



# Le BonBon Croissant Penetration Test Debrief

Team XX

# Our Team



# Agenda

---

Overview



Metrics



Statistics



Compliance



Key Findings



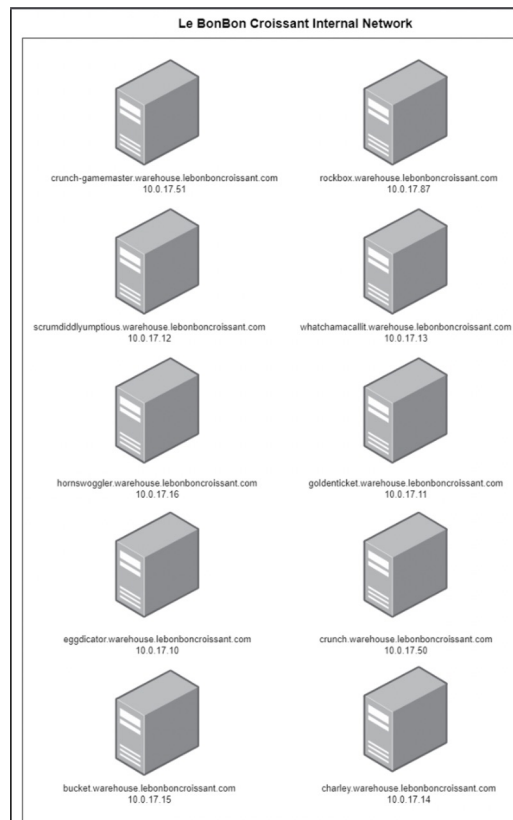
Recommendations



# Overview

# Overview of Engagement

- Risk Assessment
- Focus on user data and compliance
- Critical Infrastructure
- Recommendations





# Metrics

# Metrics



Severity = Impact Rating x Likelihood

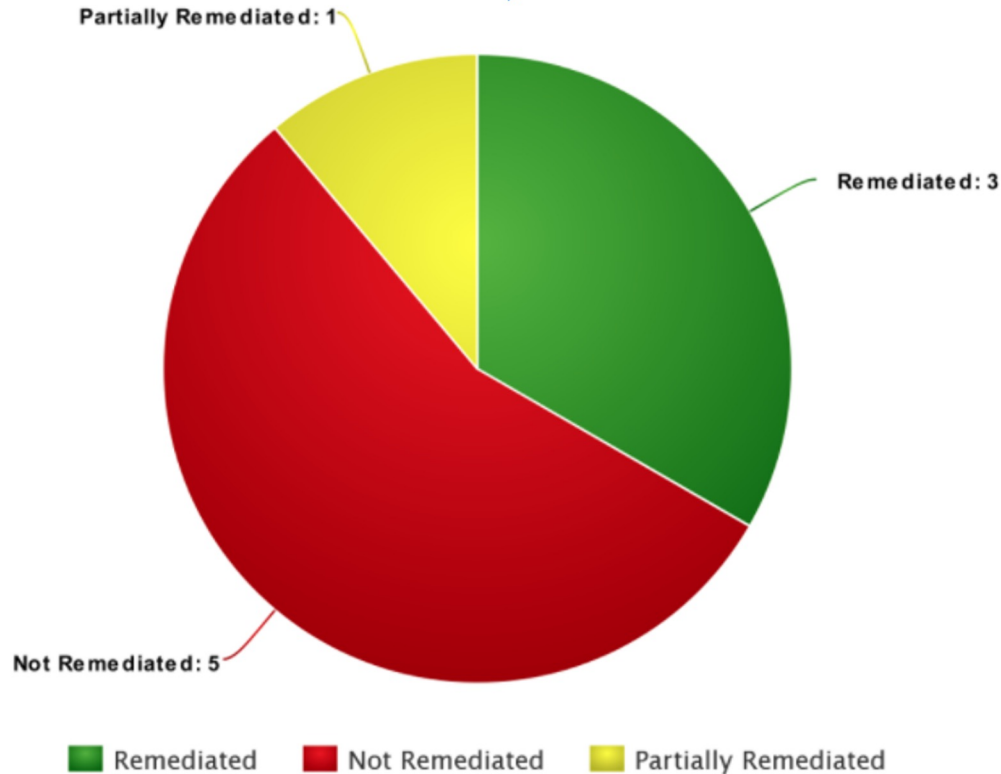
Likelihood	Impact Rating			
	LOW	MEDIUM	HIGH	CRITICAL
LOW	Low	Low	Medium	High
MEDIUM	Low	Medium	High	Critical
HIGH	Low	Medium	Critical	Critical



# Statistics



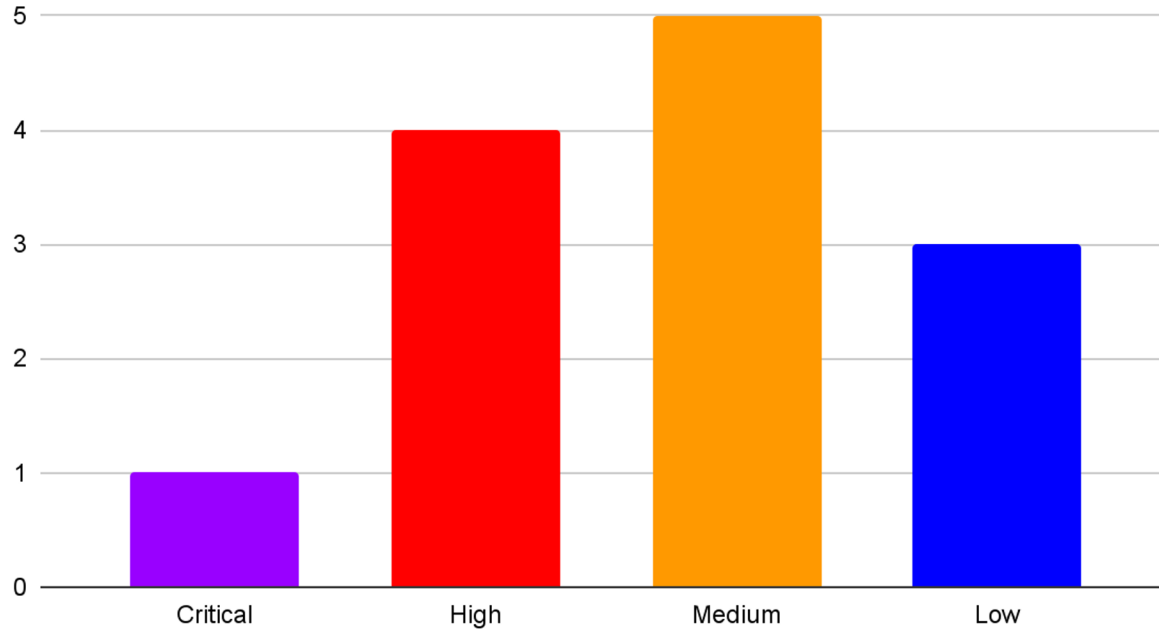
# Previous Findings Comparison



# Findings Found



Total Findings Found





# Compliance

# Compliance



Compliance Framework	Violations	Description
GDPR	1	Article 32, insecure storage of Personally Identifiable Information (PII)
PCI DSS	1	Inadequate password policies



# Key Findings



# Key Findings - High

## Description

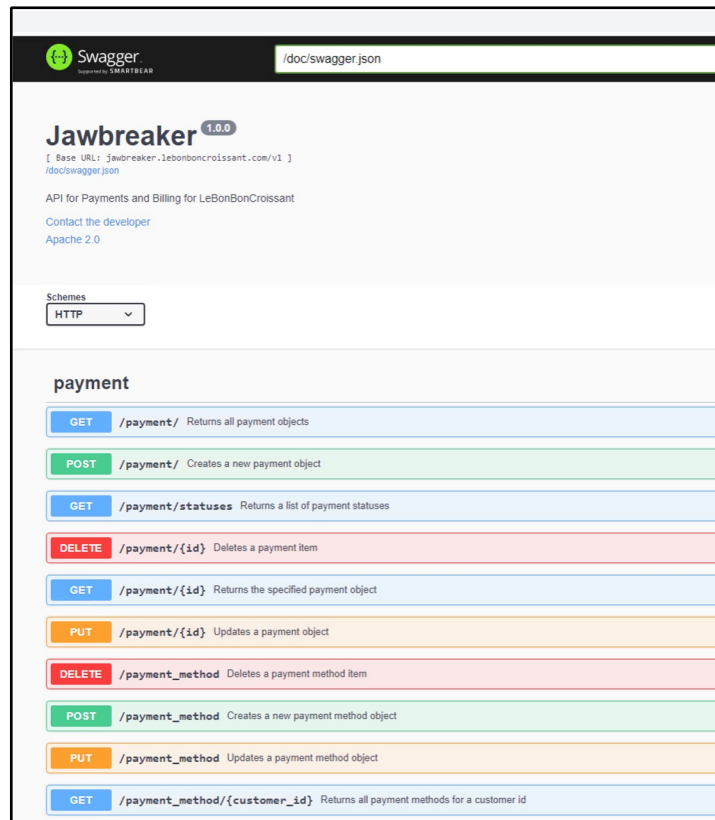
Lack of proper authentication and authorization on sensitive systems.

## Business Impact

- Vulnerable to Denial of Service (DoS)
- Insecure user data

## Remediations

- Enforce strong password policy
- Ensure proper authentication & authorization



# Summary of Current Security Posture



## Positive Security Controls

- Input Sanitization
- Minimal Attack Surface
- Remediations

## Areas for Improvement

- Network Segmentation
- Application Deployment Process
- Weak Passwords





# Recommendations

# Recommendations



- Enforce strong password policies
- Encrypt sensitive information within databases
- Secure coding practices to ensure proper access controls
- Improving application deployment process to improve security posture



# Questions?