Continuous Hacking: Pentest no seu pipeline de mobile

creditas

Rita Lino

creditas

Pedro Santiago

creditas

Terras, o principal ativo. A única pessoa que comandava tinha muito poder. Ex: Rei.

Máquinas viram o principal ativo. O governo que tem mais máquinas possui mais poder.

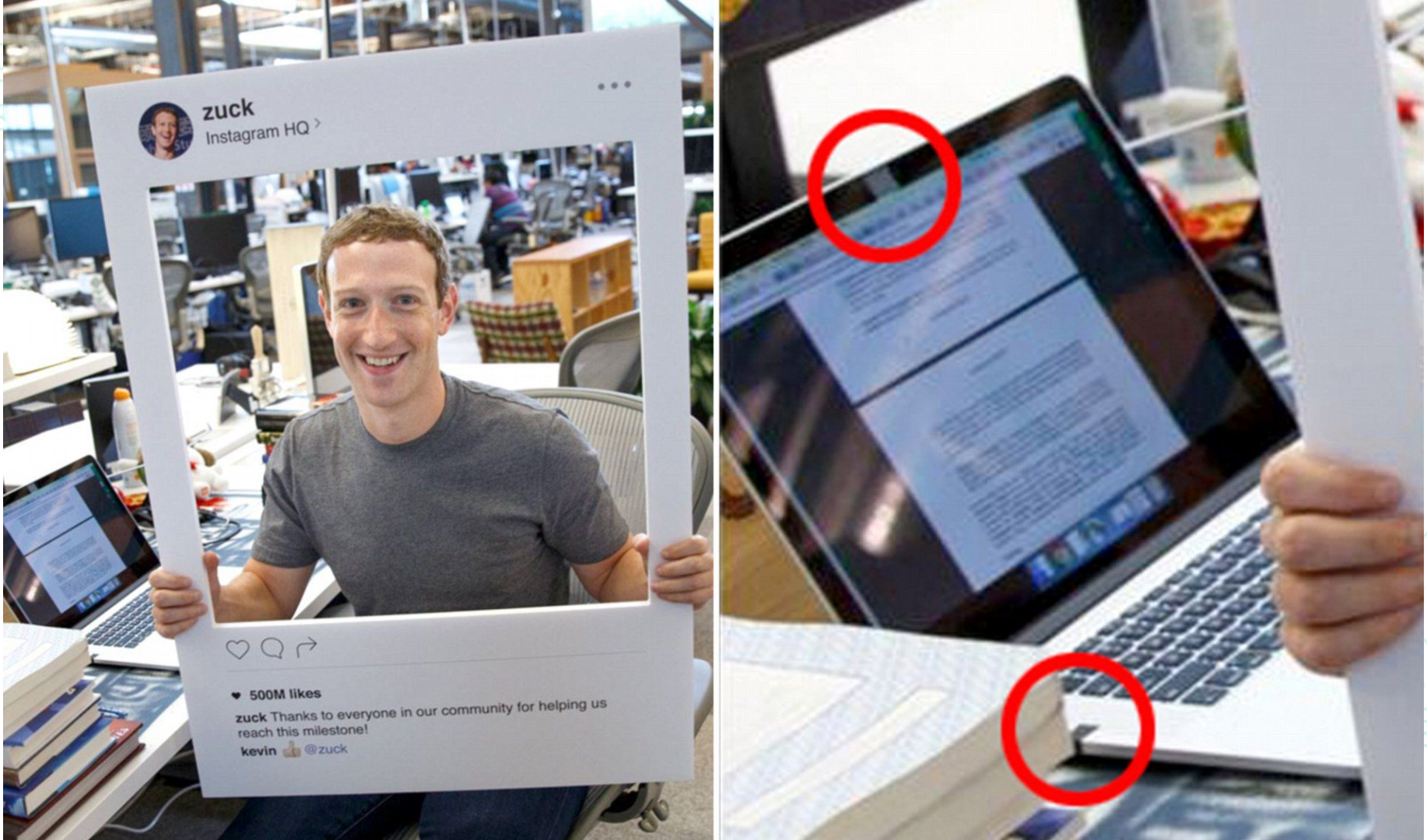
Dados estão virando o principal ativo.
Quem detém possui muito poder.

Quantas pessoas usam dispositivos móveis?

Desde 2008 o uso de mobile cresceu exponencialmente, hoje mais que metade da população mundial usa dispositivos móveis.

Dispositivos cada vez mais próximos

Gerando cada vez mais dados


zuck
Instagram HQ
500M likes
zuck Thanks to everyone in our community for helping us reach this milestone!
kevin @zuck


Messages
Calendar
Photos
Weather
Clock
Maps
Videos
Notes
Reminders
Stocks
Game Center
Newsstand
iTunes Store
App Store
iBooks
Phone
Health
Passbook
Settings
Camera
Safari
WhatsApp
Google Maps


iTunes Store
App Store
Phone
Health
Passbook
Settings
Camera
Safari
WhatsApp
Google Maps

Por que se preocupar com segurança?

O que pode acontecer com vazamento de informações?

O GLOBO ECONOMIA BUSCAR ACESSE NO

Facebook perde US$ 36,7 bi, após escândalo de uso de dados

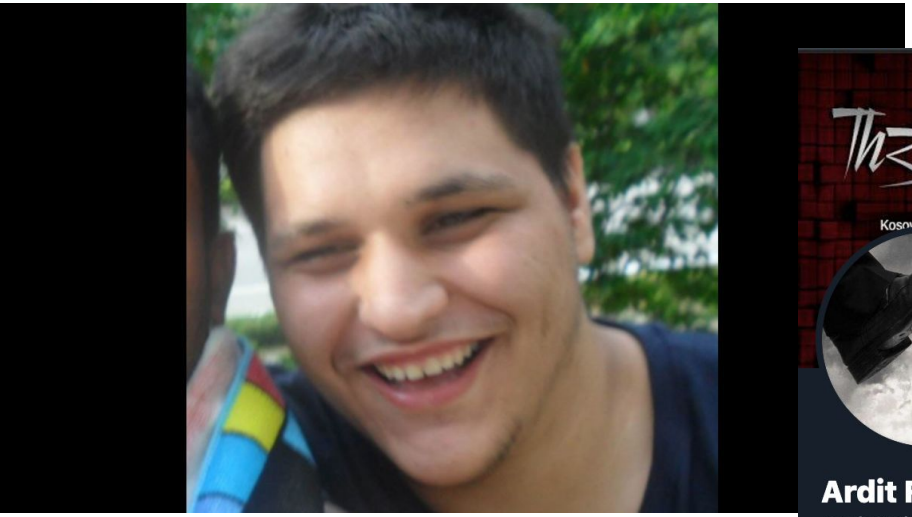
Ações caíram 6,72% nesta segunda-feira. Bolsa brasileira caiu 1,1%

O Globo e Com agências internacionais
19/03/2018 - 12:07 / Atualizado em 20/03/2018 - 09:40

Foto: Justin Tallis/AFP

creditas

Por que se preocupar com segurança?



Ardit Ferizi

Ferizi hackeou nomes, emails, senhas e outros dados de uma empresa de varejo e expôs 1.351 militares e governantes em um estado Islâmico como "lista da morte".

creditas

Por que se preocupar com segurança?

Junaid Hussain

Um dos membros do ISIS fazia parte deste mesmo grupo e ameaçou as vítimas do ataque.

creditas

Solução

Cultural

Tem que partir das pessoas, compartilhando informações, sabendo por que importa e cada um fazendo sua parte; mesmo assim trabalhando em colaboração uns com os outros.

creditas

creditas

Se análise estática de código + testes no CI já nos ajudam tanto

Por que não ajudar nossos clientes com aplicações seguras?

creditas

Mobile Security Framework

creditas

Como funciona?

android .APK

.IPA

MOBSF

creditas

Static Analysis

- Information
- Scan Options
- Signer Certificate
- Permissions
- Binary Analysis
- Android API
- Browsable Activities
- Security Analysis
- Malware Analysis
- Reconnaissance
- Components
- Download Report
- Start Dynamic Analysis

App Icon

App Score

Average CVSS 0
Security Score 100/100
Trackers Detection 3/208

File Information

Name InsecureBankv2.apk
Size 3.3MB
MD5 5ee4829065640f9c936ac861d1650ffc
SHA1 80b53f80a3c9e6bfd98311f5b26ccddcd1bf0a98
SHA256 b18af2a0e44d7634bbcdf93664d9c78a2695e050393fcfbb5e8b91f902d194a4

App Information

Name InsecureBankv2
Package Name com.android.insecurebankv2
Main Activity com.android.insecurebankv2.LoginActivity
Target SDK 22 Min SDK 15 Max SDK
Android Version Name 1.0
Android Version Code 1

Play Store Information

10 ACTIVITIES View
0 SERVICES View
2 RECEIVERS View
1 PROVIDERS View

EXPORTED ACTIVITIES 4
EXPORTED SERVICES 0
EXPORTED RECEIVERS 1
EXPORTED PROVIDERS 1

Static Analysis

Information
Scan Options
Signer Certificate
Permissions
Binary Analysis
Android API
Browsable Activities
Security Analysis
Malware Analysis
Reconnaissance
Components
Download Report
Start Dynamic Analysis

Android Permissions

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.GET_ACCOUNTS	normal	discover known accounts	Allows an application to access the list of accounts known by the phone.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

Static Analysis

Information
Scan Options
Signer Certificate
Permissions
Binary Analysis
Android API
Browsable Activities
Security Analysis
Manifest Analysis
Code Analysis
File Analysis
Malware Analysis
Reconnaissance
Components
Download Report
Start Dynamic Analysis

Manifest Analysis

ISSUE	SEVERITY	DESCRIPTION
Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
Application Data can be Backed up [android:allowBackup=true]	medium	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
Activity (com.android.insecurebankv2.PostLogin) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Activity (com.android.insecurebankv2.DoTransfer) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Activity (com.android.insecurebankv2.ViewStatement) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Content Provider (com.android.insecurebankv2.TrackUserContentProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Broadcast Receiver (com.android.insecurebankv2.MyBroadCastReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Activity (com.android.insecurebankv2.ChangePassword) is not Protected.	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

Como ele testa?

```
# Stack Smashing Protection & ARC
dat = get_otool_out(tools_dir, 'symbols', bin_path, bin_dir)
if b'stack_chk_guard' in dat:
    ssmash = {
        'issue': 'fstack-protector-all flag is Found',
        'level': SECURE,
        'description': ('App is compiled with Stack Smashing Protector'
                        ' (SSP) flag and is having protection against'
                        ' Stack Overflows/Stack Smashing Attacks.'),
        'cvss': 0,
        'cwe': '',
        'owasp': '',
    }
else:
    ssmash = {
        'issue': 'fstack-protector-all flag is not Found',
        'level': IN_SECURE,
        'description': ('App is not compiled with Stack Smashing '
                        'Protector (SSP) flag. It is vulnerable to'
                        'Stack Overflows/Stack Smashing Attacks.'),
        'cvss': 2,
        'cwe': 'CWE-119',
        'owasp': 'M1: Improper Platform Usage',
    }
```

creditas

Como fica no CI?

```yaml
version: 2
jobs:
  mobsf:
    machine:
      image: ubuntu-1604:201903-01
    steps:
      - checkout
      - run:
          name: "Prepare for it"
          command: docker pull opensecurity/mobile-security-framework-mobsf

      - run:
          name: "set env"
          command: echo "MOBSF_API_KEY=$MOBSF_API_KEY" > env.list

      - run:
          name: "get the server running"
          command: docker run -it
            --env-file ./env.list -p 8000:8000 opensecurity/mobile-security-framework-mobsf:latest
          background: true

      - run:
          name: "json pkg"
          command: sudo apt-get install jq
```

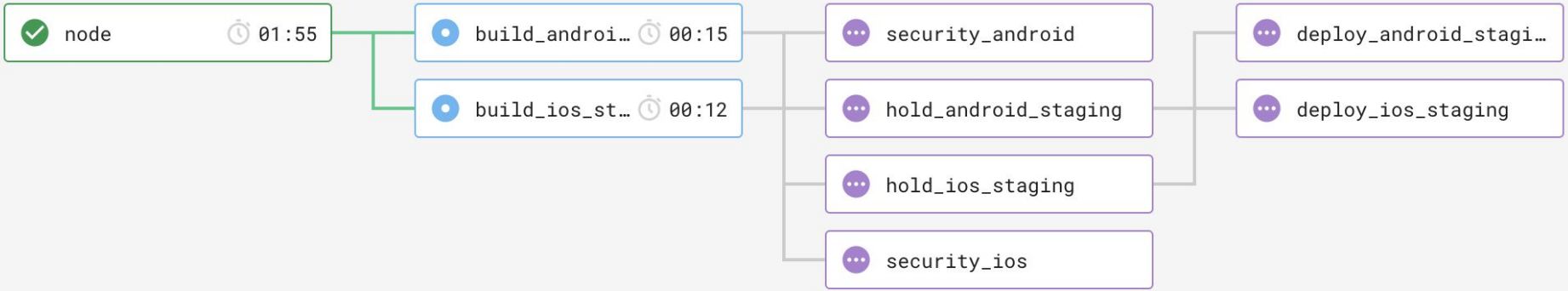
Como fica no CI?

```
- run:
    name: "upload file"
    command: |
      response=`curl -F 'file=@./InsecureBankv2.apk' http://localhost:8000/api/v1/upload
        -H "Authorization:$MOBSF_API_KEY"`
      SCAN_TYPE=`echo $response | jq '.scan_type' | sed 's/"//g'`
      FILE_NAME=`echo $response | jq '.file_name' | sed 's/"//g'`
      HASH=`echo $response | jq '.hash' | sed 's/"//g'`
      echo "export SCAN_TYPE=$SCAN_TYPE" >> $BASH_ENV
      echo "export FILE_NAME=$FILE_NAME" >> $BASH_ENV
      echo "export HASH=$HASH" >> $BASH_ENV

- run:
    name: "run scan"
    command: |
      response=`curl -X POST --url http://localhost:8000/api/v1/scan
        --data "scan_type=$SCAN_TYPE&file_name=$FILE_NAME&hash=$HASH"
        -H "Authorization:$MOBSF_API_KEY"`
      echo $response >> report.json
      echo $response

- run:
    name: "get glue result"
    command: docker run -it -v $(pwd):/app owasp/glue:raw-latest
      ruby bin/glue -t Dynamic -T /app/report.json
      --mapping-file mobsf --finding-file-path /app/android.json -z
```

creditas

Como fica no CI?

9 jobs in this workflow



creditas

Some checks were not successful

2 failing, 2 pending, and 5 successful checks

Hide all checks

✕	**ci/circleci: security_android** — Your tests failed on CircleCI		Details
✕	**ci/circleci: security_ios** — Your tests failed on CircleCI		Details
●	**ci/circleci: build/hold_android_staging** *Pending — Your job is on hold on ...*		Details
●	**ci/circleci: build/hold_ios_staging** *Pending — Your job is on hold on Circl...*		Details
✓	**ci/circleci: build_android_staging** — Your tests passed on CircleCI!	**Required**	Details
✓	**ci/circleci: build_ios_staging** — Your tests passed on CircleCI!	**Required**	Details

creditas

Erros mais comuns

M1 - Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.
M2 - Insecure Data Storage	This new category is a combination of M2 + M4 from Mobile Top Ten 2014. This covers insecure data storage and unintended data leakage.
M3 - Insecure Communication	This covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.
M4 - Insecure Authentication	This category captures notions of authenticating the end user or bad session management. This can include: • Failing to identify the user at all when that should be required • Failure to maintain the user's identity when it is required • Weaknesses in session management
M5 - Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasn't done correctly.

creditas

Não se trata de empresas

Trata-se de pessoas

Não se corrige apenas com ferramenta e estratégia

É necessário mudar a cultura

Conheça nossos canais

Nosso Twitter
@CreditasTech

Blog sobre Tech
medium.com/creditas-tech

Comunidade no Meetup
meetups Creditas

Linkedin e Instagram
Creditas Br

creditas