
PicPay

Alex Soares

Desenvolvedor Android

@a.soares.siqueira

/alex-soares-siqueira /AlexSoaresDeSiqueira

PicPay

Segurança para android

O que eu preciso saber?

PicPay

Você já deu permissão de acesso a seus dados só para usar um app?

PicPay

Vamos quebrar o nosso app!

PicPay

Ferramentas

PicPay

Ferramentas

- ApkTool

PicPay

Ferramentas

- ApkTool
  - ➜ **release** apktool d app-release.apk

PicPay

Ferramentas

- ApkTool
  - ➜ **release** apktool d app-release.apk

PicPay

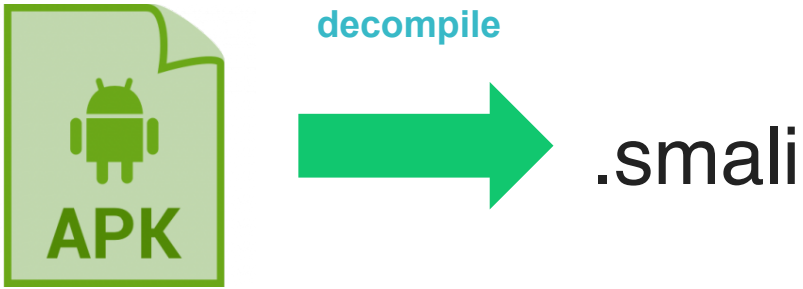
Ferramentas

- ApkTool
  - **release** apktool d app-release.apk

PicPay

Ferramentas

- ApkTool
  - **release** apktool d app-release.apk

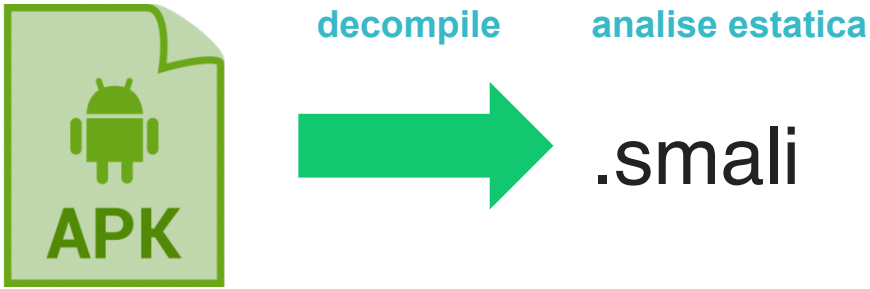


PicPay

```
.method protected onCreate(Landroid/os/Bundle;)V
    .locals 1

    .line 14
    invoke-super {p0, p1}, Landroidx/appcompat/app/AppCompatActivity;->onCreate(Landroid/os/Bundle;)V

    const p1, 0x7f09001c

    .line 15
    invoke-virtual {p0, p1}, Lcom/example/sample/MainActivity;->setContentView(I)V

    .line 16
    invoke-virtual {p0}, Lcom/example/sample/MainActivity;->getWindow()Landroid/view/Window;

    move-result-object p1

    const/16 v0, 0x2000
    invoke-virtual {p1, v0, v0}, Landroid/view/Window;->setFlags(II)V
```

Ferramentas

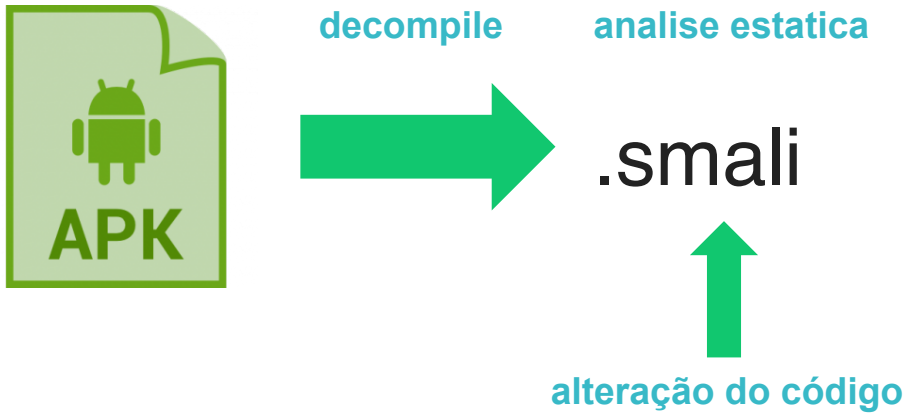
- ApkTool
  - **release** apktool d app-release.apk



PicPay

Ferramentas

- ApkTool
  - **release** apktool d app-release.apk



PicPay

Ferramentas

- ApkTool
  - **release** apktool d app-release.apk

PicPay

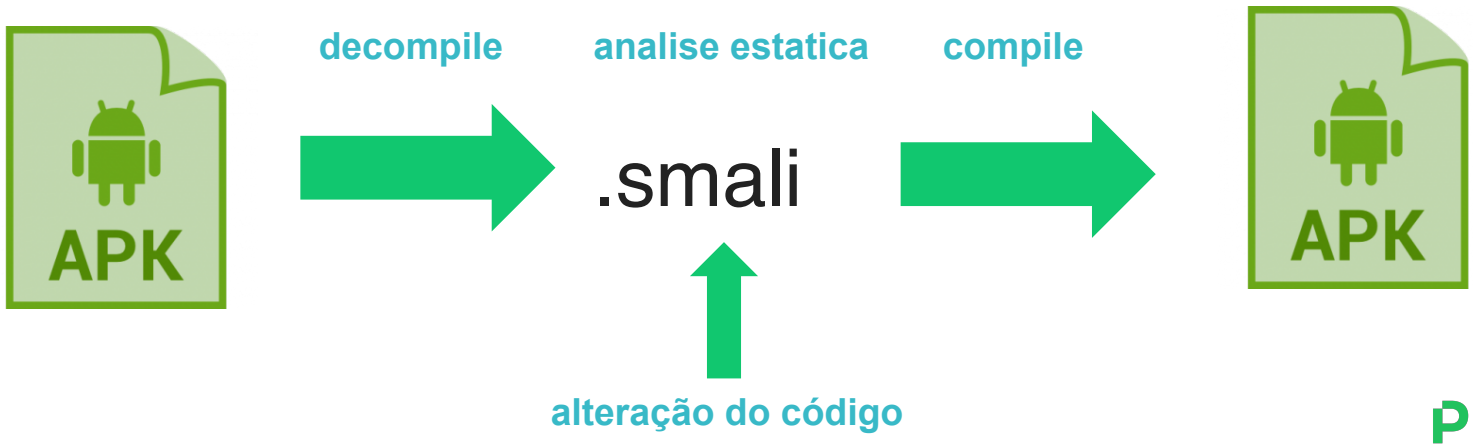
Ferramentas

- ApkTool
  - **release** apktool d app-release.apk
  - **release** apktool b app-release -o new_app_release.apk

PicPay

Ferramentas

- ApkTool
  - release apktool d app-release.apk
  - release apktool b app-release -o new_app_release.apk



PicPay

Ferramentas

- Jadx

PicPay

Ferramentas

- Jadx
  - `release` jadx -d jadx-release-pro app-release.apk

PicPay

Ferramentas

- Jadx
  - release jadx -d jadx-release-pro app-release.apk

PicPay

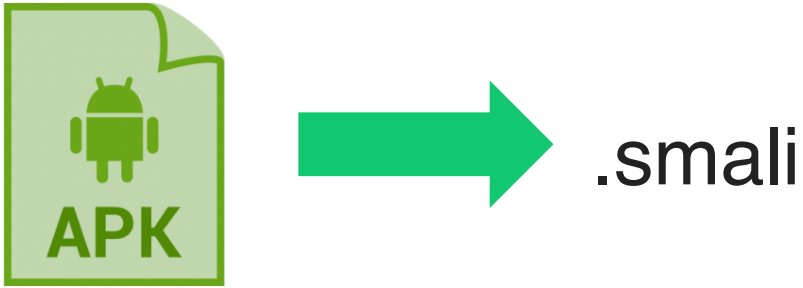
Ferramentas

- Jadx
  - `release jadx -d jadx-release-pro app-release.apk`

PicPay

Ferramentas

- Jadx
  - `release jadx -d jadx-release-pro app-release.apk`



PicPay

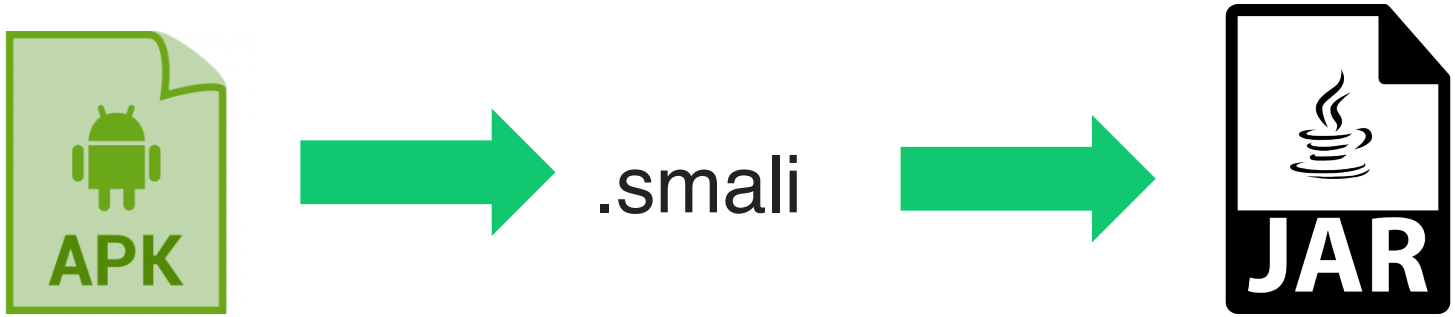
Ferramentas

- Jadx
  - `release jadx -d jadx-release-pro app-release.apk`

PicPay

Ferramentas

- Jadx
  - release jadx -d jadx-release-pro app-release.apk



PicPay

```java
/* access modifiers changed from: protected */
public void onCreate(Bundle bundle) {
    super.onCreate(bundle);
    setContentView((int) R.layout.activity_main);
    getWindow().setFlags(8192, 8192);
    EditText editText = (EditText) _$_findCachedViewById(R.id.etTest);
    Intrinsics.checkExpressionValueIsNotNull(editText, "etTest");
    editText.setCustomSelectionActionModeCallback(new MainActivity$onCreate$1());
}
```

Minimizando os riscos de segurança

Minimizando os riscos de segurança

- Cuidado com o log

PicPay

Minimizando os riscos de segurança

- Cuidado com o log
- Não salve chaves e tokens no seu app

PicPay

Minimizando os riscos de segurança

- Cuidado com o log
- Não salve chaves e tokens no seu app
- Cuidado com as informações transitadas

PicPay

Minimizando os riscos de segurança

- Cuidado com o log
- Não salve chaves e tokens no seu app
- Cuidado com as informações transitadas
- Proteja contra Printscreens e clipboard

PicPay

Minimizando os riscos de segurança

- Cuidado com o log
- Não salve chaves e tokens no seu app
- Cuidado com as informações transitadas
- Proteja contra Printscreens e clipboard
- Cuidado com as libs de terceiros

PicPay

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & WidgetsNew www.itsecdb.c

Enter a CVE id, product, vendor, vulnerability type...

Search

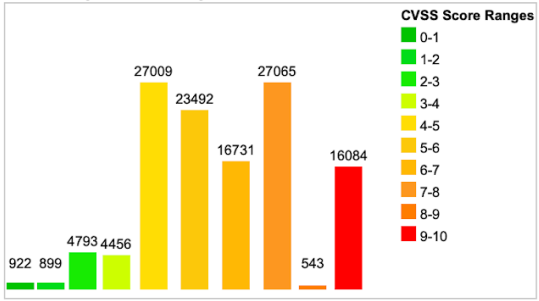
Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	922	0.80
1-2	899	0.70
2-3	4793	3.90
3-4	4456	3.70
4-5	27009	22.10
5-6	23492	19.30
6-7	16731	13.70
7-8	27065	22.20
8-9	543	0.40
9-10	16084	13.20
Total	121994	

Weighted Average CVSS Score: **6.6**

Vulnerability Distribution By CVSS Scores



Looking for OVAL (Open Vulnerability and Assessment Language) definitions? **http://www.itsecdb.com** allows you to view exact details of OVAL(Open Vulnerability and Assessment Language) definitions and see exactly what you should do to verify a vulnerability. It is fully integrated with cvedetails so you will be able to see OVAL definitions related to a product or a CVE entry.
Sample CVE entry with OVAL definitions : CVE-2007-0994

www.cvedetails.com provides an easy to use web interface to CVE vulnerability data. You can browse for vendors, products and versions and view cve entries, vulnerabilities, related to them. You can view statist about vendors, products and versions of products. CVE details are displayed in a single, easy to use page, see a sample here.

CVE vulnerability data are taken from National Vulnerability Database (NVD) xml feeds provided by National Institue of Standards and Technology. Additional data from several sources like exploits from www.exploit db.com, vendor statements and additional vendor supplied data, Metasploit modules are also published in addition to NVD CVE data.

Minimizando os riscos de segurança

- Cuidado com o log
- Não salve chaves e tokens no seu app
- Cuidado com as informações transitadas
- Proteja contra Printscreens e clipboard
- Cuidado com as libs de terceiros
- Cuide da sua rede

PicPay

Cuide da sua rede

- Certificate Pinning

PicPay

Cuide da sua rede

- Certificate Pinning
- Token Rolante

PicPay

Cuide da sua rede

- Certificate Pinning
- Token Rolante
- Não utilize protocolos inseguros

PicPay

Cuide da sua rede

- Certificate Pinning
- Token Rolante
- Não utilize protocolos inseguros
- Network Security Configuration

PicPay

Cuide da sua rede

- Certificate Pinning
- Token Rolante
- Não utilize protocolos inseguros
- Network Security Configuration
- usesClearTextTraffic

PicPay

Cuide da sua rede

- Certificate Pinning
- Token Rolante
- Não utilize protocolos inseguros
- Network Security Configuration
- usesClearTextTraffic
- StrictMode.VmPolicy.Builder().detectCleartextNetwork()

PicPay

Cuide da sua rede

- Certificate Pinning
- Token Rolante
- Não utilize protocolos inseguros
- Network Security Configuration
- usesClearTextTraffic
- StrictMode.VmPolicy.Builder().detectCleartextNetwork()
- Criptografia

PicPay

Minimizando os riscos de segurança

- Cuidado com o log
- Não salve chaves e tokens no seu app
- Cuidado com as informações transitadas
- Proteja contra Printscreens e clipboard
- Cuidado com as libs de terceiros
- Cuide da sua rede
- SafetyNet

PicPay

SafetyNet

- Conjunto de APIs

PicPay

SafetyNet

- Conjunto de APIs
- Attestation

PicPay

SafetyNet

- Conjunto de APIs
- Attestation
- Safe Browsing

PicPay

SafetyNet

- Conjunto de APIs
- Attestation
- Safe Browsing
- reCAPTCHA

PicPay

SafetyNet

- Conjunto de APIs
- Attestation
- Safe Browsing
- reCAPTCHA
- Verify Apps

PicPay

Minimizando os riscos de segurança

- Cuidado com o log
- Não salve chaves e tokens no seu app
- Cuidado com as informações transitadas
- Proteja contra Printscreens e clipboard
- Cuidado com as libs de terceiros
- Cuide da sua rede
- SafetyNet
- Force update

PicPay

Minimizando os riscos de segurança

- Cuidado com o log
- Não salve chaves e tokens no seu app
- Cuidado com as informações transitadas
- Proteja contra Printscreens e clipboard
- Cuidado com as libs de terceiros
- Cuide da sua rede
- SafetyNet
- Force update
- Ofusque o seu código

PicPay

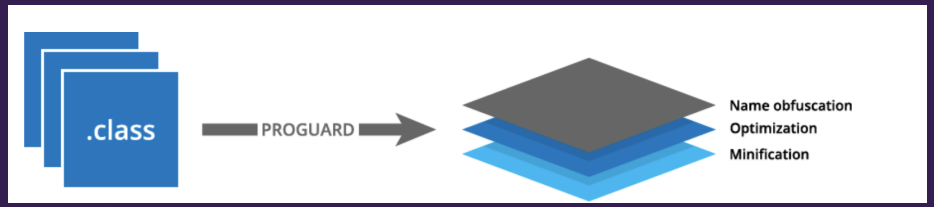
Ofuscação de código

- ProGuard

PicPay

Ofuscação de código

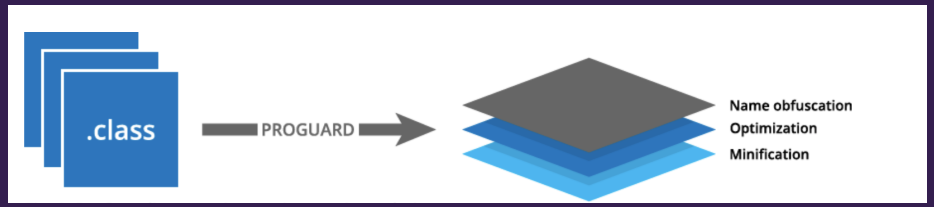
- ProGuard



PicPay

Ofuscação de código

- ProGuard

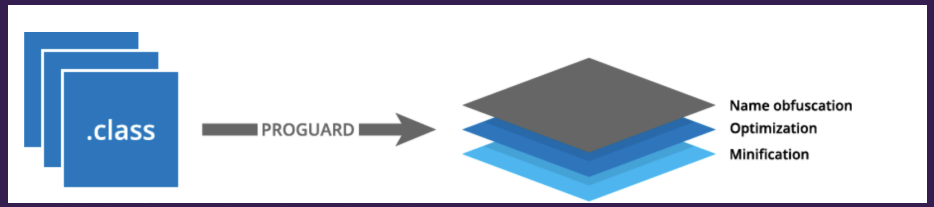


- DexGuard

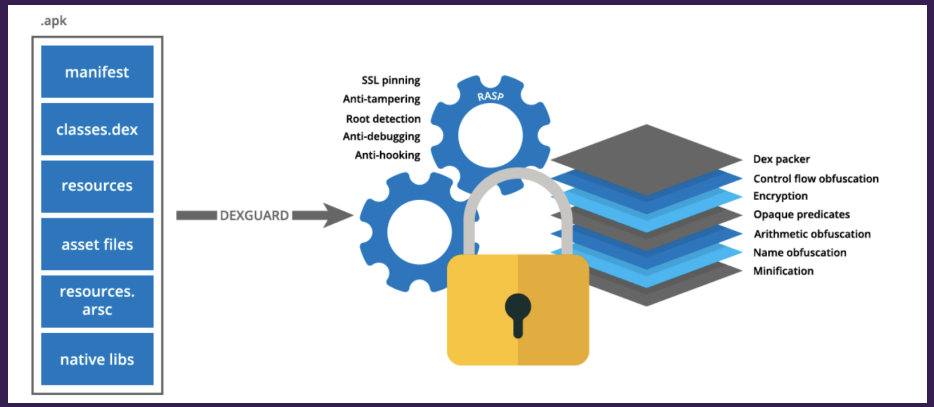
PicPay

Ofuscação de código

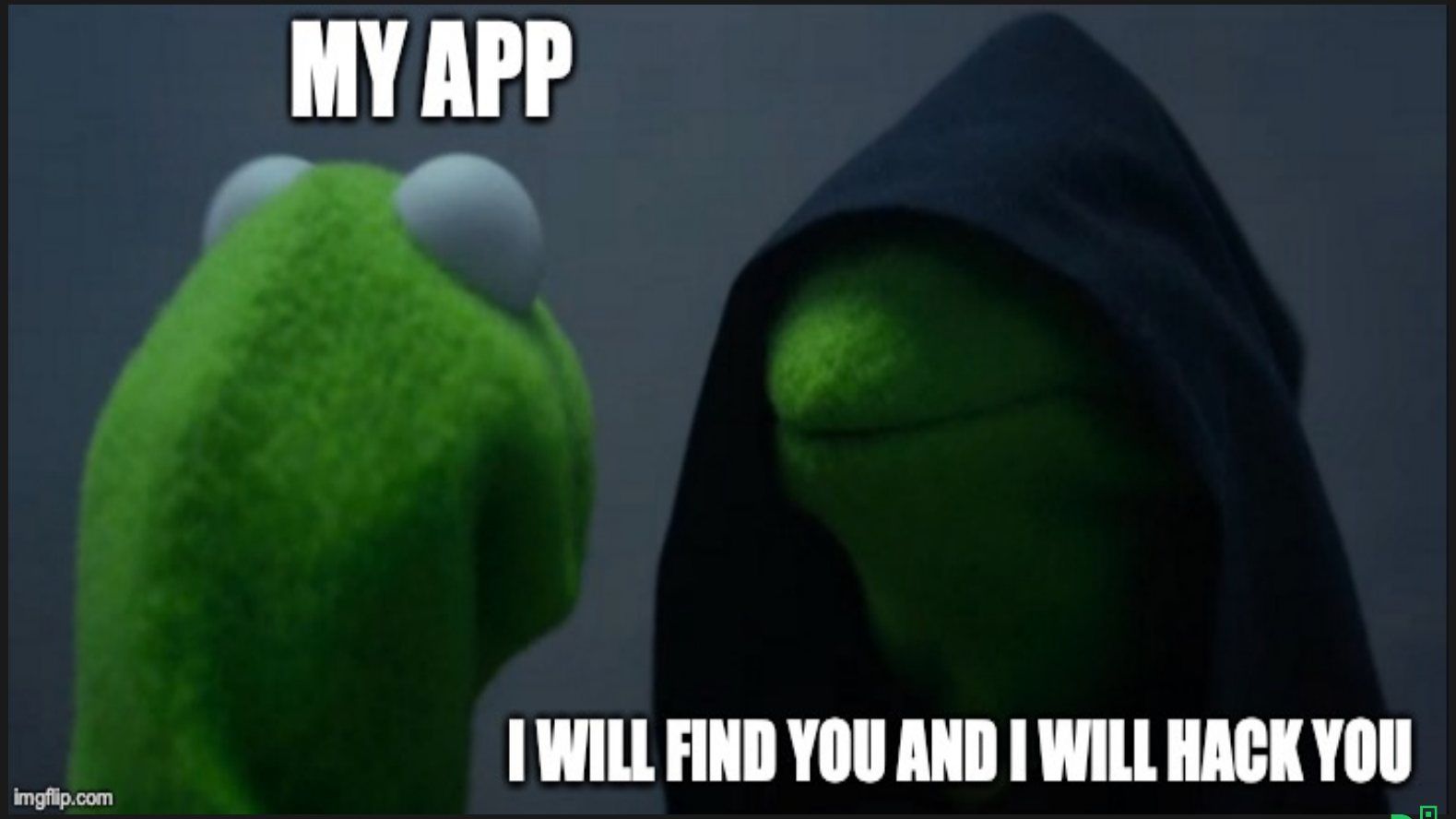
- ProGuard



- DexGuard



PicPay

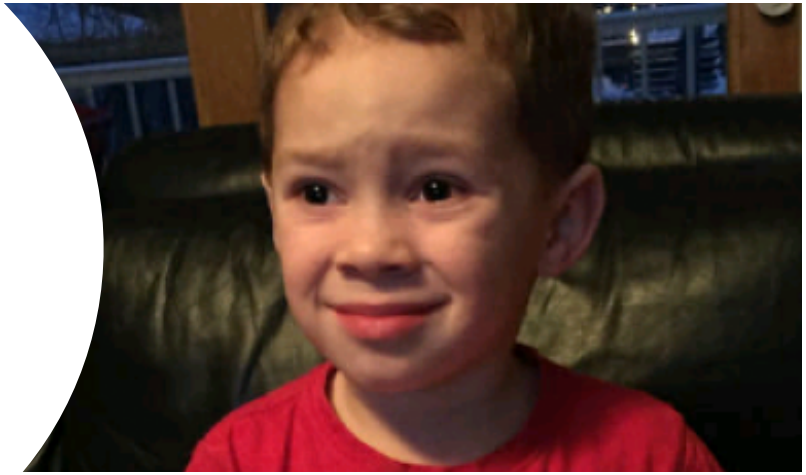

MY APP
I WILL FIND YOU AND I WILL HACK YOU
imgflip.com

Podemos diminuir os riscos do nosso app ficar vulnerável

Insight

PicPay

Dúvidas?



PicPay

Muito obrigado!

 /alex-soares-siqueira  /AlexSoaresDeSiqueira

PicPay


PicPay

Referências

Politica de software indesejado da google
https://www.google.com/about/unwanted-software-policy.html

OWASP Mobile
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

Documentação sobre segurança no android
https://developer.android.com/topic/security/best-practices

Ferramentas
https://techbeacon.com/app-dev-testing/16-tools-bulletproof-android-app-security