|  |
| --- |
| {name} |
| Vulnerability Report |
| {date | convertDateLocale: 'us': 'full'} |

Table of Contents

[1. Introduction 3](#_Toc177396537)

[1.1. Contexte et objectifs de la mission 3](#_Toc177396538)

[1.2. Périmètre de la mission 3](#_Toc177396539)

[1.3. Méthodologie 3](#_Toc177396540)

[1.4. Déroulement des travaux 3](#_Toc177396541)

[1.5. Limites 4](#_Toc177396542)

[1.6. Remise en état 4](#_Toc177396543)

[2. Summary 5](#_Toc177396544)

[2.1. Executive summary 5](#_Toc177396545)

[2.1. Vulnérabilités et recommandations 6](#_Toc177396546)

[3. Constats détaillés 7](#_Toc177396547)

# Introduction

## Contexte et objectifs de la mission

{company.name} ask to carry out {pentest.type}. The objectives of these tests were to:

* Identify vulnerabilities in the web application and the mobile application (iOS for iPad);
* Identify the risks associated with the identified vulnerabilities;
* To propose prioritized corrective actions;
* Formalize these elements in a clear and understandable report for technical and business contacts.

## Périmètre de la mission

{company.name} has mandated us to perform security tests on the following scope:

* {-w:p scope}{name}{/scope}

## Méthodologie

The engagement was based the following approaches:

* Phase 1: Information gathering & target mapping;
* Phase 2: Vulnerability scan & attack plan identification;
* Phase 3: Exploitation of identified vulnerabilities & elevation of privileges;
* Phase 4: Consolidation & results restitution.

## Déroulement des travaux

The testing activities were performed between {date\_start | convertDateLocale} and {date\_end | convertDateLocale}.

## Limites

## Remise en état

# Summary

## Executive summary

IBC a mandaté Corellia afin d’effectuer des tests d’intrusion sur ses applications web «sudo.co.il», «securebank.com». Le but de ces tests était de s’assurer que ces applications sont protégées contre des cyberattaques. Lors de nos tests d’intrusions, nous avons identifié deux vulnérabilités de gravité très élevée (V01 & V02), qui pourrait permettre à un attaquant opérant depuis Internet d’usurper l’identité de n’importe quel utilisateur des applications web sudo.co.il et securebank.com, et ce, sans authentification. Cela lui permettrait ainsi d’accéder aux informations du compte et d’effectuer toutes les actions disponibles à partir de celui-ci. Nous avons également identifié une vulnérabilité de gravité modérée. La vulnérabilité (V03) pourrait permettre à un attaquant d’obtenir les identifiants de connexion des utilisateurs du serveurs hébergeant l’application securebank.com. Cela pourrait permettre à l’attaquant de prendre le contrôle à distance du serveur. Les risques métiers associées à ces différentes vulnérabilités sont les suivants :

· Mise en cause par rapport aux réglementations de la protection des données personnelles, telles que le RGPD : un attaquant pourrait parvenir à récupérer des données personnelles (données personnelles, transactions bancaires, factures, RIB, numéro de sécurité sociale) des utilisateurs de securebank.com, ce qui exposerait IBC à un risque de sanction par les organismes de régulation.

· Fraude / Usurpation d'identité : un attaquant pourrait exploiter diverses vulnérabilités afin d’usurper l’identité d’un utilisateur et accéder à ses données personnelles stockées sur l’application securebank.com. · Contournement de contrôle interne : un attaquant pourrait obtenir des accès non autorisés à des ressources de securebank.com.

· Aide à l’exploitation d’autres vulnérabilités. Corellia estime que les vulnérabilités identifiées peuvent constituer une menace grave pour le système d’information de IBC. De ce fait, Corellia préconise de corriger au plus vite les vulnérabilités en appliquant les recommandations associées.

## Vulnérabilités et recommandations

Following vulnerabilities have been discovered:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Vulnérabilités | Gravité | Recommandations | Priorité |
| {#findings}{#cvss.baseSeverity == 'Critical'}{identifier | changeID: 'V'} | {title} | {cvss.baseSeverity} | {title\_reco} | {priority}{/cvss.baseSeverity == 'Critical'}{/findings} |
| {#findings}{#cvss.baseSeverity == 'High'}{identifier | changeID: 'V'} | {title} | {cvss.baseSeverity} | {title\_reco} | {priority}{/cvss.baseSeverity == 'High'}{/findings} |
| {#findings}{#cvss.baseSeverity == 'Medium'}{identifier | changeID: 'V'} | {title} | {cvss.baseSeverity} | {title\_reco} | {priority}{/cvss.baseSeverity == 'Medium'}{/findings} |
| {#findings}{#cvss.baseSeverity == 'Low'}{identifier | changeID: 'V'} | {title} | {cvss.baseSeverity} | {title\_reco} | {priority}{/cvss.baseSeverity == 'Low'}{/findings} |

# Constats détaillés

The following details the vulnerabilities identified in the scope, together with an estimate of the impact of the exploitation of the vulnerability, the ease of exploitation of the vulnerability and its criticality. Also referenced are the business risks associated with the vulnerability in the context of your environment, as well as the recommendation for remediating the vulnerability and reducing the risks.

{#findings}

|  |  |  |
| --- | --- | --- |
| {identifier | changeID: 'V'} | {title} | Gravité |
| {@cvss.cellColor}  {cvss.baseSeverity} |
| Libellé | {#description}  {@text | convertHTML}  {/description} | |
| Périmètre | {@affected | convertHTML} | |

|  |  |  |
| --- | --- | --- |
| Recommandation | | |
| {identifier | changeID: 'E'} | {title\_reco} | Priorité |
| {priority} |
| Libellé | {#remediation}  {@text | convertHTML}  {/remediation} | |

{#poc}

{@text | convertHTML}

{#images}

{%image}

Image **1** – {caption}

{/images}

{/poc}

{/findings}