Bulletproof Android

Godfrey Nolan

Godfrey Nolan

Bulletproof Android™

Practical Advice for Building Secure Apps

Agenda

○ How did we get here

○ OWASP Top 10

○ What's New

○ Recommendations

How Did We Get Here
Background

○ Virtual Machines

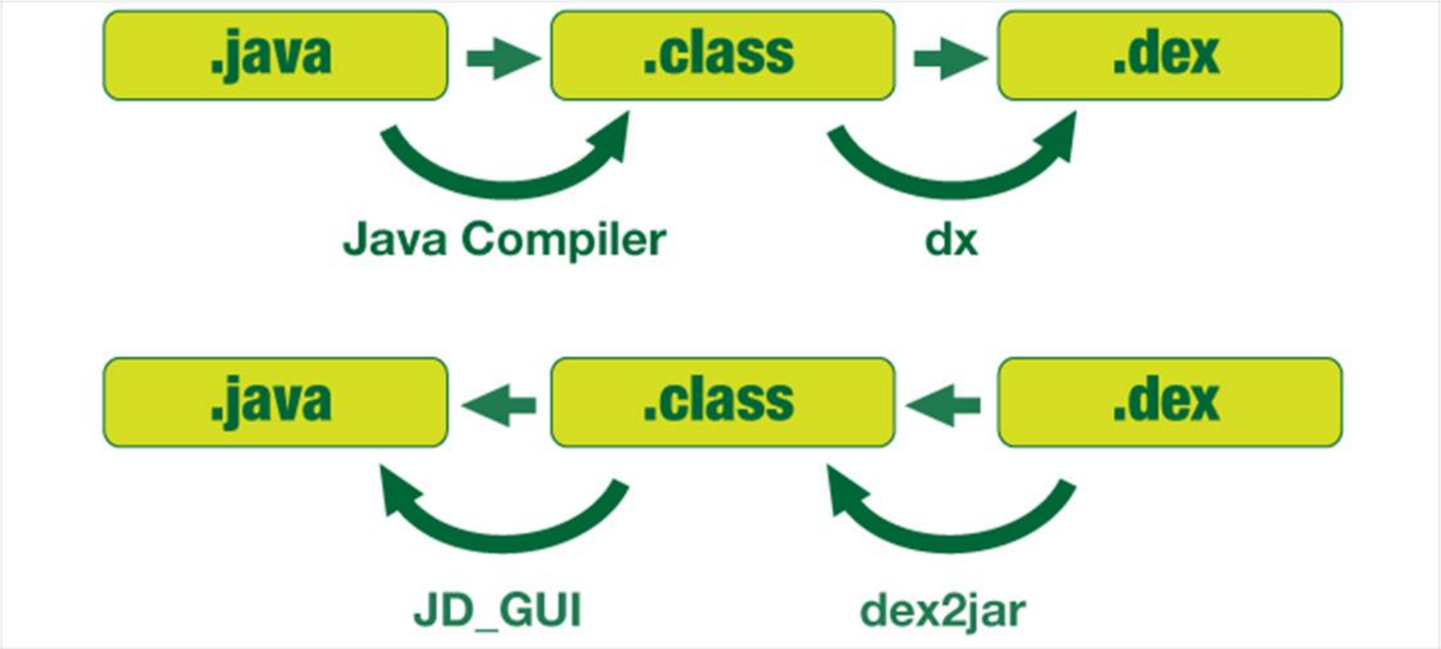
○ Static information

○ Decompilation demo

○ Dynamic information

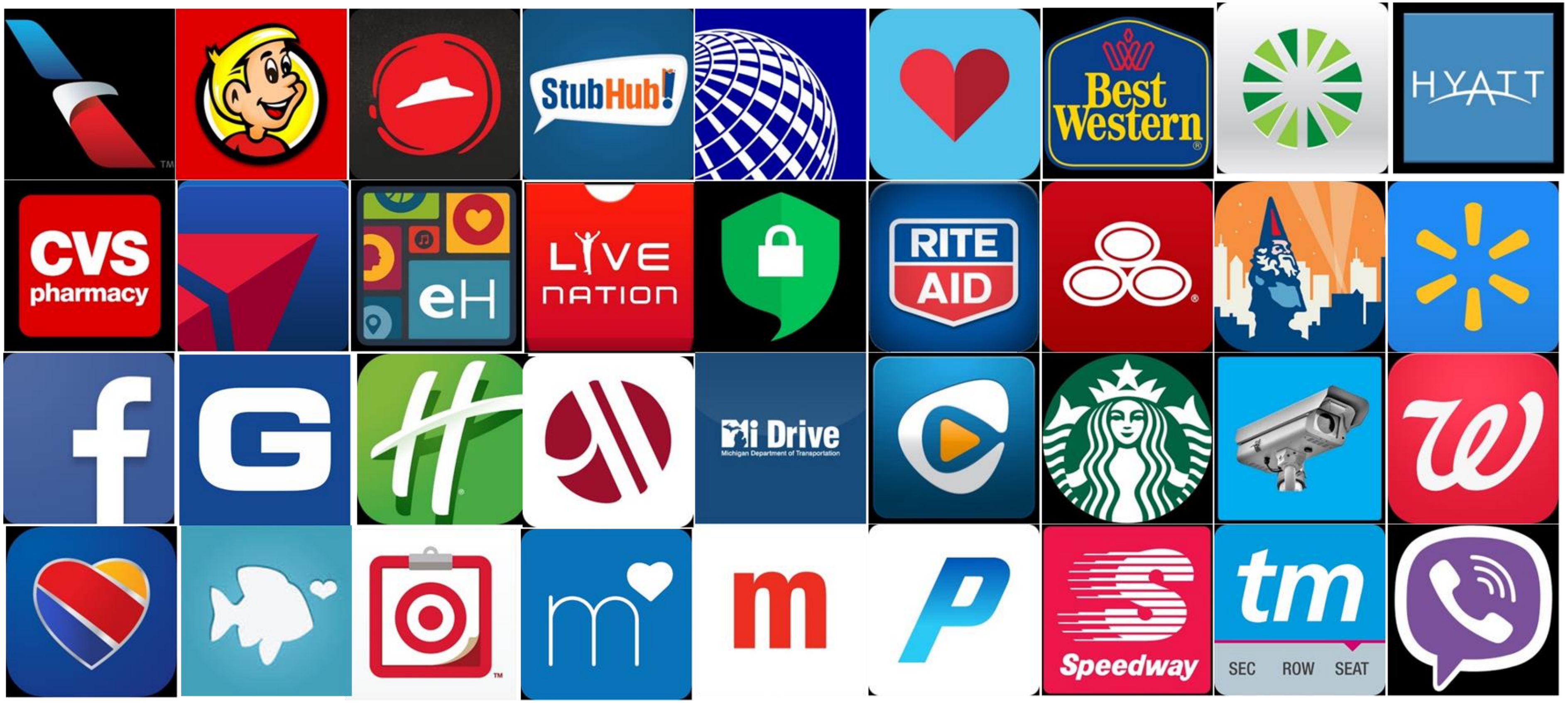
○ Adb backup demo

How Did We Get Here
Decompilation 101



How Did We Get Here
Audit Reports

How Did We Get Here
Hacked Apps



How Did We Get Here
Hacked Twice

LIVE NATION
RITE AID
FREE
eH

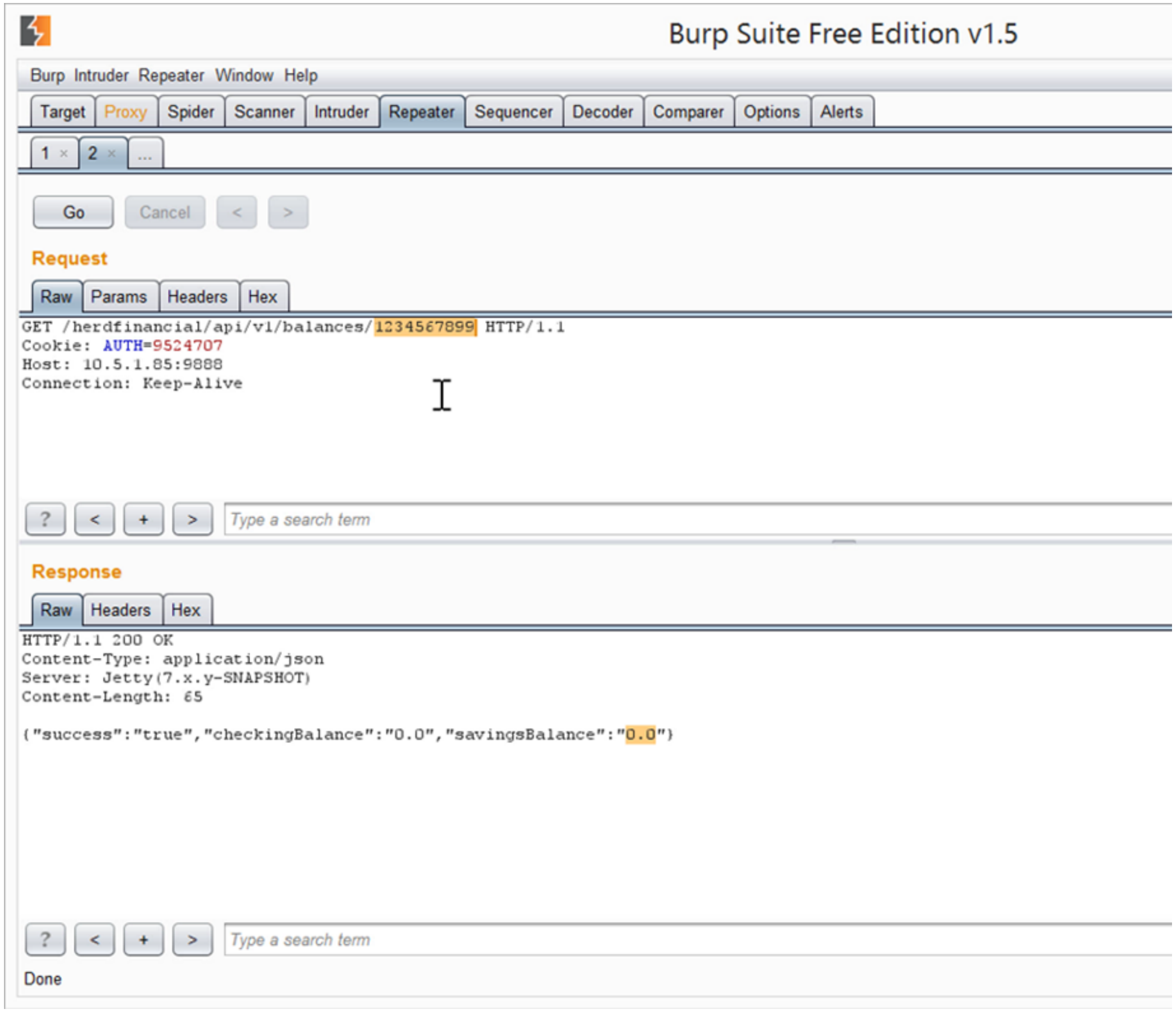
How Did We Get Here

Hacked Three Times

OWASP Top 10

- Weak Server Side Controls
- Insecure Data Storage
- Insufficient Transport Layer Protection
- Unintended Data Leakage
- Poor Authorization and Authentication
- Broken Cryptography
- Client Side Injection
- Security Decision via Untrusted Input
- Improper Session Handling
- Lack of Binary Protections

OWASP Top 10
Weak Server Side Controls



Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
1 × 2 × ...
Go Cancel < >
Request
Raw Params Headers Hex

```
GET /herdfinancial/api/v1/balances/1234567899 HTTP/1.1
Cookie: AUTH=9524707
Host: 10.5.1.85:9888
Connection: Keep-Alive
```

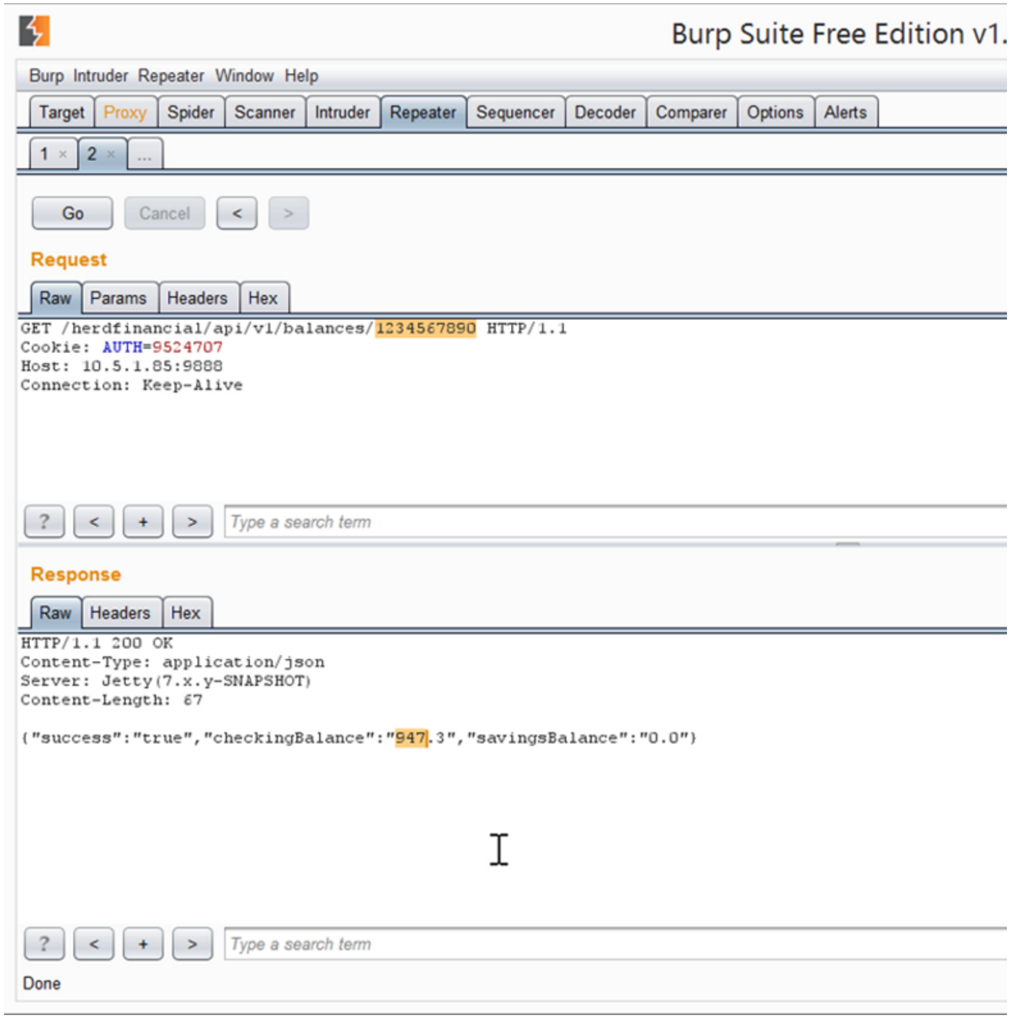
? < + > Type a search term
Response
Raw Headers Hex

```
HTTP/1.1 200 OK
Content-Type: application/json
Server: Jetty(7.x.y-SNAPSHOT)
Content-Length: 65

{"success":"true","checkingBalance":"0.0","savingsBalance":"0.0"}
```

? < + > Type a search term
Done

OWASP Top 10
Weak Server Side Controls

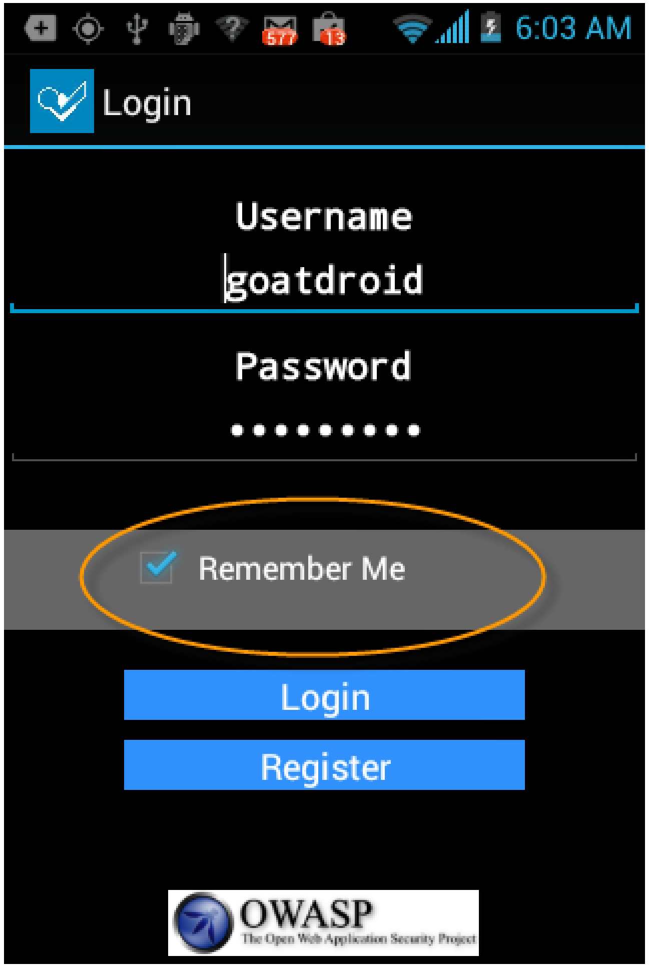

Burp Suite Free Edition v1.
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
1 × 2 × ...
Go Cancel < >
Request
Raw Params Headers Hex
? < + > Type a search term
Response
Raw Headers Hex
? < + > Type a search term
Done

```
GET /herdfinancial/api/v1/balances/1234567890 HTTP/1.1
Cookie: AUTH=9524707
Host: 10.5.1.85:9888
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Server: Jetty(7.x.y-SNAPSHOT)
Content-Length: 67

{"success":"true","checkingBalance":"947.3","savingsBalance":"0.0"}
```

OWASP Top 10
Insecure Data Storage



6:03 AM

Login

Username

goatdroid

Password

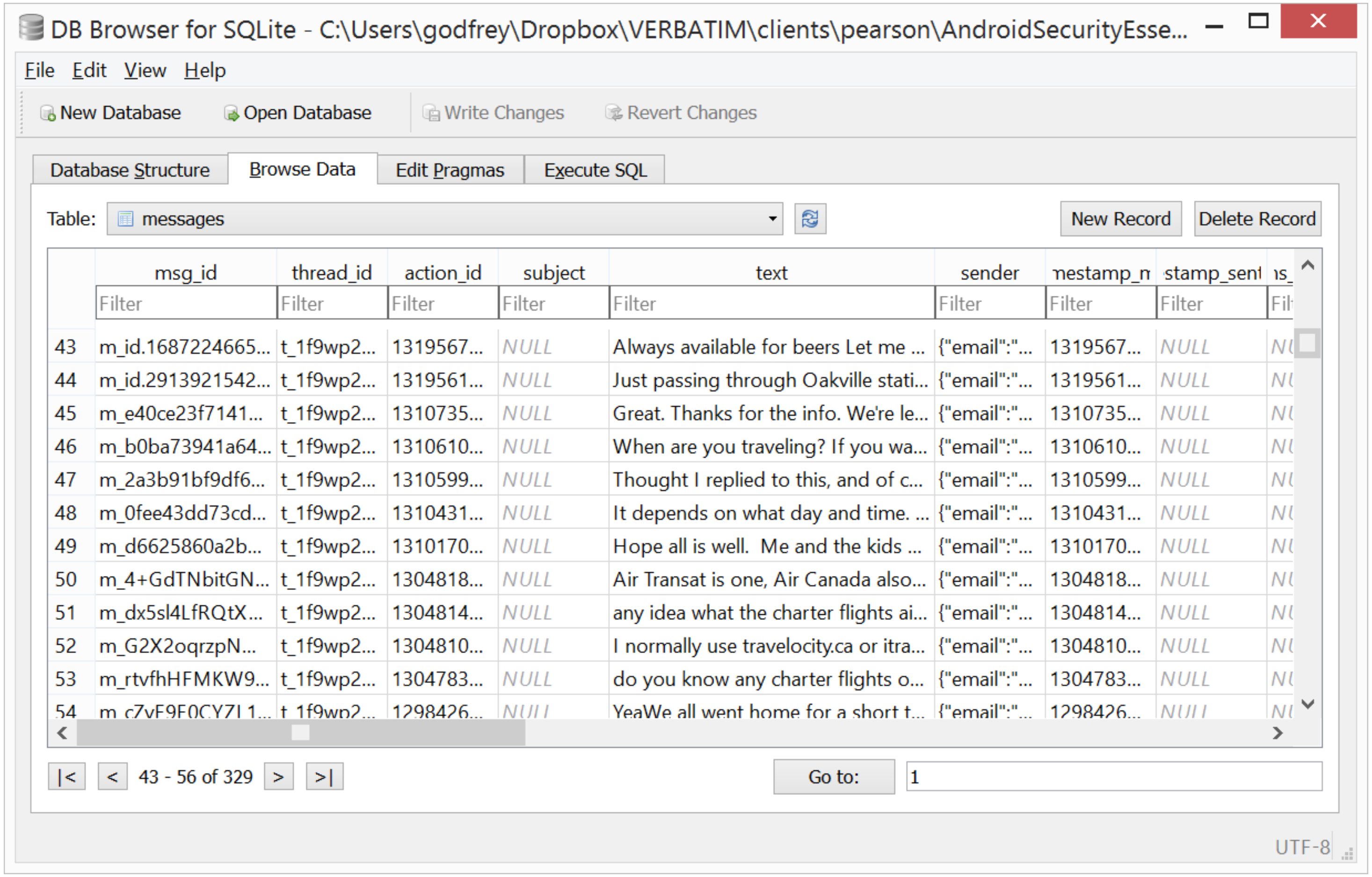
••••••••••

☑ Remember Me

Login

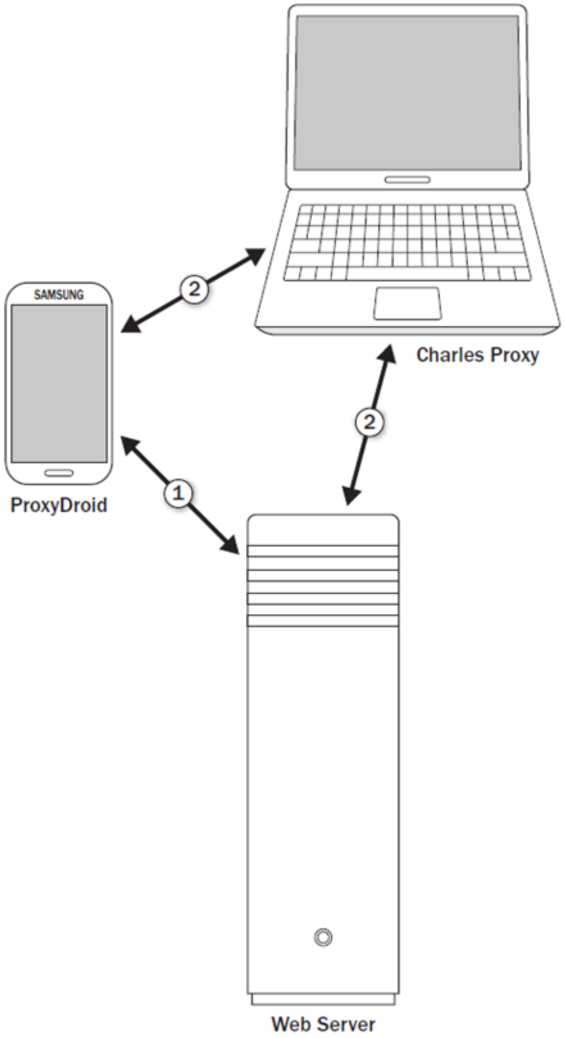
Register

OWASP Top 10
Insecure Data Storage

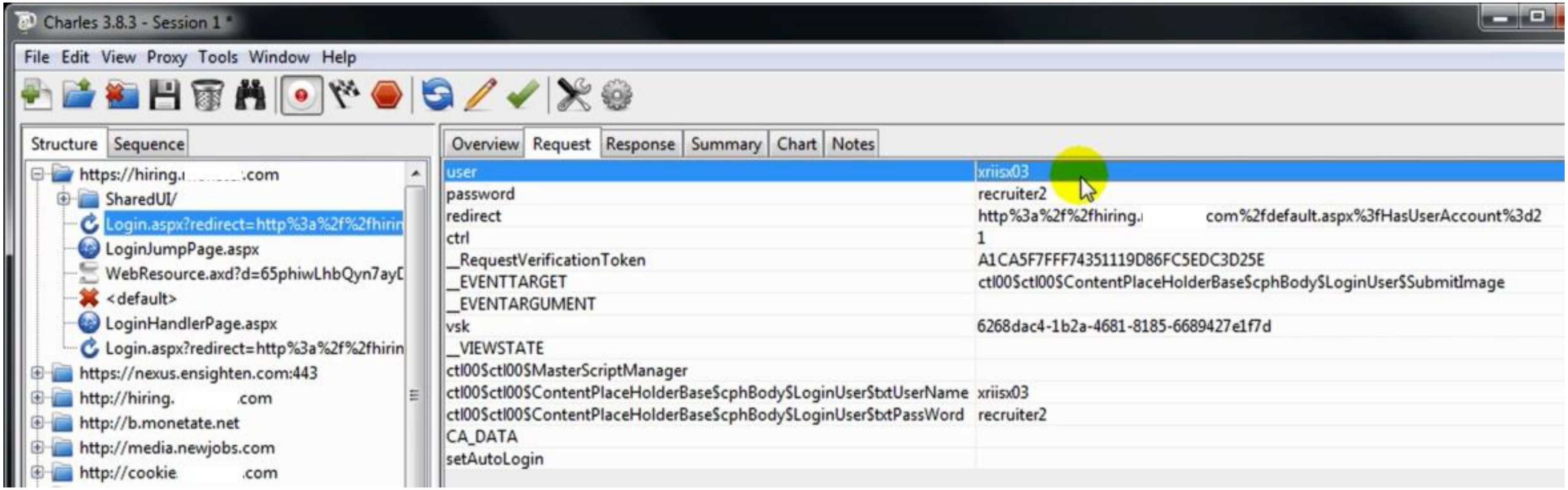


	msg_id	thread_id	action_id	subject	text	sender	nestamp_n	stamp_sent	ıs_
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Fil
43	m_id.1687224665...	t_1f9wp2...	1319567...	NULL	Always available for beers Let me ...	{"email":"...	1319567...	NULL	NU
44	m_id.2913921542...	t_1f9wp2...	1319561...	NULL	Just passing through Oakville stati...	{"email":"...	1319561...	NULL	NU
45	m_e40ce23f7141...	t_1f9wp2...	1310735...	NULL	Great. Thanks for the info. We're le...	{"email":"...	1310735...	NULL	NU
46	m_b0ba73941a64...	t_1f9wp2...	1310610...	NULL	When are you traveling? If you wa...	{"email":"...	1310610...	NULL	NU
47	m_2a3b91bf9df6...	t_1f9wp2...	1310599...	NULL	Thought I replied to this, and of c...	{"email":"...	1310599...	NULL	NU
48	m_0fee43dd73cd...	t_1f9wp2...	1310431...	NULL	It depends on what day and time. ...	{"email":"...	1310431...	NULL	NU
49	m_d6625860a2b...	t_1f9wp2...	1310170...	NULL	Hope all is well. Me and the kids ...	{"email":"...	1310170...	NULL	NU
50	m_4+GdTNbitGN...	t_1f9wp2...	1304818...	NULL	Air Transat is one, Air Canada also...	{"email":"...	1304818...	NULL	NU
51	m_dx5sl4LfRQtX...	t_1f9wp2...	1304814...	NULL	any idea what the charter flights ai...	{"email":"...	1304814...	NULL	NU
52	m_G2X2oqrzpN...	t_1f9wp2...	1304810...	NULL	I normally use travelocity.ca or itra...	{"email":"...	1304810...	NULL	NU
53	m_rtvfhHFMKW9...	t_1f9wp2...	1304783...	NULL	do you know any charter flights o...	{"email":"...	1304783...	NULL	NU
54	m_cZvF9F0CYZL1...	t_1f9wp2...	1298426...	NULL	YeaWe all went home for a short t...	{"email":"...	1298426...	NULL	NU

OWASP Top 10
Insufficient Transport Layer Protection



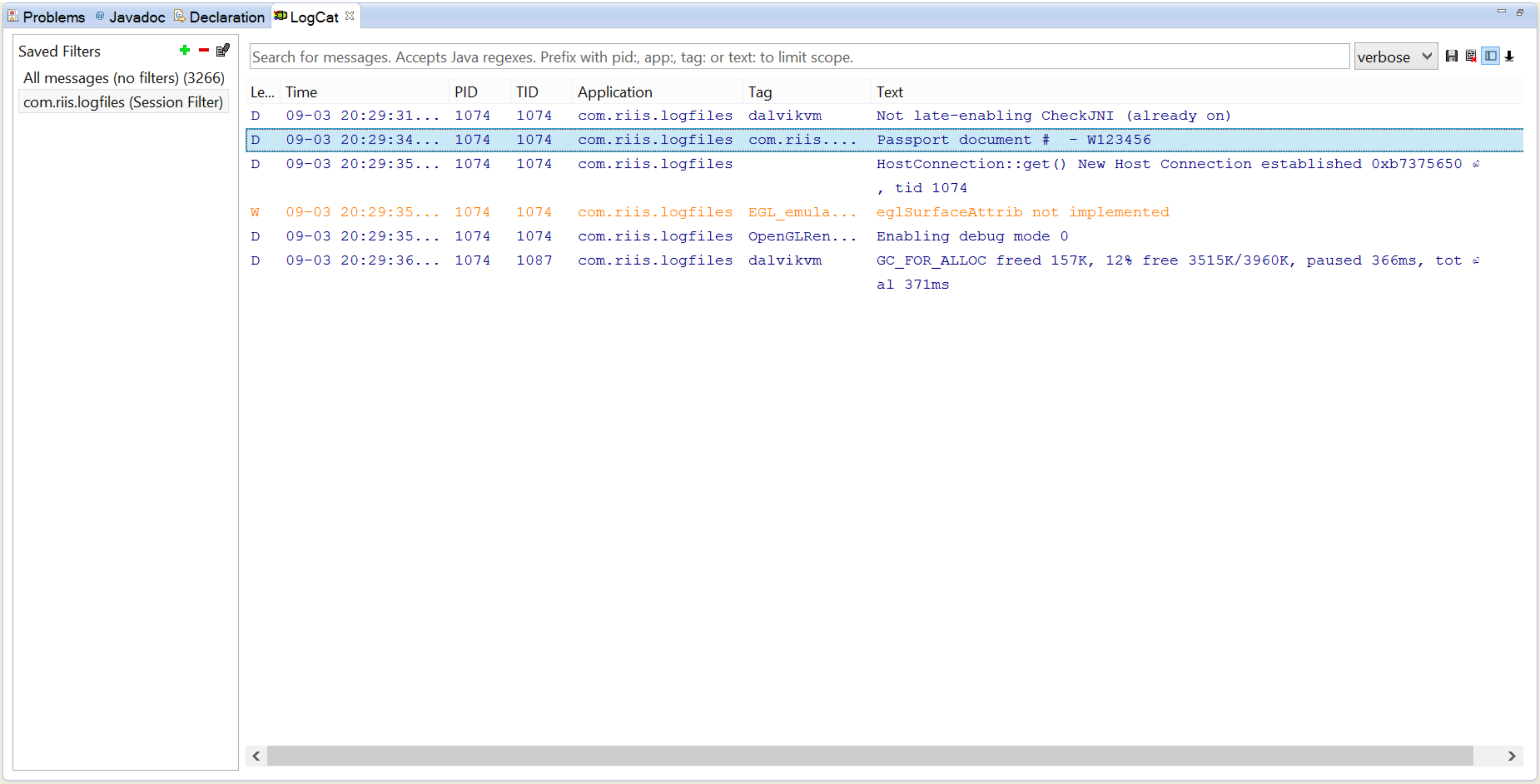
OWASP Top 10
Insufficient Transport Layer Protection


Charles 3.8.3 - Session 1 *
File Edit View Proxy Tools Window Help
Structure Sequence
Overview Request Response Summary Chart Notes

https://hiring.[redacted].com
SharedUI/
Login.aspx?redirect=http%3a%2f%2fhirin
LoginJumpPage.aspx
WebResource.axd?d=65phiwLhbQyn7ayD
<default>
LoginHandlerPage.aspx
Login.aspx?redirect=http%3a%2f%2fhirin
https://nexus.ensighten.com:443
http://hiring.[redacted].com
http://b.monetate.net
http://media.newjobs.com
http://cookie[redacted].com

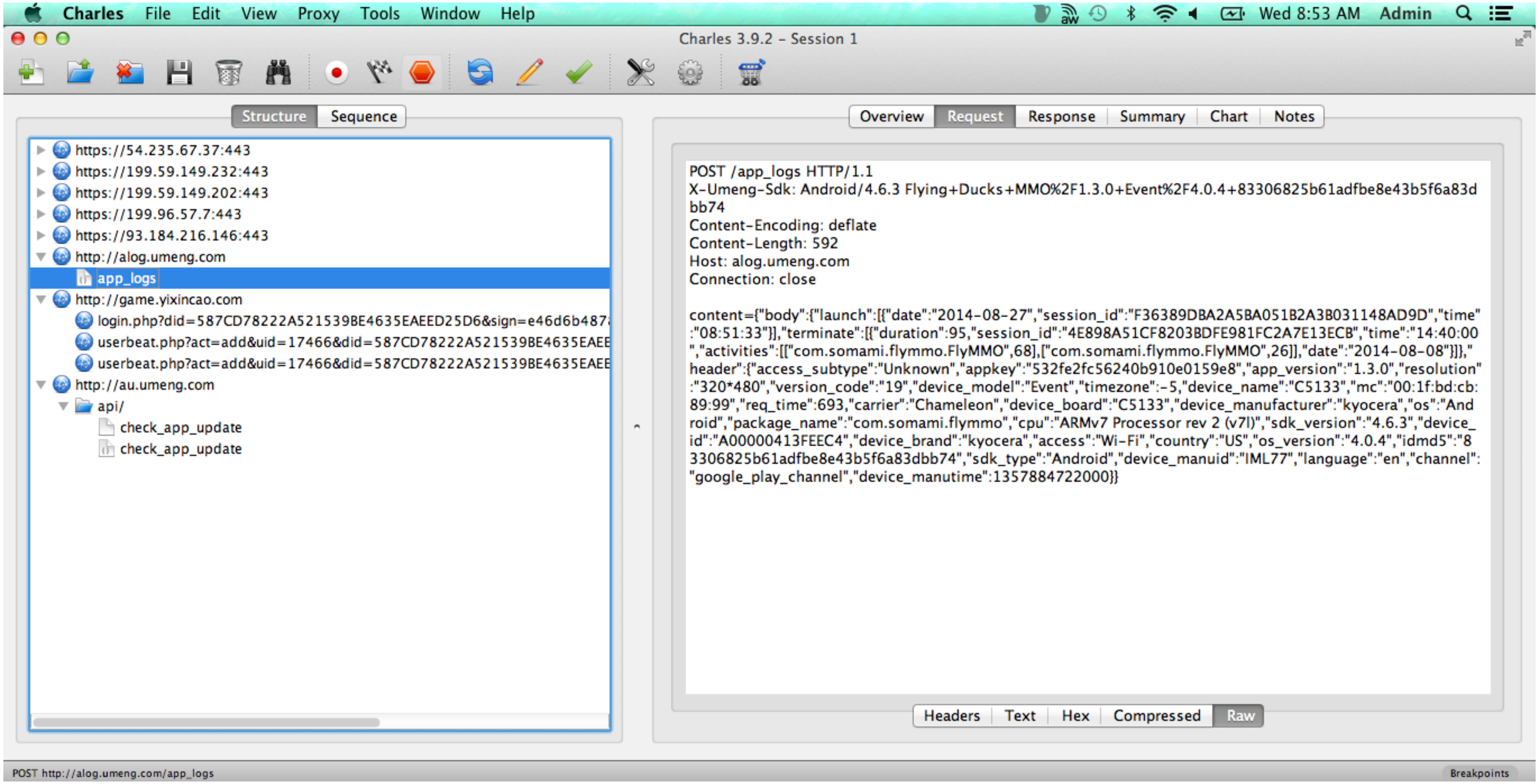
user	xriisx03
password	recruiter2
redirect	http%3a%2f%2fhiring.[redacted]com%2fdefault.aspx%3fHasUserAccount%3d2
ctrl	1
__RequestVerificationToken	A1CA5F7FFF74351119D86FC5EDC3D25E
__EVENTTARGET	ctl00$ctl00$ContentPlaceHolderBase$cphBody$LoginUser$SubmitImage
__EVENTARGUMENT	
vsk	6268dac4-1b2a-4681-8185-6689427e1f7d
__VIEWSTATE	
ctl00$ctl00$MasterScriptManager	
ctl00$ctl00$ContentPlaceHolderBase$cphBody$LoginUser$txtUserName	xriisx03
ctl00$ctl00$ContentPlaceHolderBase$cphBody$LoginUser$txtPassWord	recruiter2
CA_DATA	
setAutoLogin	

OWASP Top 10
Unintended Data Leakage


Problems
Javadoc
Declaration
LogCat
Saved Filters
All messages (no filters) (3266)
com.riis.logfiles (Session Filter)
Search for messages. Accepts Java regexes. Prefix with pid:, app:, tag: or text: to limit scope.
verbose

```
Le...  Time                PID    TID    Application        Tag            Text
D      09-03 20:29:31...   1074   1074   com.riis.logfiles  dalvikvm       Not late-enabling CheckJNI (already on)
D      09-03 20:29:34...   1074   1074   com.riis.logfiles  com.riis....   Passport document #  - W123456
D      09-03 20:29:35...   1074   1074   com.riis.logfiles                 HostConnection::get() New Host Connection established 0xb7375650
                                                                           , tid 1074
W      09-03 20:29:35...   1074   1074   com.riis.logfiles  EGL_emula...   eglSurfaceAttrib not implemented
D      09-03 20:29:35...   1074   1074   com.riis.logfiles  OpenGLRen...   Enabling debug mode 0
D      09-03 20:29:36...   1074   1087   com.riis.logfiles  dalvikvm       GC_FOR_ALLOC freed 157K, 12% free 3515K/3960K, paused 366ms, tot
                                                                           al 371ms
```

OWASP Top 10
Unintended Data Leakage



```
▶ https://54.235.67.37:443
▶ https://199.59.149.232:443
▶ https://199.59.149.202:443
▶ https://199.96.57.7:443
▶ https://93.184.216.146:443
▼ http://alog.umeng.com
    app_logs
▼ http://game.yixincao.com
    login.php?did=587CD78222A521539BE4635EAEED25D6&sign=e46d6b487
    userbeat.php?act=add&uid=17466&did=587CD78222A521539BE4635EAEE
    userbeat.php?act=add&uid=17466&did=587CD78222A521539BE4635EAEE
▼ http://au.umeng.com
  ▼ api/
      check_app_update
      check_app_update
```

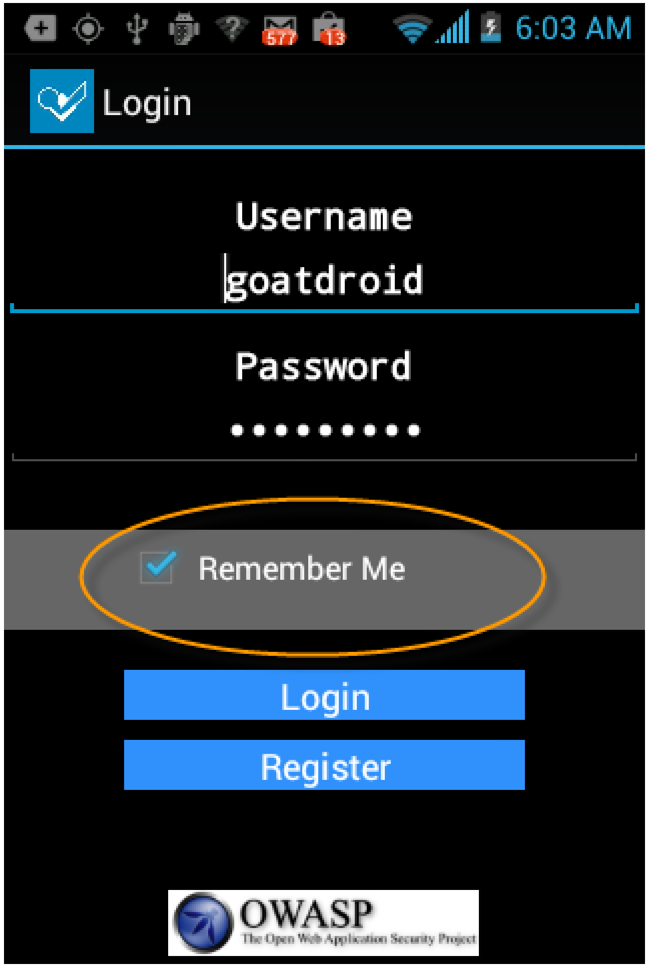
```
POST /app_logs HTTP/1.1
X-Umeng-Sdk: Android/4.6.3 Flying+Ducks+MMO%2F1.3.0+Event%2F4.0.4+83306825b61adfbe8e43b5f6a83d
bb74
Content-Encoding: deflate
Content-Length: 592
Host: alog.umeng.com
Connection: close

content={"body":{"launch":[{"date":"2014-08-27","session_id":"F36389DBA2A5BA051B2A3B031148AD9D","time"
:"08:51:33"}],"terminate":[{"duration":95,"session_id":"4E898A51CF8203BDFE981FC2A7E13ECB","time":"14:40:00
","activities":[["com.somami.flymmo.FlyMMO",68],["com.somami.flymmo.FlyMMO",26]],"date":"2014-08-08"}]},"
header":{"access_subtype":"Unknown","appkey":"532fe2fc56240b910e0159e8","app_version":"1.3.0","resolution"
:"320*480","version_code":"19","device_model":"Event","timezone":-5,"device_name":"C5133","mc":"00:1f:bd:cb:
89:99","req_time":693,"carrier":"Chameleon","device_board":"C5133","device_manufacturer":"kyocera","os":"And
roid","package_name":"com.somami.flymmo","cpu":"ARMv7 Processor rev 2 (v7l)","sdk_version":"4.6.3","device_
id":"A00000413FEEC4","device_brand":"kyocera","access":"Wi-Fi","country":"US","os_version":"4.0.4","idmd5":"8
3306825b61adfbe8e43b5f6a83dbb74","sdk_type":"Android","device_manuid":"IML77","language":"en","channel":
"google_play_channel","device_manutime":1357884722000}}
```

POST http://alog.umeng.com/app_logs

OWASP Top 10

Poor Authorization and Authentication



6:03 AM

Login

Username

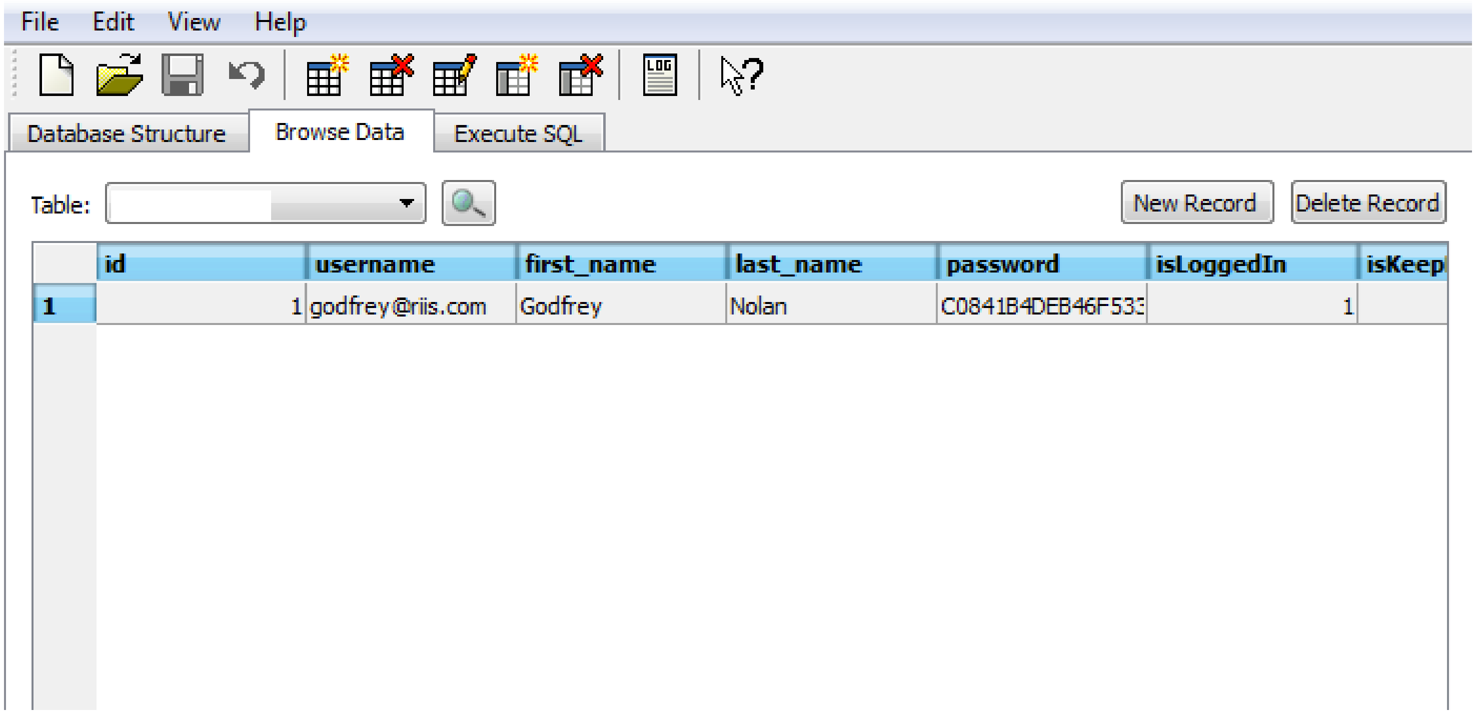
goatdroid

Password

••••••••••

☑ Remember Me

OWASP Top 10
Broken Cryptography

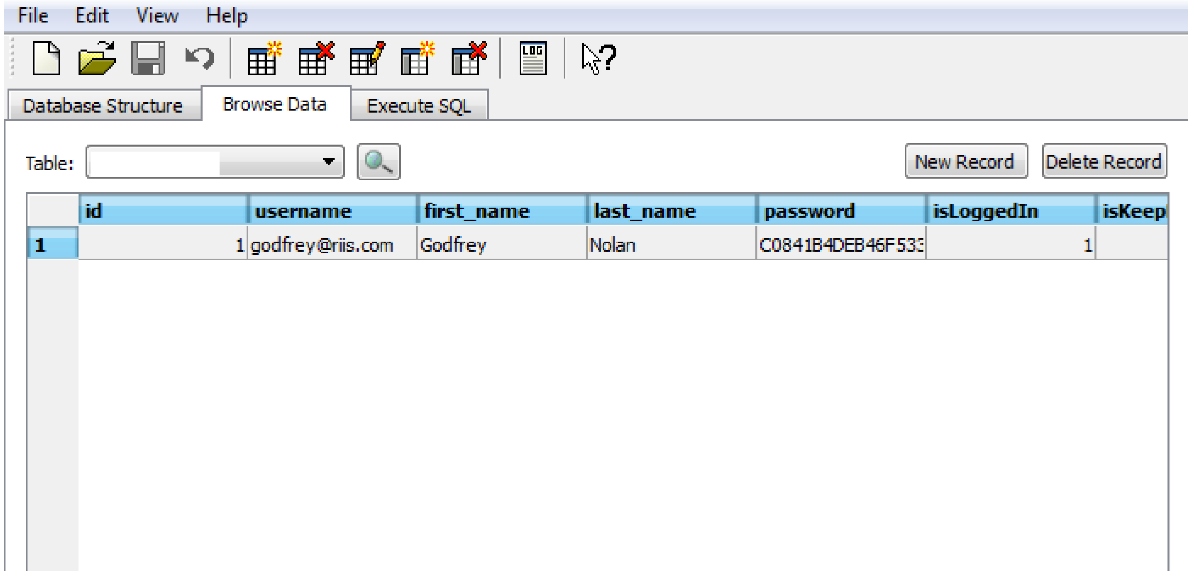


	id	username	first_name	last_name	password	isLoggedIn	isKeep
1	1	godfrey@riis.com	Godfrey	Nolan	C0841B4DEB46F533	1	

OWASP Top 10
Broken Cryptography

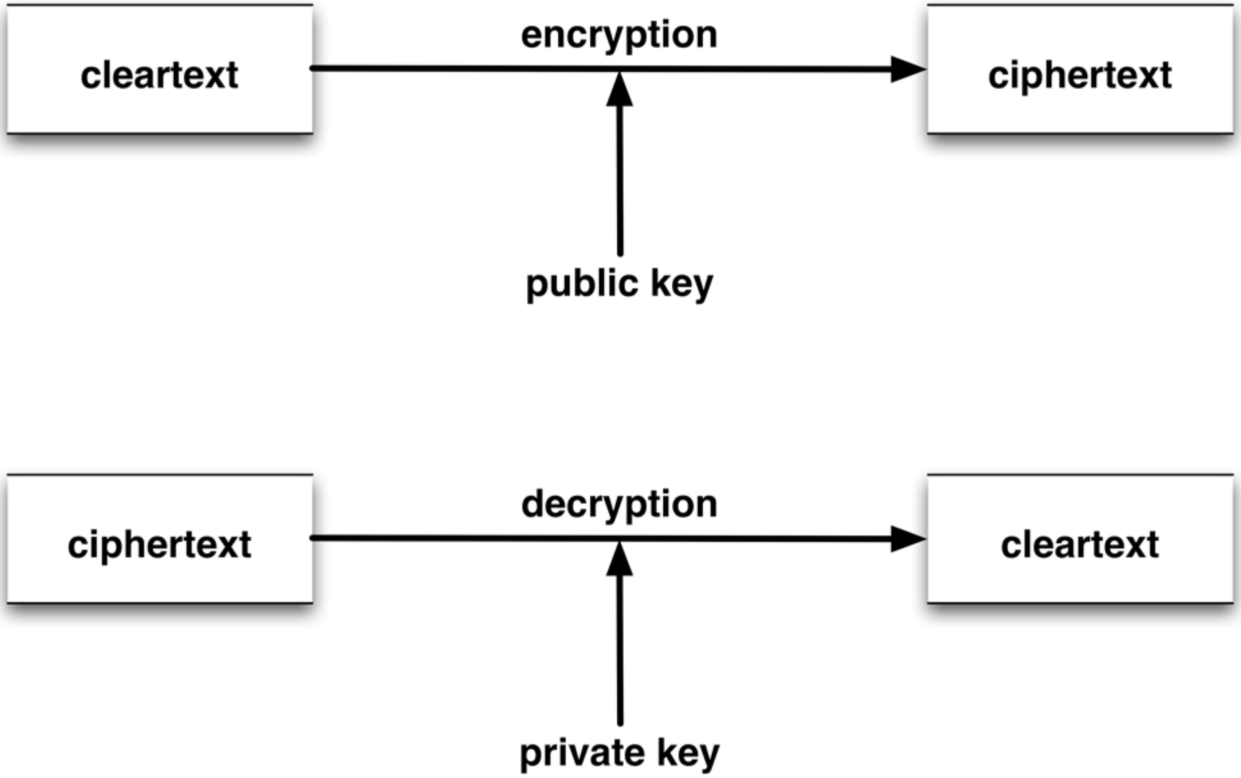
```
public static String decrypt(String paramString)
  throws Exception
{
  if (paramString != null)
    return new String(decrypt(getRawKey("3lIoM_d0idrn4|4TleD".getBytes()), toByte(paramString)));
  return null;
}

private static byte[] decrypt(byte[] paramArrayOfByte1, byte[] paramArrayOfByte2)
  throws Exception
{
  SecretKeySpec localSecretKeySpec = new SecretKeySpec(paramArrayOfByte1, "AES");
  Cipher localCipher = Cipher.getInstance("AES");
  localCipher.init(2, localSecretKeySpec);
  return localCipher.doFinal(paramArrayOfByte2);
}
```

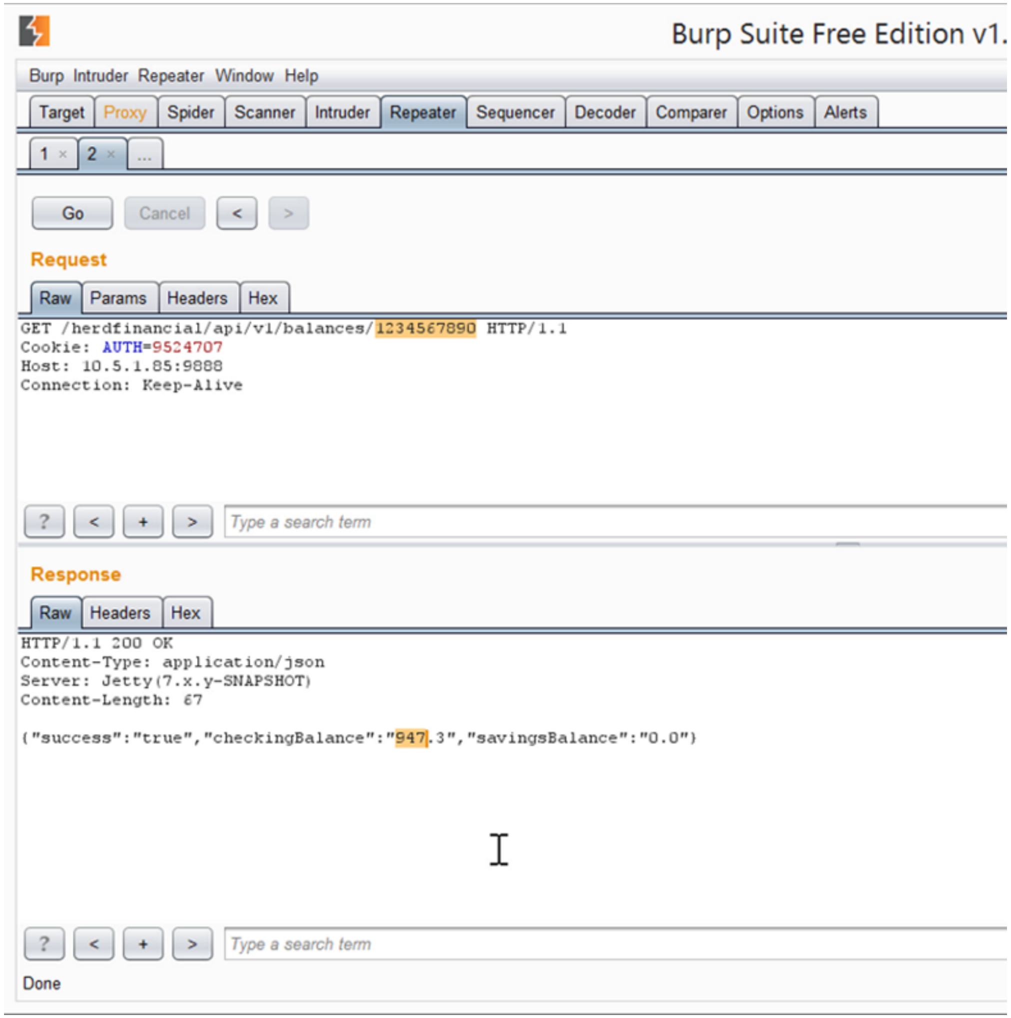


	id	username	first_name	last_name	password	isLoggedIn	isKeep
1	1	godfrey@riis.com	Godfrey	Nolan	C0841B4DEB46F533	1	

OWASP Top 10
Broken Cryptography



OWASP Top 10
Client Side Injection



Burp Suite Free Edition v1.
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
1 × 2 × ...
Go Cancel < >
Request
Raw Params Headers Hex

```
GET /herdfinancial/api/v1/balances/1234567890 HTTP/1.1
Cookie: AUTH=9524707
Host: 10.5.1.85:9888
Connection: Keep-Alive
```

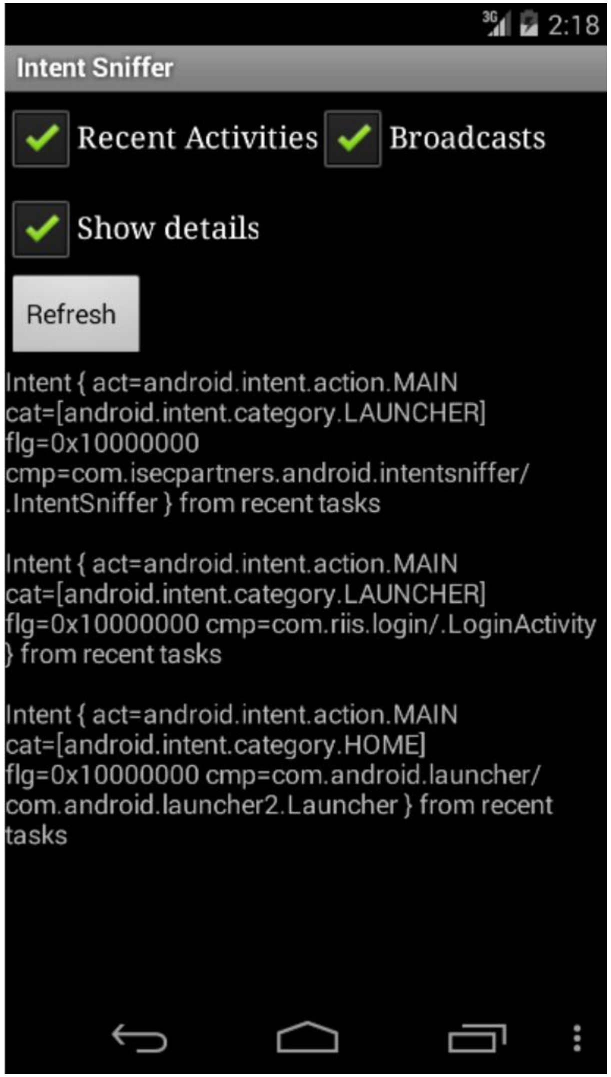
? < + >
Type a search term
Response
Raw Headers Hex

```
HTTP/1.1 200 OK
Content-Type: application/json
Server: Jetty(7.x.y-SNAPSHOT)
Content-Length: 67

{"success":"true","checkingBalance":"947.3","savingsBalance":"0.0"}
```

? < + >
Type a search term
Done

OWASP Top 10
Security Decisions via Untrusted Inputs



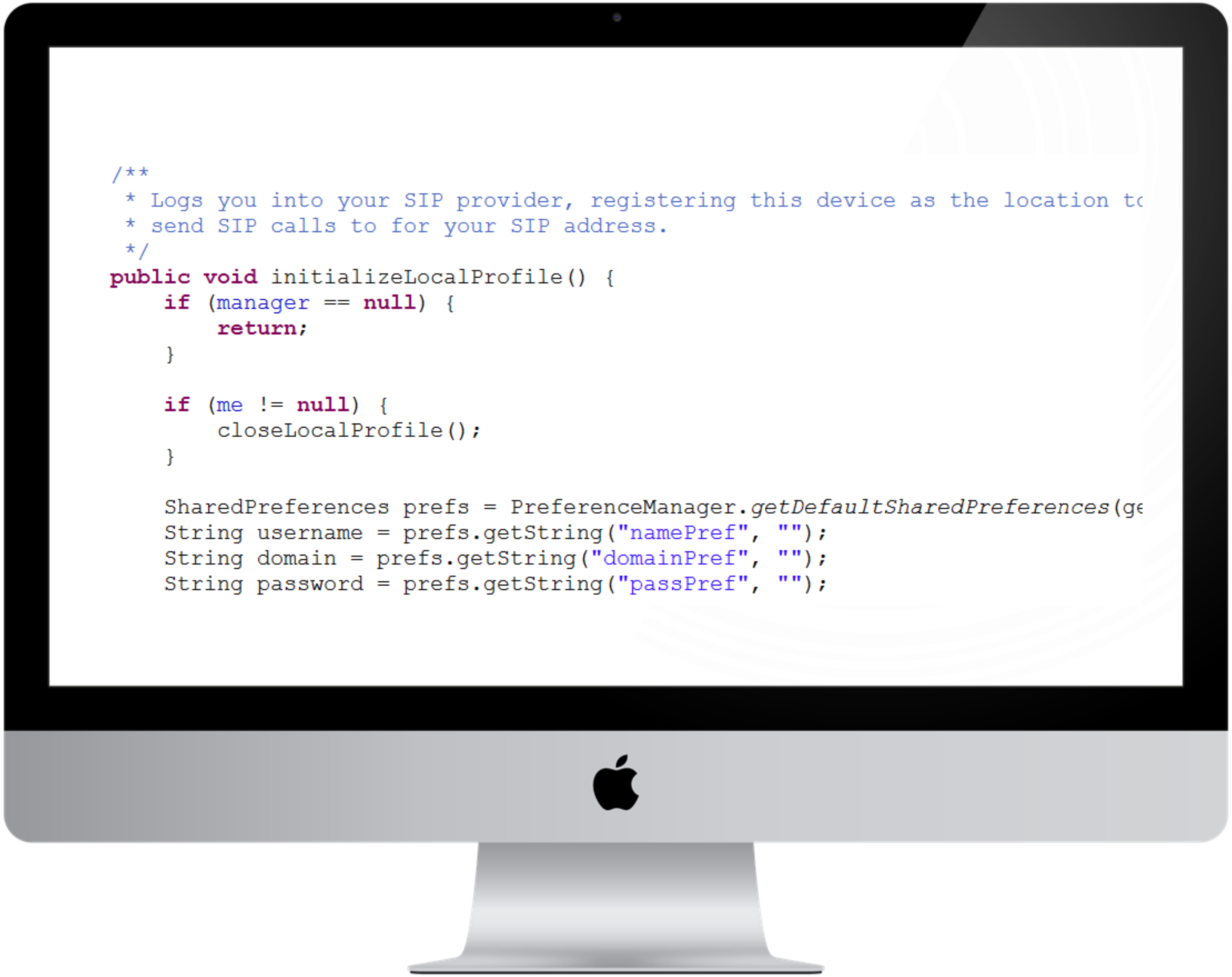
```
Intent { act=android.intent.action.MAIN
cat=[android.intent.category.LAUNCHER]
flg=0x10000000
cmp=com.isecpartners.android.intentsniffer/
.IntentSniffer } from recent tasks

Intent { act=android.intent.action.MAIN
cat=[android.intent.category.LAUNCHER]
flg=0x10000000 cmp=com.riis.login/.LoginActivity
} from recent tasks

Intent { act=android.intent.action.MAIN
cat=[android.intent.category.HOME]
flg=0x10000000 cmp=com.android.launcher/
com.android.launcher2.Launcher } from recent
tasks
```

OWASP Top 10

Lack of Binary Protections – Original Code



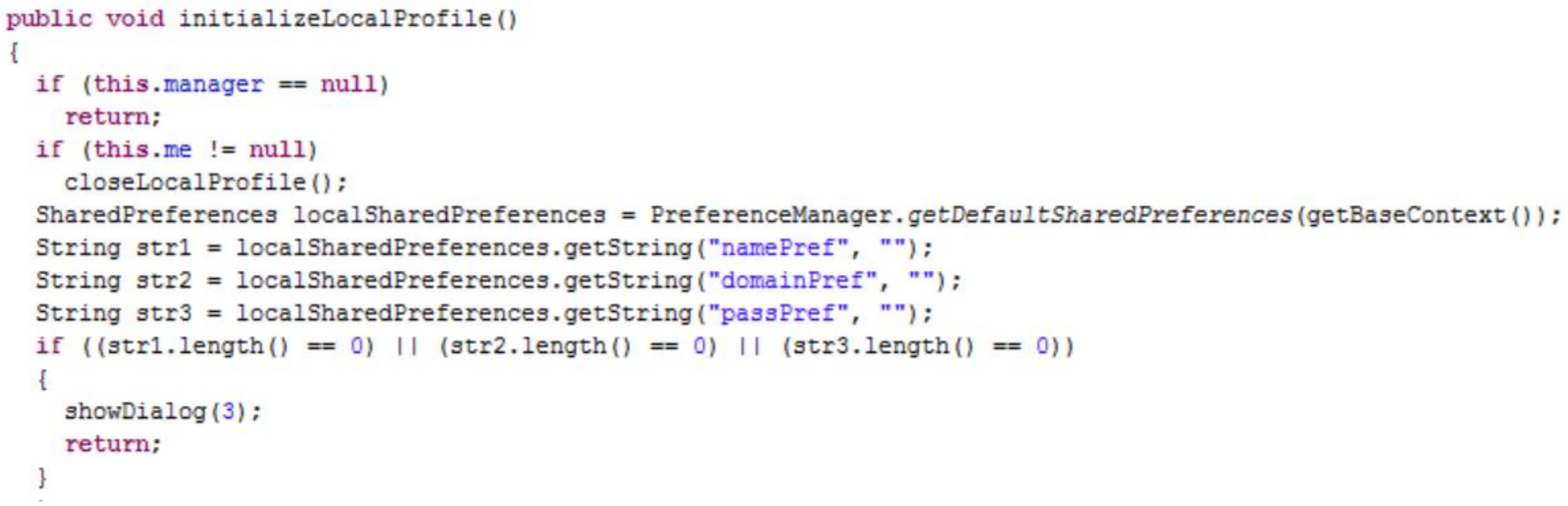
```
/**
 * Logs you into your SIP provider, registering this device as the location to
 * send SIP calls to for your SIP address.
 */
public void initializeLocalProfile() {
    if (manager == null) {
        return;
    }

    if (me != null) {
        closeLocalProfile();
    }

    SharedPreferences prefs = PreferenceManager.getDefaultSharedPreferences(ge
    String username = prefs.getString("namePref", "");
    String domain = prefs.getString("domainPref", "");
    String password = prefs.getString("passPref", "");
```

OWASP Top 10

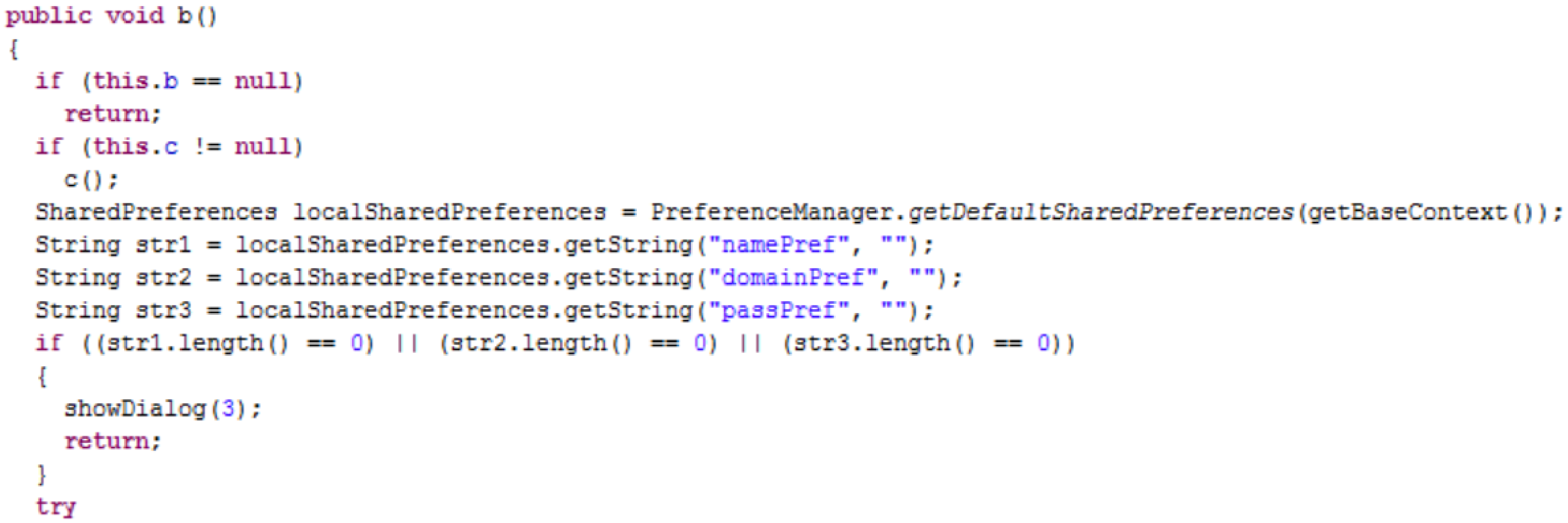
Lack of Binary Protections – No Obfuscation



```
public void initializeLocalProfile()
{
  if (this.manager == null)
    return;
  if (this.me != null)
    closeLocalProfile();
  SharedPreferences localSharedPreferences = PreferenceManager.getDefaultSharedPreferences(getBaseContext());
  String str1 = localSharedPreferences.getString("namePref", "");
  String str2 = localSharedPreferences.getString("domainPref", "");
  String str3 = localSharedPreferences.getString("passPref", "");
  if ((str1.length() == 0) || (str2.length() == 0) || (str3.length() == 0))
  {
    showDialog(3);
    return;
  }
```

OWASP Top 10

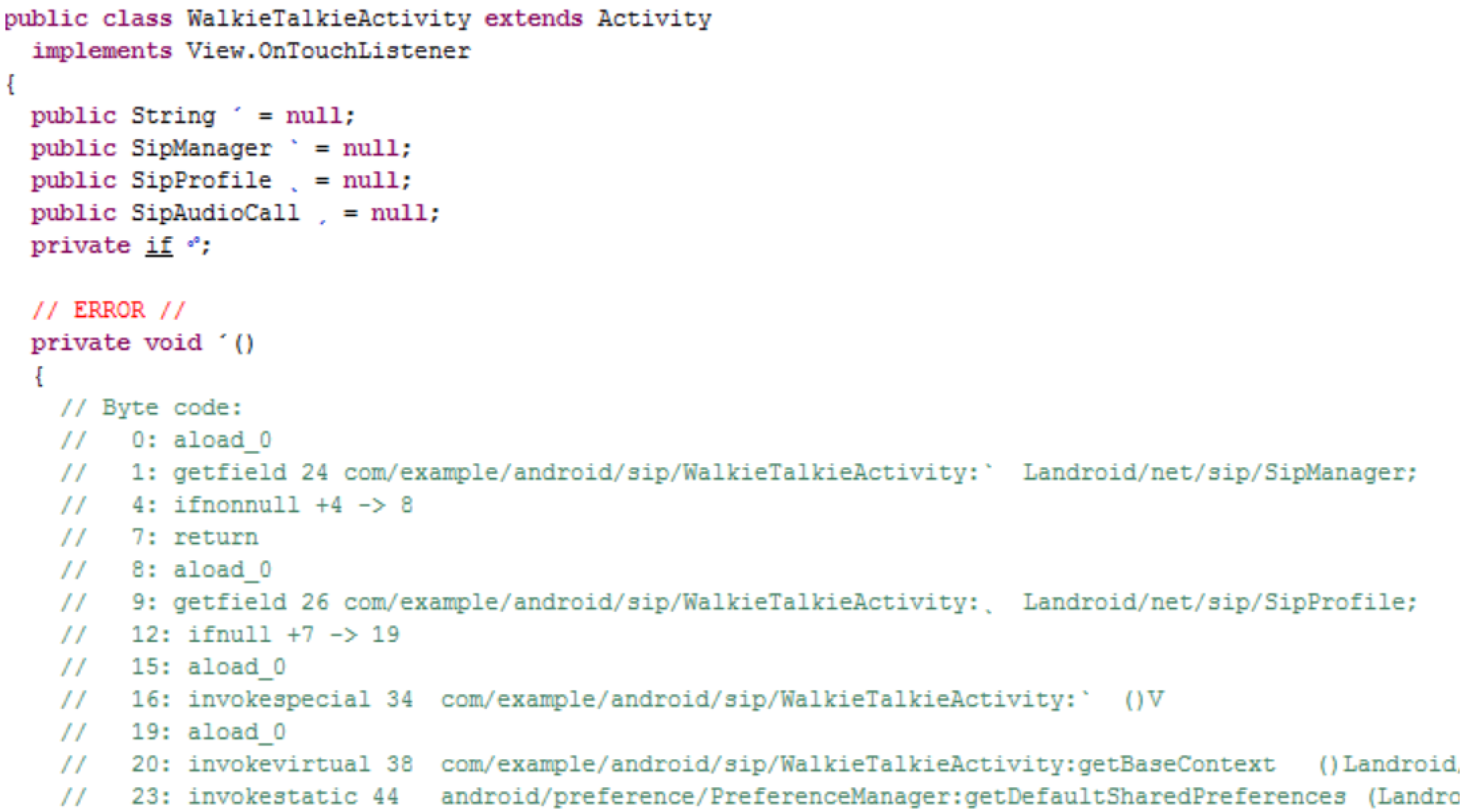
Lack of Binary Protections - ProGuard



```
public void b()
{
  if (this.b == null)
    return;
  if (this.c != null)
    c();
  SharedPreferences localSharedPreferences = PreferenceManager.getDefaultSharedPreferences(getBaseContext());
  String str1 = localSharedPreferences.getString("namePref", "");
  String str2 = localSharedPreferences.getString("domainPref", "");
  String str3 = localSharedPreferences.getString("passPref", "");
  if ((str1.length() == 0) || (str2.length() == 0) || (str3.length() == 0))
  {
    showDialog(3);
    return;
  }
  try
```

OWASP Top 10

Lack of Binary Protections - DexGuard



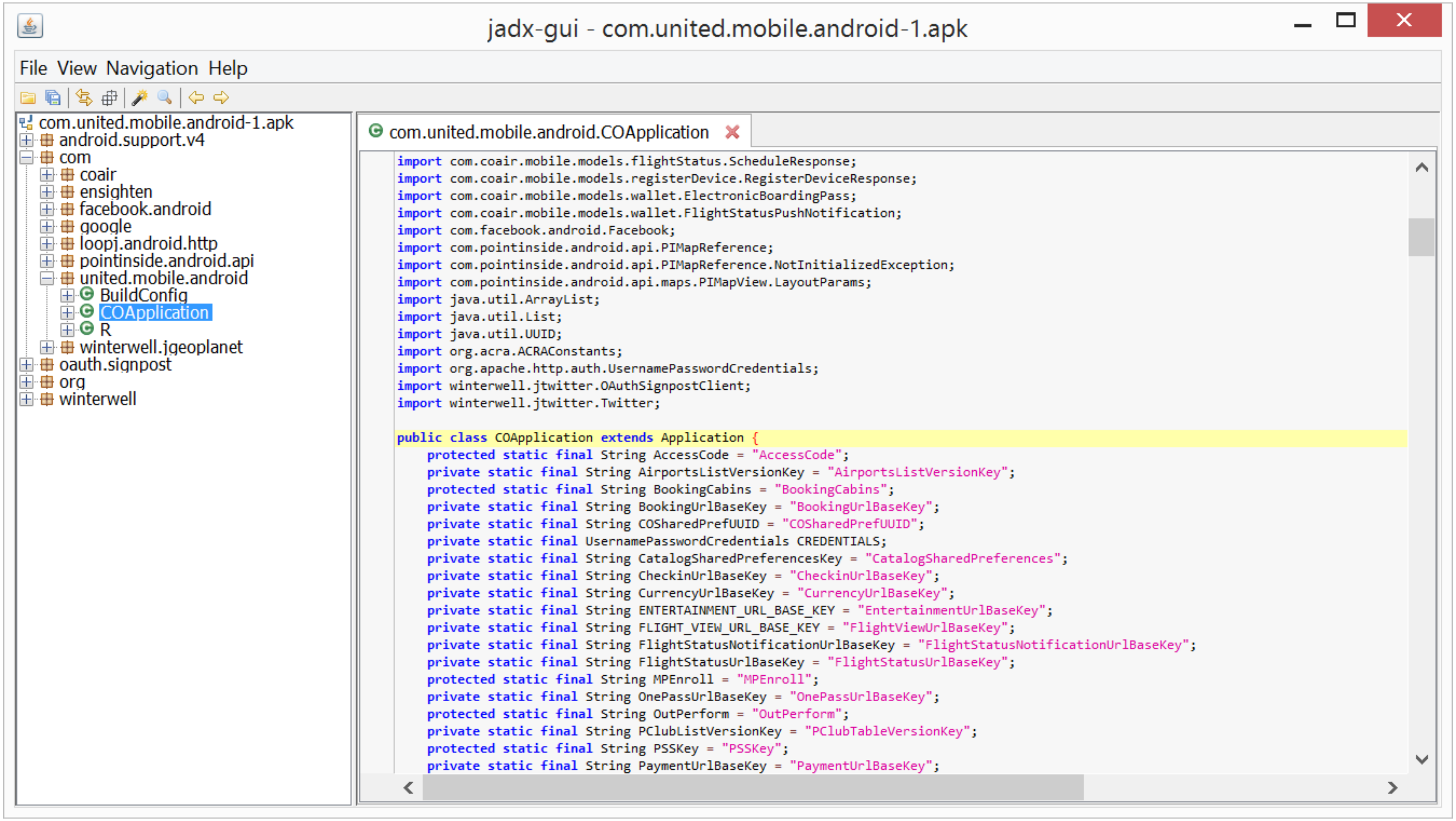
```
public class WalkieTalkieActivity extends Activity
  implements View.OnTouchListener
{
  public String ´ = null;
  public SipManager ` = null;
  public SipProfile ˛ = null;
  public SipAudioCall ˏ = null;
  private if ᵒ;

  // ERROR //
  private void ´()
  {
    // Byte code:
    //   0: aload_0
    //   1: getfield 24 com/example/android/sip/WalkieTalkieActivity:`  Landroid/net/sip/SipManager;
    //   4: ifnonnull +4 -> 8
    //   7: return
    //   8: aload_0
    //   9: getfield 26 com/example/android/sip/WalkieTalkieActivity:˛  Landroid/net/sip/SipProfile;
    //   12: ifnull +7 -> 19
    //   15: aload_0
    //   16: invokespecial 34  com/example/android/sip/WalkieTalkieActivity:`  ()V
    //   19: aload_0
    //   20: invokevirtual 38  com/example/android/sip/WalkieTalkieActivity:getBaseContext   ()Landroid
    //   23: invokestatic 44   android/preference/PreferenceManager:getDefaultSharedPreferences  (Landro
```

What's New

- Jadx
- android:debuggable=true (always)
- SSL Pinning
- Drozer
- Bug Bounty

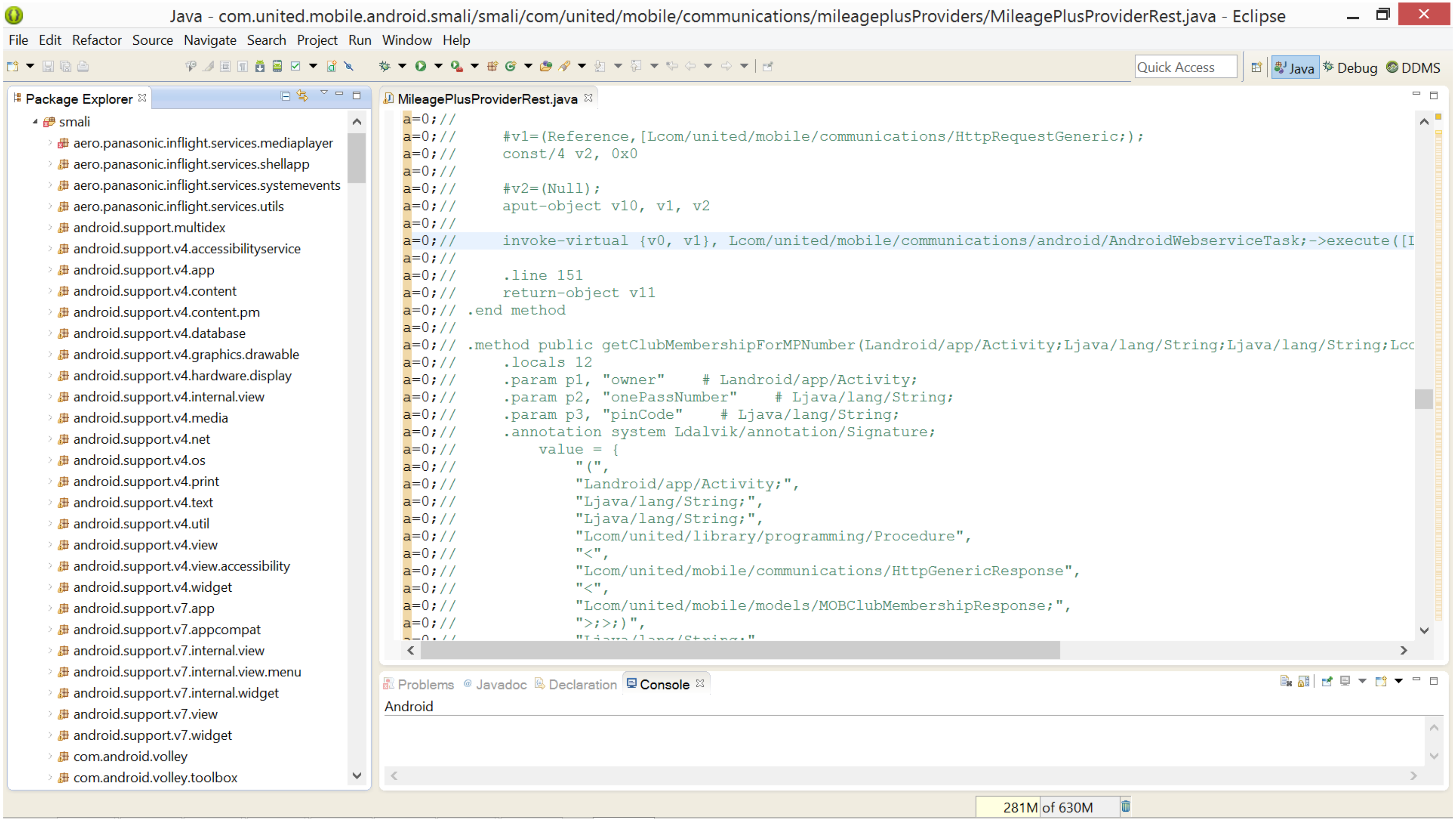
What's New
Jadx



```
import com.coair.mobile.models.flightStatus.ScheduleResponse;
import com.coair.mobile.models.registerDevice.RegisterDeviceResponse;
import com.coair.mobile.models.wallet.ElectronicBoardingPass;
import com.coair.mobile.models.wallet.FlightStatusPushNotification;
import com.facebook.android.Facebook;
import com.pointinside.android.api.PIMapReference;
import com.pointinside.android.api.PIMapReference.NotInitializedException;
import com.pointinside.android.api.maps.PIMapView.LayoutParams;
import java.util.ArrayList;
import java.util.List;
import java.util.UUID;
import org.acra.ACRAConstants;
import org.apache.http.auth.UsernamePasswordCredentials;
import winterwell.jtwitter.OAuthSignpostClient;
import winterwell.jtwitter.Twitter;

public class COApplication extends Application {
    protected static final String AccessCode = "AccessCode";
    private static final String AirportsListVersionKey = "AirportsListVersionKey";
    protected static final String BookingCabins = "BookingCabins";
    private static final String BookingUrlBaseKey = "BookingUrlBaseKey";
    private static final String COSharedPrefUUID = "COSharedPrefUUID";
    private static final UsernamePasswordCredentials CREDENTIALS;
    private static final String CatalogSharedPreferencesKey = "CatalogSharedPreferences";
    private static final String CheckinUrlBaseKey = "CheckinUrlBaseKey";
    private static final String CurrencyUrlBaseKey = "CurrencyUrlBaseKey";
    private static final String ENTERTAINMENT_URL_BASE_KEY = "EntertainmentUrlBaseKey";
    private static final String FLIGHT_VIEW_URL_BASE_KEY = "FlightViewUrlBaseKey";
    private static final String FlightStatusNotificationUrlBaseKey = "FlightStatusNotificationUrlBaseKey";
    private static final String FlightStatusUrlBaseKey = "FlightStatusUrlBaseKey";
    protected static final String MPEnroll = "MPEnroll";
    private static final String OnePassUrlBaseKey = "OnePassUrlBaseKey";
    protected static final String OutPerform = "OutPerform";
    private static final String PClubListVersionKey = "PClubTableVersionKey";
    protected static final String PSSKey = "PSSKey";
    private static final String PaymentUrlBaseKey = "PaymentUrlBaseKey";
```

What's New
android:debuggable=true



Java - com.united.mobile.android.smali/smali/com/united/mobile/communications/mileageplusProviders/MileagePlusProviderRest.java - Eclipse
File Edit Refactor Source Navigate Search Project Run Window Help
Quick Access
Java
Debug
DDMS
Package Explorer
MileagePlusProviderRest.java
Problems
Javadoc
Declaration
Console
Android
281M of 630M

```
smali
  aero.panasonic.inflight.services.mediaplayer
  aero.panasonic.inflight.services.shellapp
  aero.panasonic.inflight.services.systemevents
  aero.panasonic.inflight.services.utils
  android.support.multidex
  android.support.v4.accessibilityservice
  android.support.v4.app
  android.support.v4.content
  android.support.v4.content.pm
  android.support.v4.database
  android.support.v4.graphics.drawable
  android.support.v4.hardware.display
  android.support.v4.internal.view
  android.support.v4.media
  android.support.v4.net
  android.support.v4.os
  android.support.v4.print
  android.support.v4.text
  android.support.v4.util
  android.support.v4.view
  android.support.v4.view.accessibility
  android.support.v4.widget
  android.support.v7.app
  android.support.v7.appcompat
  android.support.v7.internal.view
  android.support.v7.internal.view.menu
  android.support.v7.internal.widget
  android.support.v7.view
  android.support.v7.widget
  com.android.volley
  com.android.volley.toolbox
```

```
a=0;//
a=0;//     #v1=(Reference,[Lcom/united/mobile/communications/HttpRequestGeneric;);
a=0;//     const/4 v2, 0x0
a=0;//
a=0;//     #v2=(Null);
a=0;//     aput-object v10, v1, v2
a=0;//
a=0;//     invoke-virtual {v0, v1}, Lcom/united/mobile/communications/android/AndroidWebserviceTask;->execute([I
a=0;//
a=0;//     .line 151
a=0;//     return-object v11
a=0;// .end method
a=0;//
a=0;// .method public getClubMembershipForMPNumber(Landroid/app/Activity;Ljava/lang/String;Ljava/lang/String;Lcc
a=0;//     .locals 12
a=0;//     .param p1, "owner"    # Landroid/app/Activity;
a=0;//     .param p2, "onePassNumber"    # Ljava/lang/String;
a=0;//     .param p3, "pinCode"    # Ljava/lang/String;
a=0;//     .annotation system Ldalvik/annotation/Signature;
a=0;//         value = {
a=0;//             "(",
a=0;//             "Landroid/app/Activity;",
a=0;//             "Ljava/lang/String;",
a=0;//             "Ljava/lang/String;",
a=0;//             "Lcom/united/library/programming/Procedure",
a=0;//             "<",
a=0;//             "Lcom/united/mobile/communications/HttpGenericResponse",
a=0;//             "<",
a=0;//             "Lcom/united/mobile/models/MOBClubMembershipResponse;",
a=0;//             ">;>;)",
a=0;//             "Ljava/lang/String;"
```

What's New
android:debuggable=true

- Disassemble using apktool

```
java -jar apktool.jar d -d test.apk -o out
```

- Find main class in AndroidManifest.xml

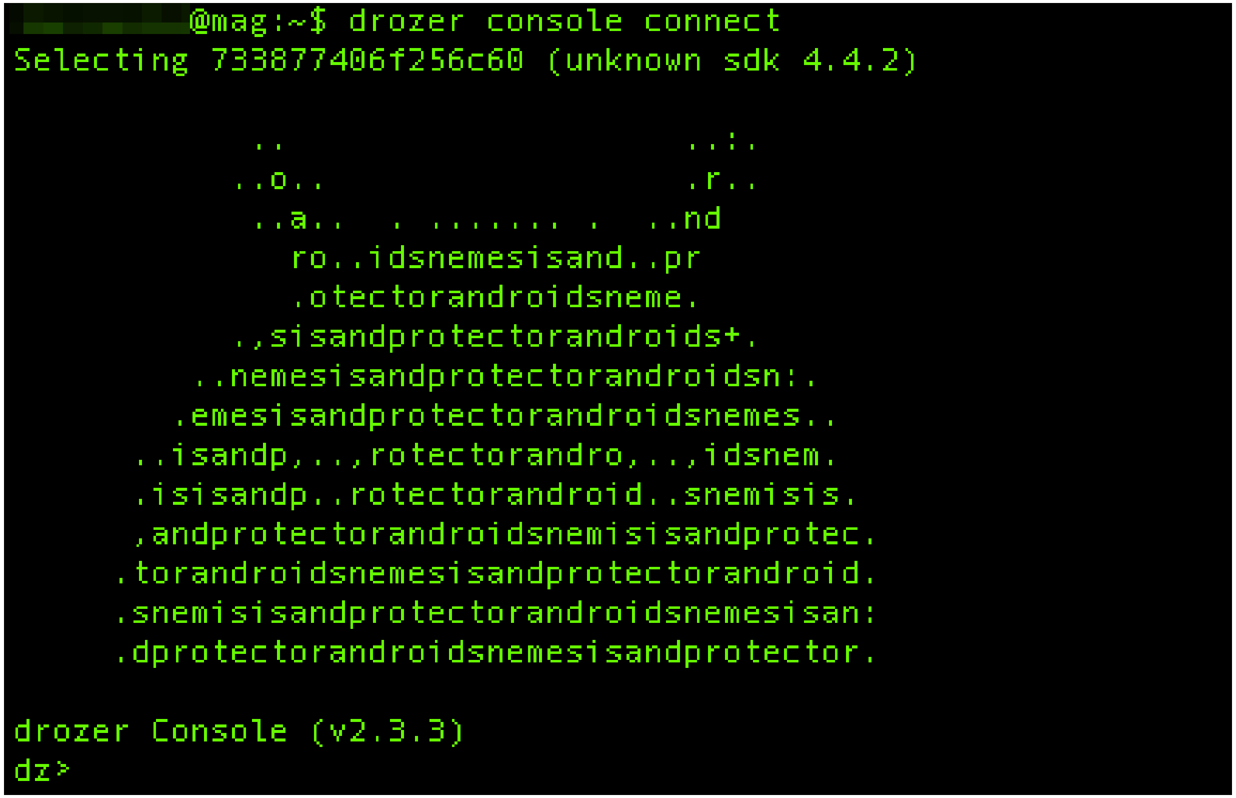
```
<activity android:label="@string/app_name"
android:name="com.acids.helloworld.MainActivity">
```

- Add debug wait to onCreate method

```
invoke-static {}, Landroid/os/Debug;->waitForDebugger()V
```

- Recompile using apktool
- Sign and install

What's New
Drozer



```
[redacted]@mag:~$ drozer console connect
Selecting 733877406f256c60 (unknown sdk 4.4.2)

            ..                    ..:.
           ..o..                  .r..
            ..a..  . ....... .  ..nd
              ro..idsnemesisand..pr
              .otectorandroidsneme.
           .,sisandprotectorandroids+.
         ..nemesisandprotectorandroidsn:.
        .emesisandprotectorandroidsnemes..
      ..isandp,..,rotectorandro,..,idsnem.
      .isisandp..rotectorandroid..snemisis.
      ,andprotectorandroidsnemisisandprotec.
     .torandroidsnemesisandprotectorandroid.
     .snemisisandprotectorandroidsnemesisan:
     .dprotectorandroidsnemesisandprotector.

drozer Console (v2.3.3)
dz>
```

What's New
Bug Bounty

- Security is too difficult to keep up with??
- Crowdsoure it
- Alternative to security firms
- United Airlines offering substantial airmiles, many others
- Beware, takes a lot of effort to keep up
- Update your app often to keep interest alive

Non Technical Top 10
Forrester

- ○ Inadequate developer incentives
- ○ Lack of mobile-specific security education
- ○ Inadequate resources available for mobile devsec
- ○ Security without consideration for human factors
- ○ Taking security out of the hands of the developer
- ○ Ignorance of the business need
- ○ Securing mobile, which means securing Agile
- ○ Focusing on security while ignoring privacy
- ○ Lack of security in design, development, and QA
- ○ Security as a bolt-on: post-production security

Recommendations

○ Understand debuggable=true

○ Rewrite your SSL code

○ Provide an email for white hats

○ Attacks are going to be more complex

○ Bug Bounty

Resources

- http://www.decompilingandroid.com
- http://www.owasp.org
- https://github.com/nelenkov/android-backup-extractor
- http://www.charlesproxy.com
- https://code.google.com/p/dex2jar
- https://www.mwrinfosecurity.com/products/drozer
- https://github.com/skylot/jadx
- http://keyczar.org
- http://www.saikoa.com
- http://sqlitebrowser.org

Contact Details

godfrey@riis.com,
@godfreynolan