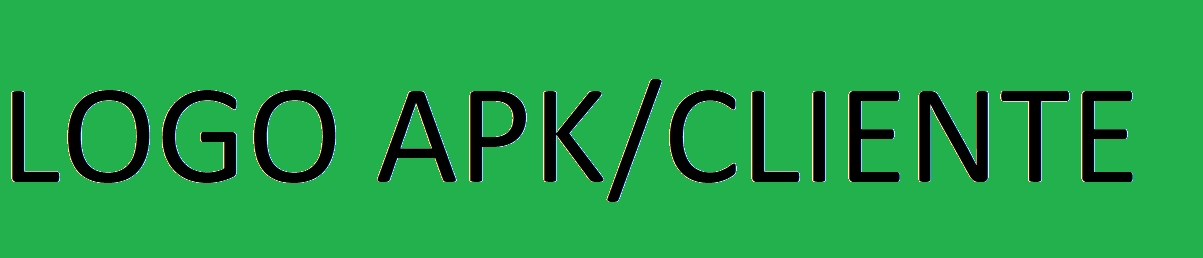
Relatório - Teste intrusão Mobile

Cliente XXXXXXX



Data: 12/12/12  
Cliente: xxxx  
Analista: xxxxx

Dest: xxx

Copyright © 2021 **EMPRESA\_DE\_VOCES**. All rights reserved.

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from **EMPRESA\_DE\_VOCES**.

**Sumário**

[1.0 Sumário 3](#_Toc88503002)

[1.1 Objetivo 3](#_Toc88503003)

[1.3 Metodologia 3](#_Toc88503004)

[1.3 Escopo 3](#_Toc88503005)

[1.4 Classificação da Severidade/Criticidade das Vulnerabilidades 3](#_Toc88503006)

[2.0 Resumo das Vulnerabilidades 4](#_Toc88503007)

[2.1 Vulnerabilidades Altas 4](#_Toc88503008)

[2.2 Vulnerabilidades Médias 5](#_Toc88503009)

[2.3 Vulnerabilidades Baixas 5](#_Toc88503010)

[3. Conclusão 6](#_Toc88503011)

## 1.1 Objetivo

- data de ocorrência

- quais testes foram realizados (estática e dinâmica)

- Graybox

## 1.3 Metodologia

- **NIST/OSSTMM**: as fases do ataque (reconhecimento, planejamento, exploração, pos exploração e report)

- **OWASP TOP 10 MOBILE**: explicar o que é por cima e para que serve.

* [M1: Improper Platform Usage](https://owasp.org/www-project-mobile-top-10/2016-risks/m1-improper-platform-usage)
* [M2: Insecure Data Storage](https://owasp.org/www-project-mobile-top-10/2016-risks/m2-insecure-data-storage)
* [M3: Insecure Communication](https://owasp.org/www-project-mobile-top-10/2016-risks/m3-insecure-communication)
* [M4: Insecure Authentication](https://owasp.org/www-project-mobile-top-10/2016-risks/m4-insecure-authentication)
* [M5: Insufficient Cryptography](https://owasp.org/www-project-mobile-top-10/2016-risks/m5-insufficient-cryptography)
* [M6: Insecure Authorization](https://owasp.org/www-project-mobile-top-10/2016-risks/m6-insecure-authorization)
* [M7: Client Code Quality](https://owasp.org/www-project-mobile-top-10/2016-risks/m7-client-code-quality)
* [M8: Code Tampering](https://owasp.org/www-project-mobile-top-10/2016-risks/m8-code-tampering)
* [M9: Reverse Engineering](https://owasp.org/www-project-mobile-top-10/2016-risks/m9-reverse-engineering)
* [M10: Extraneous Functionality](https://owasp.org/www-project-mobile-top-10/2016-risks/m10-extraneous-functionality)

## 1.3 Escopo

- (OPCIONAL) URLs API/IP TESTADAS

- **Versão do aplicativo** / hash / nome / endereço da playstore/applestore

- Credenciais fornecidas (x, y)

- Documentação da API (Swagger / Postman)

## 1.4 Classificação da Severidade/Criticidade das Vulnerabilidades

- CVSS / impact vs probabilities

- Score:

**Probabilidade vs Impacto**

- Crítico: sao as falhas que expõem dados da empresa ou queima a reputação.   
- Alta: para ataque ser explorado precisa de mais tempo para atacante executar a técnica.  
- Média: ausência de *httpOnly=protege cookie de sessao contra ataque de XSS*, SSL obsoleto,   
- Baixa: politica de senha fraca (permite cadastrar senhas sem critérios de segurança)

# 2.0 Resumo das Vulnerabilidades

* Gráfico de pizza
* Tabela do resumo das vulnerabilidades

# 2.1 Vulnerabilidades Altas

**2.1.2 Dados Armazenados Localmente**

**Descrição**: xxxxxxxxxxxxxxxxx

**Host Afetado**: URL / caminho do arquivo *(/data/data/nome\_app/databases/****mydata.xml***)

**Evidencia**: narrar cenário de ataque + prints

**Solução**: não armazenar dados sensivéis localmente sem uso de uma criptografia segura. Utilizar dados sensiveís apenas no beck-end com consulta de uma chave assimétrica.

**Referência**: Links (owasp mobile, MSTG mobile,etc)

**2.1.3 xxxxxxxx**

**Descrição**: xxxxxxxxxxxxxxxxx

**Host Afetado**: xxxxx

**Evidencia**: xxxxxxx

**Solução**: xxxxxxx

**Referencia**: xxxxxxxx

# 2.2 Vulnerabilidades Médias

**Não foram identificadas vulnerabilidades Médias.**

# 2.3 Vulnerabilidades Baixas

**2.3.1 xxxxxxxx**

**Descrição**: xxxxxxxxxxxxxxxxx

**Host Afetado**: xxxxx

**Evidencia**: xxxxxxx

**Solução**: xxxxxxx

**Referencia**: xxxxxxxx

# 3. Conclusão

Resumo de tudo que você encontrou e tudo que você nao encontrou.

* Nivel de maturidade
* Narrativa do relatório (contar as falhas encontradas como se fosse seu amigo)
* Recomendações genêricas (testes recorrentes para realizar a cada alteração de feature ou a “x” tempo).

### 