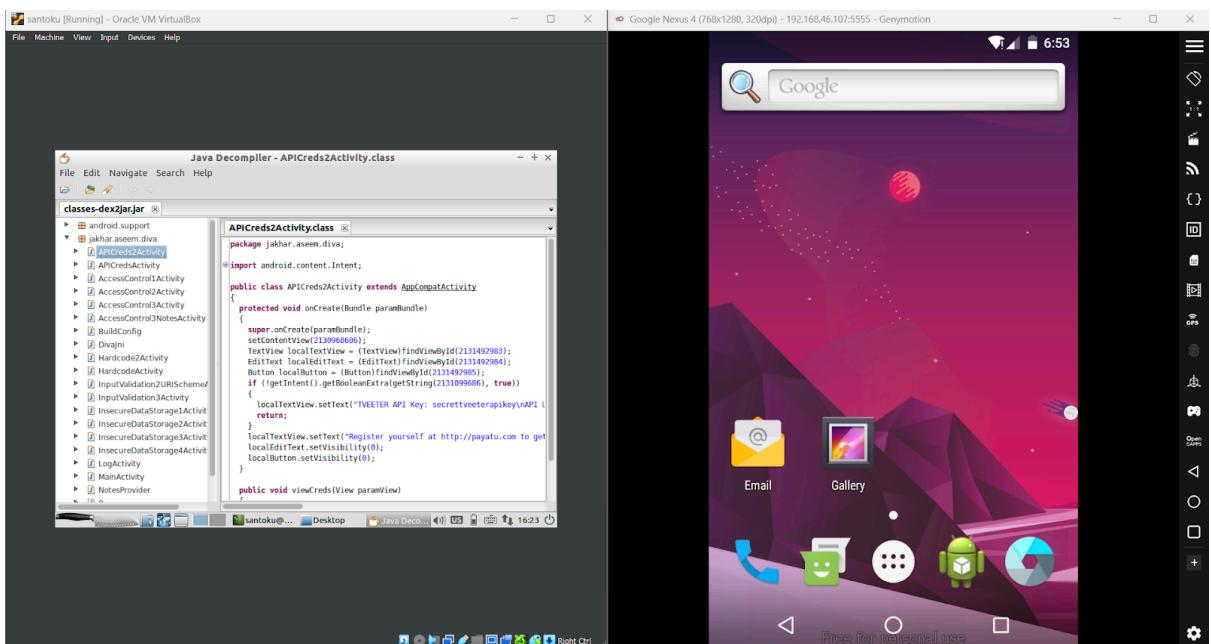
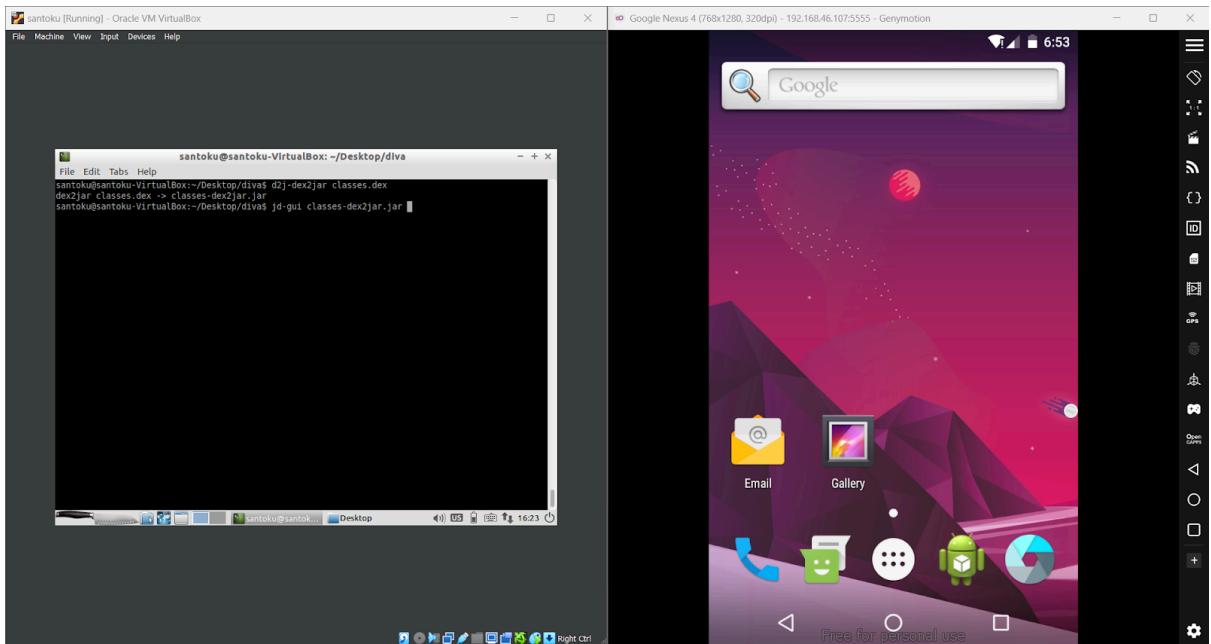




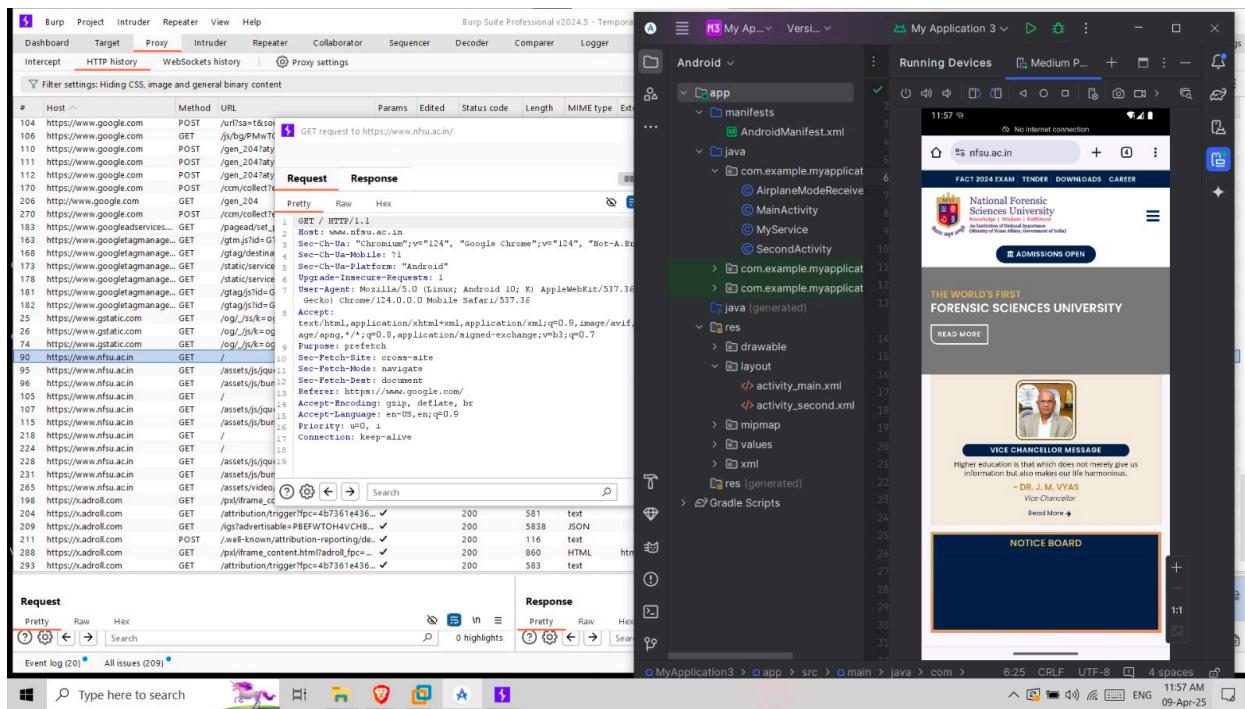


Reverse Engineering using dex2jar and JDGUI

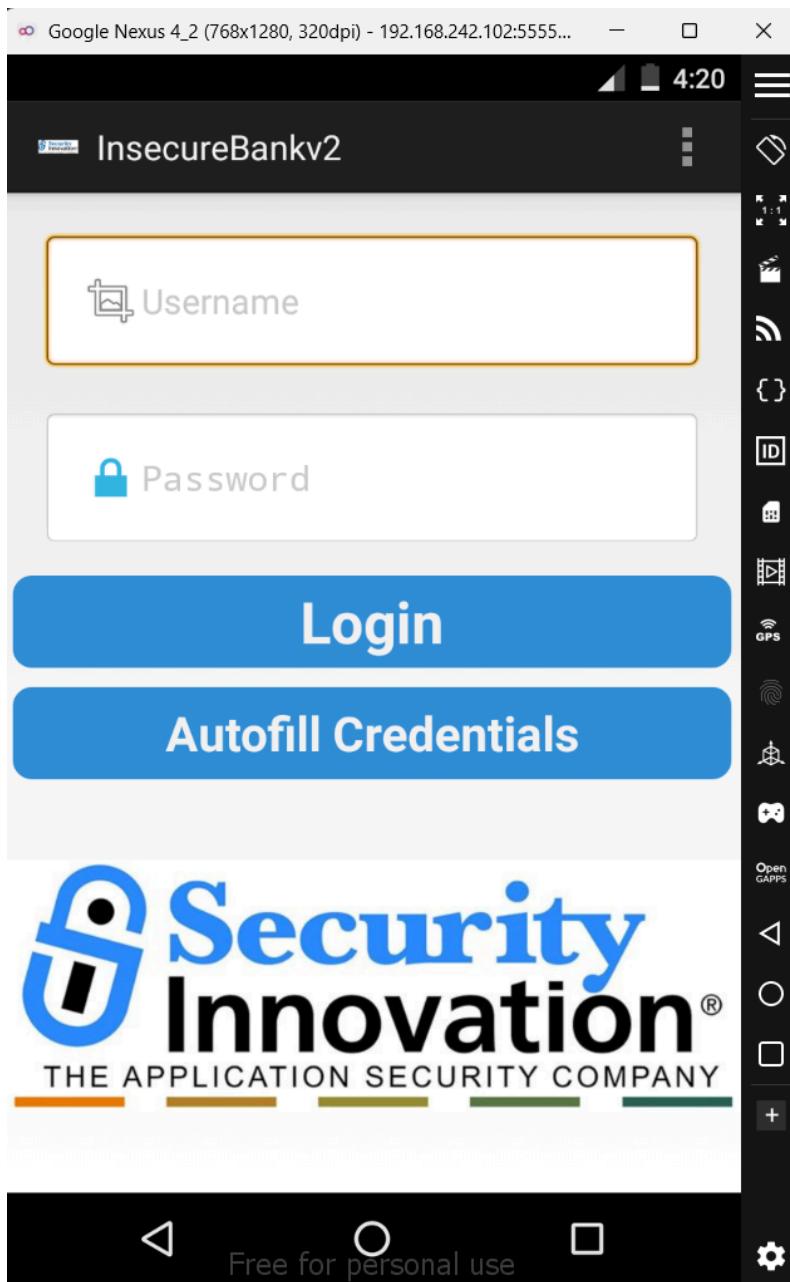




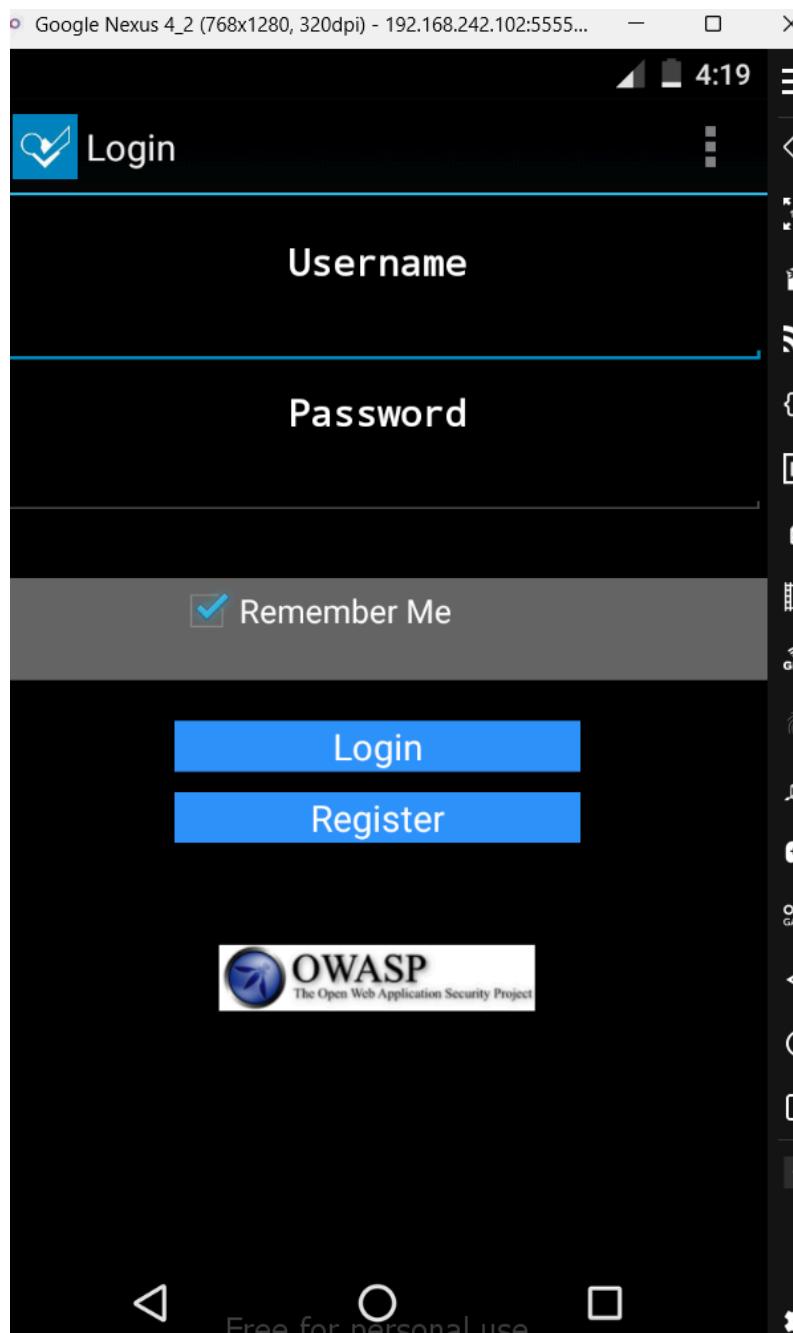
Request interception using BurpSuite



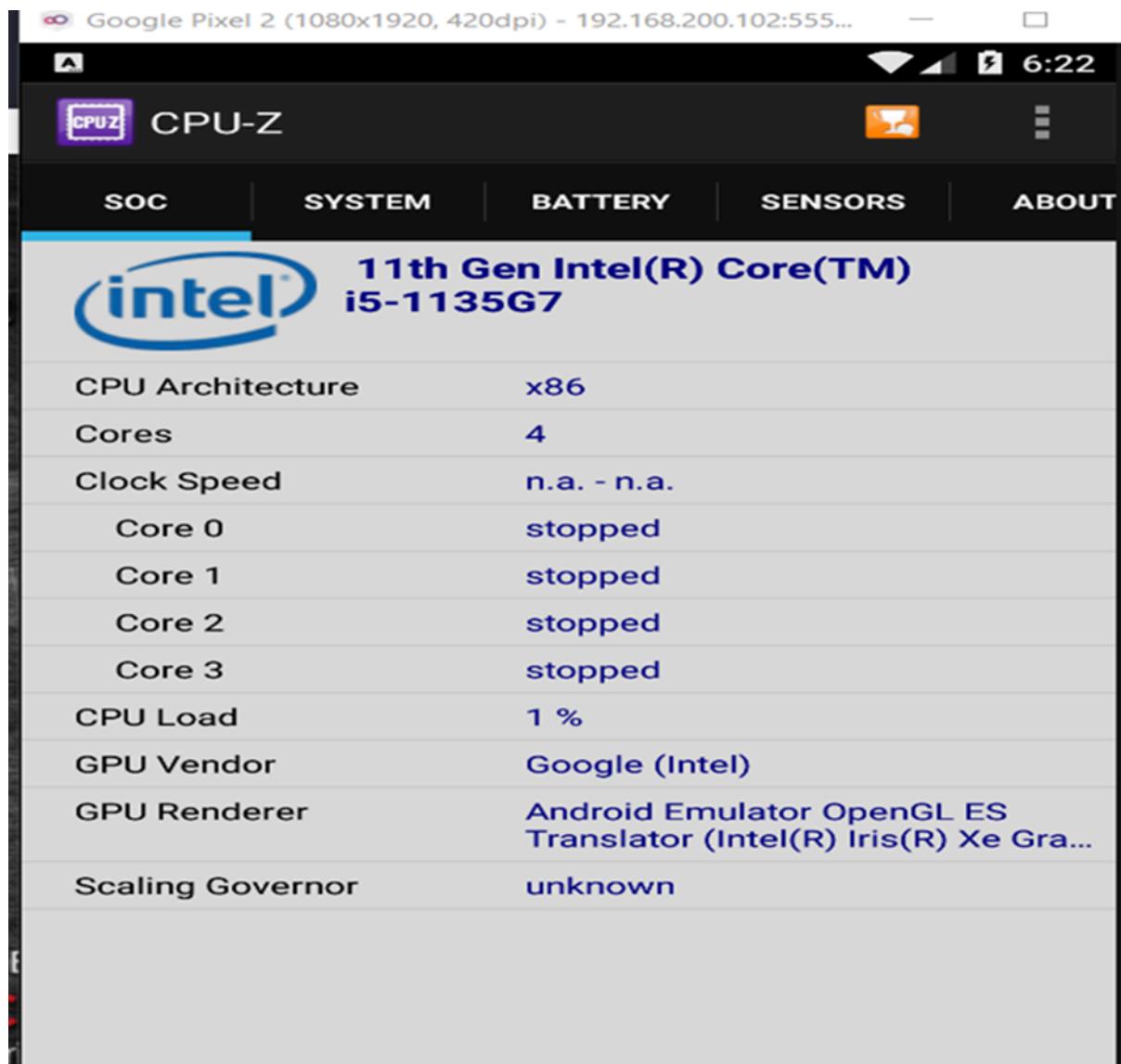
Configuration of Insecure Bank2



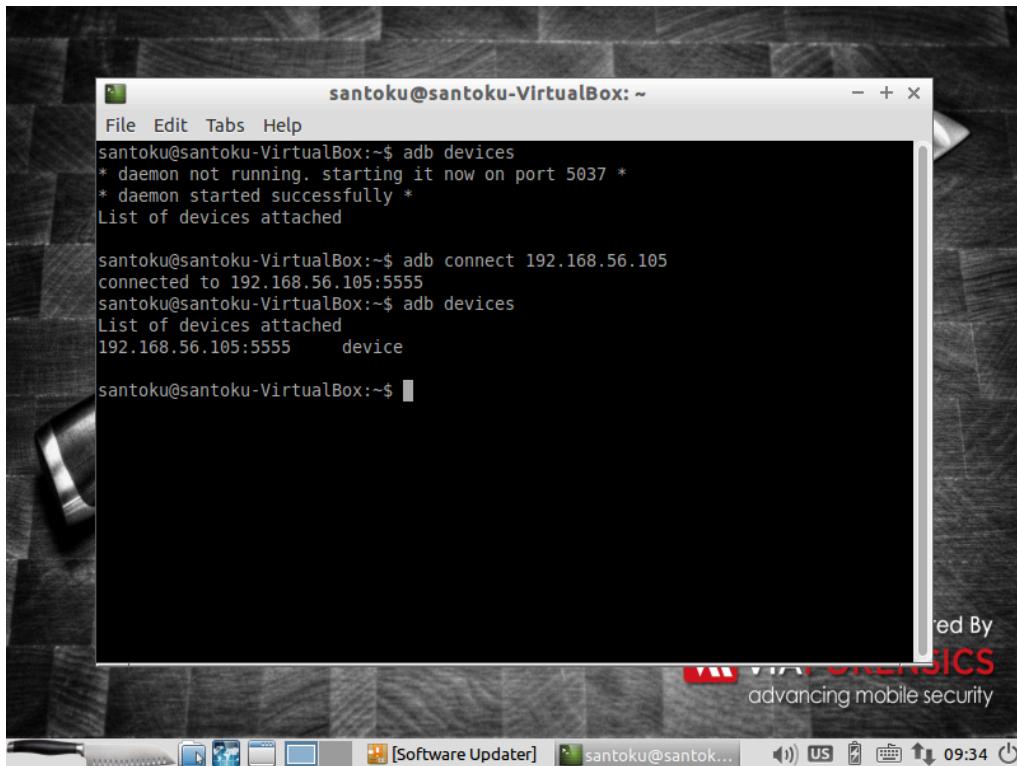
Configuration of OWASP GoatDroid



Configuration of Open GApps



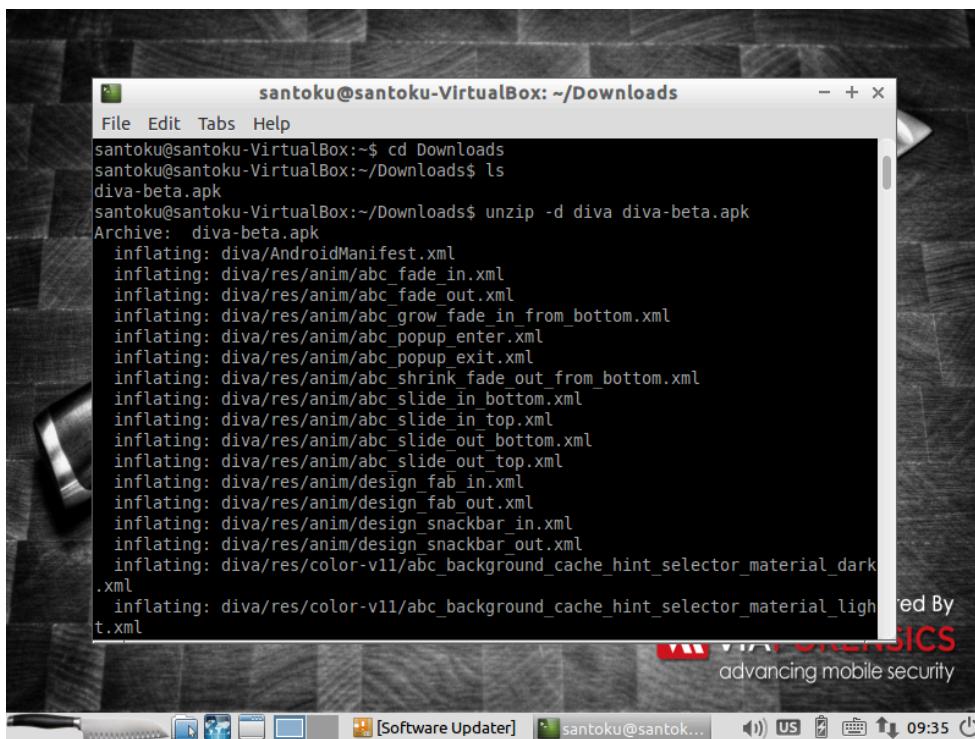
Insecure Logging – Vulnerability



```
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ adb devices
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
List of devices attached

santoku@santoku-VirtualBox:~$ adb connect 192.168.56.105
connected to 192.168.56.105:5555
santoku@santoku-VirtualBox:~$ adb devices
List of devices attached
192.168.56.105:5555      device

santoku@santoku-VirtualBox:~$
```



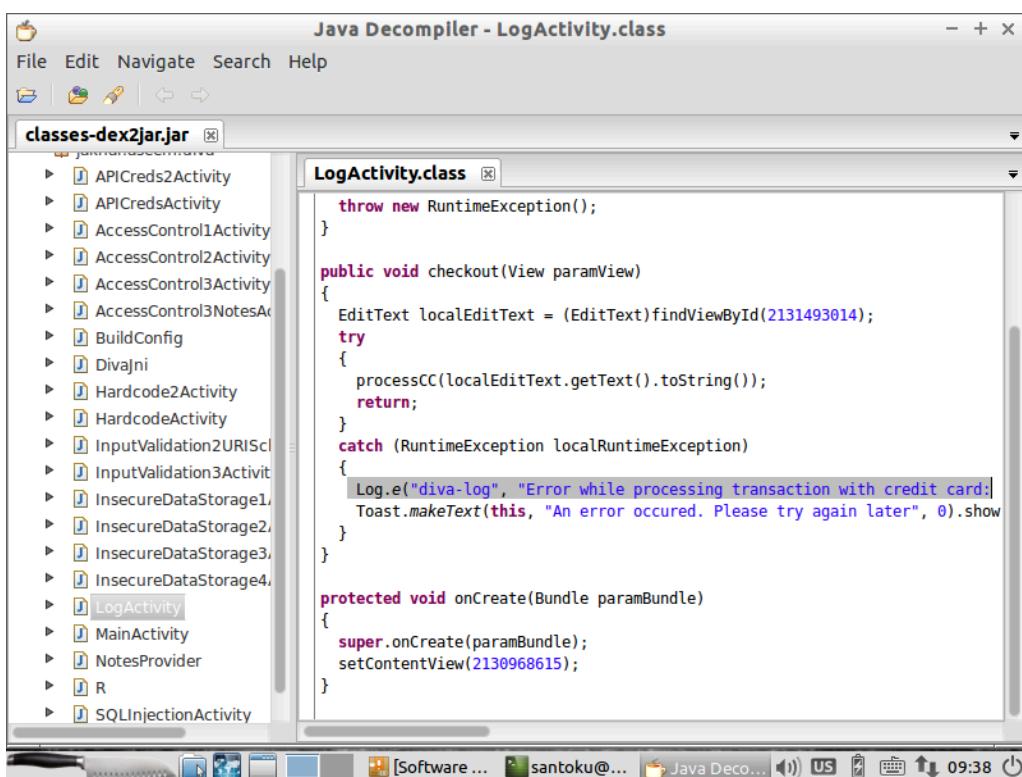
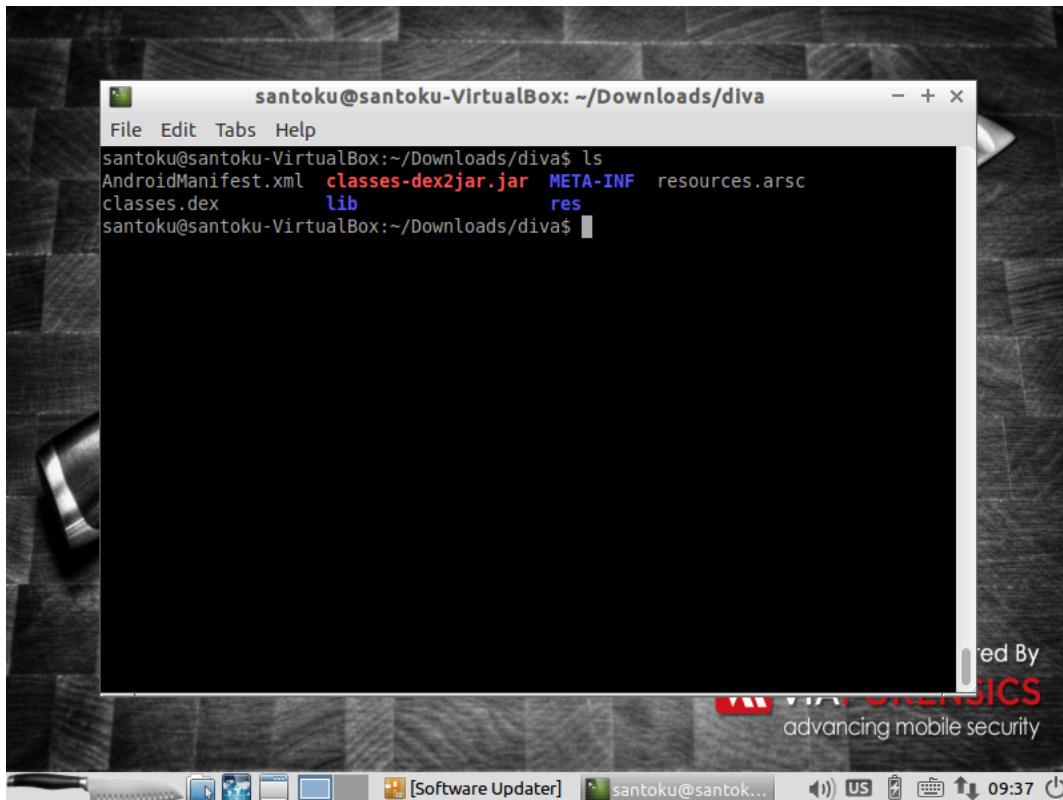
```
santoku@santoku-VirtualBox: ~/Downloads
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ cd Downloads
santoku@santoku-VirtualBox:~/Downloads$ ls
diva-beta.apk
santoku@santoku-VirtualBox:~/Downloads$ unzip -d diva diva-beta.apk
Archive: diva-beta.apk
    inflating: diva/AndroidManifest.xml
    inflating: diva/res/anim/abc_fade_in.xml
    inflating: diva/res/anim/abc_fade_out.xml
    inflating: diva/res/anim/abc_grow_fade_in_from_bottom.xml
    inflating: diva/res/anim/abc_popup_enter.xml
    inflating: diva/res/anim/abc_popup_exit.xml
    inflating: diva/res/anim/abc_shrink_fade_out_from_bottom.xml
    inflating: diva/res/anim/abc_slide_in_bottom.xml
    inflating: diva/res/anim/abc_slide_in_top.xml
    inflating: diva/res/anim/abc_slide_out_bottom.xml
    inflating: diva/res/anim/abc_slide_out_top.xml
    inflating: diva/res/anim/design_fab_in.xml
    inflating: diva/res/anim/design_fab_out.xml
    inflating: diva/res/anim/design_snackbar_in.xml
    inflating: diva/res/anim/design_snackbar_out.xml
    inflating: diva/res/color-v11/abc_background_cache_hint_selector_material_dark
.xml
    inflating: diva/res/color-v11/abc_background_cache_hint_selector_material_light
.xml
```

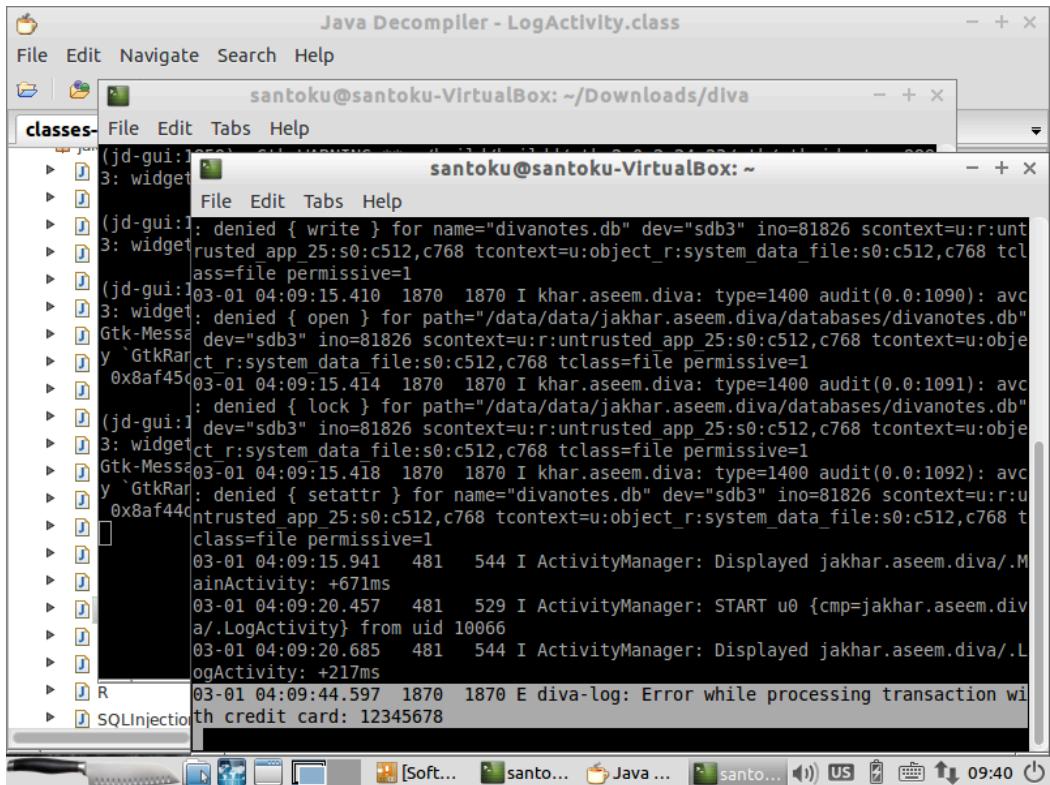
A screenshot of a Linux desktop environment, likely Kali Linux, showing a terminal window and a taskbar.

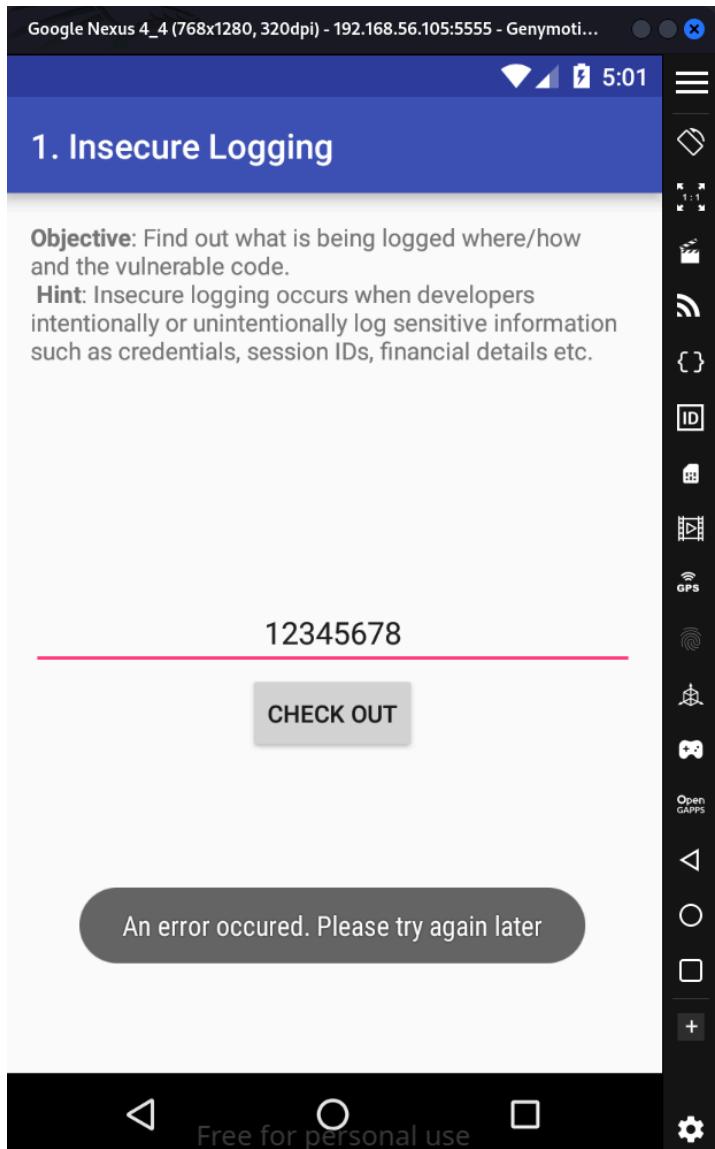
The terminal window title is "santoku@santoku-VirtualBox: ~/Downloads/diva". The terminal content shows the following command sequence:

```
santoku@santoku-VirtualBox:~/Downloads$ ls
diva diva-beta.apk
santoku@santoku-VirtualBox:~/Downloads$ cd diva
santoku@santoku-VirtualBox:~/Downloads/diva$ ls
AndroidManifest.xml classes.dex lib META-INF res resources.arsc
santoku@santoku-VirtualBox:~/Downloads/diva$ d2j-dex2jar classes.dex
dex2jar classes.dex -> classes-dex2jar.jar
santoku@santoku-VirtualBox:~/Downloads/diva$
```

The taskbar at the bottom includes icons for Software Updater, a terminal window labeled "santoku@santoku...", and system status indicators for battery, signal, and time (09:36).



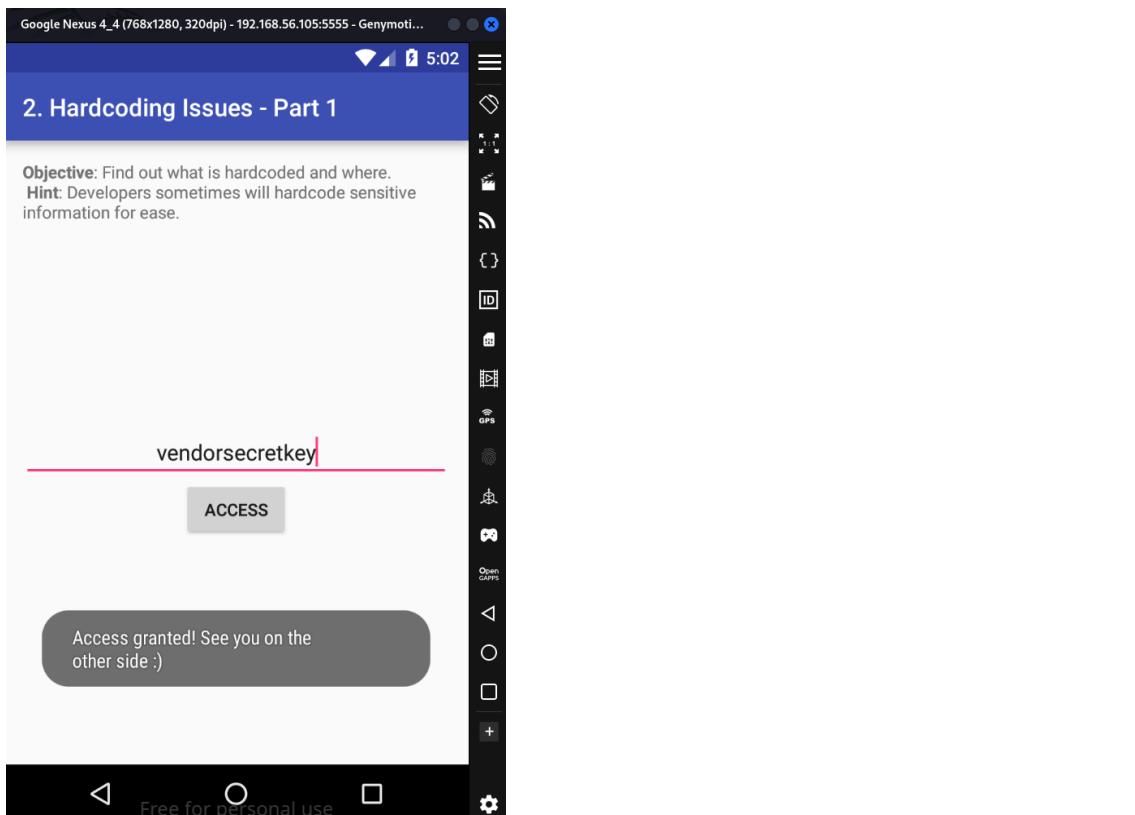




Hard Coding Issue – Vulnerability

The screenshot shows the JD-GUI Java decompiler interface. The left pane displays a tree view of the class hierarchy under 'classes-dex2jar.jar', including classes like APIcreds2Activity, APIcredsActivity, AccessControl1Activity, etc. The right pane shows the decompiled code for 'HardcodeActivity.class'. The code contains a hardcoded string 'vendorsecretkey' used for password verification.

```
java -jar jd-gui.jar classes-dex2jar.jar
File Edit Navigate Search Help
classes-dex2jar.jar HardcodeActivity.class
jakhar.aseem.diva;
android.os.Bundle;
class HardcodeActivity extends AppCompatActivity
    void access(View paramView)
        ((EditText)findViewById(2131492987)).getText().toString().equals("vendorsecretkey")
            toast.makeText(this, "Access granted! See you on the other side :)", 0).show();
        return;
    st.makeText(this, "Access denied! See you in hell :D", 0).show();
}
protected void onCreate(Bundle paramBundle)
    super.onCreate(paramBundle);
    setContentView(2130968607);
}
```



Insecure Data Storage (Shared Preference) –Vulnerability

The screenshot shows the JD-GUI Java decompiler interface. The left pane displays a tree view of class files from 'classes-dex2jar.jar', including API Creds2Activity, API CredsActivity, Access Control 1 Activity, Access Control 2 Activity, Access Control 3 Activity, Access Control 3 Notes Activity, BuildConfig, DivaJni, Hardcode 2 Activity, Hardcode Activity, Input Validation 2 URI Scan, Input Validation 3 Activity, InsecureDataStorage1Activity, InsecureDataStorage2Activity, InsecureDataStorage3Activity, InsecureDataStorage4Activity, LogActivity, MainActivity, NotesProvider, R, and SQLInjectionActivity. The right pane shows the source code for InsecureDataStorage1Activity.java:

```
package jakhar.aseem.diva;

import android.content.SharedPreferences;

public class InsecureDataStorage1Activity extends AppCompatActivity
{
    protected void onCreate(Bundle savedInstanceState)
    {
        super.onCreate(savedInstanceState);
        setContentView(2130968611);
    }

    public void saveCredentials(View paramView)
    {
        SharedPreferences.Editor localEditor = PreferenceManager.getDefaultSharedPreferences();
        EditText localEditText1 = (EditText)findViewById(2131493000);
        EditText localEditText2 = (EditText)findViewById(2131493001);
        localEditor.putString("user", localEditText1.getText().toString());
        localEditor.putString("password", localEditText2.getText().toString());
        localEditor.commit();
        Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
    }
}
```

The screenshot shows the JD-GUI Java decompiler interface with a terminal window integrated into the bottom pane. The terminal window shows the following session:

```
santoku@santoku-VirtualBox: ~/Downloads/diva
File Edit Tabs Help
(jd-gui:1250) [JD-GUI] > santoku@santoku-VirtualBox:~$ adb devices
3: widget
(jd-gui:1250) [JD-GUI] > santoku@santoku-VirtualBox:~$ adb shell
santoku@santoku-VirtualBox:~# cd /data/data
santoku@santoku-VirtualBox:~/data/data # ls
192.168.56.105:5555 device
santoku@santoku-VirtualBox:~/data/data # adb shell
santoku@santoku-VirtualBox:~/data/data # ls
0x8af45c android
0x8af45c android.ext.services
0x8af45c android.ext.shared
0x8af45c com.amaze.filemanager
0x8af45c com.android.backupconfirm
0x8af45c com.android.bips
0x8af45c com.android.bluetooth
0x8af45c com.android.bluetoothmidiservice
0x8af45c com.android.bookmarkprovider
0x8af45c com.android.calculator2
0x8af45c com.android.calendar
0x8af45c com.android.callogbackup
0x8af45c com.android.camera2
0x8af45c com.android.captiveportallogin
0x8af45c com.android.carrierconfig
0x8af45c com.android.carrierdefaultapp
0x8af45c com.android.cellbroadcastreceiver
```

Java Decomplier - InsecureDataStorage1Activity.class

File Edit Navigate Search Help

santoku@santoku-VirtualBox: ~/Downloads/diva

classes- > J

vbox86p:/ # cd /data/data
vbox86p:/data/data # cd jakhar.aseem.diva/
vbox86p:/data/data/jakhar.aseem.diva # ls
cache code cache databases lib shared_prefs
d shared_prefs/
vbox86p:/data/data/jakhar.aseem.diva/shared_prefs # ls
jakhar.aseem.diva_preferences.xml
vbox86p:/data/data/jakhar.aseem.diva/shared_prefs #

tSharedPr
;
g());
0).show()

SQLInjectionActivity

Java Decomplier - InsecureDataStorage1Activity.class

File Edit Navigate Search Help

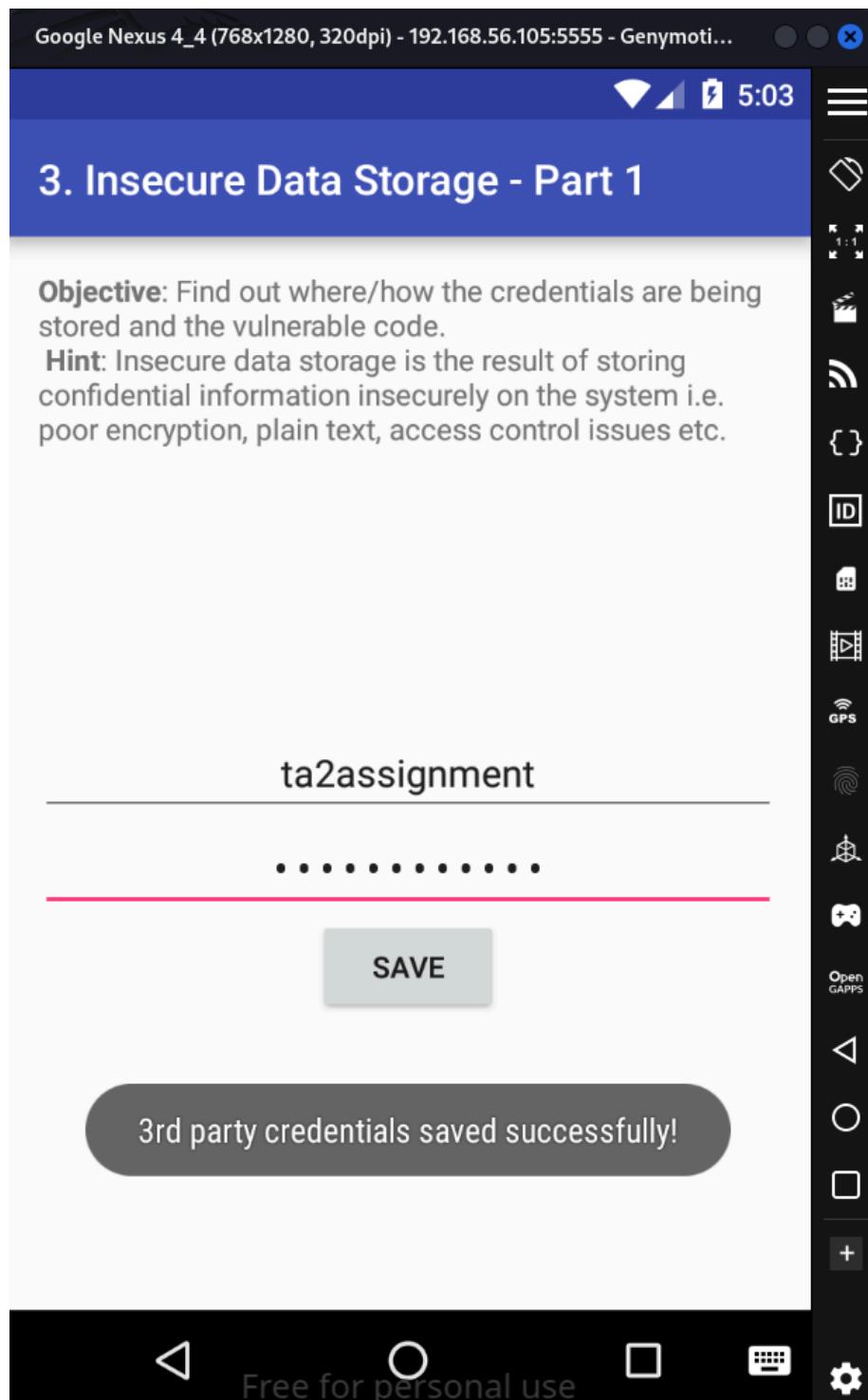
santoku@santoku-VirtualBox: ~/Downloads/diva

classes- > J

vbox86p:/ # cd /data/data
vbox86p:/data/data # cd jakhar.aseem.diva/
vbox86p:/data/data/jakhar.aseem.diva # ls
cache code cache databases lib shared_prefs
d shared_prefs/
vbox86p:/data/data/jakhar.aseem.diva/shared_prefs # ls
jakhar.aseem.diva_preferences.xml
at jakhar.aseem.diva_preferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<string name="password">practicalssss</string>
<string name="user">ta2assignment</string>
</map>
vbox86p:/data/data/jakhar.aseem.diva/shared_prefs #

tSharedPr
;
g());
0).show()

SQLInjectionActivity



Insecure Data Storage (SD Card) –Vulnerability

The screenshot shows a Java Decompiler interface with the title "Java Decompiler - InsecureDataStorage4Activity.class". Below the title is a menu bar with File, Edit, Navigate, Search, and Help. A toolbar with icons for file operations is visible. The main area displays a terminal window titled "santoku@santoku-VirtualBox: ~". The terminal shows the following command-line session:

```
vbox86p:/ # cd mnt  
vbox86p:/mnt # cd sdcard  
vbox86p:/mnt/sdcard # ls -al  
total 100  
drwxrwx--x 12 root sdcard_rw 4096 2025-03-01 04:27 .  
drwx--x--x 4 root sdcard_rw 4096 2025-01-24 05:31 ..  
-rw-rw---- 1 root sdcard_rw 8 2025-03-01 04:27 .uinfo.txt  
drwxrwx--x 2 root sdcard_rw 4096 2025-01-24 05:31 Alarms  
drwxrwx--x 3 root sdcard_rw 4096 2025-01-24 05:31 Android  
drwxrwx--x 2 root sdcard_rw 4096 2025-02-26 02:48 DCIM  
drwxrwx--x 2 root sdcard_rw 4096 2025-01-24 05:31 Download  
drwxrwx--x 2 root sdcard_rw 4096 2025-01-24 05:31 Movies  
drwxrwx--x 2 root sdcard_rw 4096 2025-01-24 05:31 Music  
drwxrwx--x 2 root sdcard_rw 4096 2025-01-24 05:31 Notifications  
drwxrwx--x 2 root sdcard_rw 4096 2025-01-24 05:31 Pictures  
drwxrwx--x 2 root sdcard_rw 4096 2025-01-24 05:31 Podcasts  
drwxrwx--x 2 root sdcard_rw 4096 2025-01-24 05:31 Ringtones  
vbox86p:/mnt/sdcard # cat .uinfo.txt  
123:123  
vbox86p:/mnt/sdcard #
```

The terminal window has a scroll bar on the right. The status bar at the bottom shows various icons and the time "09:58".

Insecure Data Storage (Temp File) –Vulnerability

The screenshot shows the Java Decompiler interface with the title "Java Decomplier - InsecureDataStorage3Activity.class". The left pane displays a tree view of the class hierarchy under "classes-dex2jar.jar", including classes like APIcreds2Activity, APIcredsActivity, AccessControl1Activity, etc. The right pane shows the decompiled code for InsecureDataStorage3Activity.class:

```
setContentView(2130968613);

public void saveCredentials(View paramView)
{
    EditText localEditText1 = (EditText)findViewById(2131493006);
    EditText localEditText2 = (EditText)findViewById(2131493007);
    File localFile1 = new File(getApplicationContext().dataDir);
    try
    {
        File localFile2 = File.createTempFile("userinfo", "tmp", localFile1);
        localFile2.setReadable(true);
        localFile2.setWritable(true);
        FileWriter localFileWriter = new FileWriter(localFile2);
        localFileWriter.write(localEditText1.getText().toString() + ":" + localEditText2.getText().toString());
        localFileWriter.close();
        Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
        return;
    }
    catch (Exception localException)
    {
        Toast.makeText(this, "File error occurred", 0).show();
        Log.d("Diva", "File error: " + localException.getMessage());
    }
}
```

The screenshot shows the Java Decompiler interface with the title "Java Decomplier - InsecureDataStorage3Activity.class". The left pane shows the class hierarchy. The right pane shows the decompiled code for InsecureDataStorage3Activity.class. A terminal window is open in the background, showing the following command and output:

```
vbox86p:/ # cd /data/data
vbox86p:/data/data # cd jakhar.aseem.diva/
vbox86p:/data/data/jakhar.aseem.diva # ls
Acache code cache databases lib shared_prefs userinfo2575623383759548244tmp
dat userinfo2575623383759548244tmp
data2assignment:practicalssss
vbox86p:/data/data/jakhar.aseem.diva #
```

5:04

5. Insecure Data Storage - Part 3

Objective: Find out where/how the credentials are being stored and the vulnerable code.

Hint: Insecure data storage is the result of storing confidential information insecurely on the system i.e. poor encryption, plain text, access control issues etc.

ta2assignment

• • • • • • • •

SAVE



Free for personal use



Insecure Data Storage (SQLLight Database) –Vulnerability

The screenshot shows the JD-GUI Java decompiler interface. The left pane displays a tree view of the class hierarchy under 'classes-dex2jar.jar'. The right pane shows the source code for the `InsecureDataStorage2Activity` class.

```
package jakhar.aseem.diva;

import android.database.sqlite.SQLiteDatabase;

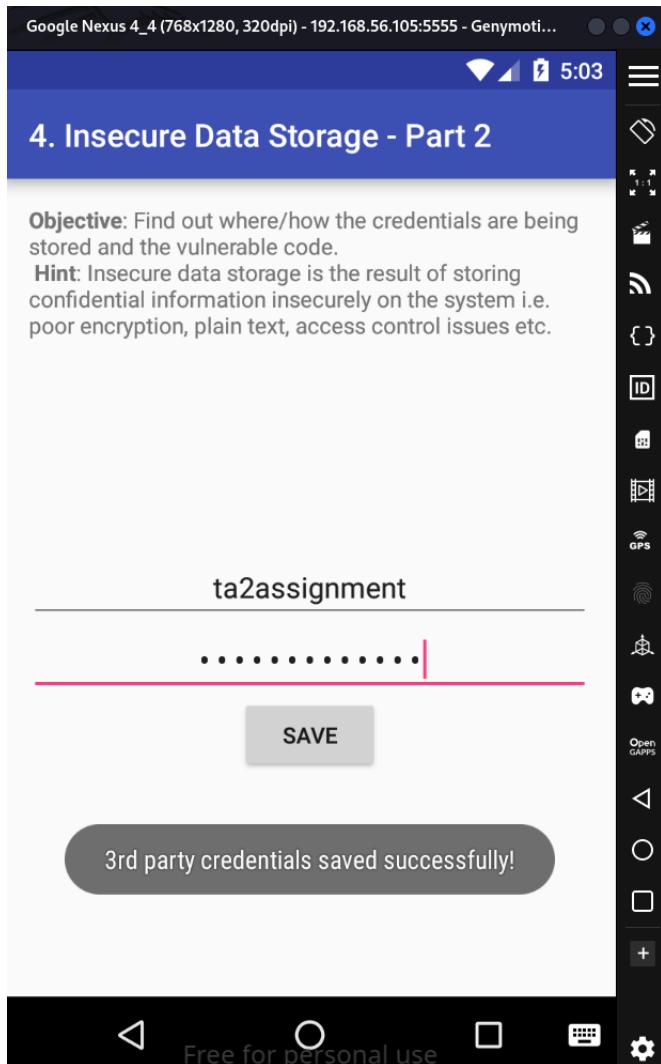
public class InsecureDataStorage2Activity extends AppCompatActivity
{
    private SQLiteDatabase mDB;

    protected void onCreate(Bundle savedInstanceState)
    {
        super.onCreate(savedInstanceState);
        try
        {
            this.mDB = openOrCreateDatabase("ids2", 0, null);
            this.mDB.execSQL("CREATE TABLE IF NOT EXISTS myuser(user VARCHAR, password VARCHAR);");
            setContentView(2130968612);
            return;
        }
        catch (Exception localException)
        {
            while (true)
                Log.d("Div", "Error occurred while creating database: " + localException);
        }
    }
}
```

The screenshot shows the JD-GUI Java decompiler interface with a terminal window open. The terminal window displays a Linux shell session where the user navigates to the application's data directory and runs an SQLite command to select from a table named 'myuser'.

```
santoku@santoku-VirtualBox:~
```

```
Vbox86p:/ # cd /data/data
Vbox86p:/data/data # cd jakhar.aseem.diva/
Vbox86p:/data/data/jakhar.aseem.diva # ls
cache code databases lib shared_prefs
Vbox86p:/data/data/jakhar.aseem.diva # cd databases/
Vbox86p:/data/data/jakhar.aseem.diva/databases # ls
divanotes.db divanotes.db-journal ids2 ids2-journal
Vbox86p:/data/data/jakhar.aseem.diva/databases # cd ids2
/Vbox86p:/data/data/jakhar.aseem.diva/databases/ids2: Not a directory
/Vbox86p:/data/data/jakhar.aseem.diva/databases # sqlite3 ids2
SQLite version 3.18.2 2017-07-21 07:56:09
Enter ".help" for usage hints.
sqlite> .tables
android_metadata myuser
sqlite> select * from myuser;
ta2assignment|practicalssss
sqlite>
```



Input Validation and Data Sanitization (SQLInjection) – Vulnerability

The screenshot shows the Java Decomiler interface with the file `SQLInjectionActivity.class` open. The code reveals a SQL injection vulnerability where user input is directly inserted into an SQL query without proper sanitization.

```
package jakhar.aseem.diva;

import android.database.Cursor;

public class SQLInjectionActivity extends AppCompatActivity
{
    private SQLiteDatabase mDB;

    protected void onCreate(Bundle savedInstanceState)
    {
        super.onCreate(savedInstanceState);
        try
        {
            this.mDB = openOrCreateDatabase("sqli", 0, null);
            this.mDB.execSQL("DROP TABLE IF EXISTS sqliuser;");
            this.mDB.execSQL("CREATE TABLE IF NOT EXISTS sqliuser(user VARCHAR, pass VARCHAR);");
            this.mDB.execSQL("INSERT INTO sqliuser VALUES ('admin', 'passwd123', '123')");
            this.mDB.execSQL("INSERT INTO sqliuser VALUES ('diva', 'p@ssword', '111')");
            this.mDB.execSQL("INSERT INTO sqliuser VALUES ('john', 'password123', '123')");
            setContentView(R.layout.activity_main);
        }
        catch (Exception localException)
        {
        }
    }
}
```

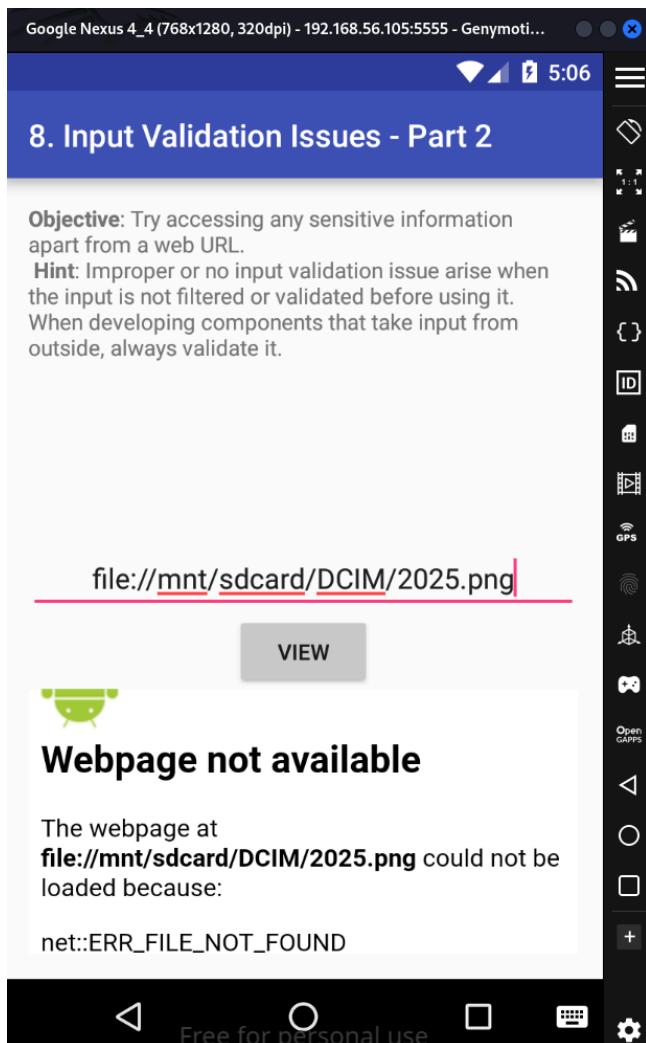
The screenshot shows the Java Decomiler interface with the file `SQLInjectionActivity.class` open. Below it, a terminal window displays the results of a database query, showing three entries: 'admin', 'passwd123', '123'; 'diva', 'p@ssword', '111'; and 'john', 'password123', '123'.

```
santoku@santoku-VirtualBox: ~
vbox86p:/ # cd mnt
vbox86p:/mnt # cd sdcard
vbox86p:/mnt/sdcard # ls
Alarms DCIM Movies Notifications Podcasts
Android Download Music Pictures Ringtones
vbox86p:/mnt/sdcard # cd DCIM
vbox86p:/mnt/sdcard/DCIM # ls
2025-02-26-074109_800x600 scrot.png
vbox86p:/mnt/sdcard/DCIM #
```

Terminal Output (partial):

```
AR, pass
23', '1
', '11
123', '
```

Input Validation and Data Sanitization (WebView) – Vulnerability



Access Control Issue – Vulnerability

The screenshot shows the Java Decomplier interface with the file `AccessControl1Activity.class` open. The code implements an `onCreate` method and a `viewAPICredentials` method. The `viewAPICredentials` method creates an intent with action `"jakhar.aseem.diva.action.VIEW_CREDS"` and starts an activity if it can resolve it.

```
package jakhar.aseem.diva;

import android.content.Intent;

public class AccessControl1Activity extends AppCompatActivity
{
    protected void onCreate(Bundle savedInstanceState)
    {
        super.onCreate(savedInstanceState);
        setContentView(2130968601);
    }

    public void viewAPICredentials(View paramView)
    {
        Intent localIntent = new Intent();
        localIntent.setAction("jakhar.aseem.diva.action.VIEW_CREDS");
        if (localIntent.resolveActivity(getApplicationContext()) != null)
        {
            startActivity(localIntent);
            return;
        }
        Toast.makeText(this, "Error while getting API details", 0).show();
        Log.e("Diva-acil", "Couldn't resolve the Intent VIEW_CREDS to our activit");
    }
}
```

The screenshot shows the Java Decomplier interface with the file `santoku@anteku-VirtualBox: ~/Downloads` open. It displays the command `santoku@anteku-VirtualBox:~/Downloads$ apktool d diva-beta.apk` and its output. The output shows an exception being thrown due to an ARSC file decoding issue, specifically related to the `getResTable` method in `AndrolibResources`.

```
santoku@anteku-VirtualBox:~/Downloads$ apktool d diva-beta.apk
I: Baksmaling...
I: Loading resource table...
E: Exception in thread "main" brut.androlib.AndrolibException: Could not decode arsc file
    at brut.androlib.res.decoder.ARSCDecoder.decode(ARSCDecoder.java:56)
    at brut.androlib.res.AndrolibResources.getResPackagesFromApk(AndrolibResources.java:491)
    at brut.androlib.res.AndrolibResources.loadMainPkg(AndrolibResources.java:74)
    at brut.androlib.res.AndrolibResources.getResTable(AndrolibResources.java:66)
    at brut.androlib.Androlib.getResTable(Androlib.java:50)
    at brut.androlib.ApkDecoder.getResTable(ApkDecoder.java:189)
    at brut.androlib.ApkDecoder.decode(ApkDecoder.java:114)
    at brut.apktool.Main.cmdDecode(Main.java:146)
    at brut.apktool.Main.main(Main.java:77)
Caused by: java.io.IOException: Expected: 0x001c0001, got: 0x00000000
    at brut.util.ExtDataInput.skipCheckInt(ExtDataInput.java:48)
    at brut.androlib.res.decoder.StringBlock.read(StringBlock.java:44)
    at brut.androlib.res.decoder.ARSCDecoder.readPackage(ARSCDecoder.java:102)
    at brut.androlib.res.decoder.ARSCDecoder.readTable(ARSCDecoder.java:83)
```

```
santoku@santoku-VirtualBox: ~/Downloads/diva-beta/smali
```

```
File Edit Tabs Help
```

```
Santoku@santoku-VirtualBox:~/Downloads$ ls
diva  diva-beta  diva-beta.apk
Santoku@santoku-VirtualBox:~/Downloads$ cd diva-beta/
Santoku@santoku-VirtualBox:~/Downloads/diva-beta$ ls
smali
Santoku@santoku-VirtualBox:~/Downloads/diva-beta$ cd smali
Santoku@santoku-VirtualBox:~/Downloads/diva-beta/smali$ ls
android  jakhar
Santoku@santoku-VirtualBox:~/Downloads/diva-beta/smali$
```

Java Decomplier - AccessControl1Activity.class

File Edit Navigate Search Help

classes-dex2jar.jar santoku@ santoku-VirtualBox: ~

```
dialer
Find suid/sgid binaries in the given folder (default is /system).

scanner.misc.sflagbinaries
Find world-writable files in the given folder

scanner.provider.finduris
Search for content providers that can be queried from our context.

scanner.provider.injection
Test content providers for SQL injection vulnerabilities.

scanner.provider.sqltables
Find tables accessible through SQL injection vulnerabilities.

scanner.provider.traversal
Test content providers for basic directory traversal vulnerabilities.

shell.exec
Execute a single Linux command.

shell.send
Send an ASH shell to a remote listener.

shell.start
Enter into an interactive Linux shell.

tools.file.download
Download a File

tools.file.md5sum
Get md5 Checksum of file

tools.file.size
Get size of file

tools.file.upload
Upload a File

tools.setup.busybox
Install Busybox.

tools.setup.minimalsu
Prepare 'minimal-su' binary installation on the device.

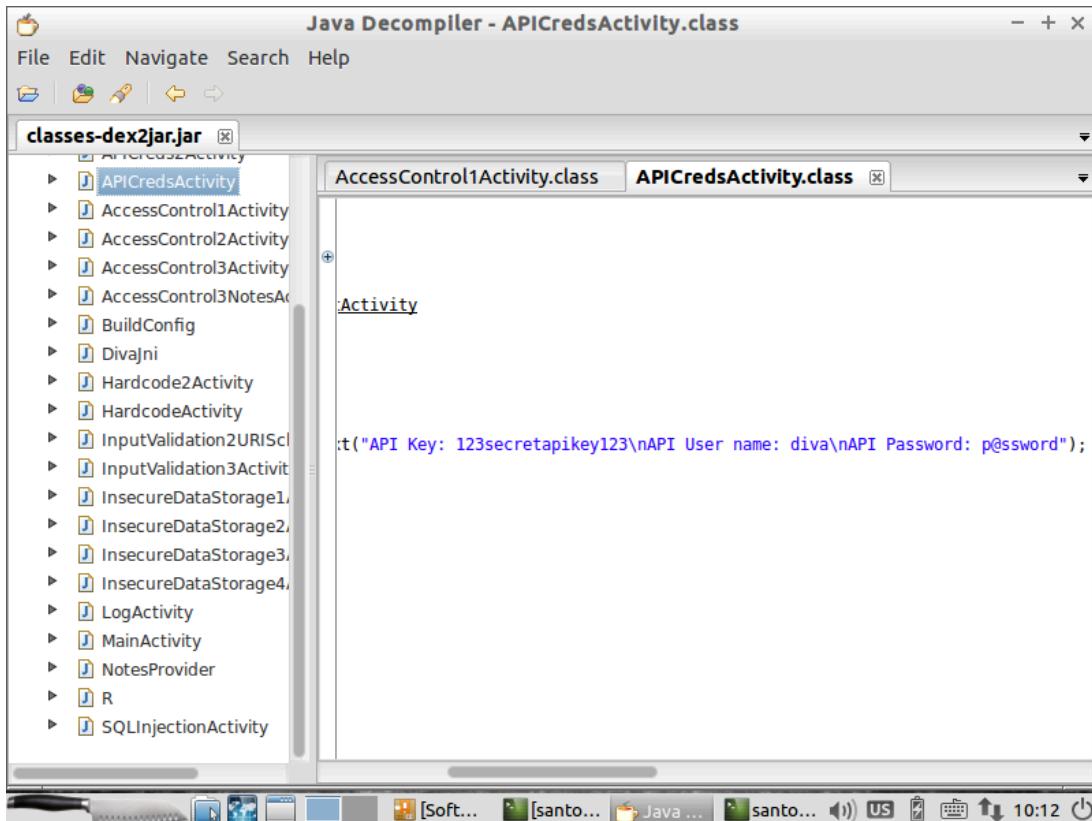
dz> run app.package.manifest jakhar.aseem.diva
```

Java Decomplier - AccessControl1Activity.class

File Edit Navigate Search Help

classes-dex2jar.jar santoku@ santoku-VirtualBox: ~

```
<activity label="@2131099688"
    name="jakhar.aseem.diva.AccessControl2Activity">
</activity>
<activity label="@2131099681"
    name="jakhar.aseem.diva.APICreds2Activity">
    <intent-filter>
        <action name="jakhar.aseem.diva.action.VIEW_CREDS2">
        </action>
        <category name="android.intent.category.DEFAULT">
        </category>
    </intent-filter>
</activity>
<provider name="jakhar.aseem.diva.NotesProvider"
    enabled="true"
    exported="true"
    authorities="jakhar.aseem.diva.provider.notesprovider">
</provider>
<activity label="@2131099689"
    name="jakhar.aseem.diva.AccessControl3Activity">
</activity>
<activity label="@2131099690"
    name="jakhar.aseem.diva.Hardcode2Activity">
</activity>
<activity label="@2131099723"
```



The screenshot shows the Java Decomplier interface with the title "Java Decomplier - AccessControl1Activity.class". The left pane displays a tree view of the class hierarchy under "classes-dex2jar.jar", including classes like AccessControl1Activity, AccessControl2Activity, and AccessControl3Activity. The right pane shows the decompiled code for AccessControl1Activity.class:

```
santoku@santoku-VirtualBox: ~/Downloads/diva-beta
File Edit Tabs Help
santoku@santoku-VirtualBox:~/Downloads/diva-beta$ adb forward tcp:31415 tcp:31415
santoku@santoku-VirtualBox:~/Downloads/diva-beta$ drozer console connect
>Selecting a8291d93fd50d8a7 (unknown unknown 8.0.0)
A
B
C
D
E
F
G
H
I
J
K
L
M
N
drozer Console (v2.3.3)
dz> [REDACTED]
```

Java Decomplier - AccessControl2Activity.class

File Edit Navigate Search Help

classes-dex2jar.jar

```
public class AccessControl2Activity extends AppCompatActivity
{
    protected void onCreate(Bundle paramBundle)
    {
        super.onCreate(paramBundle);
        setContentView(2130968602);
    }

    public void viewAPICredentials(View paramView)
    {
        RadioButton localRadioButton = (RadioButton)findViewById(2131492973);
        Intent localIntent = new Intent();
        boolean bool = localRadioButton.isChecked();
        localIntent.setAction("jakhar.aseem.diva.action.VIEW_CREDS2");
        localIntent.putExtra(getString(2131099686), bool);
        if (localIntent.resolveActivity(getApplicationContext()) != null)
        {
            startActivity(localIntent);
            return;
        }
        Toast.makeText(this, "Error while getting Tweeter API details", 0).show();
        Log.e("Div-a-cil", "Couldn't resolve the Intent VIEW_CREDS2 to our activi");
    }
}
```

[Soft... [santo... Java ... santo... 10:20]

Java Decomplier - APIcreds2Activity.class

File Edit Navigate Search Help

classes-dex2jar.jar

```
package jakhar.aseem.diva;

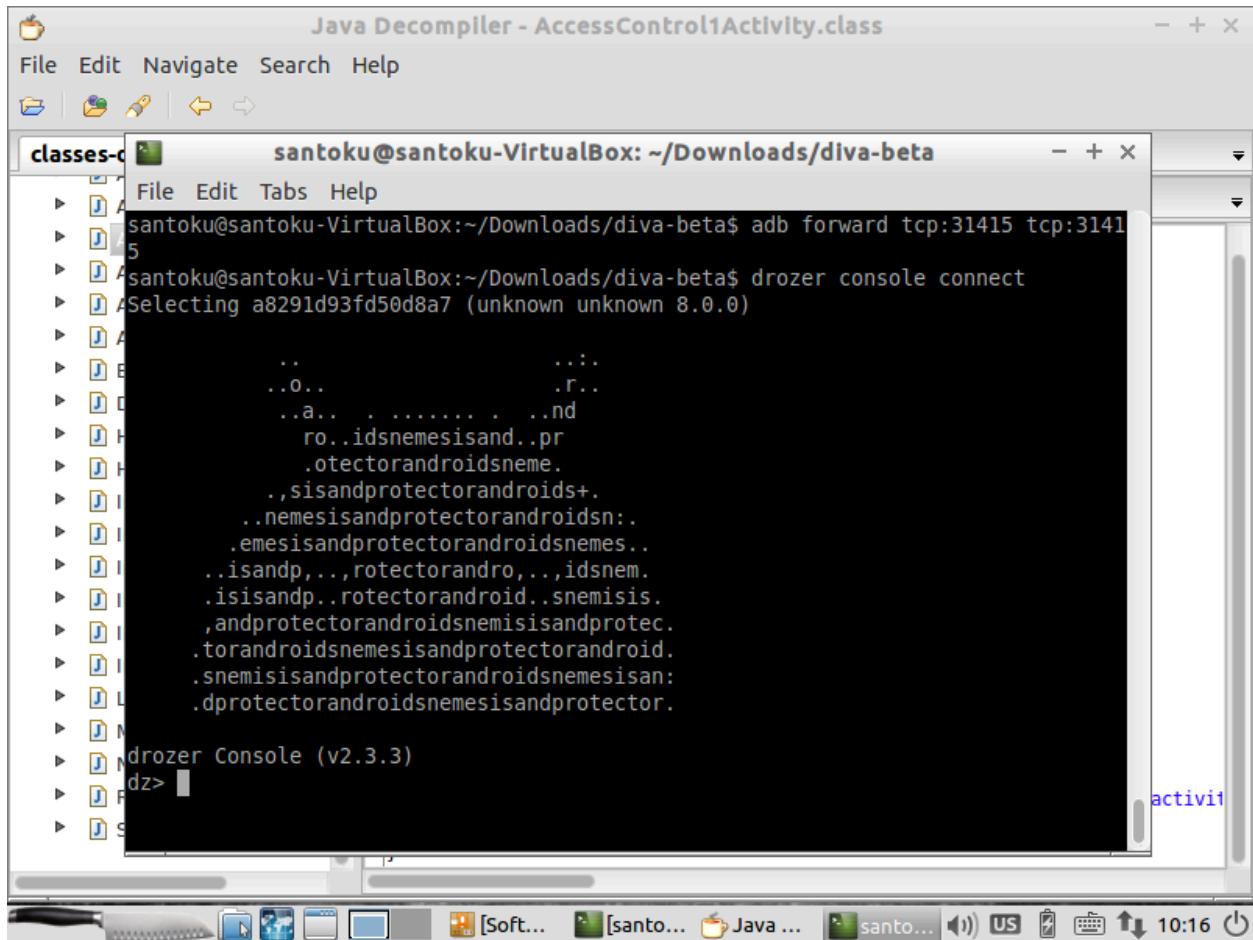
import android.content.Intent;

public class APIcreds2Activity extends AppCompatActivity
{
    protected void onCreate(Bundle paramBundle)
    {
        super.onCreate(paramBundle);
        setContentView(2130968606);
        TextView localTextView = (TextView)findViewById(2131492983);
        EditText localEditText = (EditText)findViewById(2131492984);
        Button localButton = (Button)findViewById(2131492985);
        if (!getIntent().getBooleanExtra(getString(2131099686), true))
        {
            localTextView.setText("TVEETER API Key: secrettveeterapikey\nAPI User r
            return;
        }
        localTextView.setText("Register yourself at http://payatu.com to get your
        localEditText.setVisibility(0);
        localButton.setVisibility(0);
    }

    public void viewCreds(View paramView)
}
```

[Soft... [santo... Java ... santo... 10:21]

Configuration of Drozer



Security Auditing of DIVA using Drozer

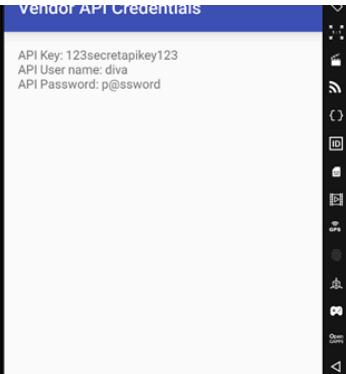
```
drozer Console (v3.1.0)
dz> run app.package.list -f diva
Attempting to run shell module
jakhar.aseem.diva (Divा)
dz> run app.package.attacksurface jakhar.aseem.diva
Attempting to run shell module
Attack Surface:
  3 activities exported
  0 broadcast receivers exported
  1 content providers exported
  0 services exported
    is debuggable
dz> |
```

```
z> run app.activity.info -a jakhar.aseem.diva
Attempting to run shell module
Package: jakhar.aseem.diva
  jakhar.aseem.diva.MainActivity
    Permission: null
  jakhar.aseem.diva.APICredsActivity
    Permission: null
  jakhar.aseem.diva.APICreds2Activity
    Permission: null

z> run app.activity.start --component jakhar.aseem.diva.APICre
sActivity
Attempting to run shell module
Exception occurred: argument --component: expected 2 arguments
z> run app.activity.start --component jakhar.aseem.diva jakhar
aseem.diva.APICredsActivity
.....
```

```
drozer Console (v3.1.0)
dz> run app.package.list -f diva
Attempting to run shell module
jakhar.aseem.diva (Divा)
dz> run app.package.attacksurface jakhar.aseem.diva
Attempting to run shell module
Attack Surface:
  3 activities exported
  0 broadcast receivers exported
  1 content providers exported
  0 services exported
    is debuggable
dz> run app.activity.info -a jakhar.aseem.diva
Attempting to run shell module
Package: jakhar.aseem.diva
  jakhar.aseem.diva.MainActivity
    Permission: null
  jakhar.aseem.diva.APICredsActivity
    Permission: null
  jakhar.aseem.diva.APICreds2Activity
    Permission: null

dz> run app.activity.start --component jakhar.aseem.diva.APICredsActivity
Attempting to run shell module
Exception occurred: argument --component: expected 2 arguments
dz> run app.activity.start --component jakhar.aseem.diva jakhar
aseem.diva.APICredsActivity
Attempting to run shell module
```



Security Auditing of Insecure Bank using Drozer



```
$ drozer console connect
Selecting 4284e90cbdb5d97e (unknown Nexus 4 7.0)

...
.o.. .r..
.a.. .nd
ro..idsnemesisand.pr
.otectorandrodnemis.
.sisandprotectorandrodnemis+.
.nemesisandprotectorandrodnemis:.
.emesisandprotectorandrodnemesis..
.isandp...rotocyayandro...idsnemis.
.isisandp..rotectorandroid..snemisis.
.andprotectorandrodnemesisandprotec.
.torandrodnemesisandprotectorandrodnemis.
.snemisisandprotectorandrodnemesisan:.
.dprotectorandrodnemesisandprotector.

drozer Console (v3.1.0)
z> run app.package.list -f bank
Attempting to run shell module
com.android.insecurebankv2 (InsecureBankv2)
z> run app.activity.info -a com.android.insecurebankv2
Attempting to run shell module
Package: com.android.insecurebankv2
    com.android.insecurebankv2 LoginActivity
        Permission: null
    com.android.insecurebankv2.PostLogin
        Permission: null
    com.android.insecurebankv2.DoTransfer
        Permission: null
    com.android.insecurebankv2.ViewStatement
        Permission: null
    com.android.insecurebankv2.ChangePassword
        Permission: null

z> |
```

Security Auditing of OWASP GoatDroid using Drozer



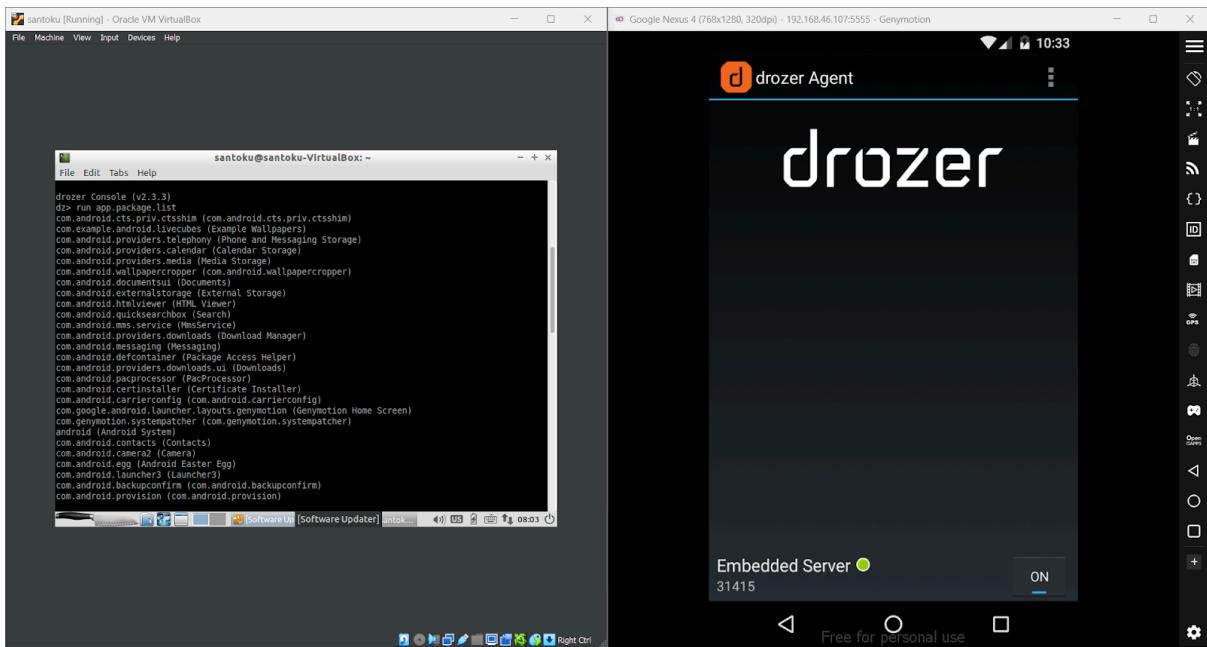
```
(nobbie@LAPTOP-0SQU21D0)-[~]
$ drozer console connect
Selecting 4284e90cbdb5d97e (unknown Nexus 4 7.0)

...
.o.. .r..
.a.. .nd
ro..idsnemesisand.pr
.otectorandrodnemis.
.sisandprotectorandrodnemis+.
.nemesisandprotectorandrodnemis:.
.emesisandprotectorandrodnemesis..
.isandp...rotocyayandro...idsnemis.
.isisandp..rotectorandroid..snemisis.
.andprotectorandrodnemesisandprotec.
.torandrodnemesisandprotectorandrodnemis.
.snemisisandprotectorandrodnemesisan:.
.dprotectorandrodnemesisandprotector.

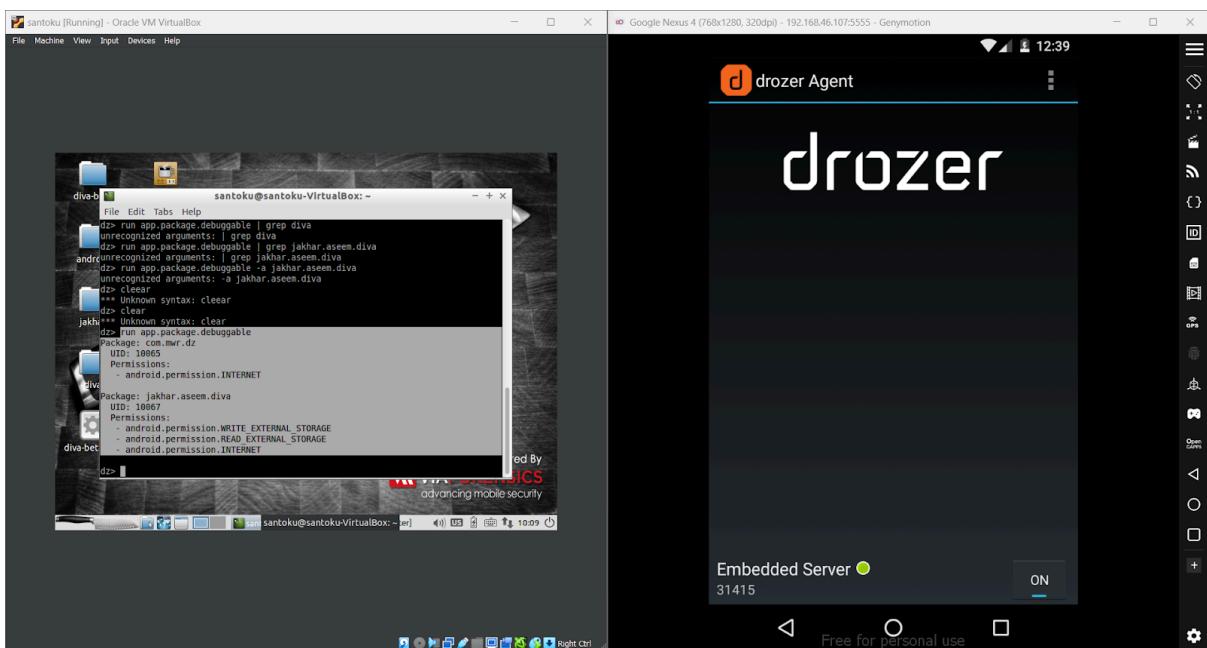
drozer Console (v3.1.0)
dz> run app.package.list -f goat
Attempting to run shell module
org.owasp.goatdroid.fourgoats (FourGoats)
dz> run app.activity.info -a org.owasp.goatdroid.fourgoats
Attempting to run shell module
Package: org.owasp.goatdroid.fourgoats
    org.owasp.goatdroid.fourgoats.activities.Main
        Permission: null
    org.owasp.goatdroid.fourgoats.activities.ViewCheckin
        Permission: null
    org.owasp.goatdroid.fourgoats.activities.ViewProfile
        Permission: null
    org.owasp.goatdroid.fourgoats.activities.SocialAPIAuthentication
        Permission: null

dz> |
```

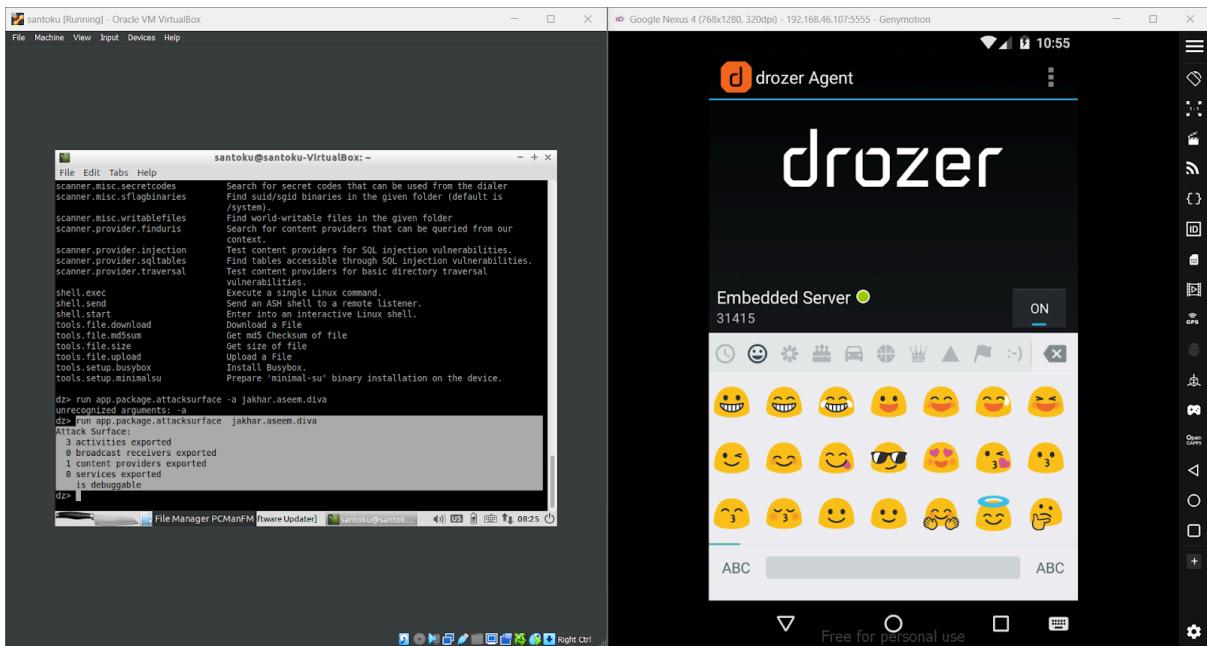
Package listing of android app using app.package.list



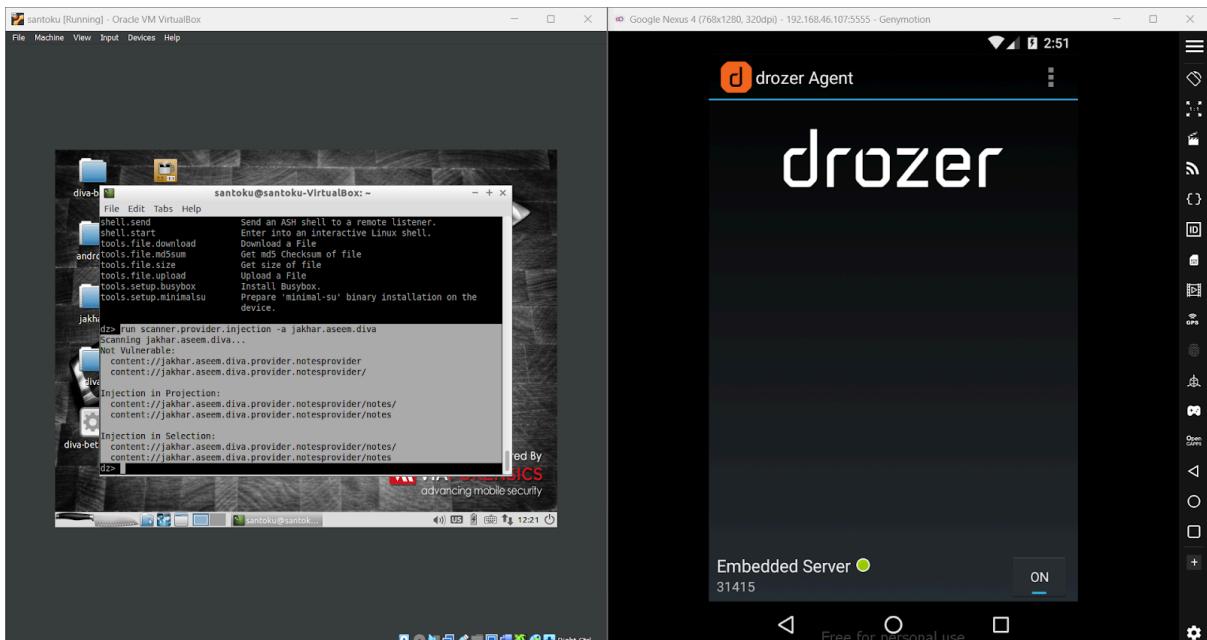
Find Debuggable android application

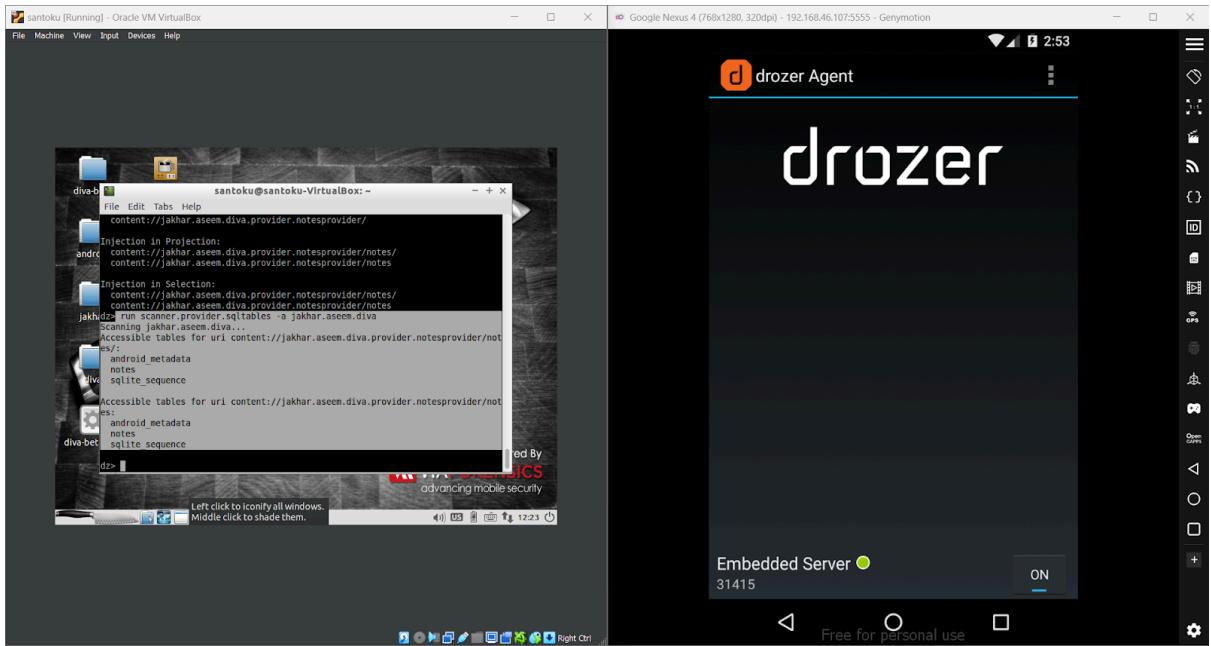


Find attack surface of DIVA



SQL Injection Vulnerability of DIVA using Drozer Modules





Configuration of MobSF (Mobile Security Framework)

Windows PowerShell

```

PS D:\Mobile-Security-Framework-MobSF-master\Mobile-Security-Framework-MobSF-master> .\run.bat 127.0.0.1:8080
Running MobSF on 127.0.0.1:8080
[INFO] 09/Apr/2025 11:34:37 - Loading User config from: C:/Users/MSCS/.MobSF/config.py
[INFO] 09/Apr/2025 11:34:54 -

```

MobSF Dynamic Analysis

MobSF Dynamic Analyzer Supports

- Genymotion Android VM version 4.1 - 11.0 (arm64, x86, and x86_64 upto API 30)
- Android Emulator AVD (non production) version 5.0 - 11.0 (arm, arm64, x86, and x86_64 upto API 30)
- Corelium Android VM (userdebug builds) version 7.1.2 - 11.0 (arm64 upto API 30)

Android version >= 9.0 recommended
Detected Android Version: 8.0, SDK API level 28
Android Instance: 192.168.211.105:5555

APP	LOCATION IN DEVICE	ACTION
com.mwr.dz	/data/app/com.mwr.dz-xuPDIFXACK3KdzEuQkka9A==/base.apk	Start Dynamic Analysis Build & Static Analysis View Report
com.withsecure.example.sieve	/data/app/com.withsecure.example.sieve-x14tSpKrtlmsy2lDz78A==/base.apk	Start Dynamic Analysis Build & Static Analysis View Report
jakhar.aseem.diva	/data/app/jakhar.aseem.diva-1P8dA3BLCP5o4x9t1dw==/base.apk	Start Dynamic Analysis Build & Static Analysis

Security Auditing using MobSF (Mobile Security Framework)

The screenshot shows the MobSF web application interface. On the left, there's a sidebar with various analysis options like Static Analyzer, Scan Options, Signer Certificate, Permissions, and Dynamic Analysis. The main area is titled 'FILE INFORMATION' and shows details about an APK file named 'a2-beta.apk'. It lists several SHA-1 hash entries. Below this are four summary cards: 'EXPORTED ACTIVITIES' (2/17), 'EXPORTED SERVICES' (0/0), 'EXPORTED RECEIVERS' (0/0), and 'EXPORTED PROVIDERS' (1/1). Further down are sections for 'SCAN OPTIONS' (with tabs for Device, Storage Scanning, and Dynamic Analysis) and 'DECOMPRESSED CODE' (with links to view decompiled Java, XML, and API code). At the bottom is a 'SIGNER CERTIFICATE' section detailing the certificate's signature status and expiration information.

Configuration of Frida

```
[(nobbie@LAPTOP-0SQU2TDO)-[~/Mobile-Security-Framework-MobSF]]$ pip install frida-tools --break-system
Collecting frida-tools
  Downloading frida-tools-13.6.1.tar.gz (4.6 MB)
    4.6/4.6 MB 522.5 kB/s eta 0:00:00
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
  collecting colorama<1.0.0,>=0.2.7 (from frida-tools)
    Downloading colorama-0.4.6-py2.py3-none-any.whl.metadata (17 kB)
  collecting frida<17.0.0,>=16.2.2 (from frida-tools)
    Downloading frida-16.7.9-cp37abi3-manylinux_2_5_x86_64.whl.metadata (2.3 kB)
  collecting prompt_toolkit<0.0.0,>=2.0.0 (from frida-tools)
    Downloading prompt_toolkit-3.0.50-py3-none-any.whl.metadata (6.6 kB)
  collecting pygments<3.0.0,>=2.0.0 (from frida-tools)
    Downloading pygments-2.19.1-py3-none-any.whl.metadata (2.5 kB)
  collecting websockets<13.1-cp312-cp312-manylinux_2_5_x86_64.manylinux1_x86_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (6.8 kB)
  collecting wcwidth (from prompt-toolkit<4.0.0,>=2.0.0->frida-tools)
    Downloading wcwidth-0.2.13-py2.py3-none-any.whl.metadata (14 kB)
  collecting colorama-0.4.6-py2.py3-none-any.whl (25 kB)
  downloading frida-16.7.9-cp37abi3-manylinux_2_5_x86_64.whl (30.3 MB)
    30.3/30.3 MB 164.6 kB/s eta 0:00:00
  downloading prompt_toolkit-3.0.50-py3-none-any.whl (1.2 MB)
    1.2/1.2 MB 176.9 kB/s eta 0:00:00
  downloading websockets-13.1-cp312-cp312-manylinux_2_5_x86_64.manylinux1_x86_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl (165 kB)
  downloading wcwidth-0.2.13-py2.py3-none-any.whl (34 kB)
  building wheels for collected packages: frida-tools
    Building wheel for frida-tools (pyproject.toml) ... done
    Created wheel for frida-tools: filename=frida_tools-13.6.1-py3-none-any.whl size=4639057 sha256=412b80463684f06b342b96352485eafb499caf21690ce9d5ea88786fd3842d87
  Stored in directory: /home/nobbie/.cache/pip/wheels/82/a1/77/421c5c5548e42558b8e86b4dbc2a9ca4f9721cd76b5385217f7
  successfully built frida-tools
  installing collected packages: wcwidth, websockets, pygments, prompt-toolkit, frida, colorama, frida-tools
  successfully installed colorama-0.4.6 frida-16.7.9 frida-tools-13.6.1 prompt-toolkit-3.0.50 pygments-2.19.1 wcwidth-0.2.13 websockets-13.1
```

Testing and Evaluation of Android App using Frida

```
(nobbie@LAPTOP-0SQU2TDO) [~/Mobile-Security-Framework-MobSF]
$ frida -U -n Diva

    /_ _\|  Frida 16.7.9 - A world-class dynamic instrumentation toolkit
   | ( )| |
 > _ _ _ Commands:
/_/_/_/_ help      -> Displays the help system
 . . . . object?   -> Display information about 'object'
 . . . . exit/quit -> Exit
 . . . .
 . . . . More info at https://frida.re/docs/home/
 . . . .
 . . . . Connected to Nexus 4 (id=192.168.242.102:5555)

[Nexus 4::Diva ]-> Java.perform(function () {
  var Log = Java.use("android.util.Log");
  Log.d.implementation = function(tag, msg) {
    console.log("🔥 Log.d called: " + tag + " → " + msg);
    return this.d(tag, msg);
  };
});
```

Dynamic Analysis using MobSF and Frida

Windows PowerShell

```
PS D:\Mobile-Security-Framework-MobSF-master\Mobile-Security-Framework-MobSF-master> \run.bat 127.0.0.1:8800
Running MobSF on 127.0.0.1:8800
[INFO] 09/Apr/2025 11:34:37 - Loading User config from: C:/Users/MSCS/.MobSF/config.py
[INFO] 09/Apr/2025 11:34:54 -
```

Frida 16.7.9 - A world-class dynamic instrumentation toolkit

Commands:

- help -> Displays the help system
- object? -> Display information about 'object'
- exit/quit -> Exit

More info at <https://frida.re/docs/home/>

Connected to Nexus 4 (id=192.168.242.102:5555)

[Nexus 4::Diva]-> Java.perform(function () {
 var Log = Java.use("android.util.Log");
 Log.d.implementation = function(tag, msg) {
 console.log("🔥 Log.d called: " + tag + " → " + msg);
 return this.d(tag, msg);
 };});

MobSF Dynamic Analyzer Supports

- Genymotion Android VM version 4.1 - 11.0 (arm64, x86, and x86_64 upto API 30)
- Android Emulator AVD (non production) version 5.0 - 11.0 (arm, arm64, x86, and x86_64 upto API 30)
- Corelium Android VM (userdebug builds) version 7.1.2 - 11.0 (arm64 upto API 30)

Android version → 9.0 recommended
Detected Android Version: 9.0, SDK: API level 28

MobSF Dynamic Analysis

Apps in Device

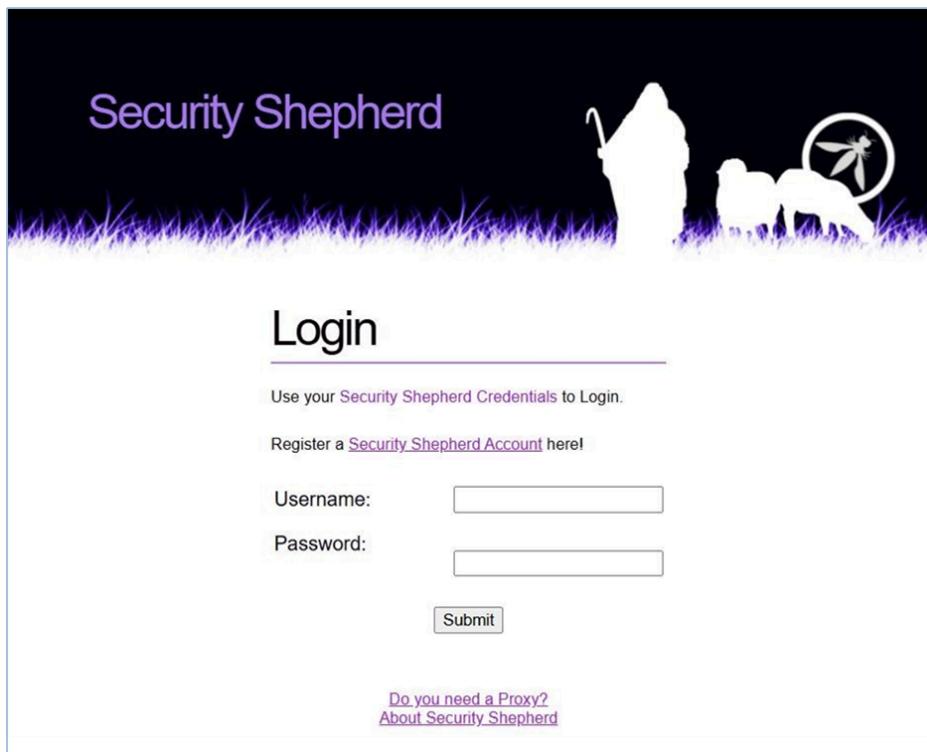
APP	LOCATION IN DEVICE	ACTION
com.mwr.dz	/data/app/com.mwr.dz-xuPDFXACK3kdxEuQkk94==/base.apk	Start Dynamic Analysis Pull & Static Analysis View Report
com.withsecure.example.sieve	/data/app/com.withsecure.example.sieve-XIVSp2Krtlmsy2qD0u78A==/base.apk	Start Dynamic Analysis Pull & Static Analysis View Report
jakhar.aseem.diva	/data/app/jakhar.aseem.diva-1P8dA3B1cP5o4x9t1dw==/base.apk	Start Dynamic Analysis Pull & Static Analysis View Report

```

[INFO] 09/Apr/2025 11:34:54 - Author: Ajin Abraham | opensecurity.in
[INFO] 09/Apr/2025 11:34:54 - Mobile Security Framework v3.3.2
[REST API] Key: b3bbP77c02518009749a2501586ad4c7e7dd6aa21b6ea51ea208d0896025a0
Default Credentials: mobsf/mobsf
[INFO] 09/Apr/2025 11:34:54 - OS Environment: Windows Windows-11-10.0.22631-SP0
[INFO] 09/Apr/2025 11:34:54 - CPU Cores: 6, Threads: 12, RAM: 31.78 GB
[INFO] 09/Apr/2025 11:34:54 - MobsF Basic Environment Check
[INFO] 09/Apr/2025 11:34:54 - Checking for Update
[INFO] 09/Apr/2025 11:34:55 - No updates available.
[INFO] 09/Apr/2025 11:34:55 - Connected to Android 192.168.211.105:5555
[INFO] 09/Apr/2025 11:36:00 - Waiting for 2 seconds
[INFO] 09/Apr/2025 11:39:58 - Creating Dynamic Analysis Environment for jakhar.assem.diva
[WARNING] 09/Apr/2025 11:39:59 - Failed to get Activities/Deeplinks. Static Analysis not completed for the app.
[INFO] 09/Apr/2025 11:40:04 - ADB Restarted
[INFO] 09/Apr/2025 11:40:04 - Waiting for 2 seconds...
[INFO] 09/Apr/2025 11:40:06 - Connecting to Android 192.168.211.105:5555
[INFO] 09/Apr/2025 11:40:06 - Waiting for 2 seconds...
[INFO] 09/Apr/2025 11:40:08 - Restarting ADB Daemon as root
[INFO] 09/Apr/2025 11:40:08 - Waiting for 2 seconds...
[INFO] 09/Apr/2025 11:40:10 - Reconnecting to Android Device
[INFO] 09/Apr/2025 11:40:10 - Waiting for 2 seconds...
[INFO] 09/Apr/2025 11:40:12 - Performing System Automation Android VM
[INFO] 09/Apr/2025 11:40:13 - Resuming...
[INFO] 09/Apr/2025 11:40:13 - Performing System check
[INFO] 09/Apr/2025 11:40:13 - Android API Level Identified as 28
[INFO] 09/Apr/2025 11:40:13 - Android Version Identified as 9.0
[INFO] 09/Apr/2025 11:40:13 - Environment MobsFyed Check
[INFO] /system/mobsf-f: No such file or directory
[WARNING] 09/Apr/2025 11:40:13 - This Android instance is not MobsFyed/Outdated.
MobsFyng the android runtime environment
[INFO] 09/Apr/2025 11:40:13 - Android Version Identified as 9.0
[INFO] 09/Apr/2025 11:40:13 - Android OS architecture Identified as x86
[INFO] 09/Apr/2025 11:40:14 - Downloading binary frida-server-16.7.9-android-x86
[INFO] 09/Apr/2025 11:40:14 - Copying frida-server for x86
[INFO] 09/Apr/2025 11:40:14 - Installing RootCA
[INFO] 09/Apr/2025 11:40:51 - MobsFyng Completed!
[INFO] 09/Apr/2025 11:40:52 - Installing MobsF RootCA
[INFO] 09/Apr/2025 11:40:52 - Starting HTTPS Proxy on 1337
[INFO] 09/Apr/2025 11:41:23 - Enabling ADB Reverse TCP on 1337
[INFO] 09/Apr/2025 11:41:23 - Setting Global Proxy for Android VM
[INFO] 09/Apr/2025 11:42:20 - Testing Environment is Ready!
[INFO] 09/Apr/2025 11:42:20 - Starting Logcat streaming
[INFO] 09/Apr/2025 11:42:24 - Starting Logcat streaming
[INFO] 09/Apr/2025 11:42:24 - Not Found: /favicon.ico
[WARNING] 09/Apr/2025 11:42:24 - Not Found: /favicon.ico

```

Configuration of OWASP Security Shepherd – Mobile Security platform



Practical: 01 OWASP Security Shepherd – Mobile Security platform

```
root@x86:/ # cd data/data
root@x86:/data/data # cd com.mobshep.insecuredata
root@x86:/data/data/com.mobshep.insecuredata # cd databases
root@x86:/data/data/com.mobshep.insecuredata/databases # ls
Members
Members.journal
root@x86:/data/data/com.mobshep.insecuredata/databases # cat Me
Members      Members.journal
root@x86:/data/data/com.mobshep.insecuredata/databases # cat Members
==>h*tableMembersMembersCREATE TABLE Members (id integer primary key, name VARCHAR, password VARCHAR
***!AdminBattery??root@x86:/data/data/com.mobshep.insecuredata/databases # _cale TEXT)
```

The screenshot shows the 'Lessons' section of the OWASP Security Shepherd platform. On the left, there's a sidebar with buttons for 'Admin', 'Scoreboard', 'Lessons', and 'Challenges'. Below the sidebar is a search bar labeled 'Search Modules...'. The main content area has a title 'What is Mobile Insecure Data Storage?' and a sub-section titled 'Insecure Data Storage occurs when an App stores sensitive data such as user credentials, API keys, Credit Card information insecurely. This issue occurs in numerous ways. Generally, for storing client side information, an App will use an [Sqlite database](#).'. It includes two paragraphs of text about hashing and collisions, and a note about SQLite databases. There's also a 'Hide Lesson Introduction' button.

Battery777

What is Mobile Insecure Data Storage?

Insecure Data Storage occurs when an App stores sensitive data such as user credentials, API keys, Credit Card information insecurely. This issue occurs in numerous ways. Generally, for storing client side information, an App will use an [Sqlite database](#).

This can be a favoured, cheaper method of storage instead of using a more expensive back end service. As a result, any user can access the data stored by the App. Insecure Data Storage becomes a danger when a user's App caches sensitive data, their phone is stolen or the attacker steals this information from local databases. Malware can also access this information easily. This risk is increased by the popularity of [rooting devices](#) which makes it much easier for an attacker to access this information.

There are other ways to store data insecurely. Using known broken hashing algorithms can lead to pain for the Apps users. Not only are they susceptible to [collisions](#), where two different passwords can potentially generate the same hash and be interpreted as the same password, the developer would have to assume that their user's use strong passwords. This is generally never the case and once a hashed value has been cracked, an attacker merely needs to update their tables.

This method still uses no key, Therefore one could assume it is not truly encryption? Hashing algorithms are useful for comparing two different files but should not be used for storage of passwords (Unless done correctly).

Hide Lesson Introduction

Typically an Android app will store its database in the `/data/data/com.app.exampleApp/database/` directory. Anyone with a rooted device can access this directory. The Android App for this lesson stores its under credentials in an [SQLite database](#). The Admin's password is the result key to this lesson.

To complete this challenge you'll need to use the InsecureData.apk app found in the [Security Shepherd Android Virtual Machine](#).

The screenshot shows the 'Lessons' section of the OWASP Security Shepherd platform after a submission. The sidebar and search bar are identical to the previous screenshot. The main content area now displays a success message 'Solution Submission Success' and a note 'Insecure Data Storage completed! Congratulations.' There is also a 'Submit Result Key Here...' input field and a 'Submit' button.

Submit Result Key Here...

Solution Submission Success

Insecure Data Storage completed! Congratulations.

Practical: 02 OWASP Security Shepherd – Mobile Security platform

```
root@x86:/ # cd data/data
root@x86:/data/data # cd com.mobshep.udataleakage
root@x86:/data/data/com.mobshep.udataleakage # ls
cache
files
lib
root@x86:/data/data/com.mobshep.udataleakage # cd files
root@x86:/data/data/com.mobshep.udataleakage/files # ls
Tue Jul 08 172618 EDT 2014
root@x86:/data/data/com.mobshep.udataleakage/files # cat "Tue Jul 08 172618 EDT 2014"
The Key is: "SilentButSteadyRedLed" nullTue Jul 08 17:26:18 EDT 2014nullroot@x86:/data/data/com.mobshep.udataleakage/files #
```

Admin Submit

Scoreboard

Lessons

X Broken Crypto
X Client Side Injection
X Content Provider Leakage
✓ Insecure Data Storage
X Poor Authentication
X Reverse Engineering
X Unintended Data Leakage
X Untrusted Input

Challenges

Search Modules...

What is Mobile Unintended Data Leakage?

Unintended data leakage occurs when an App inadvertently places sensitive information or data in a location on the mobile device that is accessible by attackers or other Apps on the device.

Unintended Data Leakage comes in many forms, including:

- URL Caching (Both request and response)
- Keyboard Press Caching
- Copy/Paste buffer Caching
- Application backgrounding
- Logging
- HTML5 data storage
- Browser cookie objects
- Analytic data sent to third parties

Unintended data leakage occurs when an App inadvertently places sensitive information or data in a location on the mobile device that is accessible by attackers or other Apps on the device.

Hide Lesson Introduction

Apps won't always use a SQLite database to store data. In some cases, logs yield useful information about the App and its users. Use this information to find the result key. In this lesson, the App [caches logs](#) on the device. The App itself acts as a notice board or to do list. Everything a user adds to the [ListView](#) in the App is logged.

To complete this challenge you'll need to use the UDataLeakage.apk app found in the [Security Shepherd Android Virtual Machine](#).

Admin Submit

Scoreboard

Lessons

Challenges

Search Modules...

Solution Submission Success

Unintended Data Leakage completed! Congratulations.

Practical: 03 OWASP Security Shepherd – Mobile Security platform

```
root@x86:/ # adb shell content query --uri content://com.somewhere.hidden.SecretProvider/data
* daemon not running. starting it now on port 5038 *
* daemon started successfully *
Row: 0 id=1, key=LazerLizardsFlamingWizards
root@x86:/ #
```

Admin Scoreboard Lessons Challenges

Search Modules...

LazerLizardsFlamingWizards

What is Content Provider Leakage?

A Content Provider is used by Android to provide access to a structured set of data within a central repository. Content Providers are intended to be accessed by other applications, however with the [Android Debug Bridge](#), they can be accessed by anyone with access to a device.

In order to query a Content Provider without an App, perform the following adb commands:

- adb devices
- adb connect [device IP]
- adb shell content query --uri [Content Provider URI]

The Key can be attained by querying the Content Provider. The URI is :
content://com.somewhere.hidden.SecretProvider/data

To complete this challenge you'll need to use the CProviderLeakage.apk app found in the [Security Shepherd Android Virtual Machine](#).

Admin Scoreboard Lessons Challenges

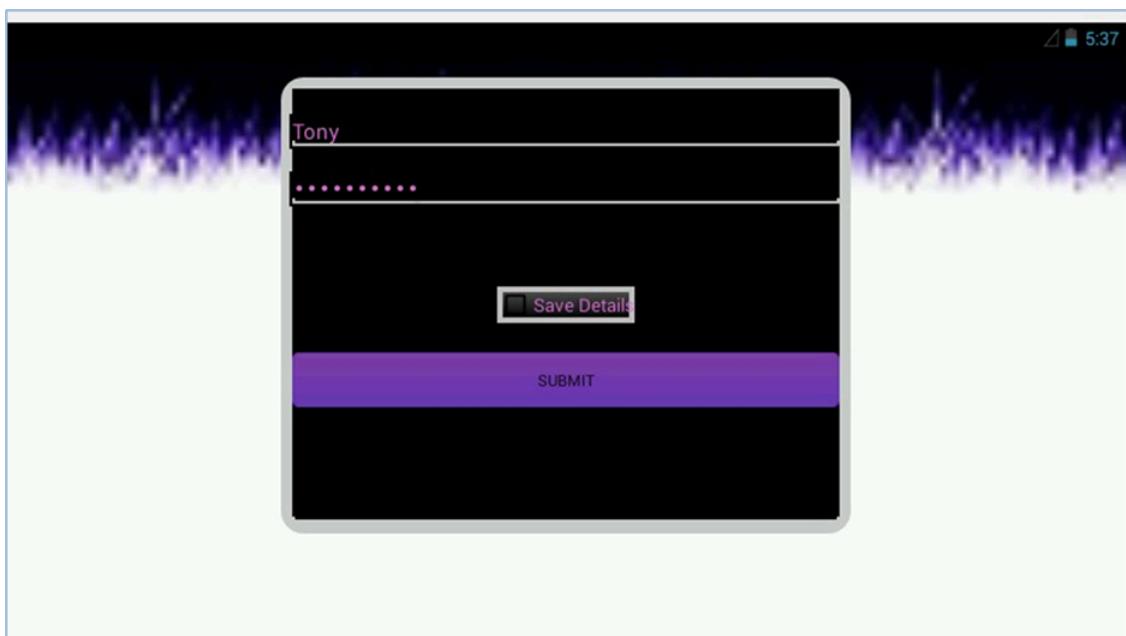
Search Modules...

Solution Submission Success

Content Provider Leakage completed! Congratulations.

Practical: 04 OWASP Security Shepherd – Mobile Security platform

```
root@x86:/ # cd data/data
root@x86:/data/data # cd com.mobshp.insecuredata3
root@x86:/data/data/com.mobshp.insecuredata3 # ls
cache
lib
shared_prefs
root@x86:/data/data/com.mobshp.insecuredata3 # cd shared_prefs
root@x86:/data/data/com.mobshp.insecuredata3/shared_prefs # ls
AppData.xml
Saved Data.xml
root@x86:/data/data/com.mobshp.insecuredata3/shared_prefs # cat Saved Data.xml
/system/bin/sh: cat: Saved: No such file or directory
/system/bin/sh: cat: Data.xml: No such file or directory
t Saved\ Data.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="Username">Tony</string>
    <string name="Password">qazwsx4562</string>
</map>
root@x86:/data/data/com.mobshp.insecuredata3/shared_prefs #
```





Admin

Scoreboard

Lessons

Challenges

Mobile Broken Crypto

Mobile Content Providers

Mobile Data Leakage

Mobile Injection

Mobile Insecure Data Storage

X Insecure Data Storage 1

X Insecure Data Storage 2

X Insecure Data Storage 3

Mobile Poor Authentication

Mobile Reverse Engineering

Mobile Insecure Data Storage 3

Not all Apps will use `sqlite` to store user data, in some cases `SharedPreferences` is used. The key to this level can be gained once you log in as a legitimate user.

To complete this challenge you'll need to use the `InsecureData4.apk` app found in the [Security Shepherd Android Virtual Machine](#).

Search Modules...