Tempest

ACADEMY

Conference

2023

Hacking Android Apps

Parte 0: Conceitos e Dificuldades Iniciais

Classificação da Informação: PÚBLICA
Autor da apresentação: Vinicius Moraes

Propósito

Compartilhar um pouco sobre as primeiras etapas que envolvem um pentest mobile

01 Conceitos e Contexto

02 Configurando o ambiente

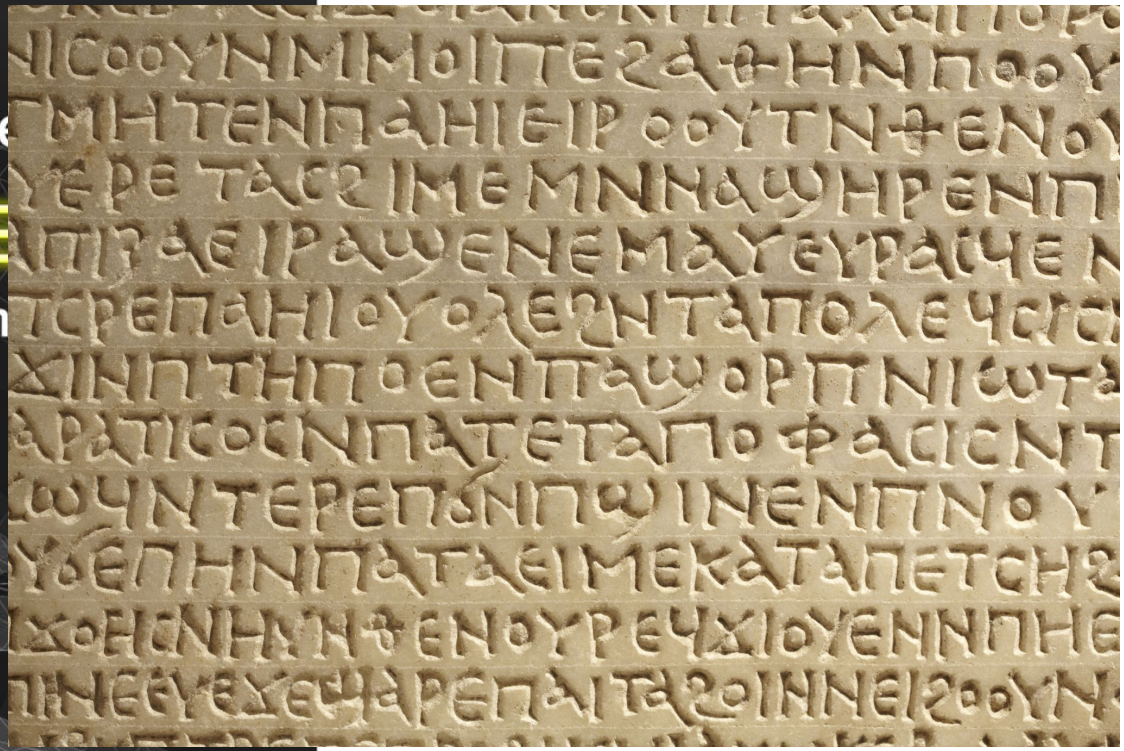
03 Evitando detecção de root

04 Evitando outras checagens

Tempe

ACADE

Conferen



Tempest

ACADEMY

Conference

FAQ

- Tenho dúvidas, quando pergunto?
- Tenho algo a complementar/corrigir, o que faço?
- Me perdi em uma parte, vou parar de entender tudo?
- Nunca fiz pentest, consigo entender?
- Faço pentest mobile, posso ir embora?⏭️

Tempest
ACADEMY
Conference

tinyurl.com/hacking-android

Cheat Sheet

Hacking Android Apps

Some tricks to deal with Android Apps

Setting proxy

- Go to Settings > WiFi > Your network > Proxy, and set the ip address and port of the proxy tool
- if there is AP isolation:
  - In computer: `adb reverse tcp:8080 tcp:8080`
  - In android: Set the WiFi proxy using 127.0.0.1 and 8080
- Apps ignoring the proxy (Flutter)
  - ProxyDroid (available in playstore, root is required)
  - Transparent Proxy
    - A) Use an WiFi adapter to create an AP on your computer and connect the Android
    - B) Use your default WiFi router (without AP isolation) (if the app does not need ipv6)

vinicius.moraes@tempest.com.br / vinicius777

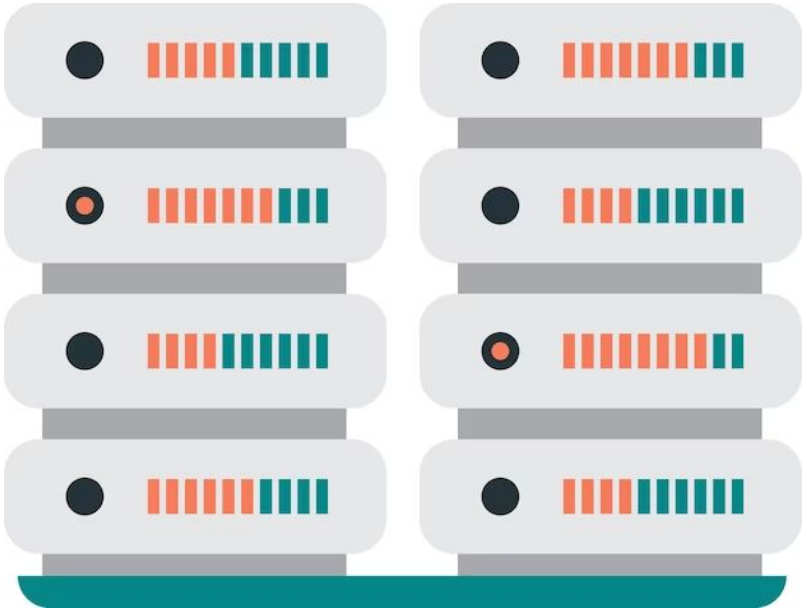
Conceitos e Contexto

- O que?
- Por que?

O que pode ser hackeado em um aplicativo?

Tempest
[ACADEMY]
Conference

- Quais os elementos que envolvem o aplicativo?
  - Modelo Client–server



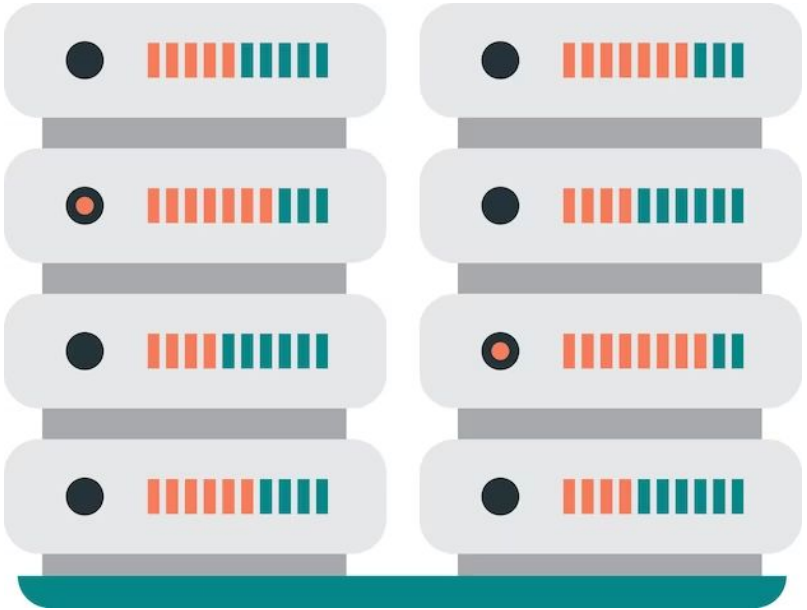
O que pode ser hackeado em um aplicativo?

Tempest
[ACADEMY]
Conference

- Quais os elementos que envolvem o aplicativo?

Cliente
Aplicativo
Front-end

Servidor
API
Back-end



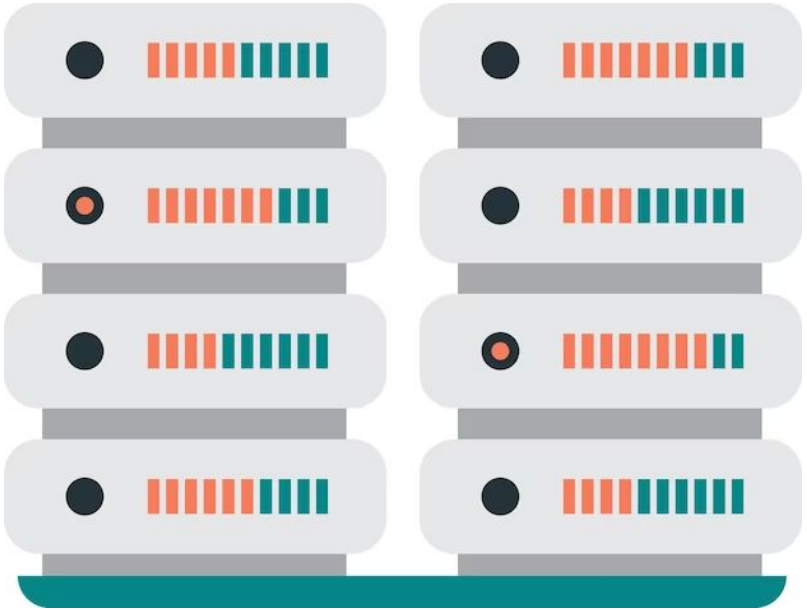
O que pode ser hackeado em um aplicativo?

Tempest
[ACADEMY]
Conference

- O que pode ser manipulado?

Cliente
Aplicativo
Front-end

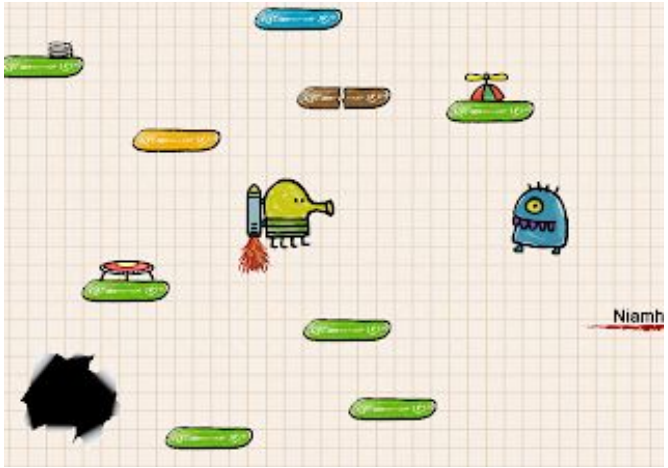
Servidor
API
Back-end

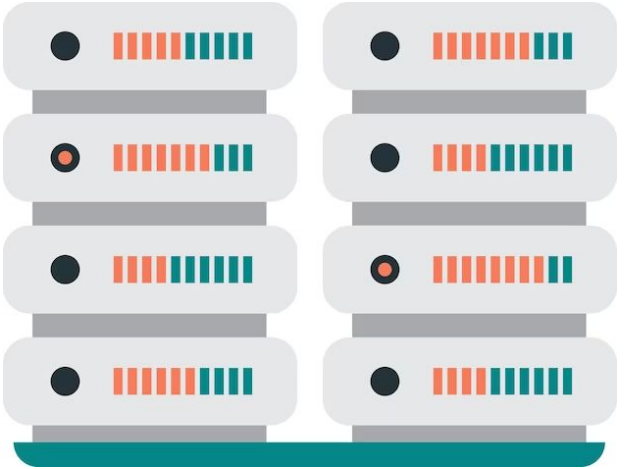


O que pode ser hackeado em um aplicativo?

Tempest
[ACADEMY]
Conference

- Jogo
- Onde está a informação a ser manipulada?
  - pulos durante o jogo
  - score do placar global



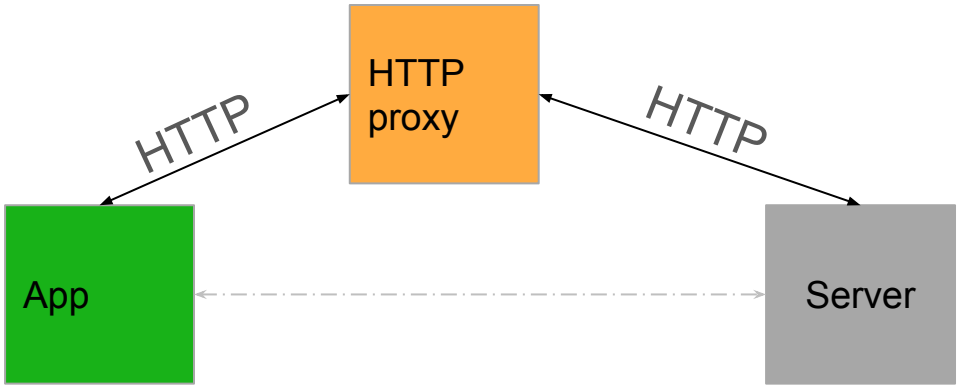


Comunicação com o servidor

- Como os apps se comunicam?
- Qual o nível de controle desejado para os testes?

Comunicação com o servidor

Comunicação com o servidor



Tempest
:ACADEMY:
Conference

Comunicação com o servidor

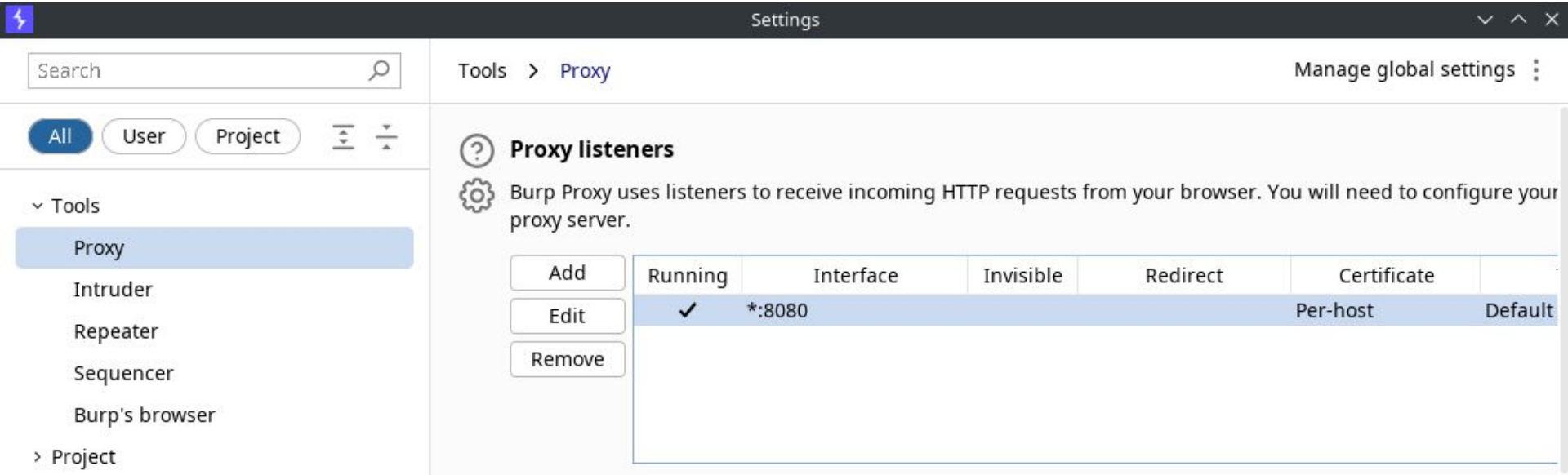
Configurando o Ambiente

- Como?

Como configurar a ferramenta de proxy?

Tempest
ACADEMY
Conference

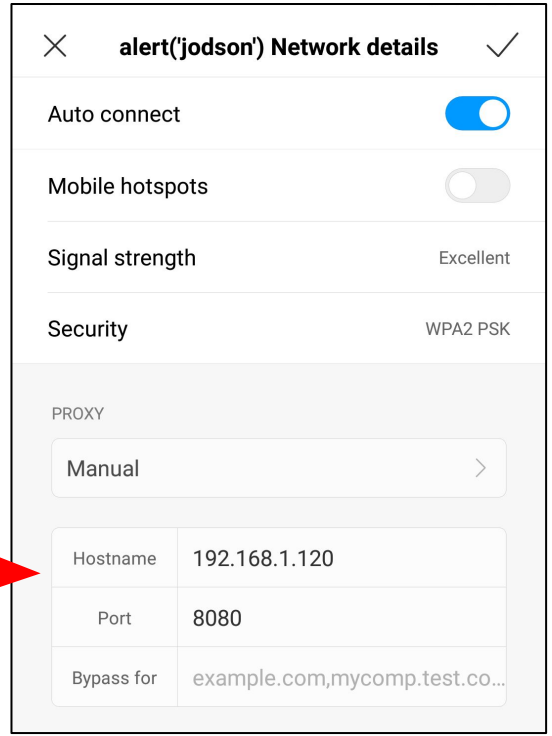
- Computador de teste > Ferramenta Proxy

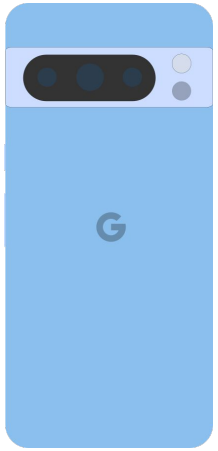


Como configurar a ferramenta de proxy?

Tempest
[ACADEMY]
Conference

- Settings > Wifi > Proxy





Como configurar a ferramenta de proxy?

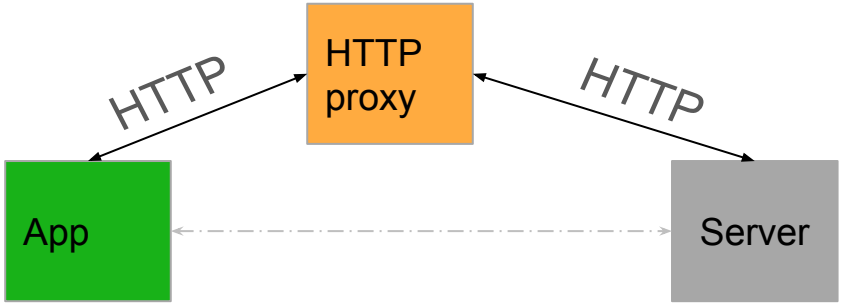
Tempest
[ACADEMY]
Conference

- Apps que ignoram o proxy
  - Framework Flutter
  - Detalhes no cheat sheet

Configurando certificado de Autoridade Certificadora

Tempest
[ACADEMY]
Conference

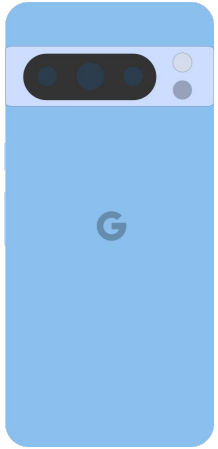
- Why?
  - Ferramenta proxy -> Ataque MITM



Configurando certificado de Autoridade Certificadora

Tempest [ACADEMY] Conference

- Why?
  - O que impede um ataque MITM no TLS?
    - Durante início da comunicação (handshake TLS), servidor envia o certificado para o cliente
    - Clientes (browser, OS) vêm embutidos com certificados padrões



Tempest
ACADEMY
Conference

dora

Settings

Firefox about:preferences#searchResults

General
Home
Search
Privacy & Securi
Sync
More from Mozi

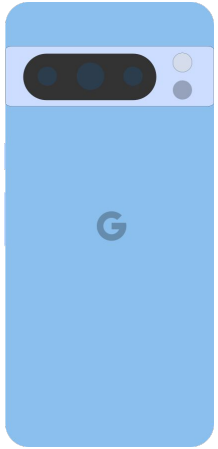
Certificate Manager

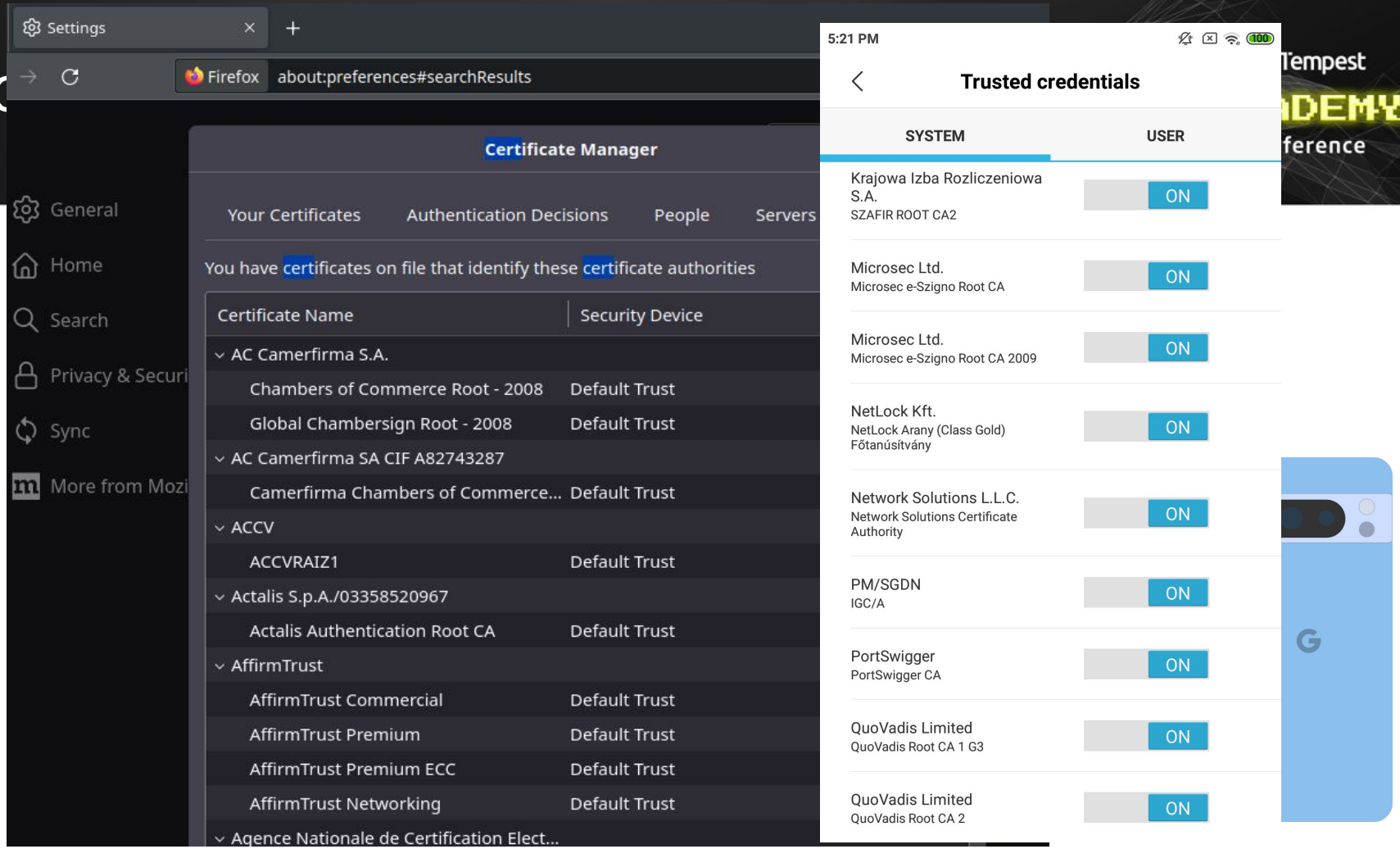
Your Certificates | Authentication Decisions | People | Servers | Authorities

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Default Trust
Global Chambersign Root - 2008	Default Trust
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce...	Default Trust
ACCV	
ACCVRAIZ1	Default Trust
Actalis S.p.A./03358520967	
Actalis Authentication Root CA	Default Trust
AffirmTrust	
AffirmTrust Commercial	Default Trust
AffirmTrust Premium	Default Trust
AffirmTrust Premium ECC	Default Trust
AffirmTrust Networking	Default Trust
Agence Nationale de Certification Elect...	

ados padrões
rvidor envia o

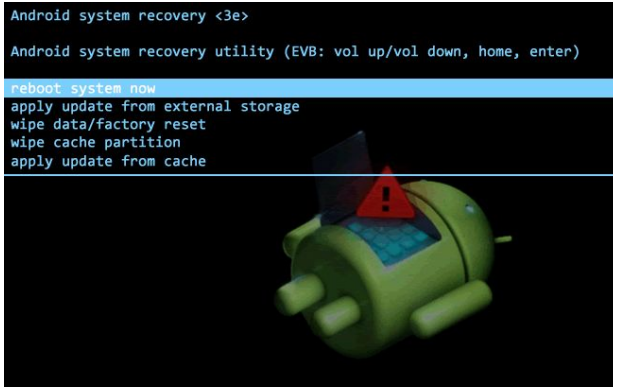



Settings
Firefox
about:preferences#searchResults
General
Home
Search
Privacy & Securi
Sync
More from Mozi
Certificate Manager
Your Certificates
Authentication Decisions
People
Servers
You have certificates on file that identify these certificate authorities
Certificate Name
Security Device
AC Camerfirma S.A.
Chambers of Commerce Root - 2008
Default Trust
Global Chambersign Root - 2008
Default Trust
AC Camerfirma SA CIF A82743287
Camerfirma Chambers of Commerce...
Default Trust
ACCV
ACCVRAIZ1
Default Trust
Actalis S.p.A./03358520967
Actalis Authentication Root CA
Default Trust
AffirmTrust
AffirmTrust Commercial
Default Trust
AffirmTrust Premium
Default Trust
AffirmTrust Premium ECC
Default Trust
AffirmTrust Networking
Default Trust
Agence Nationale de Certification Elect...
5:21 PM
Trusted credentials
SYSTEM
USER
Krajowa Izba Rozliczeniowa S.A.
SZAFIR ROOT CA2
ON
Microsec Ltd.
Microsec e-Szigno Root CA
ON
Microsec Ltd.
Microsec e-Szigno Root CA 2009
ON
NetLock Kft.
NetLock Arany (Class Gold) Főtanúsítvány
ON
Network Solutions L.L.C.
Network Solutions Certificate Authority
ON
PM/SGDN
IGC/A
ON
PortSwigger
PortSwigger CA
ON
QuoVadis Limited
QuoVadis Root CA 1 G3
ON
QuoVadis Limited
QuoVadis Root CA 2
ON

Configurando certificado de Autoridade Certificadora

Tempest
[ACADEMY]
Conference

- Como configurar certificado da ferramenta no aparelho de teste?
  - 1) Obter certificado (http://burp, http://mitm.it, ...)
  - 2) Instalar certificado
    - (Simples, menos funcional em Android 7+) Configurações
    - (Menos simples) /system/etc/security/cacerts/
      - Requer ambiente que pode acionar checagens de root e/ou bootloader



Iniciando o aplicativo

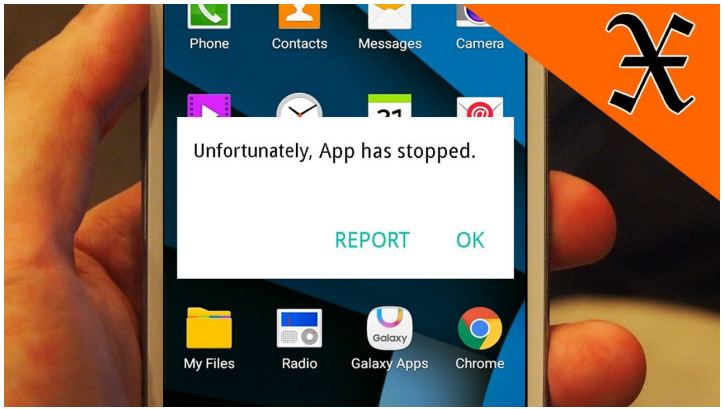
- Podemos começar os testes agora?

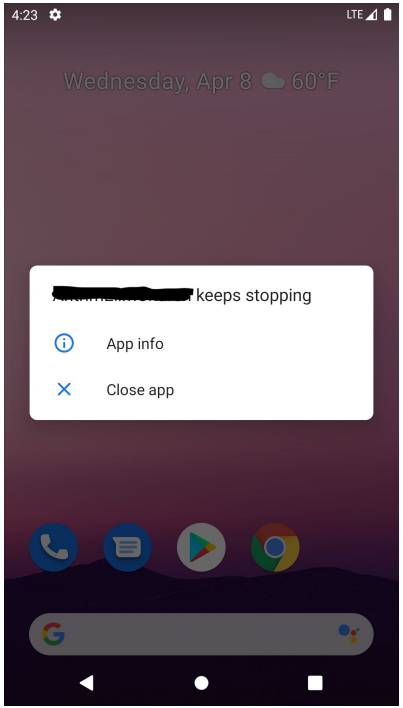
Aplicativo Iniciado

- “Você abre o app e ele roda perfeitamente, toda informação trafegada entre ele e a API aparecem na sua ferramenta de proxy e você sente que vai poder realizar testes sem problemas.”

O que pode acontecer?

- Forçar um crash
- Fechar sozinho (normalmente nos primeiros segundos)
- Apresentar uma mensagem de erro
- Falhar ao tentar fazer login
- Qual é o problema?⏭️





Qual é o problema?

Tempest
[ACADEMY]
Conference

- Pode ser alguma incompatibilidade com o aparelho (arquitetura, ...)
- Alguma checagem
  - detecção de root, bootloader unlocked, dev mode
  - certificate pinning
- Forma simples de identificar? Eliminar as possibilidades

Tempest

:ACADEMY:

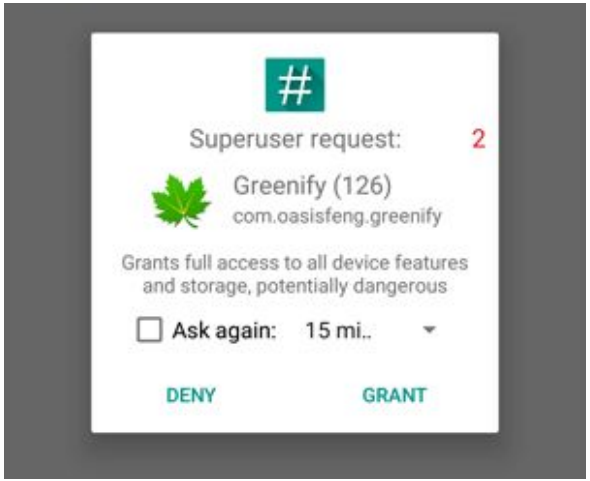
Conference

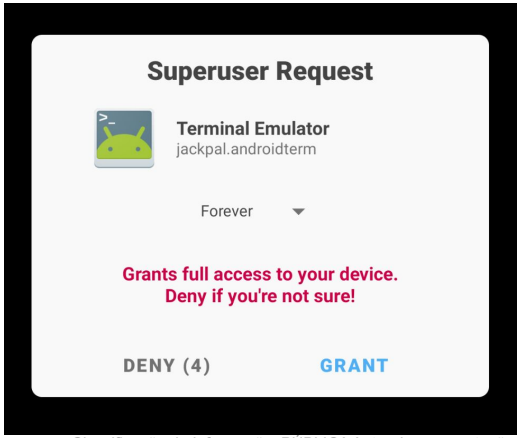
Evitando detecção de root

- O que?⏭️
- Como?⏭️

O que é root no contexto do Android?

Tempest
[ACADEMY]
Conference





Soluções genéricas para esconder root

- Aparelho sem acesso root diretamente via Android
- MagiskHide (v23) / MagiskDenyList
- ON HANDS
- Frida (Dynamic instrumentation toolkit) scripts
  - https://codeshare.frida.re/explore
  - https://github.com/sensepost/objection

Soluções manuais e específicas

- Estática
  - Decompiler/Disassembler (jadx, ida pro/ghidra/...,)
  - Beautifier (js-beautify)
- Dinâmica
  - Frida
  - Debugger (gdb)
- ON HANDS (simples)

Evitando outras checagens

Play Integrity API (~SafetyNet Attestation~)

Tempest
[ACADEMY]
Conference

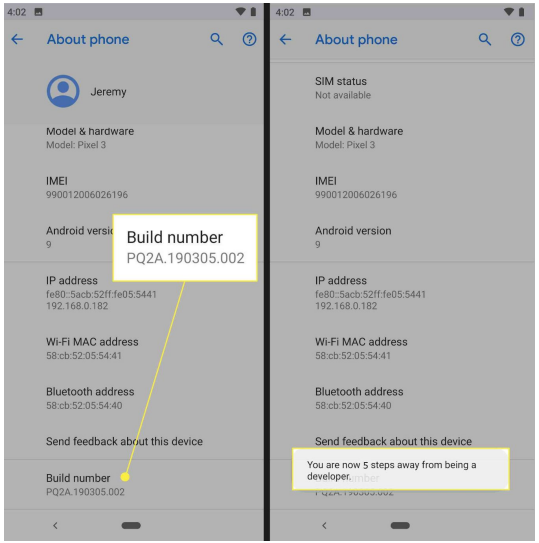
- O que é?
- Universal SafetyNet Fix (github.com/kdrag0n/safetynet-fix)
- Play Integrity Fix (github.com/chiteroman/PlayIntegrityFix)
- Aparelho Íntegro

`MEETS_DEVICE_INTEGRITY, MEETS_BASIC_INTEGRITY`

Device Status	Value of `ctsProfileMatch`	Value of `basicIntegrity`
Certified, genuine device that passes CTS	`true`	`true`
Certified device with unlocked bootloader	`false`	`true`
Genuine but uncertified device, such as when the manufacturer doesn't apply for certification	`false`	`true`
Device with custom ROM (not rooted)	`false`	`true`
Emulator	`false`	`false`
No device (such as a protocol emulating script)	`false`	`false`
Signs of system integrity compromise, one of which may be rooting	`false`	`false`
Signs of other active attacks, such as API hooking	`false`	`false`

Detecção de modo desenvolvedor

- Tentar frida script
- Não usar o modo desenvolvedor
  - Não precisa deixar ativado para usar o frida server
    - Daemon (-D) + conexão via rede
    - Aproveitar o privilégio de root (termux)
- Análise manual



Certificate Pinning

Tempest
[ACADEMY]
Conference

- Aplicativo checa CA certificate da API
- Frida scripts
  - https://codeshare.frida.re/@akabe1/frida-multiple-unpinning/
  - https://github.com/sensepost/objection
- Análise manual

Concluindo

Concluindo

- Não tem solução perfeita, depende do target
- Resumo de pontos mais diferentes
  - Android proxy settings podem ser ignoradas
  - Instalar system certificate não requer privilégios de root diretos no Android
  - Frida não exige developer mode
  - Lembre do Termux (frida client, pip, ...)
- Faça backup dos APKs no início do teste

(Algumas) Referências

- https://portswigger.net/burp/documentation/desktop/tools/proxy/invisible
- https://blog.nviso.eu/2019/08/13/intercepting-traffic-from-android-flutter-applications/
- https://portswigger.net/burp/documentation/desktop/external-browser-config/certificate
- https://android-developers.googleblog.com/2016/07/changes-to-trusted-certificate.html
- https://blog.ropnop.com/configuring-burp-suite-with-android-nougat
- https://pswalia2u.medium.com/install-burpsuites-or-any-ca-certificate-to-system-store-in-android-10-and-11-38e508a5541a
- https://github.com/NVISOsecurity/MagiskTrustUserCerts
- https://www.cin.ufpe.br/~tg/2020-3/TG_CC/tg_vrm.pdf

Tempest

[ACADEMY]

Conference

Tempest
ACADEMY
Conference

tinyurl.com/hacking-android

Cheat Sheet

Hacking Android Apps

Some tricks to deal with Android Apps

Setting proxy

- Go to Settings > WiFi > Your network > Proxy, and set the ip address and port of the proxy tool
- if there is AP isolation:
  - In computer: `adb reverse tcp:8080 tcp:8080`
  - In android: Set the WiFi proxy using 127.0.0.1 and 8080
- Apps ignoring the proxy (Flutter)
  - ProxyDroid (available in playstore, root is required)
  - Transparent Proxy
    - A) Use an WiFi adapter to create an AP on your computer and connect the Android
    - B) Use your default WiFi router (without AP isolation) (if the app does not need ipv6)

vinicius.moraes@tempest.com.br / vinicius777