The State of Security of Android Banking Apps in Poland

Tomasz Zieliński

Android Security Symposium 2017, Vienna

09.03.2017

PGS SOFTWARE

$whoami

- Software developer for ~15 years
- Android developer since 2009
- Mobile team lead at **PGS Software**,
  a nearshore Polish software house
- Recently worked for over 1.5 years on a mobile banking app for Android

18 banks, 19 Android mobile apps

The tests were conducted only on my own bank accounts, opened specifically for the purpose of R&D

White Hat – only original binaries, outgoing network traffic unchanged

All vulnerabilities and issues found were reported to the banks

Test period: July-October 2016

Important! This is not a ranking!

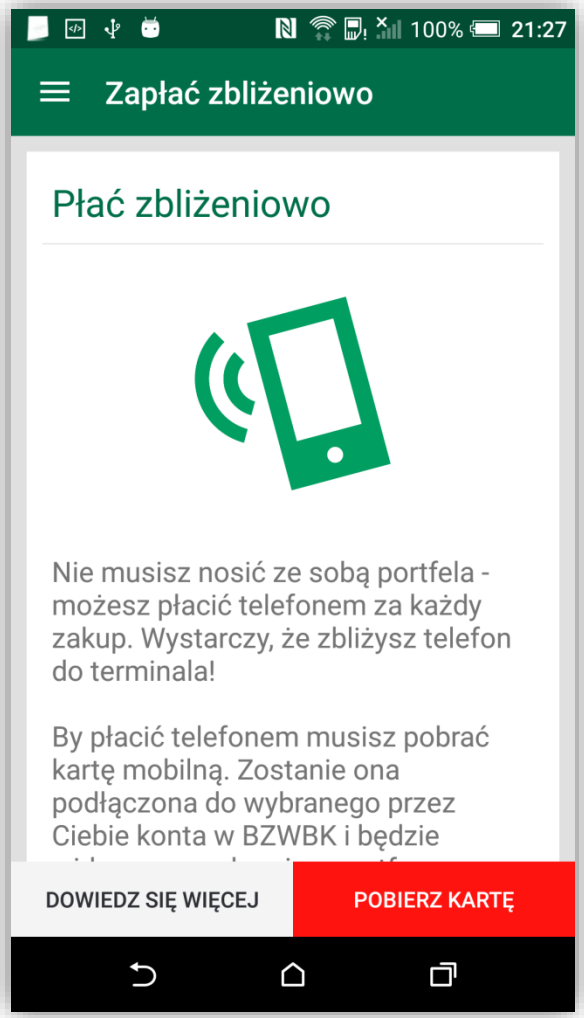
- PKO Bank Polski
- Pekao SA
- Bank Zachodni WBK
- mBank
- ING Bank Śląski
- Getin Noble Bank
- Bank Millennium
- Raiffeisen Polbank
- Citi Handlowy
- BGŻ BNP Paribas
- BPH
- Alior Bank
- IdeaBank
- Eurobank
- Credit Agricole
- T-Mobile usługi
- Orange Finanse
- Bank SMART

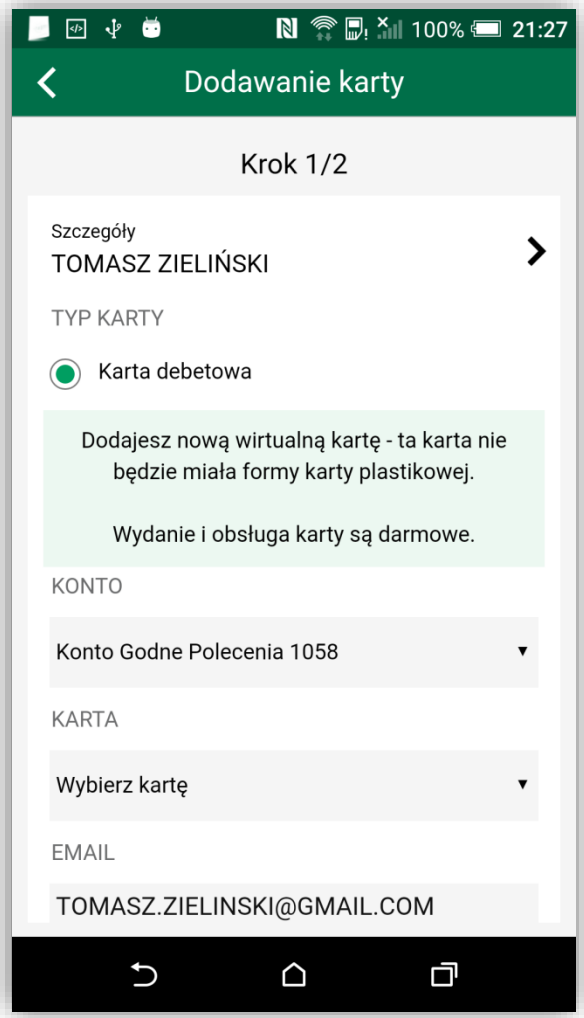
Agenda

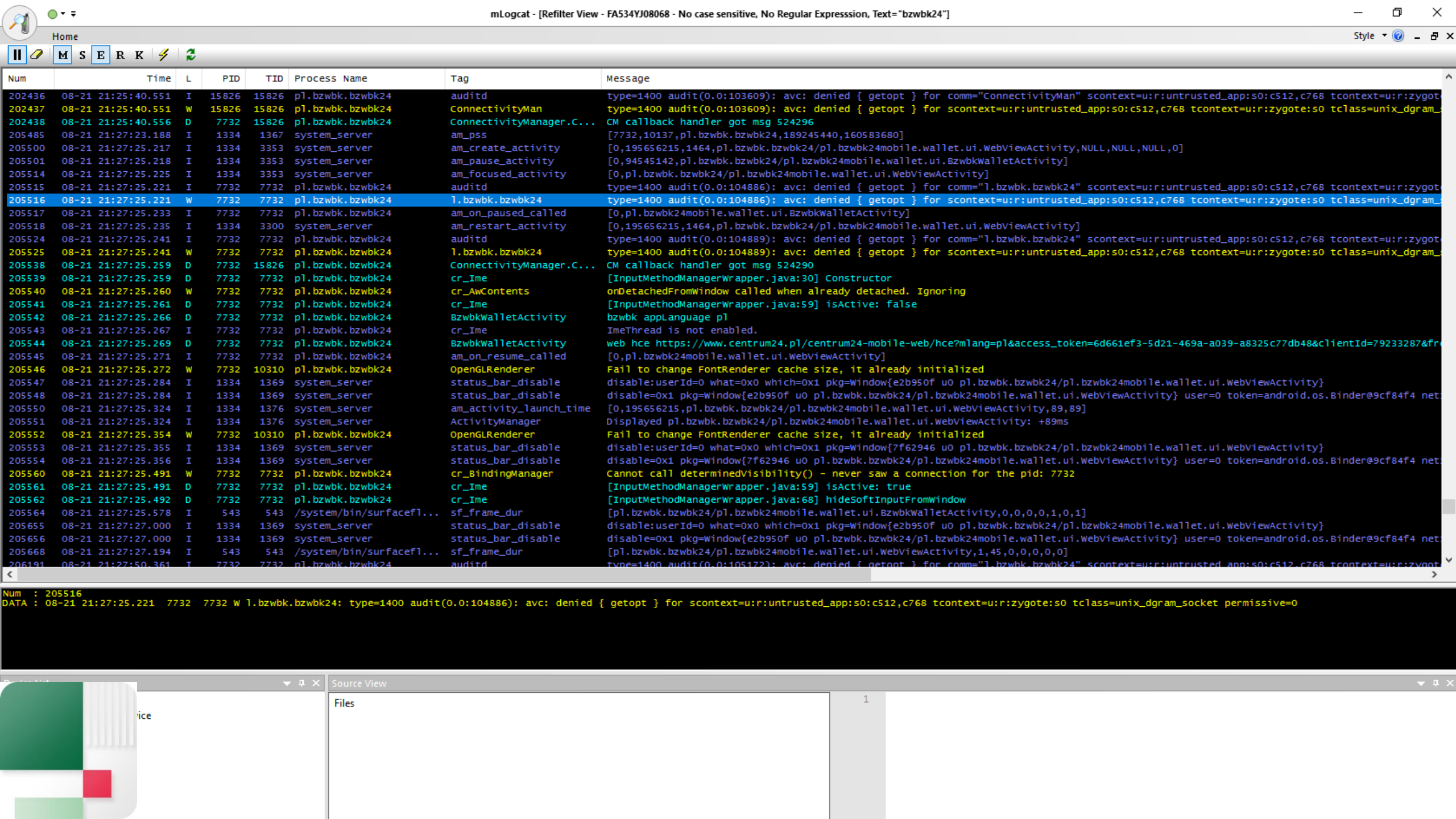
1. Critical Security Issues
2. Non-critical Security Issues
3. A Few Words About Contacting Banks
4. A Few Words About Where Our Data Goes

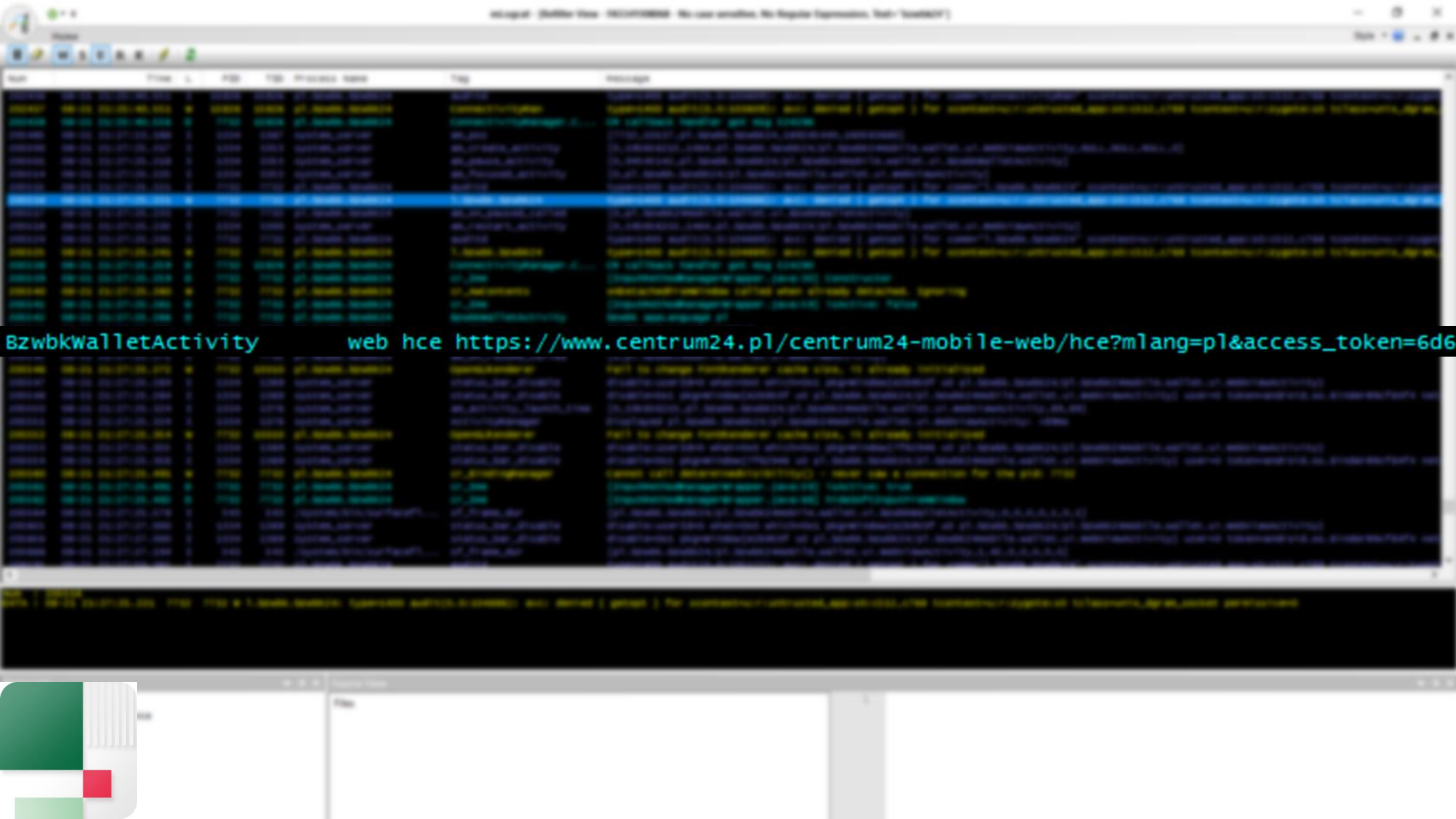
Critical Security Issues

BZ WBK – personal data leak






mLogcat - [Refilter View - FA534YJ08068 - No case sensitive, No Regular Expresssion, Text="bzwbk24"]
Home
Style
M S E R K
Num Time L PID TID Process Name Tag Message
202436 08-21 21:25:40.551 I 15826 15826 pl.bzwbk.bzwbk24 auditd type=1400 audit(0.0:103609): avc: denied { getopt } for comm="ConnectivityMan" scontext=u:r:untrusted_app:s0:c512,c768 tcontext=u:r:zygot
202437 08-21 21:25:40.551 W 15826 15826 pl.bzwbk.bzwbk24 ConnectivityMan type=1400 audit(0.0:103609): avc: denied { getopt } for scontext=u:r:untrusted_app:s0:c512,c768 tcontext=u:r:zygote:s0 tclass=unix_dgram_
202438 08-21 21:25:40.556 D 7732 15826 pl.bzwbk.bzwbk24 ConnectivityManager.C... CM callback handler got msg 524296
205485 08-21 21:27:23.188 I 1334 1367 system_server am_pss [7732,10137,pl.bzwbk.bzwbk24,189245440,160583680]
205500 08-21 21:27:25.217 I 1334 3353 system_server am_create_activity [0,195656215,1464,pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.WebViewActivity,NULL,NULL,NULL,0]
205501 08-21 21:27:25.218 I 1334 3353 system_server am_pause_activity [0,94545142,pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.BzwbkWalletActivity]
205514 08-21 21:27:25.225 I 1334 3353 system_server am_focused_activity [0,pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.WebViewActivity]
205515 08-21 21:27:25.221 I 7732 7732 pl.bzwbk.bzwbk24 auditd type=1400 audit(0.0:104886): avc: denied { getopt } for comm="l.bzwbk.bzwbk24" scontext=u:r:untrusted_app:s0:c512,c768 tcontext=u:r:zygot
205516 08-21 21:27:25.221 W 7732 7732 pl.bzwbk.bzwbk24 l.bzwbk.bzwbk24 type=1400 audit(0.0:104886): avc: denied { getopt } for scontext=u:r:untrusted_app:s0:c512,c768 tcontext=u:r:zygote:s0 tclass=unix_dgram_
205517 08-21 21:27:25.233 I 7732 7732 pl.bzwbk.bzwbk24 am_on_paused_called [0,pl.bzwbk24mobile.wallet.ui.BzwbkWalletActivity]
205518 08-21 21:27:25.235 I 1334 3300 system_server am_restart_activity [0,195656215,1464,pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.WebViewActivity]
205524 08-21 21:27:25.241 I 7732 7732 pl.bzwbk.bzwbk24 auditd type=1400 audit(0.0:104889): avc: denied { getopt } for comm="l.bzwbk.bzwbk24" scontext=u:r:untrusted_app:s0:c512,c768 tcontext=u:r:zygot
205525 08-21 21:27:25.241 W 7732 7732 pl.bzwbk.bzwbk24 l.bzwbk.bzwbk24 type=1400 audit(0.0:104889): avc: denied { getopt } for scontext=u:r:untrusted_app:s0:c512,c768 tcontext=u:r:zygote:s0 tclass=unix_dgram_
205538 08-21 21:27:25.259 D 7732 15826 pl.bzwbk.bzwbk24 ConnectivityManager.C... CM callback handler got msg 524290
205539 08-21 21:27:25.259 D 7732 7732 pl.bzwbk.bzwbk24 cr_Ime [InputMethodManagerWrapper.java:30] Constructor
205540 08-21 21:27:25.260 W 7732 7732 pl.bzwbk.bzwbk24 cr_AwContents onDetachedFromWindow called when already detached. Ignoring
205541 08-21 21:27:25.261 D 7732 7732 pl.bzwbk.bzwbk24 cr_Ime [InputMethodManagerWrapper.java:59] isActive: false
205542 08-21 21:27:25.266 D 7732 7732 pl.bzwbk.bzwbk24 BzwbkWalletActivity bzwbk appLanguage pl
205543 08-21 21:27:25.267 I 7732 7732 pl.bzwbk.bzwbk24 cr_Ime ImeThread is not enabled.
205544 08-21 21:27:25.269 D 7732 7732 pl.bzwbk.bzwbk24 BzwbkWalletActivity web hce https://www.centrum24.pl/centrum24-mobile-web/hce?mlang=pl&access_token=6d661ef3-5d21-469a-a039-a8325c77db48&clientId=79233287&fr
205545 08-21 21:27:25.271 I 7732 7732 pl.bzwbk.bzwbk24 am_on_resume_called [0,pl.bzwbk24mobile.wallet.ui.WebViewActivity]
205546 08-21 21:27:25.272 W 7732 10310 pl.bzwbk.bzwbk24 OpenGLRenderer Fail to change FontRenderer cache size, it already initialized
205547 08-21 21:27:25.284 I 1334 1369 system_server status_bar_disable disable:userId=0 what=0x0 which=0x1 pkg=Window{e2b950f u0 pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.WebViewActivity}
205548 08-21 21:27:25.284 I 1334 1369 system_server status_bar_disable disable=0x1 pkg=Window{e2b950f u0 pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.WebViewActivity} user=0 token=android.os.Binder@9cf84f4 net
205550 08-21 21:27:25.324 I 1334 1376 system_server am_activity_launch_time [0,195656215,pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.WebViewActivity,89,89]
205551 08-21 21:27:25.324 I 1334 1376 system_server ActivityManager Displayed pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.WebViewActivity: +89ms
205552 08-21 21:27:25.354 W 7732 10310 pl.bzwbk.bzwbk24 OpenGLRenderer Fail to change FontRenderer cache size, it already initialized
205553 08-21 21:27:25.355 I 1334 1369 system_server status_bar_disable disable:userId=0 what=0x0 which=0x1 pkg=Window{7f62946 u0 pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.WebViewActivity}
205554 08-21 21:27:25.356 I 1334 1369 system_server status_bar_disable disable=0x1 pkg=Window{7f62946 u0 pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.WebViewActivity} user=0 token=android.os.Binder@9cf84f4 net
205560 08-21 21:27:25.491 W 7732 7732 pl.bzwbk.bzwbk24 cr_BindingManager Cannot call determinedVisibility() - never saw a connection for the pid: 7732
205561 08-21 21:27:25.491 D 7732 7732 pl.bzwbk.bzwbk24 cr_Ime [InputMethodManagerWrapper.java:59] isActive: true
205562 08-21 21:27:25.492 D 7732 7732 pl.bzwbk.bzwbk24 cr_Ime [InputMethodManagerWrapper.java:68] hideSoftInputFromWindow
205564 08-21 21:27:25.578 I 543 543 /system/bin/surfacefl... sf_frame_dur [pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.BzwbkWalletActivity,0,0,0,0,1,0,1]
205655 08-21 21:27:27.000 I 1334 1369 system_server status_bar_disable disable:userId=0 what=0x0 which=0x1 pkg=Window{e2b950f u0 pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.WebViewActivity}
205656 08-21 21:27:27.000 I 1334 1369 system_server status_bar_disable disable=0x1 pkg=Window{e2b950f u0 pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.WebViewActivity} user=0 token=android.os.Binder@9cf84f4 net
205668 08-21 21:27:27.194 I 543 543 /system/bin/surfacefl... sf_frame_dur [pl.bzwbk.bzwbk24/pl.bzwbk24mobile.wallet.ui.WebViewActivity,1,45,0,0,0,0,0]
Num : 205516
DATA : 08-21 21:27:25.221 7732 7732 W l.bzwbk.bzwbk24: type=1400 audit(0.0:104886): avc: denied { getopt } for scontext=u:r:untrusted_app:s0:c512,c768 tcontext=u:r:zygote:s0 tclass=unix_dgram_socket permissive=0
Source View
Files
1


BzwbkWalletActivity web hce https://www.centrum24.pl/centrum24-mobile-web/hce?mlang=pl&access_token=6d6

Dodawanie karty

Bank Zachodni WBK S.A. [PL] centrum24.pl/centrum24-mobile-web/hce?mlang=pl&access_token=6d661ef3-5d21-46[redacted]db48&clientId=[redacted]&frontendId=8#/app/hce

Dodawanie karty

Krok 1/2

Szczegóły
TOMASZ ZIELIŃSKI

TYP KARTY

Karta debetowa

Dodajesz nową wirtualną kartę - ta karta nie będzie miała formy karty plastikowej.

Wydanie i obsługa karty są darmowe.

KONTO

Konto Godne Polecenia 1058

KARTA

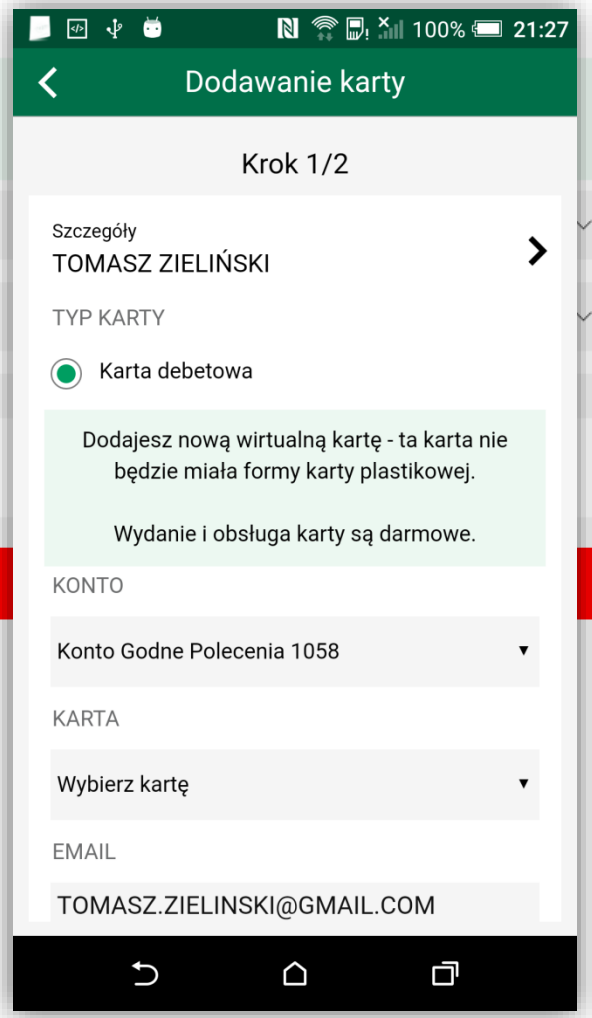
MasterCard Mobile Debetowa

EMAIL

TOMASZ.ZIELINSKI@GMAIL.COM

Wnioskuję o przesłanie przez BZ WBK regulacji bankowych

Dalej



BZ WBK – personal data leak

Logcat

- Android system logs
- Every app can write to logs
- Up to Android 4.0, app with proper permission could read all logs
- BZ WBK app worked on 4.0

Link valid for a long time (30+ minutes), independent from app logout, insensible to User-Agent and source IP changes

Dodawanie karty

Bank Zachodni WBK S.A. [PL] centrum24.pl/centrum24-mobile-web/hce?mlang=pl&access_token=6d661ef3-5d21-46 db48&clientId= &frontendId=8#/app/hce

Dodawanie karty

Krok 2/2

Umowa o kartę "MasterCard Mobile Debetowa"

Zobacz pełną treść umowy

Oświadczam, że umowa została mi dostarczo

Akceptuję warunki umowy i przesyłam wniose

Umowa o kartę

Poniższa oferta Banku Zachodniego WBK S.A. przestaje wiązać, jeśli nie zostanie przyjęta przez Posiadacza niezwłocznie.

Umowa o instrument płatniczy

zawarta w dniu 21-08-2016 pomiędzy

Bankiem Zachodnim WBK S.A. z siedzibą we Wrocławiu, ul. Rynek 9/11, 50-950 Wrocław, zarejestrowanym w Sądzie Rejonowym dla Wrocławia - Fabrycznej, VI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000008723, REGON 930041341, NIP 896 000 56 73, kapitał zakładowy i wpłacony 992 345 340 zł,

zwanym dalej **„Bankiem"**, a

TOMASZ ZIELIŃSKI — *imię, nazwisko*; *data urodzenia*; *PESEL (dotyczy rezydentów)*

seria i numer dowodu; *seria i numer paszportu*

adres do korespondencji:

ulica; *numer posesji / lokalu*

51-354 — *kod pocztowy*; WROCŁAW — *miejscowość*

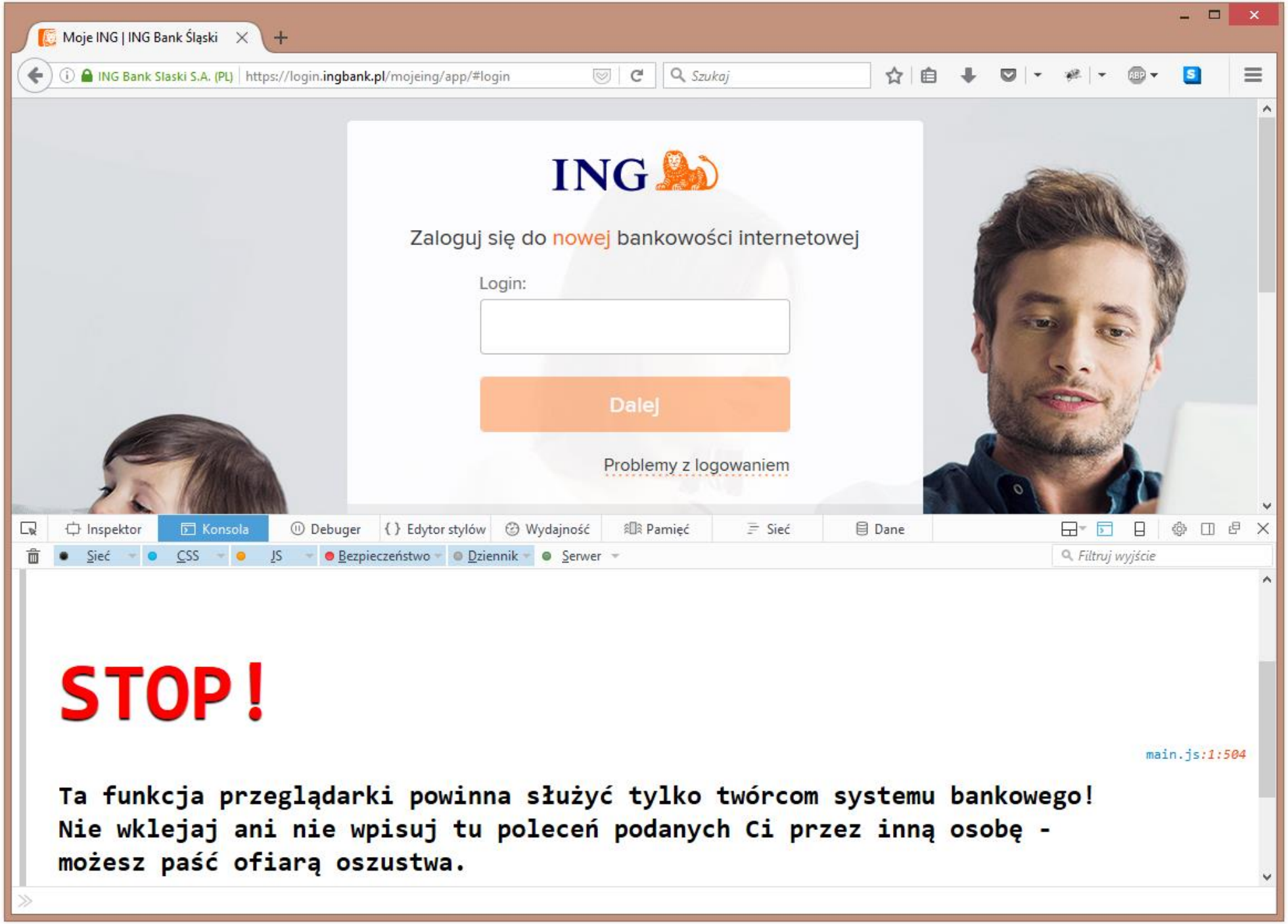
zwanym dalej **„Posiadaczem"**,
o następującej treści:

Przedmiot umowy

§1

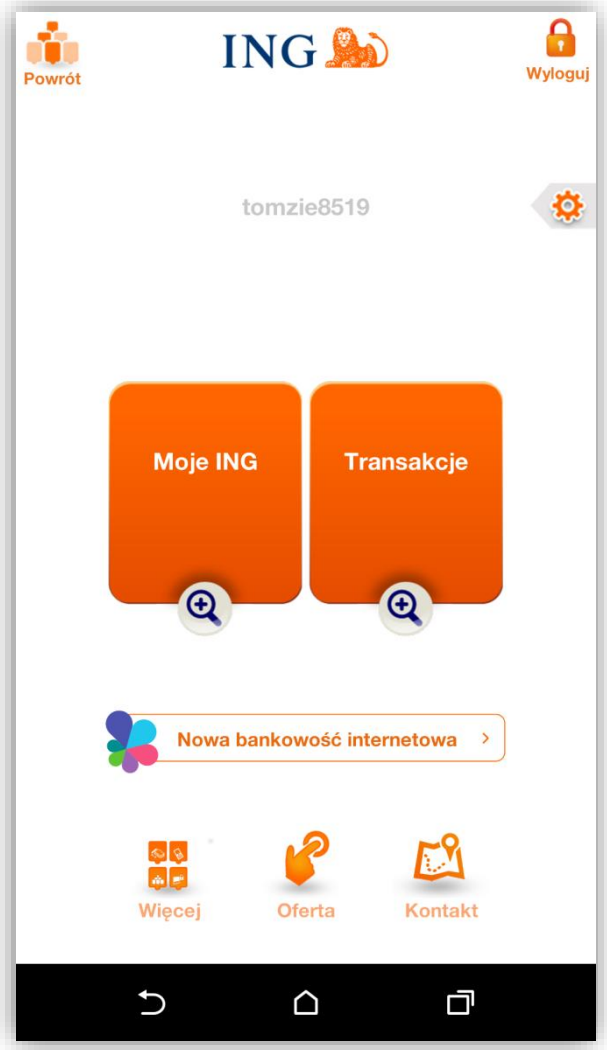
1. Na mocy niniejszej umowy Bank wydaje do rachunku o numerze 18 1090 2590 0000 58 Posiadaczowi instrument płatniczy:

ING – session takeover

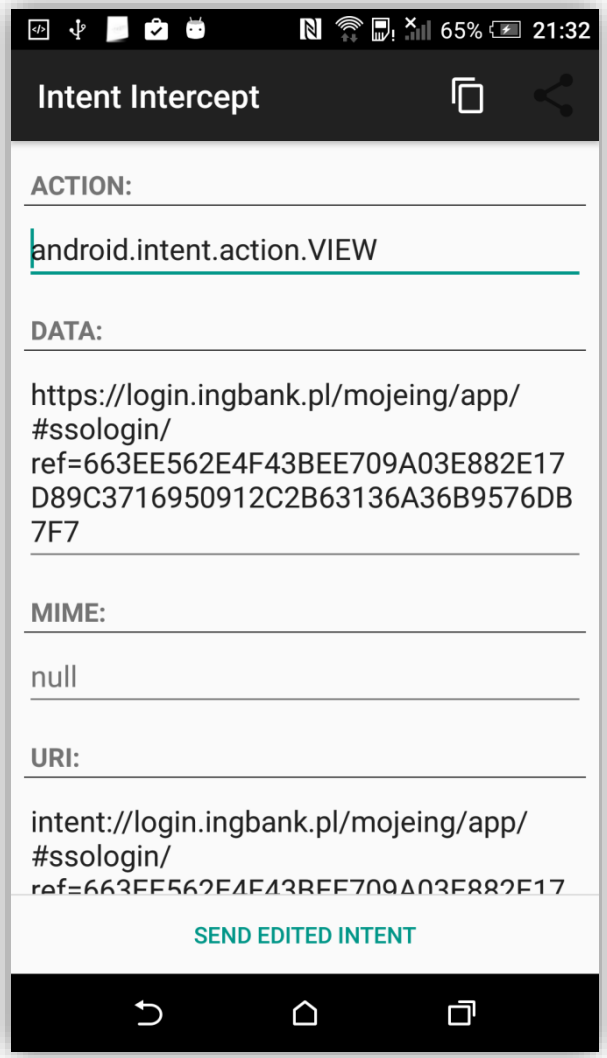

Moje ING | ING Bank Śląski
ING Bank Slaski S.A. (PL) https://login.ingbank.pl/mojeing/app/#login
Szukaj
ING
Zaloguj się do nowej bankowości internetowej
Login:
Dalej
Problemy z logowaniem
Inspektor
Konsola
Debuger
Edytor stylów
Wydajność
Pamięć
Sieć
Dane
Sieć
CSS
JS
Bezpieczeństwo
Dziennik
Serwer
Filtruj wyjście
STOP!
main.js:1:504
Ta funkcja przeglądarki powinna służyć tylko twórcom systemu bankowego!
Nie wklejaj ani nie wpisuj tu poleceń podanych Ci przez inną osobę -
możesz paść ofiarą oszustwa.

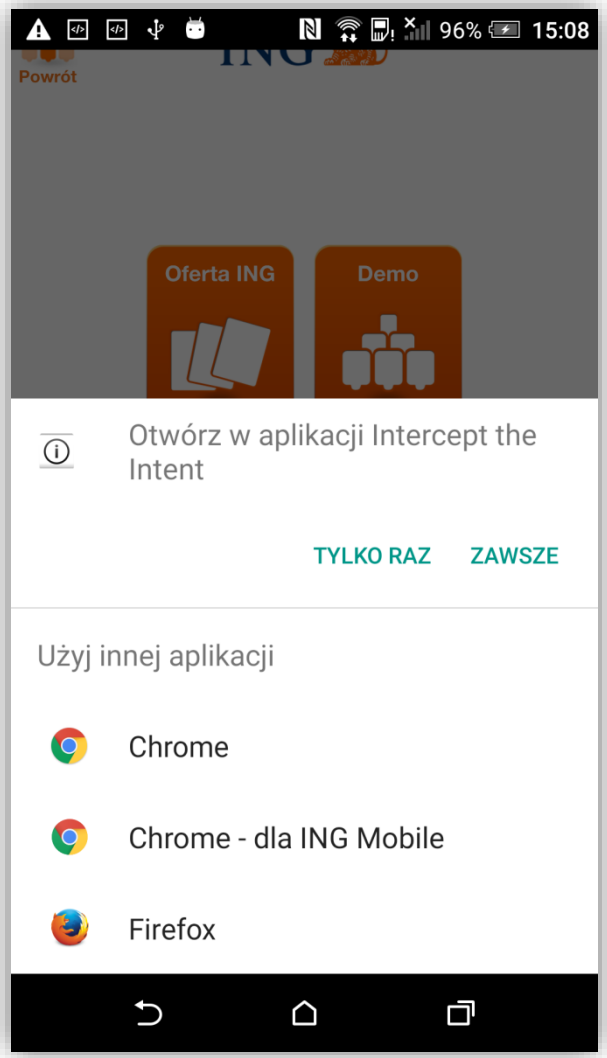
ING – session takeover

- Single Sign-On link in app
- Self-XSS warning printed in JavaScript console
- Android = logcat instead of JS console, **output contains source URL**
- (kaboom)
- SSO insensible to User-Agent change



ING – SSO link takeover





Pekao – masked password leak

Series of bad practices:

- network communication with no key/cert pinning
- masked password characters sent directly, not hashed
- whole network exchange printed to logcat

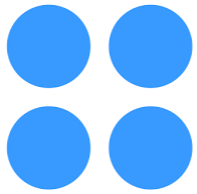
```
QUERY (SERVER): <?xml version="1.0" encoding="UTF-8"?><rt>
  <au>
    <t>[redacted]2c5685f96459[redacted]6</t>
```

```
    <n>PEKAO</n>
    <d>6.0</d>
    <f>HTC</f>
    <i>[redacted]</i>
    <a>[redacted]</a>
    <k>
      <dic>
        <o>
          <key>PACKAGE_VERSION_CF</key>
          <val>2014-08-12 10:00:00_0</val>
        </o>
        <o>
          <key>PREPAID_STATEMENT_ACCEPTED</key>
          <val>0</val>
        </o>
      </dic>
    </k>
  </pi>
  <b>
    <st>
      <sti>
        <id>SM</id>
        <ix>EMB_START_MENU</ix>
      </sti>
      <sti>
        <id>CF</id>
      </sti>
    </st>
    <post>
      <id>LOGIN_AUTH</id>
      <p0>[redacted]</p0>
      <p1>xjBrFCDj2</p1>
      <p2/>
      <p3>1</p3>
```

IdeaBank – full personal data sent to mobile

Backend sent to app:

- name, last name
- personal ID number (PESEL)
- address, phone number
- mother’s maiden name
- ID card number and validity date
- internal bank data




```
"customerDetails":{
    "address":{
        "street":"
        "country":"Polska",
        "postalCode":"51-354"
},
"pep":"no",
"cellularPhone":"+48
"surname":"ZIELIŃSKI",
"taxCountry":"Polska",
"residenceCountry":"Polska",
"shortName":"TOMASZ ZIELIŃSKI",
"oldContract":"no",
"customerOrigin":"Internet",
"defCustomerId":"
"customerClass":"Osoby fizyczne",
"isCustomerContactDetailsModifiable":"yes",
"forename":"TOMASZ",
"cardReservationAnswer":"Odp.",
"citizenship":"Polska",
"customerGroup":"Jednostki niepowiązane z Idea Bank
"birthPlace":
"phone":"+48
"bankContract":"yes",
"sex":"M",
"modificationTime":"2016-
```

IdeaBank – full personal data sent to mobile


```
"ssoRegistered":"yes",
"customerDataLevel":"1",
"contextStatus":"A",
"customerRiskLevel":"Podwyższone",
```

IdeaBank – test logins and passwords

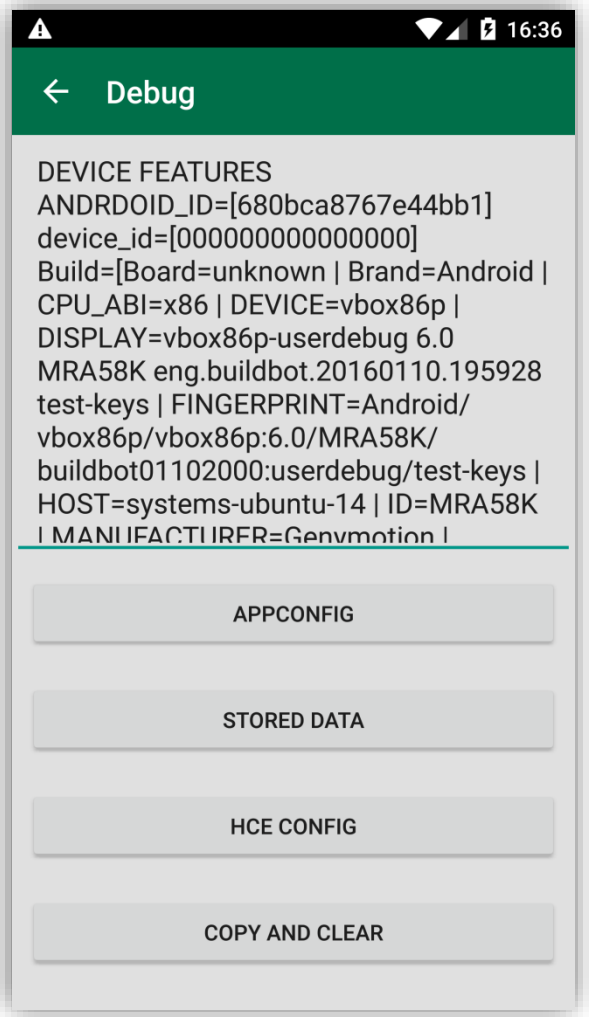
Android app is in fact a ZIP file with a well-defined directory structure.

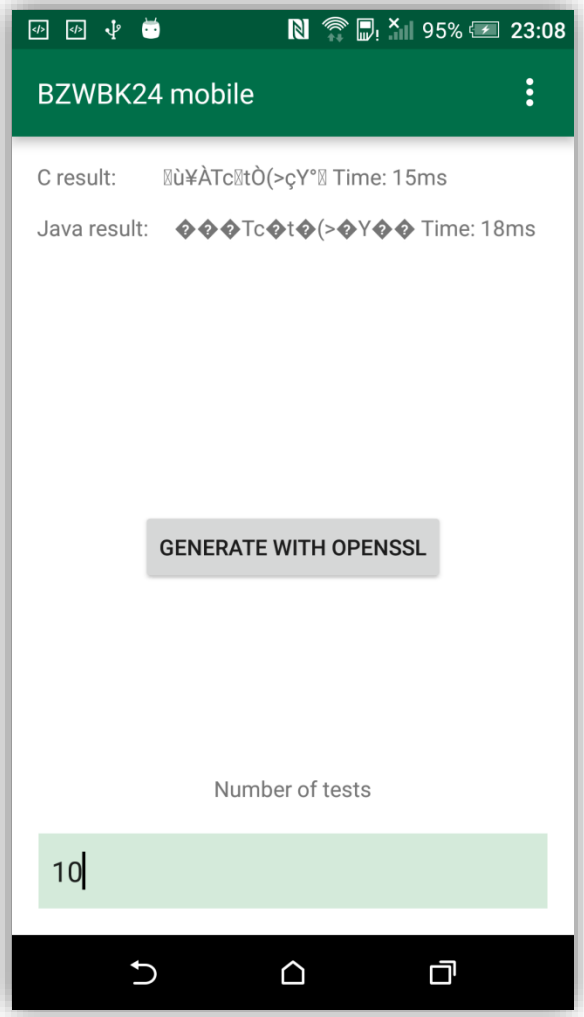
There is a directory for raw resources, with an unexpected file `/res/raw/users.csv`

```
rozne okresy w lokacie;47507073;Solaris86;1005871
57178520;57178520;123456Qq;none
Solarissss;Solarissss;Solaris86;none
edycja blad;36620706;123456Qq;none
user1;17345296;Marcin12;2964
user1a;86704303;Marcin12;1000565
user2;52160468;Marcin12;1000568
user3;56436841;123456Qq;1002921
user4;27251376;123456Qq;1002942
user5;31274110;123456Qq;1002922
user6;12083370;5169389543;1003053
user8;24843014;Przemek1;1002307
user9;44281517;123456Qq;1003462
user10;70045088;Marcin12;1000897
user12;10773883;123456Qq;1003793
user13;96659482;Marcin12;5593
user14;35767912;Kanapka6;1001703
user15;66723493;Przemek1;1002299
user16;97366064;123456Qq;1005394
user17;43279804;Marta123;1003822
user18;88309903;Goosip2008;7491
user19;60207105;123456Qq;1005442
user20;46626671;123456Qq;1005598
user21;97404421;123456Qq;1005603
AnnaMaria;AnnaMaria;Marta123;none
```

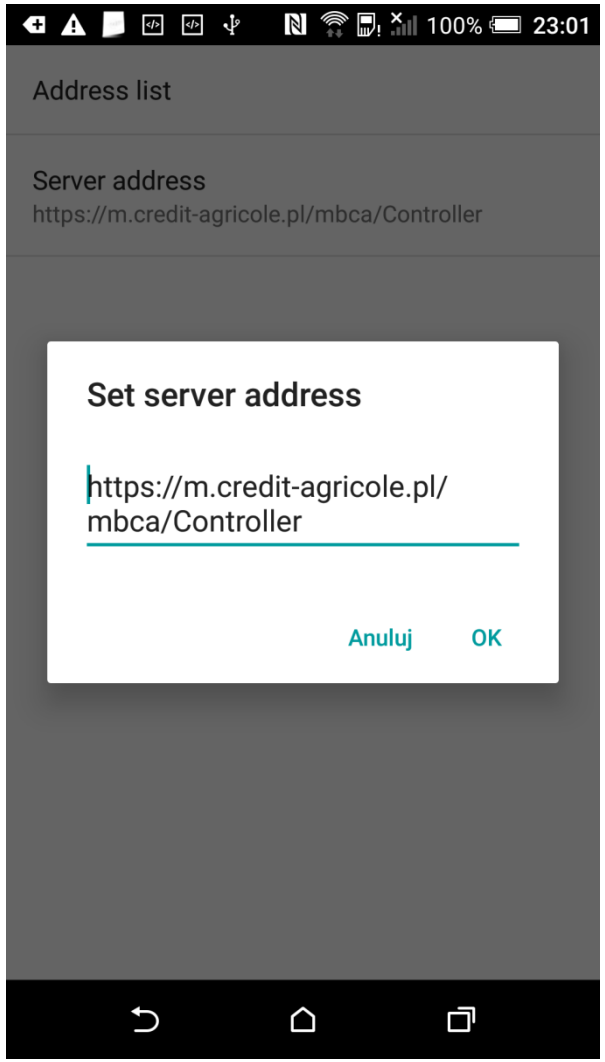
Debug Code Found in Apps

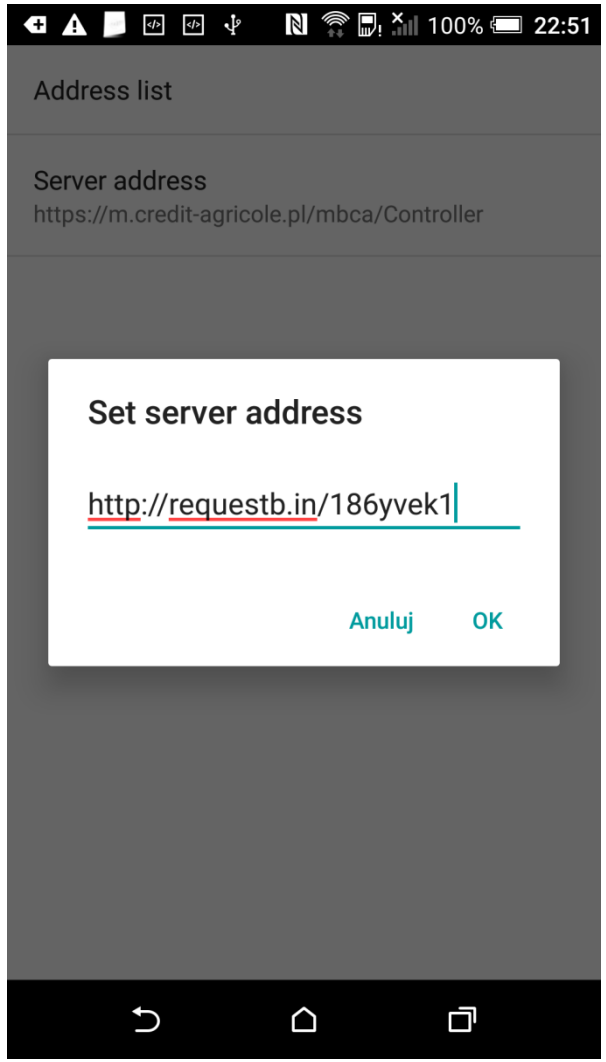
BZ WBK – debug screens

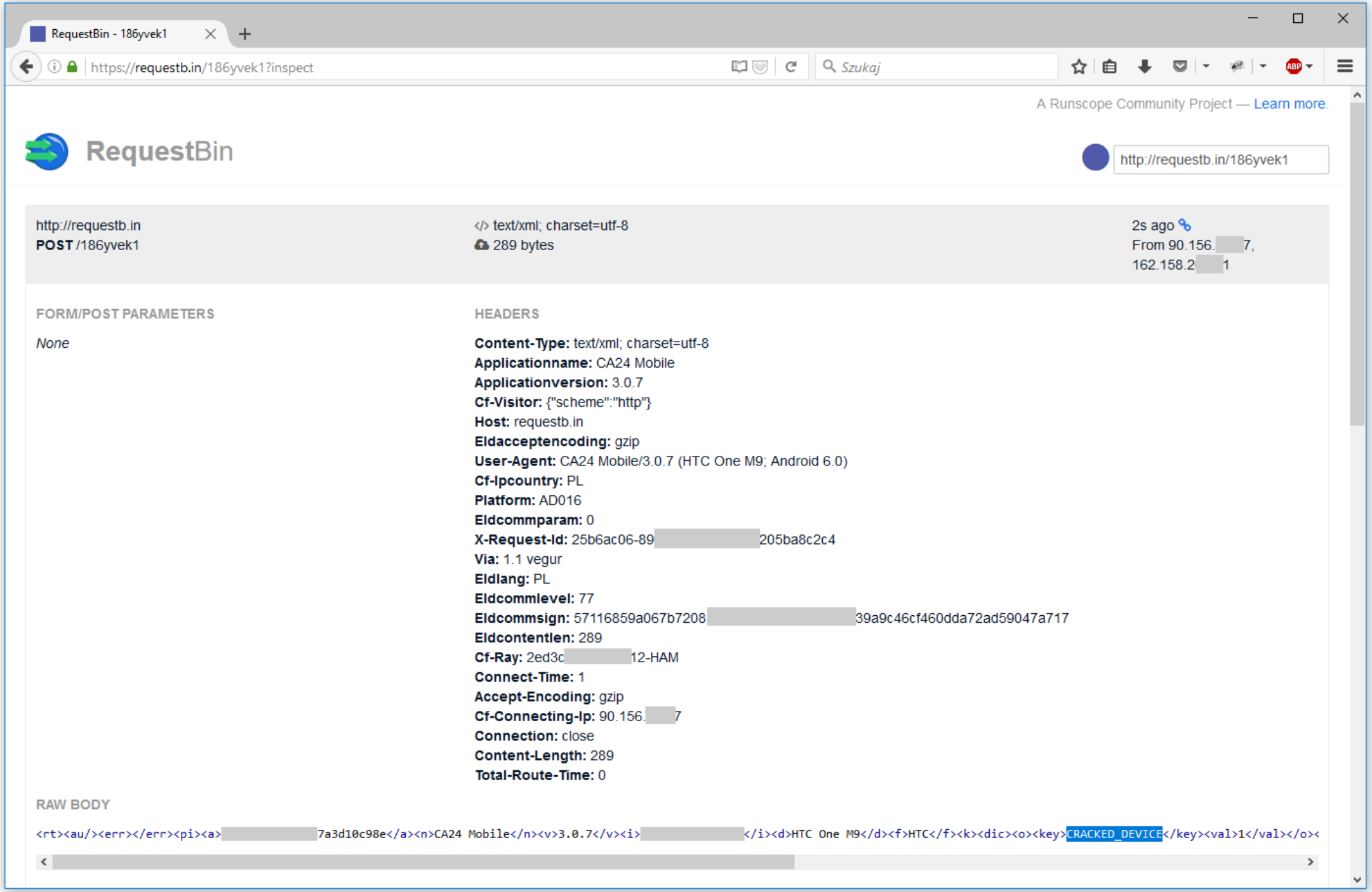




Credit Agricole – server address change



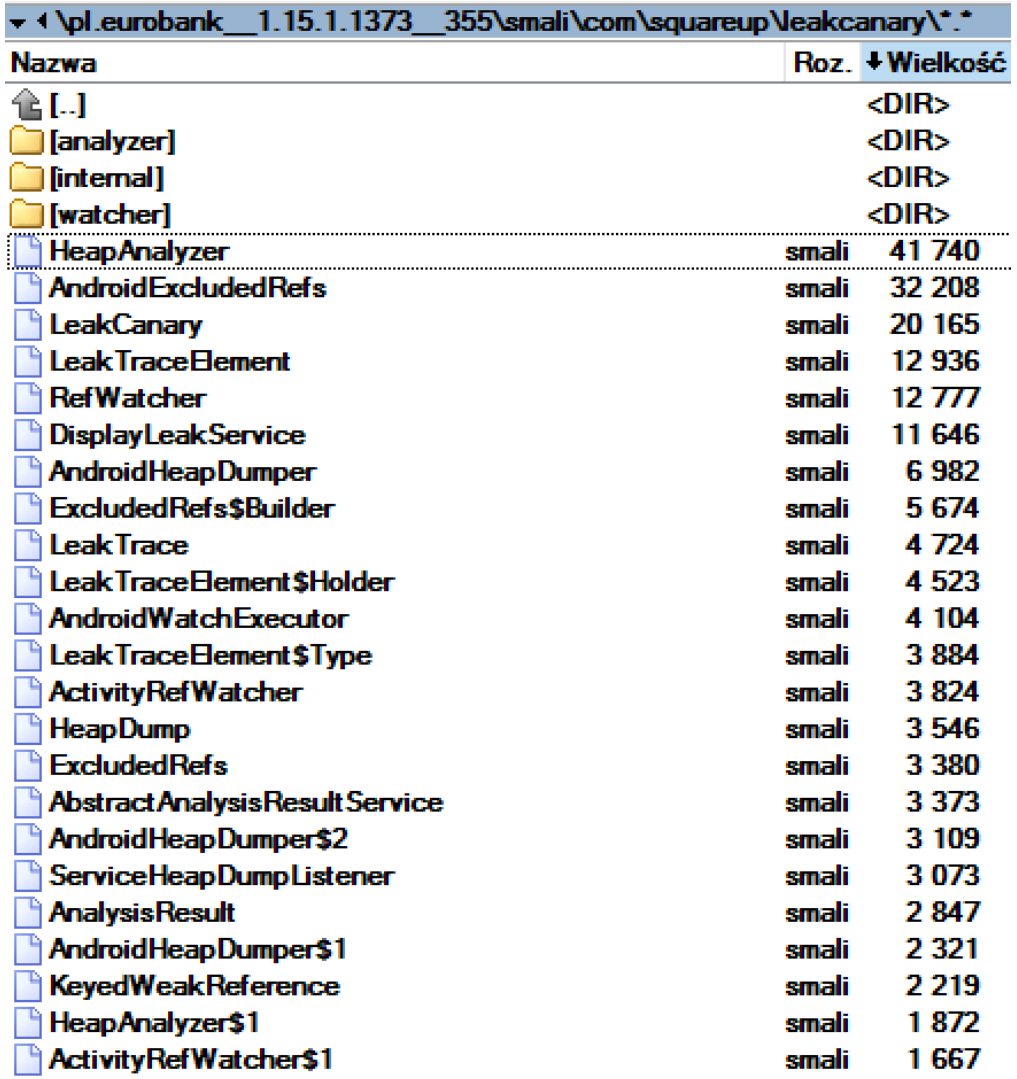



RequestBin - 186yvek1
https://requestb.in/186yvek1?inspect
Szukaj
A Runscope Community Project — Learn more.
RequestBin
http://requestb.in/186yvek1
http://requestb.in
POST /186yvek1
</> text/xml; charset=utf-8
289 bytes
2s ago
From 90.156. 7,
162.158.2 1
FORM/POST PARAMETERS
None
HEADERS
Content-Type: text/xml; charset=utf-8
Applicationname: CA24 Mobile
Applicationversion: 3.0.7
Cf-Visitor: {"scheme":"http"}
Host: requestb.in
Eldacceptencoding: gzip
User-Agent: CA24 Mobile/3.0.7 (HTC One M9; Android 6.0)
Cf-Ipcountry: PL
Platform: AD016
Eldcommparam: 0
X-Request-Id: 25b6ac06-89 205ba8c2c4
Via: 1.1 vegur
Eldlang: PL
Eldcommlevel: 77
Eldcommsign: 57116859a067b7208 39a9c46cf460dda72ad59047a717
Eldcontentlen: 289
Cf-Ray: 2ed3c 12-HAM
Connect-Time: 1
Accept-Encoding: gzip
Cf-Connecting-Ip: 90.156. 7
Connection: close
Content-Length: 289
Total-Route-Time: 0
RAW BODY
<rt><au/><err></err><pi><a> 7a3d10c98e<n>CA24 Mobile</n><v>3.0.7</v> <d>HTC One M9</d><f>HTC</f><k><dic><o><key>CRACKED_DEVICE</key><val>1</val></o><

Eurobank –LeakCanary lib

"LeakCanary should only be used in debug builds, and should be disabled in release builds. We provide a special empty dependency for your release builds: `leakcanary-android-no-op`.

The full version of LeakCanary is bigger and should never ship in your release builds."



\pl.eurobank__1.15.1.1373__355\smali\com\squareup\leakcanary*.*

Nazwa	Roz.	Wielkość
[..]		<DIR>
[analyzer]		<DIR>
[internal]		<DIR>
[watcher]		<DIR>
HeapAnalyzer	smali	41 740
AndroidExcludedRefs	smali	32 208
LeakCanary	smali	20 165
LeakTraceElement	smali	12 936
RefWatcher	smali	12 777
DisplayLeakService	smali	11 646
AndroidHeapDumper	smali	6 982
ExcludedRefs$Builder	smali	5 674
LeakTrace	smali	4 724
LeakTraceElement$Holder	smali	4 523
AndroidWatchExecutor	smali	4 104
LeakTraceElement$Type	smali	3 884
ActivityRefWatcher	smali	3 824
HeapDump	smali	3 546
ExcludedRefs	smali	3 380
AbstractAnalysisResultService	smali	3 373
AndroidHeapDumper$2	smali	3 109
ServiceHeapDumpListener	smali	3 073
AnalysisResult	smali	2 847
AndroidHeapDumper$1	smali	2 321
KeyedWeakReference	smali	2 219
HeapAnalyzer$1	smali	1 872
ActivityRefWatcher$1	smali	1 667

Surprises Inside APK Files

Surprises inside APK files

Bank Smart – debug switches manual along with sample accounts (Hans Kloss, Putin, James Blond)

BPH – unused KML files, part of helper maps library

Credit Agricole – Jenkins logs (continuous integration tool)

ING – invalid Facebook library artefacts


```
##Whether the test Pin should be used or not
shouldUseTestPin=false

##Test Pin that should be used during all pin opera
testPin=14521452

##Whether the requests for login should be skipped
skipLoginFakeSessionAndHideLoader=false

##Whether the forms should be filled with mock data
fillInFormsWithMockData=false

##Whether the loading of dictionaries should be ski
##If this is not the case this flag will default to
skipDownloadingDictionaries=false
```

Surprises inside APK files

Citi – Chinese money order template

Problems With Code and Architecture

Incompetent platform usage

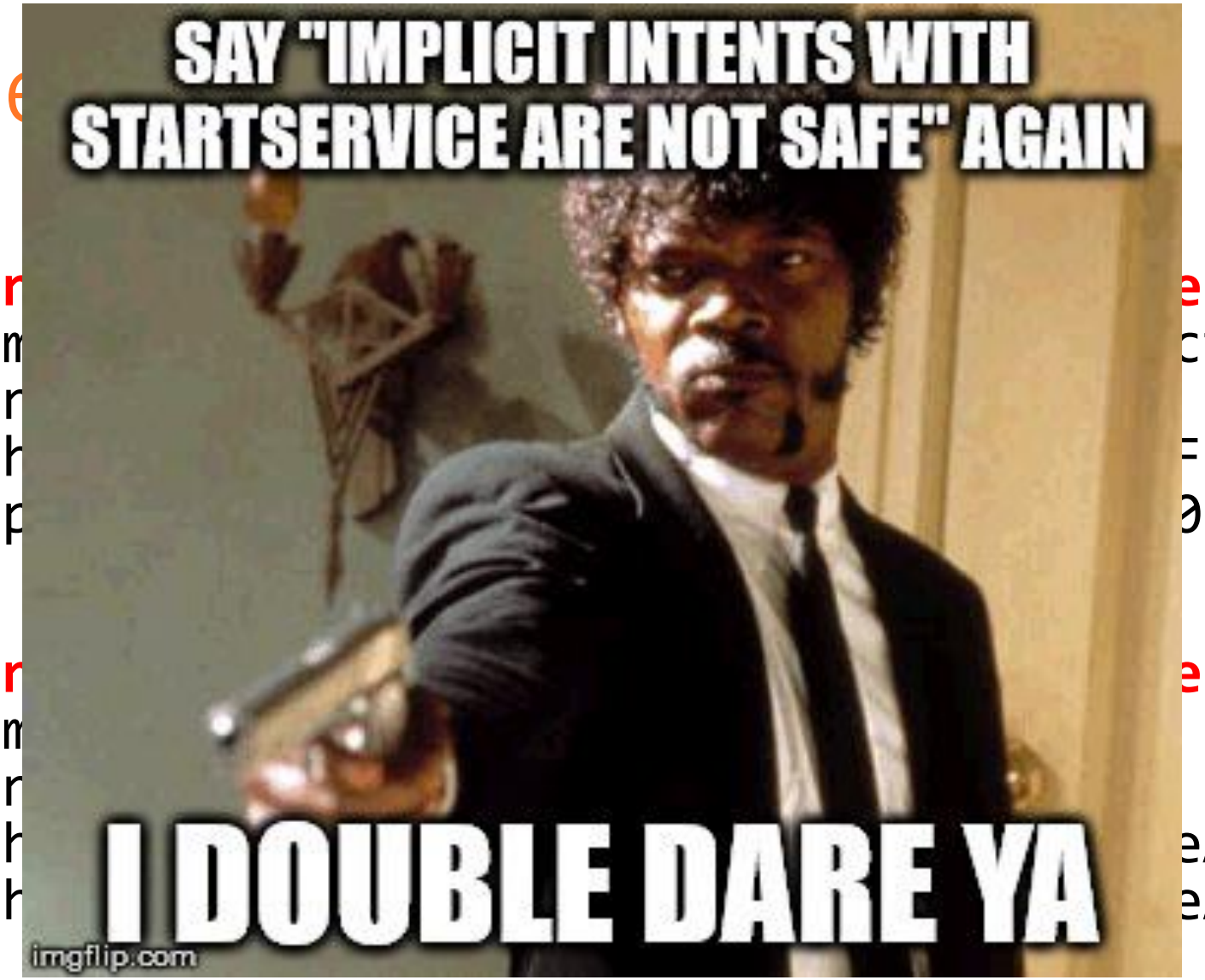
```
Implicit intents with startService are not safe: Intent {
act=com.comarch.mobile.banking.fortis.intent.action.ACTION_CON
android.content.ContextWrapper.bindService:604
com.comarch.mobile.banking.fortis.datamanager.FortisDataManage
android.app.ActivityThread.handleBindService:3031
```

```
Implicit intents with startService are not safe: Intent {
act=com.comarch.mobile.CREATE_FACTORY }
android.content.ContextWrapper.bindService:604
com.comarch.mobile.android.cib.application.BaseApplication.m:1
com.comarch.mobile.android.cib.application.BaseApplication.onC
```

Diss – A form of disrespecting someone, their homies, or their mama.
"*Don't diss on me, cause you aint me.*"

- www.urbandictionary.com

Incompe




```
Implicit ir                                  e: Intent {
act=com.com                                  ction.ACTION_CON
android.cor
com.comarch                                  FortisDataManage
android.app                                  031

Implicit ir                                  e: Intent {
act=com.com
android.cor
com.comarch                                  eApplication.m:1
com.comarch                                  eApplication.onC
```

Diss – A form of disrespecting someone, their homies, or their mama.
"*Don't diss on me, cause you aint me.*"

- www.urbandictionary.com

BGŻ BNP PARIBAS

```
public class AsyncHttpCallerService extends Service {

    @Override
    public IBinder onBind(Intent intent) {  intent: "Intent { act=com.comarch.mobile.banking.fortis.intent.action.ACTION_CONNECT

        byte[] a = intent.getByteArrayExtra("keyStoreData");  a: byte[2691]@4224  intent: "Intent { act=com.comarch.mobile.banki

        int i = Binder.getCallingUid();  i: 10210

        return null;
    }


}
```

intent

- mCategories = null
- mClipData = null
- mComponent = null
- mContentUserHint = -2
- mData = null
- mExtras = {android.os.Bundle@4231} "Bundle[{web_server_ip=planet.bgzbnpparibas.pl, debug_mode=false, web_service_url=https://planet
  - mAllowFds = true
  - mFdsKnown = true
  - mHasFds = false
  - mClassLoader = {dalvik.system.PathClassLoader@4234} "dalvik.system.PathClassLoader[DexPathList[[zip file "/data/app/com.pgssoft.fa
  - mMap = {android.util.ArrayMap@4235} android.util.ArrayMap@4235, size = 13
    - value[0] = "planet.bgzbnpparibas.pl"
    - value[1] = "false"
    - value[2] = "https://planet.bgzbnpparibas.pl/native"
    - value[3] = "AND.1.9.6"
    - value[4] = "10000"
    - value[5] = "0PfedEMzHNAfBI3jYGYph_o1ipKhjwbNrvO0RGw"
    - value[6] = "30000"
    - value[7] = "dd.MM.yyyy"
    - value[8] = {byte[2691]@4224}
    - value[9] = "HTTPS"
    - ...
  - mParcelledData = null
  - shadow$_klass_ = {java.lang.Class@1135} "class android.os.Bundle" ... Navigate
  - shadow$_monitor_ = 1073748346

ebug Android Debugger (8602)

Debugger | Console

Frames

"main"@4 218 in group "main": RUNNING

- onBind:17, AsyncHttpCallerService (com.comarch.mobile.banking.http)
- handleBindService:3031, ActivityThread (android.app)
- access$2000:150, ActivityThread (android.app)
- handleMessage:1495, ActivityThread$H (android.app)
- dispatchMessage:102, Handler (android.os)
- loop:168, Looper (android.os)
- main:5845, ActivityThread (android.app)
- invoke:-1, Method (java.lang.reflect)
- run:797, ZygoteInit$MethodAndArgsCaller (com.android.internal.os)
- main:687, ZygoteInit (com.android.internal.os)

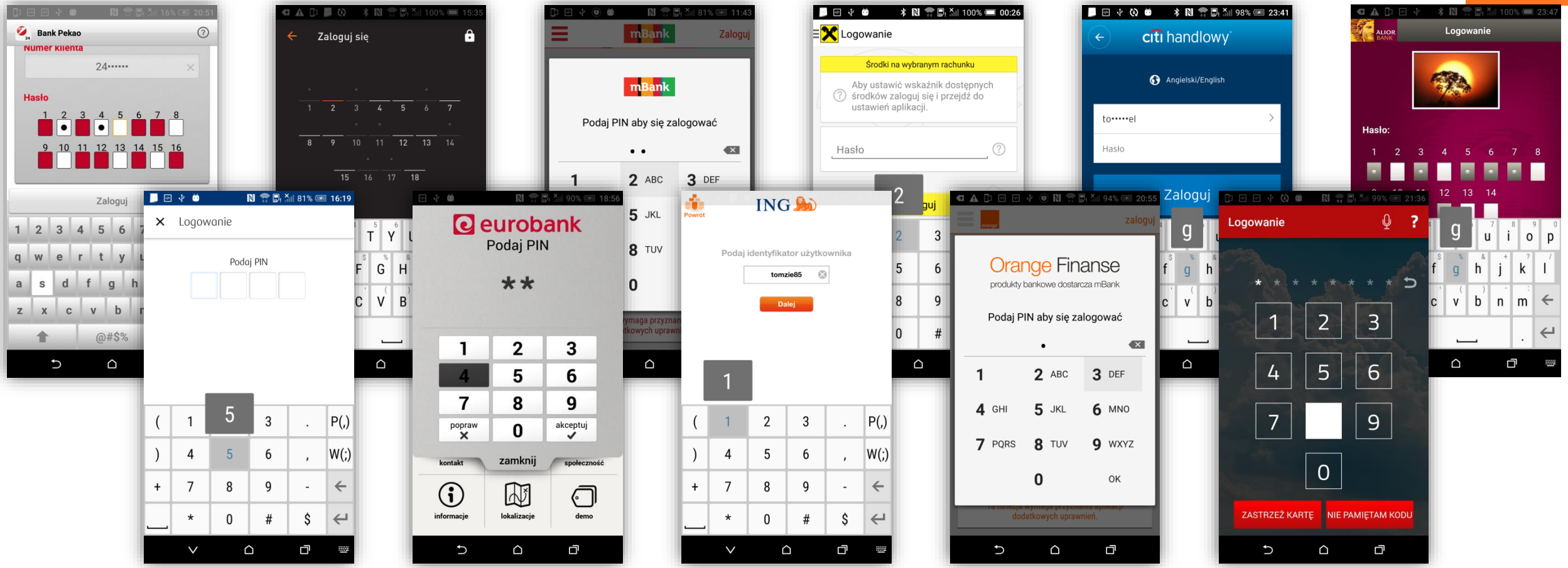
Variables

- this = {com.coma
- intent = {android.
- a = {byte[2691]@
- i = 10210

Terminal | 6: Android Monitor

BGZ BNP PARIBAS

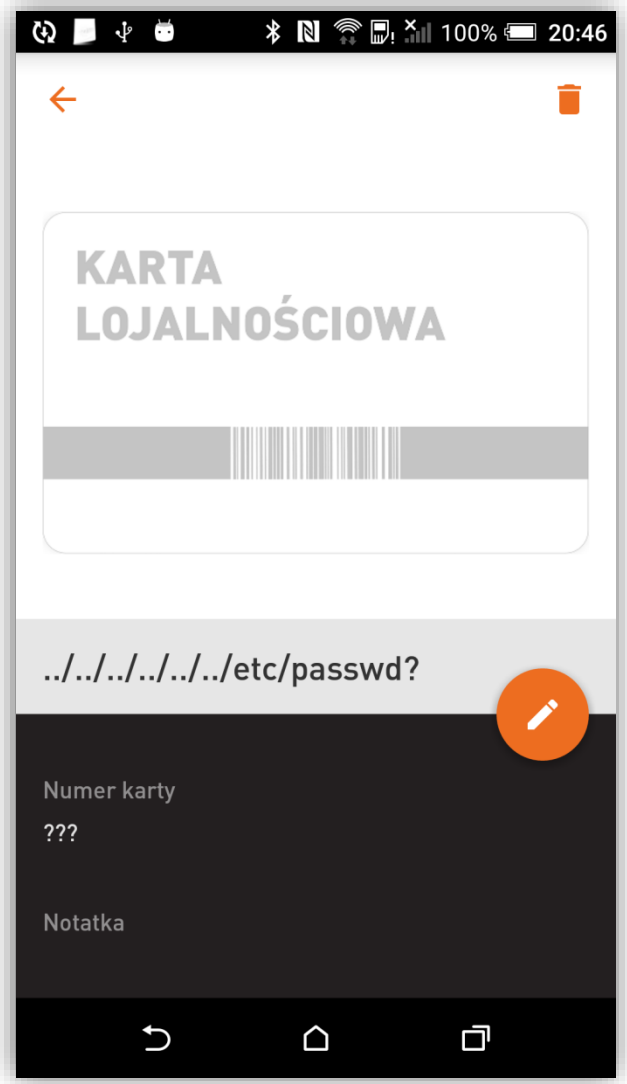
Screenshots issue



BPH: directory traversal

```
System.err:
java.io.FileNotFoundException:
/data/user/0/pl.bph/app_cards/../
../../../../../etc/passwd?1475433
122747.png: open failed: ENOENT
(No such file or directory)
```

also: Card.io library was 18 months old



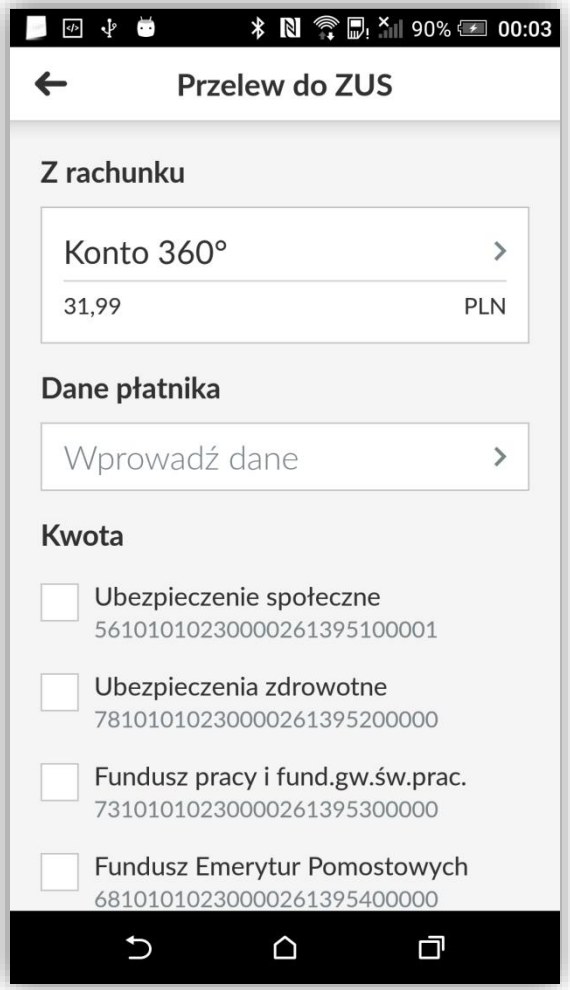
PKO BP – arbitrary object deserialisation

```
protected void onCreate(Bundle var1) {
      super.onCreate(var1);
      this.r();
      this.l().N().a((Application)this.getApplicationContext());
      dze var2 = (dze)this.getIntent().
                              getSerializableExtra("key_IKO_NOTIFICATION");
```

Millennium – XML parametrisation files

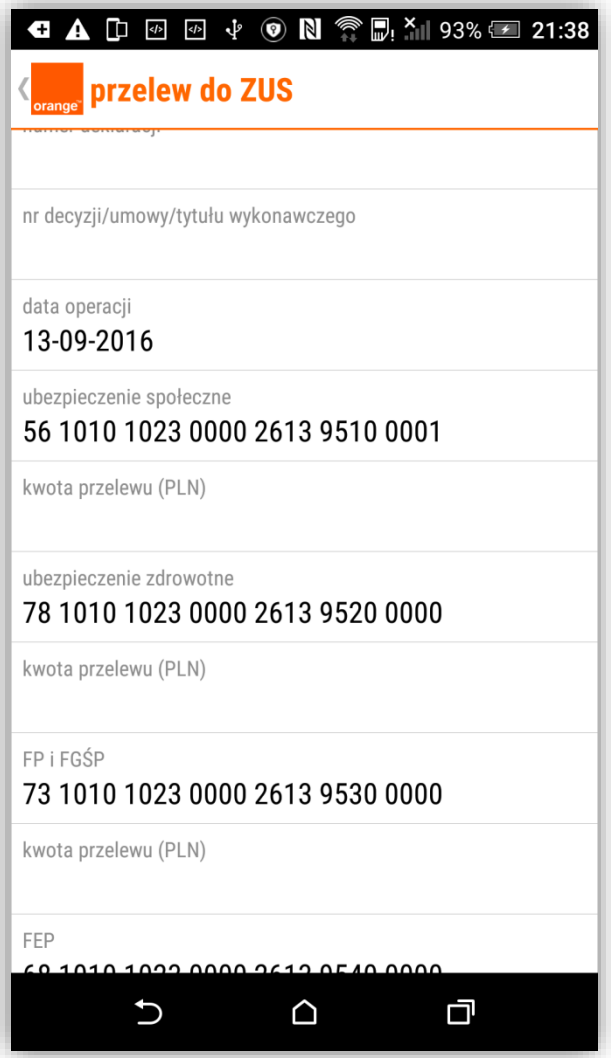
```
<string name="mlk7XTaLbS">
56101010230000261395100001</string>

<string name="forgottenPinLink">
https://www.bankmillennium.pl/osobiste
/LoginSignIn</string>
```



mBank – SQLite parametrisation

#	_id	dictionary_id	KEY	value
40	40	8	A	a - opłata dodatkowa za błędy płatnika
41	41	8	D	d - opłata dodatkowa
42	42	8	E	e - egzekucja
43	43	8	M	m - składka dłuższa niż 1 miesiąc
44	44	8	S	s - składka za 1 miesiąc
45	45	8	T	t - odroczenie terminu
46	46	8	U	u - układ ratalny
47	47	9	0	10101023-26-139-51 ubezpieczenie społeczne
48	48	9	1	10101023-26-139-52 ubezpieczenie zdrowotne
49	49	9	2	10101023-26-139-53 fp i fgśp
50	50	9	3	561010102300002613951000001 ubezpieczenie społeczne
51	51	9	4	781010102300002613952000000 ubezpieczenie zdrowotne
52	52	9	5	731010102300002613953000000 fp i fgśp
53	53	9	6	681010102300002613954000000 fundusz emerytur pomostowych
54	54	10	N	n - nip
55	55	10	P	p - pesel
56	56	10	R	r - regon
				1 - dowód osobisty
				2 - paszport
				3 - inny



Fiddler Web Debugger

File Edit Rules Tools View Help GET /book GeoEdge

WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search...

#	Result	Protocol	Host	URL
1	200	HTTP	Tunnel to	m.mbank.pl:443
2	200	HTTPS	m.mbank.pl:443	/mobileFacade/Nmb
3	200	HTTPS	m.mbank.pl:443	/mobileFacade/NmB
4	200	HTTPS	m.mbank.pl:443	/mobileFacade/NmB
5	200	HTTPS	m.mbank.pl:443	/mobileFacade/Nmb
6	-	HTTPS	m.mbank.pl:443	/mobileFacade/Nmb

Statistics Inspectors AutoResponder Composer Log Filters Timeline

Request body is encoded. Click to decode.

Headers TextView WebForms HexView Auth Cookies Raw JSON XML


```
<v:Envelope xmlns:v="http://schemas.xmlsoap.org/soap/envelope/" xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns:d="http://w
xmlns:c="http://schemas.xmlsoap.org/soap/encoding/" xmlns="http://mbank.pl/">
  <v:Header>
    <RequestInformation>
      <AppType>AND</AppType>
      <AppVersion>2.7.3</AppVersion>
      <BankId>1</BankId>
      <SessionId>scSunD-9iEy4[redacted]</SessionId>
    </RequestInformation>
  </v:Header>
  <v:Body>
    <ZUSRegisterTransfer>
      <ammount1>11.0</ammount1>
      <ammount2>11.0</ammount2>
      <ammount3>11.0</ammount3>
      <ammount4>11.0</ammount4>
      <creditAccount1Number>56101010230000261395100001</creditAccount1Number>
      <creditAccount2Number>78101010230000261395200000</creditAccount2Number>
      <creditAccount3Number>73101010230000261395300000</creditAccount3Number>
      <creditAccount4Number>68101010230000261395400000</creditAccount4Number>
      <decisionNumber></decisionNumber>
      <declaration>072016</declaration>
      <declarationNumber>01</declarationNumber>
      <documentNumber>[redacted]</documentNumber>
      <documentType>1</documentType>
      <email1></email1>
      <email2></email2>
      <isItFirstCall>true</isItFirstCall>
      <nipNumber>[redacted]</nipNumber>
      <payType>S</payType>
      <senderName>[redacted]</senderName>
```


0:0 0/1 606 Find... (press Ctrl+Enter to highlight all)

Breakpoint hit. Tamper, then: Break on Response Run to Completion Choose Response...

Transformer Headers TextView ImageView HexView WebView Auth Caching Cookies Raw JSON X

Network Communication

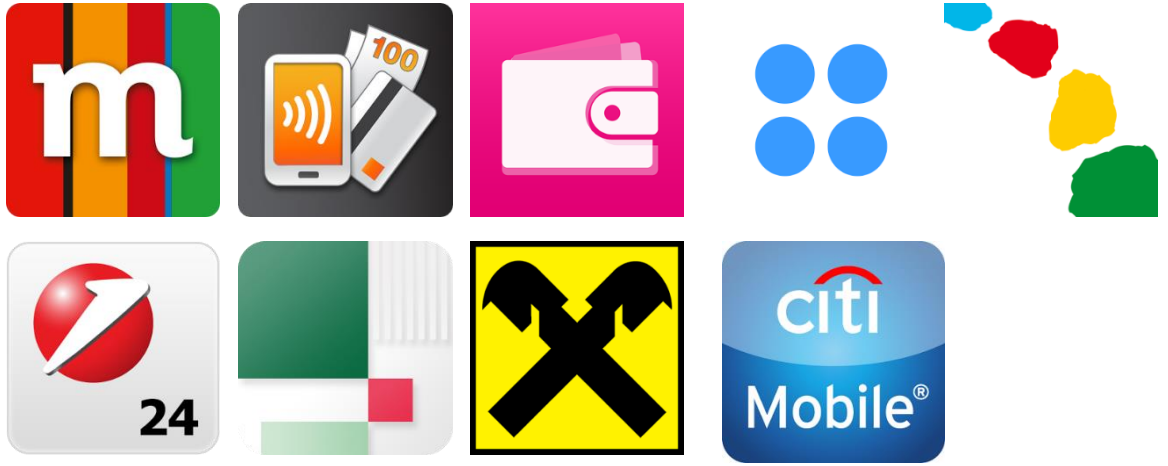
Transactional Service Communication

HTTPS everywhere

Certificates were always verified

Sadly, *user trusted certificates* were, well, trusted

Eavesdropping possible, often also network traffic modification:



Fiddler Web Debugger

File Edit Rules Tools View Help GET /book GeoEdge

WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search...

#	Result	Protocol	Host	URL	Body	Ca
1	200	HTTPS	www.telerik.com	/UpdateCheck.aspx?isBeta=False	703	pr
2	200	HTTP	Tunnel to	mobilews.getinbank.pl:443	723	
3	200	HTTP	Tunnel to	mb2.bankmillennium.pl:443	0	
4	200	HTTP	Tunnel to	mb2.bankmillennium.pl:443	833	
5	200	HTTP	Tunnel to	mb2.bankmillennium.pl:443	0	
6	200	HTTP	Tunnel to	mb1.bankmillennium.pl:443	0	
7	200	HTTPS	mb2.bankmillennium.pl	/wrr/api/common/app/info	246	no
8	200	HTTP	Tunnel to	mb1.bankmillennium.pl:443	0	
9	200	HTTP	Tunnel to	wt.bankmillennium.pl:443	727	
10	200	HTTPS	wt.bankmillennium.pl	/v1/dcs5z9h4u00000gg7pap4eww9_8s8l/event.svc	7	no
11	200	HTTP	Tunnel to	wt.bankmillennium.pl:443	727	
12	200	HTTPS	wt.bankmillennium.pl	/v1/dcs5z9h4u00000gg7pap4eww9_8s8l/event.svc	7	no
13	200	HTTP	Tunnel to	wt.bankmillennium.pl:443	727	
14	200	HTTPS	wt.bankmillennium.pl	/v1/dcs5z9h4u00000gg7pap4eww9_8s8l/event.svc	7	no
15	200	HTTP	Tunnel to	wt.bankmillennium.pl:443	727	
16	200	HTTPS	wt.bankmillennium.pl	/v1/dcs5z9h4u00000gg7pap4eww9_8s8l/event.svc	7	no
17	200	HTTP	Tunnel to	settings.crashlytics.com:443	798	
18	200	HTTP	Tunnel to	andchin-2.htc.com:443	0	

Statistics Inspectors AutoResponder Composer Log Filters Timeline

Headers TextView WebForms HexView Auth Cookies Raw JSON XML

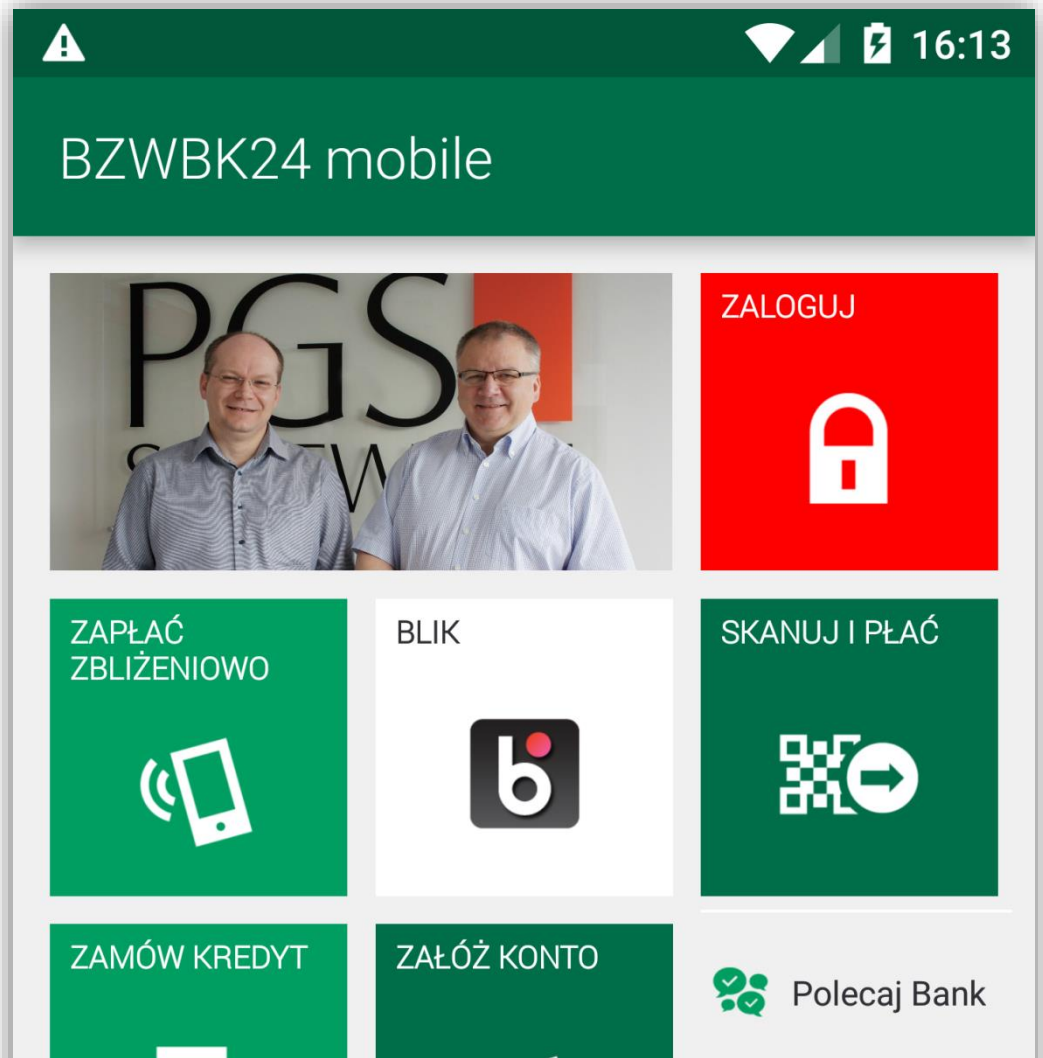
QueryString

Name	Value

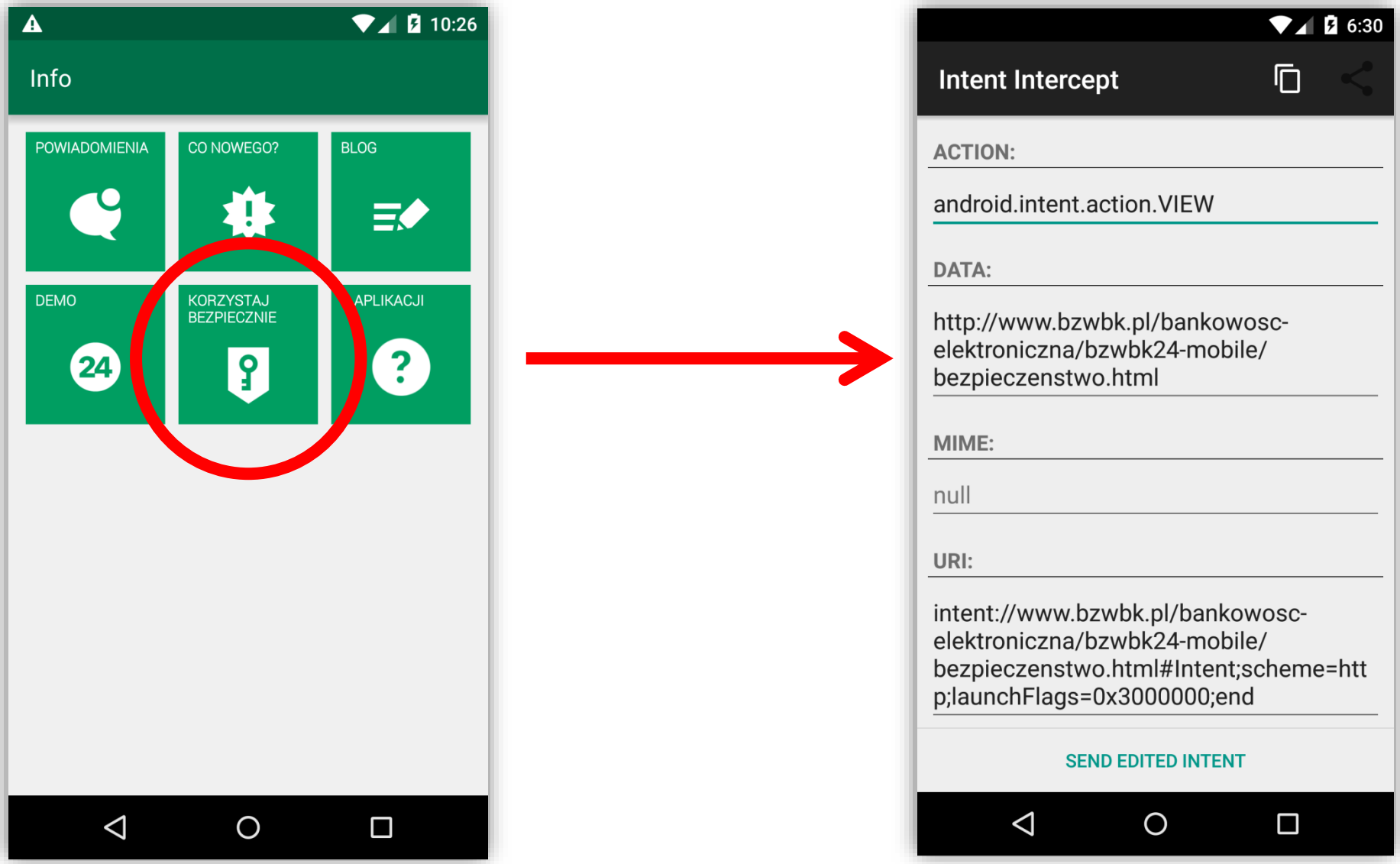
Body

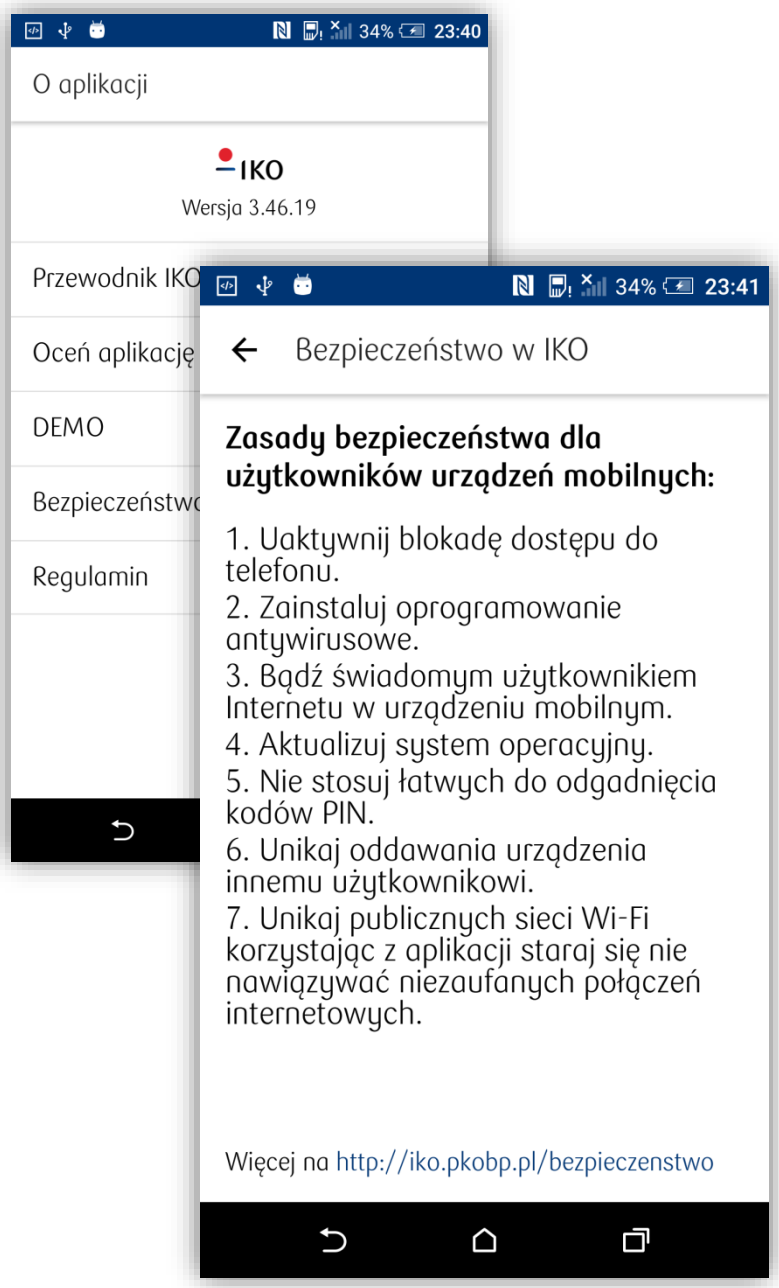
Name	Value
wt.vt_f_tlh	1465462222751
wt.ct	WIFI
wt.vt_f_d	1
wt.dm	HTC One M9
wt.sys	custom
wt.a_dc	unknown
dcsuri	/sec/cert/mb1
wt.os	6.0
prodenv	1
wt.g_co	unknown
wt.ets	1465898431257
wt.dl	0
tablet	0
wt.ti	Unexpected certificate while connecting to https://mb1.bankmillennium.pl/wrr Fingerprint: Unexpected certificate. Issuer: CN=DO_NOT_TRUST_FiddlerRoot,O=DO_NOT_TRUST_BC,OU=Created by http://www.fiddler2.com Subject: CN=mb1.bankmillennium.pl,O=DO_NOT_TRUST_BC,OU=Created by http://www.fiddler2.com
wt.vtid	95f4f019-d162-4408-8691-fbacaf28331e
wt.co	yes
wt.co_f	95f4f019-d162-4408-8691-fbacaf28331e
wt.vt_f_s	1
wt.a_nm	Millennium
wt.sdk_v	3.0
wt.sr	1080x1776
wt.ul	polski
brand	htc
wt.pi	Unexpected certificate while connecting to https://mb1.bankmillennium.pl/wrr Fingerprint: Unexpected certificate. Issuer: CN=DO_NOT_TRUST_FiddlerRoot,O=DO_NOT_TRUST_BC,OU=Created by http://www.fiddler2.com Subject: CN=mb1.bankmillennium.pl,O=DO_NOT_TRUST_BC,OU=Created by http://www.fiddler2.com
wt.vt_sid	95f4f019-d162-4408-8691-fbacaf28331e.1465898431257
wt.uc	unknown
wt.vtvs	1465898431257
wt.av	1046081

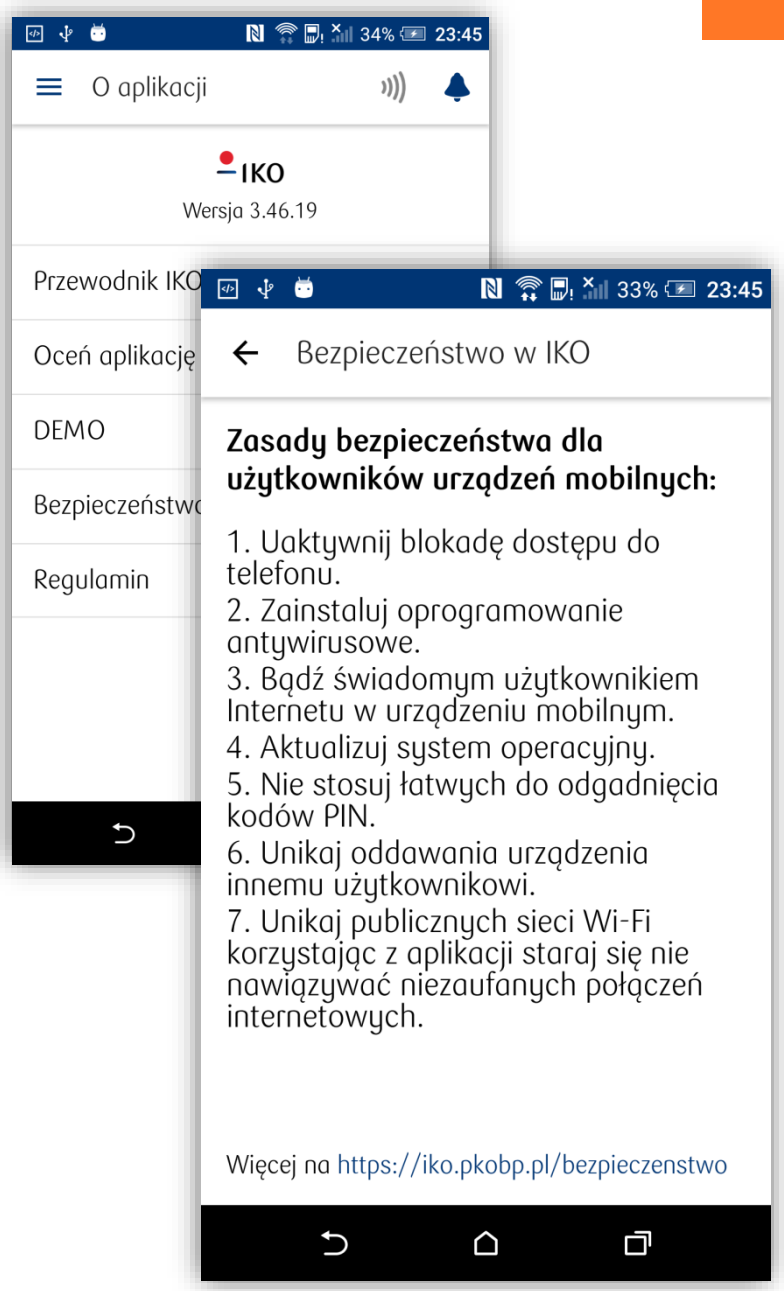
Resources downloaded with HTTP



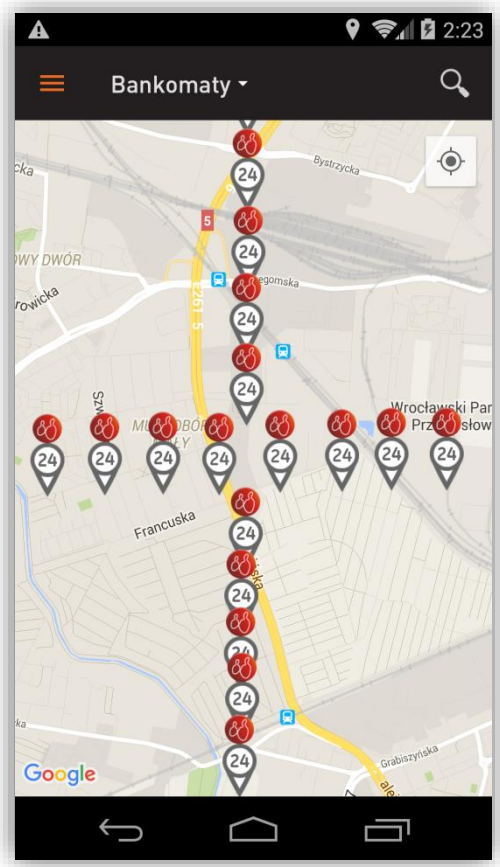
Resources downloaded with HTTP




34% 23:40
O aplikacji
IKO
Wersja 3.46.19
Przewodnik IKO
Oceń aplikację
DEMO
Bezpieczeństwo
Regulamin
34% 23:41
Bezpieczeństwo w IKO
Zasady bezpieczeństwa dla użytkowników urządzeń mobilnych:
1. Uaktywnij blokadę dostępu do telefonu.
2. Zainstaluj oprogramowanie antywirusowe.
3. Bądź świadomym użytkownikiem Internetu w urządzeniu mobilnym.
4. Aktualizuj system operacyjny.
5. Nie stosuj łatwych do odgadnięcia kodów PIN.
6. Unikaj oddawania urządzenia innemu użytkownikowi.
7. Unikaj publicznych sieci Wi-Fi korzystając z aplikacji staraj się nie nawiązywać niezaufanych połączeń internetowych.
Więcej na http://iko.pkobp.pl/bezpieczenstwo


34% 23:45
O aplikacji
IKO
Wersja 3.46.19
Przewodnik IKO
Oceń aplikację
DEMO
Bezpieczeństwo
Regulamin
33% 23:45
Bezpieczeństwo w IKO
Zasady bezpieczeństwa dla użytkowników urządzeń mobilnych:
1. Uaktywnij blokadę dostępu do telefonu.
2. Zainstaluj oprogramowanie antywirusowe.
3. Bądź świadomym użytkownikiem Internetu w urządzeniu mobilnym.
4. Aktualizuj system operacyjny.
5. Nie stosuj łatwych do odgadnięcia kodów PIN.
6. Unikaj oddawania urządzenia innemu użytkownikowi.
7. Unikaj publicznych sieci Wi-Fi korzystając z aplikacji staraj się nie nawiązywać niezaufanych połączeń internetowych.
Więcej na https://iko.pkobp.pl/bezpieczenstwo

Resources downloaded with HTTP



http://mobile.bph.pl/repo/mobile_bph/
↳app_root/data/bankomaty.csv

Websites, Domains, Package Names

```
$ curl -sS --verbose https://www.pkobp.pl/ > /dev/null
* Hostname was NOT found in DNS cache
*   Trying 193.109.225.100...
* Connected to www.pkobp.pl (193.109.225.100) port 443 (#0)
[...TLS/SSL...]
> GET / HTTP/1.1
> User-Agent: curl/7.35.0
> Host: www.pkobp.pl
> Accept: */*
>
< HTTP/1.1 302 FOUND
< Date: Mon, 11 Jul 2016 23:40:00 GMT
< Content-Type: text/html; charset=utf-8
< Transfer-Encoding: chunked
< Connection: close
< Vary: Cookie, Accept-Encoding
< Cache-Control: max-age=300, must-revalidate
< X-Frame-Options: SAMEORIGIN
< Location: http://www.pkobp.pl/
```

Try it yourself – https://inteligo.pl

```
$ curl -sS --verbose https://www.pekao.com.pl/ > /dev/null
* Hostname was NOT found in DNS cache
*   Trying 193.111.166.166...
* Connected to www.pekao.com.pl (193.111.166.166) port 443 (#0)
[...TLS/SSL...]
> GET / HTTP/1.1
> User-Agent: curl/7.35.0
> Host: www.pekao.com.pl
> Accept: */*
>
< HTTP/1.1 302 Moved Temporarily
< Date: Mon, 11 Jul 2016 22:46:23 GMT
< Content-Type: text/html
< Content-Length: 154
< Connection: keep-alive
< Location: http://www.pekao.com.pl/
< X-Frame-Options: SAMEORIGIN
< X-XSS-Protection: 1; mode=block
```

```
$ date --utc
Thu Feb  9 10:54:11 UTC 2017
$ curl -sS --verbose https://raiffeisenpolbank.com/ > /dev/null
* Hostname was NOT found in DNS cache
*   Trying 195.85.249.80...
* connect to 195.85.249.80 port 443 failed: Connection timed out
* Failed to connect to raiffeisenpolbank.com port 443: Connection timed out
* Closing connection 0
```

Połączenie nie jest bezpieczne

Właściciel witryny www.citibank.pl niepoprawnie ją skonfigurował. Program Firefox nie połączył się z nią, aby chronić użytkownika przed kradzieżą informacji.

Więcej informacji...

Wróć do poprzedniej strony

Zaawansowane

Automatyczne zgłaszanie podobnych temu błędów (pomaga Mozilli identyfikować i blokować niebezpieczne strony)

Witryna „www.citibank.pl" używa nieprawidłowego certyfikatu bezpieczeństwa.

Ten certyfikat jest prawidłowym certyfikatem tylko dla następujących nazw:
www.citibank.com, www1.citibank.com, www2.citibank.com, www.citigroup.com, www.citi.com, icg.citi.com, citigroup.com, citibank.com, citi.com

Kod błędu: SSL_ERROR_BAD_CERT_DOMAIN

Dodaj wyjątek...

Połączenie nie jest bezpieczne

Właściciel witryny orangefinanse.pl niepoprawnie ją skonfigurował. Program Firefox nie połączył się z nią, aby chronić użytkownika przed kradzieżą informacji.

Więcej informacji...

Wróć do poprzedniej strony

Zaawansowane

Automatyczne zgłaszanie podobnych temu błędów (pomaga Mozilli identyfikować i blokować niebezpieczne strony)

Witryna „orangefinanse.pl" używa nieprawidłowego certyfikatu bezpieczeństwa.

Ten certyfikat jest prawidłowy tylko dla www.orangefinanse.com.

Kod błędu: SSL_ERROR_BAD_CERT_DOMAIN

Dodaj wyjątek...

mBank PL - Android Apps...

https://play.google.com/store/apps/details?id=pl.mbank

Szukaj

Google Play

Search

Apps

Categories

Home

Top Charts

New Releases

My apps

Shop

Games

Family

Editors' Choice

Account

Redeem

Buy gift card

My wishlist

My Play activity

Parent Guide

mBank PL

mBank S.A. Finance

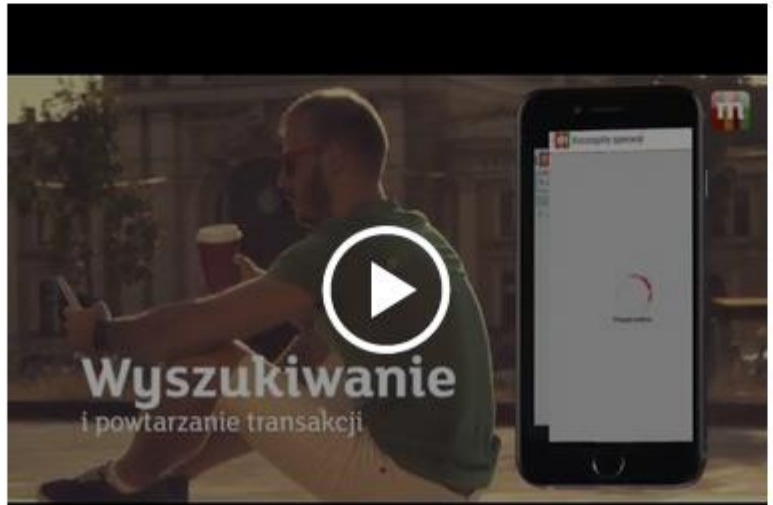
49,118

PEGI 3

This app is compatible with all of your devices.

Add to Wishlist

Install



Similar

Package Name

```
mbank.pl           – pl.mbank
eurobank.pl        – pl.eurobank

bzwbk.pl           – pl.bzwbk.bzwbk24
pkobp.pl           – pl.pkobp.iko

pekao.com.pl       – eu.eleader.mobilebanking.pekao
bgzbnpparibas.pl   – com.comarch.mobile.banking.bnpparibas
```

Package Name

```
com.konylabs.cbplpat          – ???

alior.bankingapp.android      – ???
```

Package Name

`com.konylabs.cbplpat` – Citi Handlowy

`alior.bankingapp.android` – T-Mobile Usługi Bankowe

Contacting Banks

How to report a security issue to a bank?

- Intention of informing security department only
- But how to reach it?
- Via phone and customer service centre – nope
- Webpages – no contact info
- Due to a lack of other options – e-mail and contact forms

Questions submitted to the banks

I would like to get in touch with your bank's security department. As I was unable to find the right information on your website, I would like to ask:

- *Do you have a public contact procedure regarding vulnerabilities of your website and mobile application to external attacks?*
- *Do you have a declared response time in which your specialists respond to such contact attempts?*
- ***Do you have a public PGP/GPG key which can be used to confidentially exchange information with the security department?***
- *Do you run a "bug bounty" programme which offers rewards to individuals who report vulnerabilities responsibly?*

Response Time

Questions were sent to the banks on Thursday, 30th July, after 15:00

Millenium, Alior Bank (the same day)

ING, mBank, Orange Finanse, BZ WBK (Friday or Monday)

BPH (a week later)

What about the rest?

- Suggestion of sending password protected ZIP file by e-mail and password by mobile phone text message
- No answer or empty reply promises
- LinkedIn to the rescue...
- ... as well as PR representatives

Distinct difference between improvisation and procedures.

Bug Bounty

- Hall of Fame
- Swag
- $$$

Bug Bounty

Millennium bank

Bug Bounty

ING

Crashlytics, Facebook, and Others

Crashlytics (Fabric.io)

- Remote crash reporting and report aggregation service
- Very convenient for developers

But

- Owned by ~~Twitter, Inc.~~ Google, Inc.
- All servers located in USA

Facebook and Others

Obsolete „ING dla przedsiębiorców” app (recently discontinued) reported every app start to Facebook.

Not a word in Terms and Conditions, no opt-out, no nothing.

Other apps use, among others, Gemius analytic tools (mBank, Orange Finanse), Adobe Marketing Cloud (ING, Citi) and other less known reporting solutions.

It’s a topic to investigate

… but not by a software developer…

https://www.pgs-soft.com/wp-content/uploads/2017/03/PGS_bank_security_2016.pdf

Summary

- The "bank grade security" of tested applications wasn’t very impressive
- Most of the identified flaws could have been prevented with a little more QA effort (logcat observation, APK content check)
- It’s still way too hard to report security vulnerabilities to the average bank
- The conflict between financial data privacy and a developer’s convenience is yet to be addressed

PGS SOFTWARE

Tomasz Zieliński

tzielinski@pgs-soft.com