Olá, pessoal.

Construindo aplicativos seguros

Nós queremos nossos apps mais seguros.

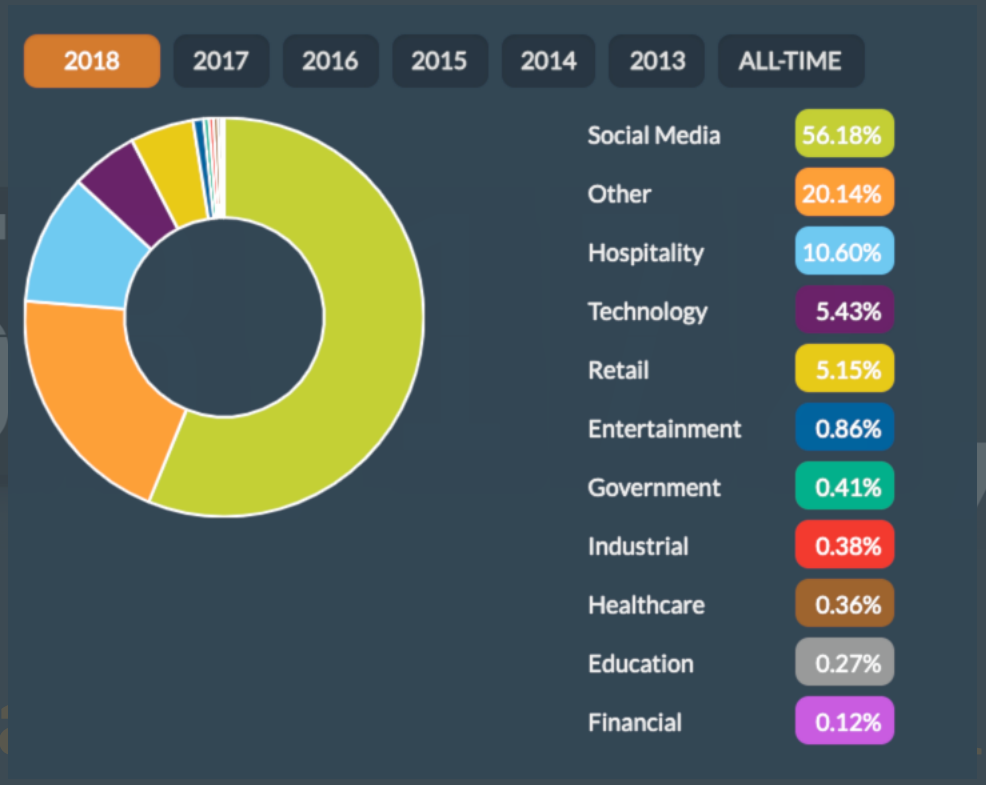
Mas temos notado uma escalada de problemas de segurança.

3,353,172,708

Registros vazados no primeiro semestre de 2018

3,35 ,708

Registros vaz estre de 2018



18,525,816 records lost or stolen **every day**

771,909 records **every hour**

12,865 records **every minute**

214 records **every second**

Por que isso acontece?

Por que isso acontece?

#whoami

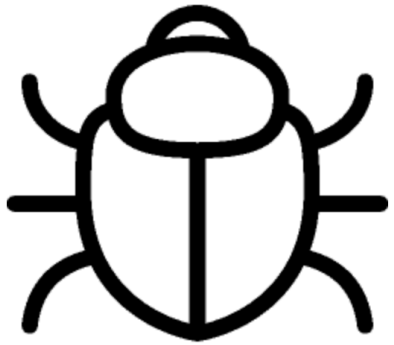
João Pimenta

- Arquiteto de segurança
- Pentester de apps
- Pesquisador de segurança
- Jazz

Além da cereja do bolo e do Forrest

- Crescimento exponencial de dados e acesso à internet
- O mercado da desinformação
- “Segurança inviabiliza o produto”
- “Terminamos o produto, agora vamos investir em segurança!”

Aonde isso nos leva?

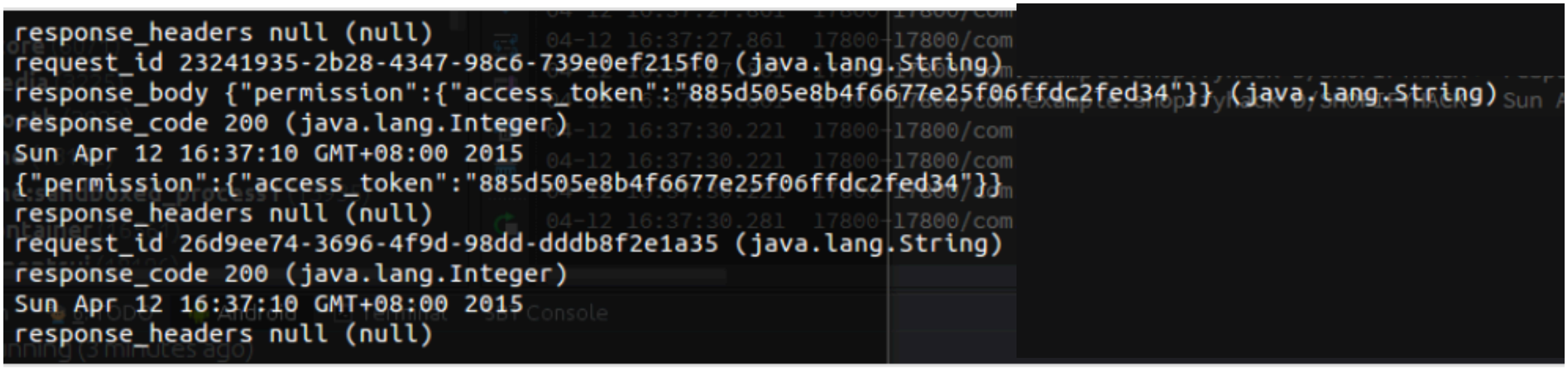


Vamos ver...

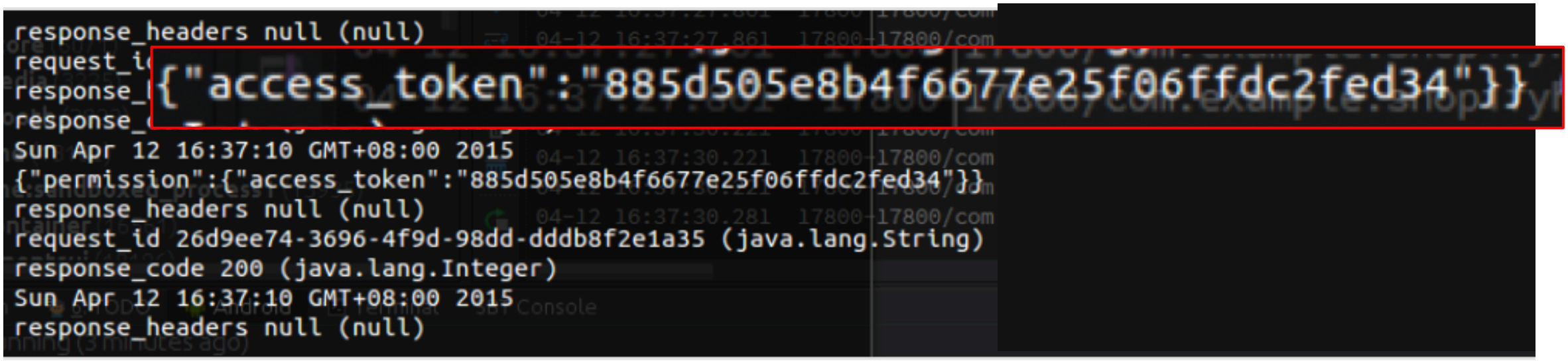
Chave de API hardcoded

```
private static final java.lang.String CONFIG = "cloudinary://434762629765715:[redacted]@reverb";
```

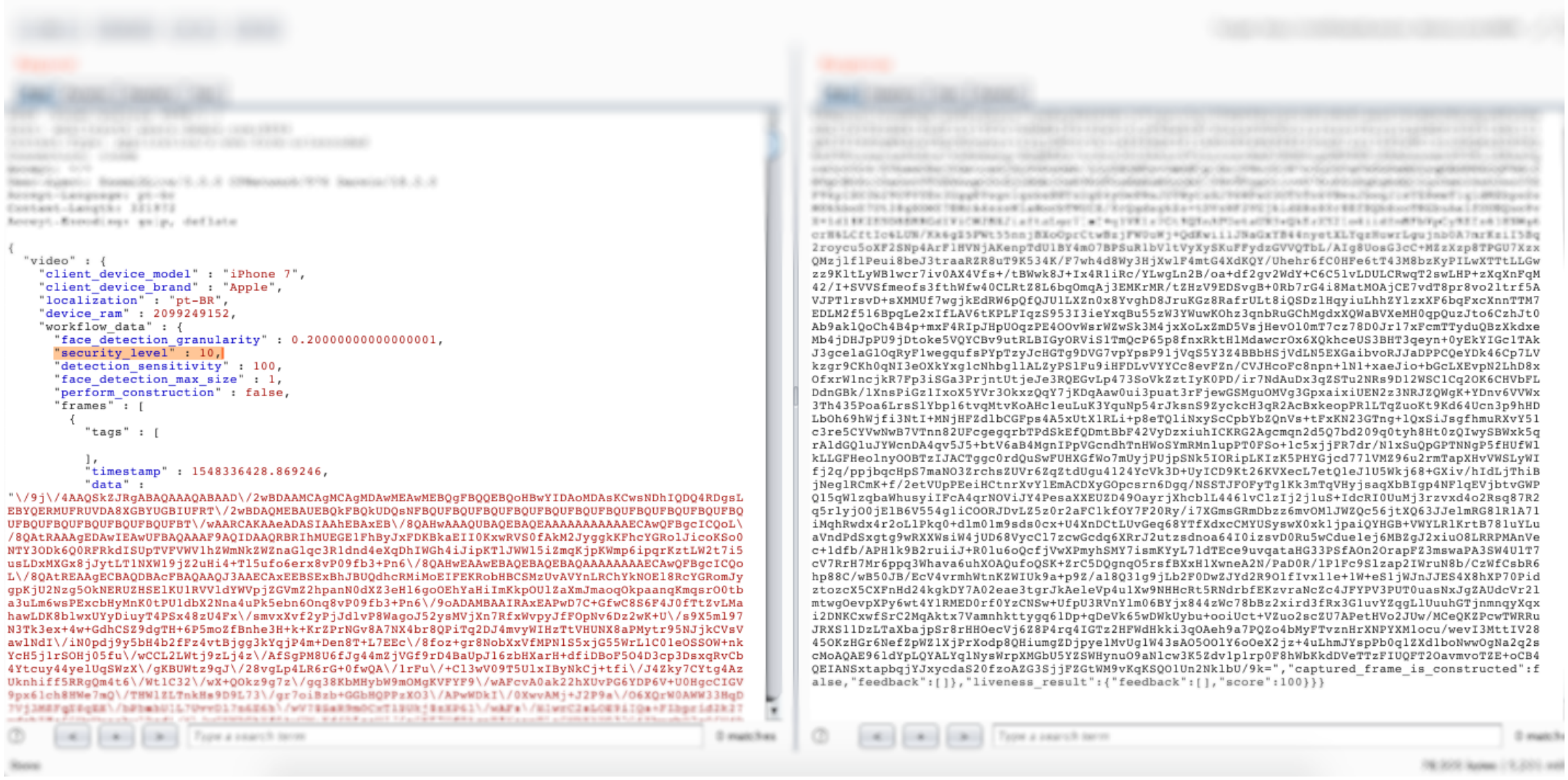
Informação sensível em log



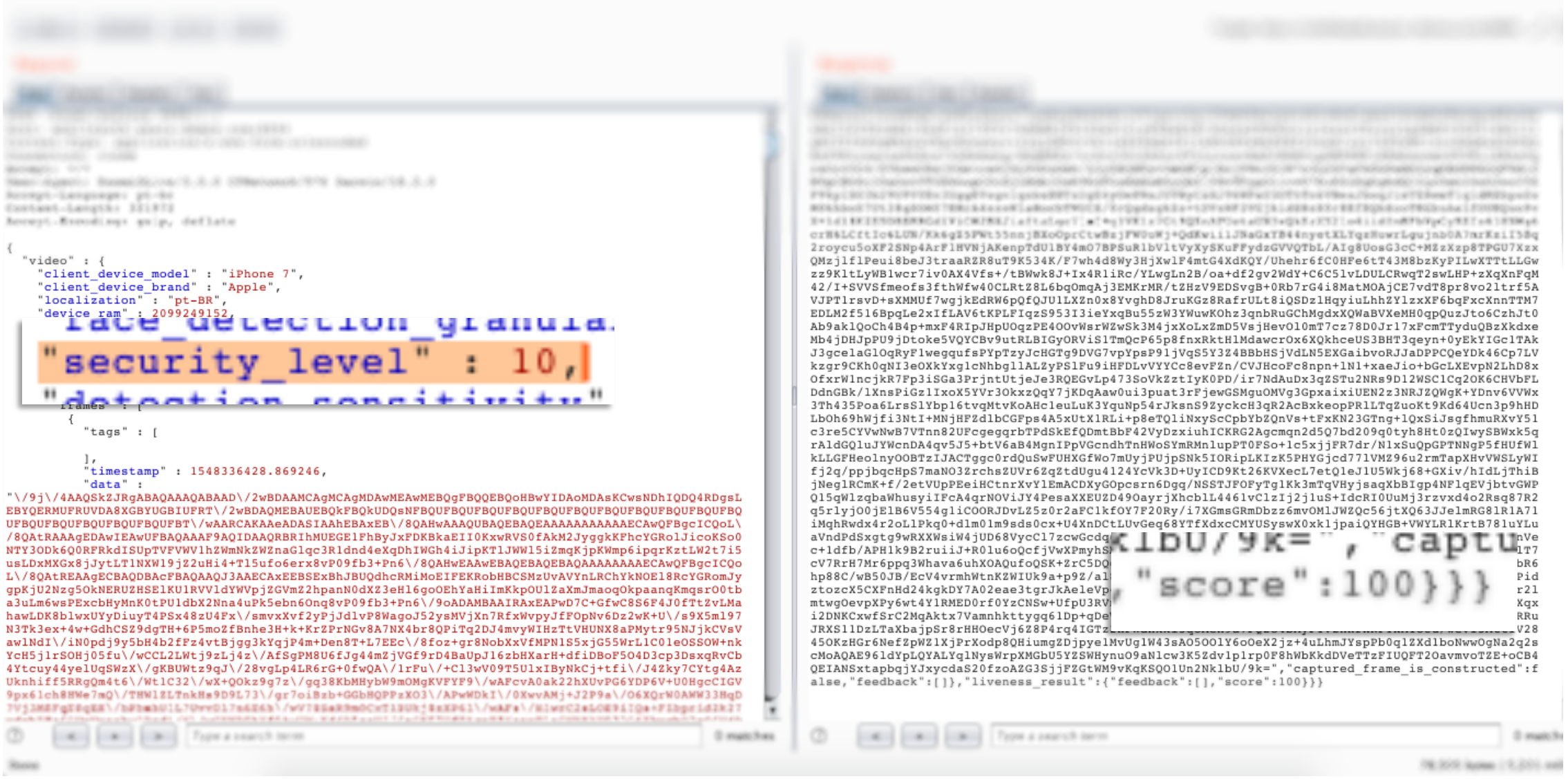
Informação sensível em log



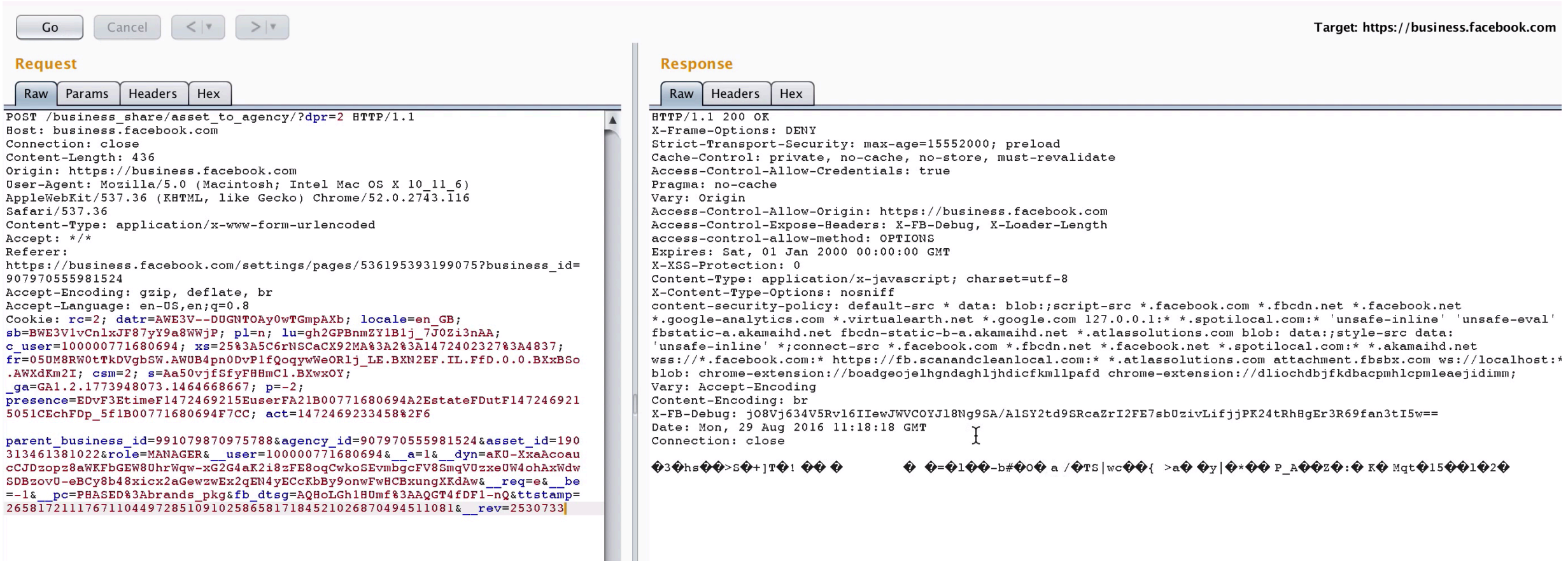
Autenticação insegura



Autenticação insegura

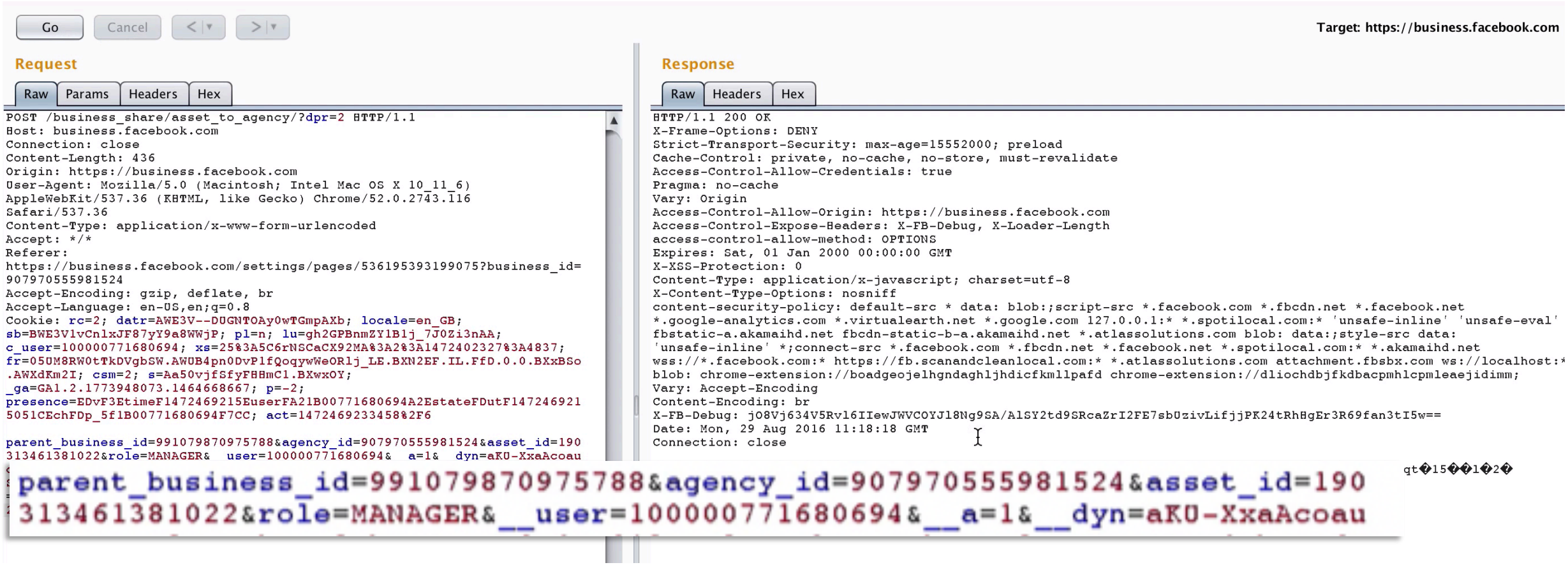


Insecure Direct Object References



Reportada por Arun Sureshkumar

Insecure Direct Object References



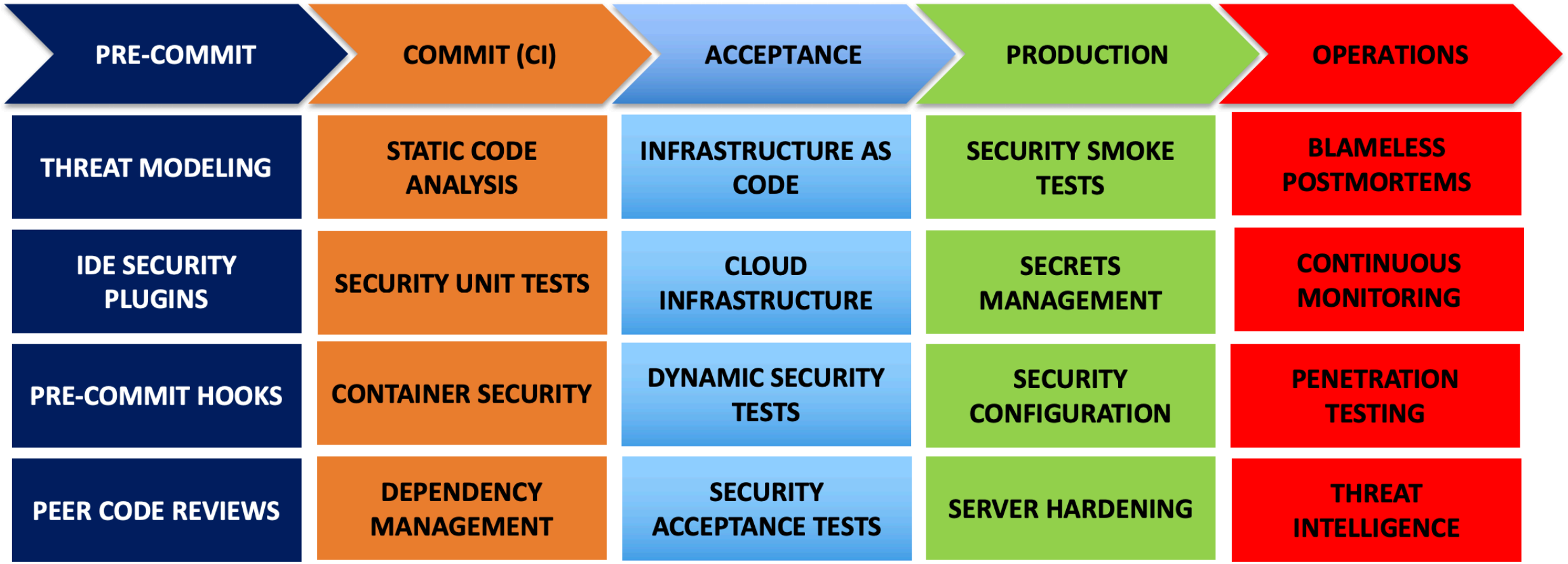
Reportada por Arun Sureshkumar

Qual nosso papel?

Me pague a segurança!

Se comunicar, integrar a segurança.

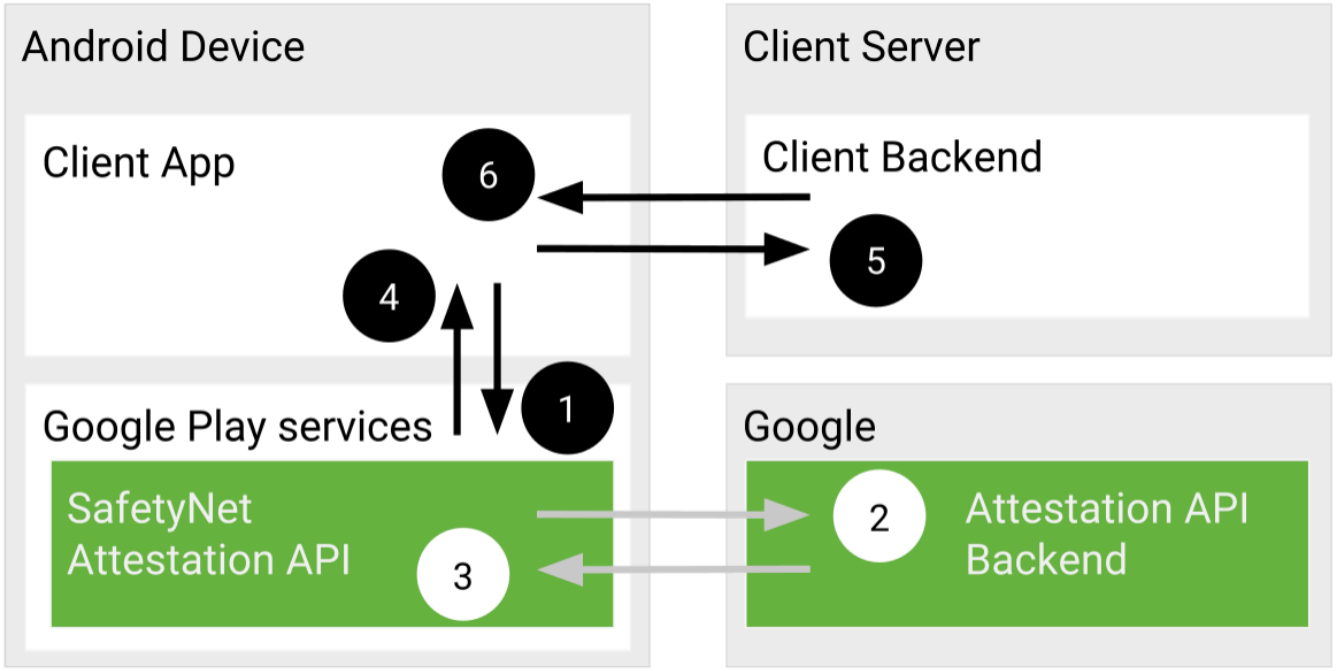
Segurança desde a concepção



Dificultar a vida do atacante

- Ofuscação do código;
- Antitamper;
- Antidebug;
- Antihooking;
- Antiemulador;
- Antiroot/Jailbreak;
- SSL Pinning;
- Criptografar e assinar Payload (RSA + AES).

SafetyNet Attestation API



1. A API SafetyNet Attestation recebe uma chamada do seu aplicativo incluindo um nonce.
2. O serviço SafetyNet Attestation avalia o ambiente de runtime e requisita aos servidores do Google um resultado através de uma mensagem assinada.
3. Servidores do Google retornam uma mensagem assinada ao device para a SafetyNet attestation.
4. SafetyNet attestation retorna esses valores para o seu app.
5. Seu app encaminha para os seus servidores.
6. Seus servidores recebem a informação e utilizam para tomada de decisões de segurança.

https://github.com/googlesamples/android-play-safetynet/

SafetyNet Attestation API

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`

Segurança é colaborativa.
É uma jornada de construção.

Segurança é colaborativa.
É uma jornada de construção.

Obrigado!

Referências

- https://blogs.sans.org/appsecstreetfighter/files/2018/10/DevSecOps_Exploring_Phase1-2.pdf
- https://arunsureshkumar.me/index.php/2016/09/16/facebook-page-takeover-zero-day-vulnerability/
- https://breachlevelindex.com/
- https://developer.android.com/training/safetynet/attestation.html