*Le BonBon Croissant*

# Security Assessment Overview

*Finals-XX*

Paris, France
LE BONBON CROISSANT
CPTC 2021

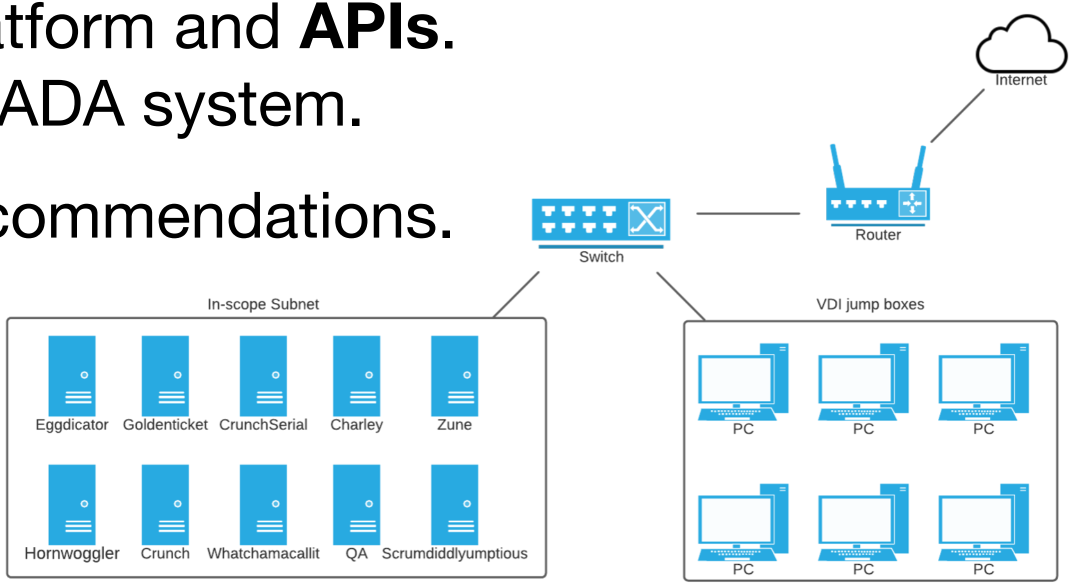
# Our Team

# Engagement Overview

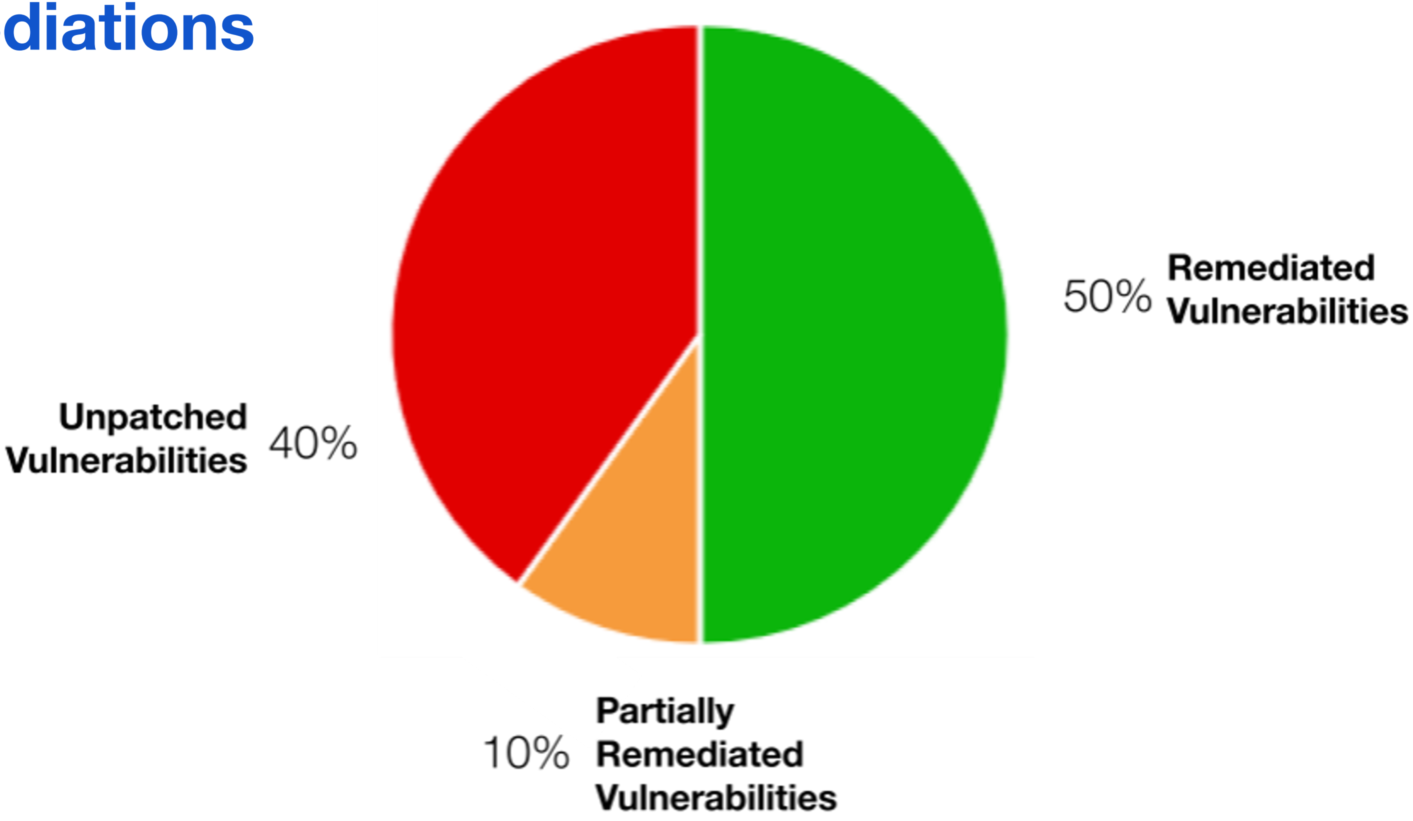
1. **Remediation** assessment.

1. System **security assessment.**
   a. **E-Commerce** platform and **APIs.**
   b. **HMI** and **PLC** SCADA system.

1. **Security posture** recommendations.



# Remediations



# Risk Categories

**Critical**

A vulnerability with **trivial complexity** that, if exploited, will cause severe and **potentially irreparable damage** to company data, systems, and assets.

**High**

A vulnerability that has **low complexity** and has potential to **directly threaten sensitive information or infrastructure** on affected systems.

**Medium**

A vulnerability that either has a **higher attack complexity**, or **requires the chaining together of multiple exploits** in order to cause serious harm.

**Low**

A finding that is **unlikely to cause any damage directly.** However, a malicious actor could leverage information gathered from a vulnerability of this severity as part of a later exploit.

**Informational**

Information gathered that presents **little to no threat** to the system it is present on, but should be noted or remediated to lessen the attack surface of the organization.

# **Key Findings**: E-Commerce Systems

1. **Improper Access Control**
   a. Default Credentials on PostgreSQL
   b. Empty Root Password on MySQL
   c. Unauthenticated Use of Gift Card API
2. **Insecure Design**
   a. Hardcoded Key on LBC Web Interface
   b. Insecure Password Storage Method Used
   c. Customer Data Exposure Through Jawbreaker API
3. **Misconfigurations**
   a. Weak Credentials on Gift Card Administrator Portal

## Findings

5 Critical
3 High
3 Medium
4 Low
2 Info.

# **Business Impacts:** E-Commerce Systems

1. Possible loss of **revenue**.
   a. API, database, or site exploitation could compromise the confidentiality, integrity, and availability of the e-commerce operation.

1. Possible loss of **reputation**.
   a. Sensitive customer data is not sufficiently safeguarded.

## Findings

5 Critical
3 High
3 Medium
4 Low
2 Info.

# **Key Findings:** SCADA Systems

1. **Patch Management**
   a. Default Credentials and Insecure Version of ScadaBR

1. **Insecure Design**
   a. Unauthenticated Read/Write to Programmable Logic Controller

**Findings**

5 Critical
3 High
3 Medium
4 Low
2 Info.

# **Business Impacts:** SCADA Systems

**Findings**

5 Critical
3 High
3 Medium
4 Low
2 Info.

1. Compromise of **monitoring integrity**.
    a. With **HMI** access, one can upload malicious files that allow them to probe and manipulate components of the OT network.

1. Danger to **business** and **employees**.
    a. With access to the **PLC**, one can remotely change the operation of the cyber-physical system (the assembly line), halt production, and possibly injure *Le BonBon Croissant* Employees.

# Standards and Regulatory Compliance

## PCI DSS

- When it comes to handling customer data, the Payment Card Industry Data Security Standard is mandated by the major credit card companies such as American Express, Discover, JCB International, Mastercard and Visa Incorporated.
- This standard outlines goals such as “Build and Maintain a Secure Network and Systems” and “Protect Cardholder Data.”

PCI DSS v3.2.1 Quick Reference Guide (pcisecuritystandards.org)

# Standards and Regulatory Compliance

## ISO 27001

- “[S]ecurity standard that formally specifies an Information Security Management System (ISMS) that is intended to bring information security under explicit management control” - Microsoft
- Details implementation, monitoring, maintenance, and improvement of systems

ISO/IEC 27001:2013 Information Security Management Standards - Microsoft Compliance | Microsoft Docs

# Business Comparisons

In comparison to other businesses of similar scale, *Le BonBon Croissant* boasts better than average security posture.

- Cyber Security Breaches Survey 2021
  - Monitoring Tools Down to 35%
  - User Monitoring Down to 32%
  - Cybersecurity high priority for 77%
  - A minority are performing tests

- Cybersecurity Has Become More Difficult During COVID-19

Cyber Security Breaches Survey 2021 - GOV.UK (www.gov.uk)

# Security Strengths

Despite some areas for improvement being found, we believe that *Le BonBon Croissant* has made great improvements in their security posture.

- Impressive user account discipline and adherence to the **principle of least privilege.**
- Excellent **communication and incident response** times to reported issues.
- Minimal **unnecessary services** and machines on the network.

# Next Steps

1. **Critical**
   1. Implement remediations for the reported vulnerabilities.
2. **Short Term**
   1. Conduct an incident response operation to ensure that no existing vulnerabilities have been exploited.
   2. Encourage employee participation in secure coding courses.
3. **Long Term**
   1. Begin to isolate and segment systems across networks.
   2. Pursue best security practices for company systems (defense in depth/zero trust).

Paris, France

LE BONBON CROISSANT

CPTC 2021

# Thank you.

*Questions?*