



# Le BonBon Croissant

Penetration Test Debrief



Prepared by Finals-TeamXX

# Team Introduction








# Agenda

-  Summary of Engagement
-  Key Strengths
-  Key Findings
-  Recommendations
-  Business Impact



# Summary of Engagement

-  2nd Penetration Test of the Le BonBon Croissant warehouse network
-  Evaluated the strengths and vulnerabilities of the hosts on the network
-  Reevaluated the vulnerabilities found in our initial penetration test

# Summary of Engagement

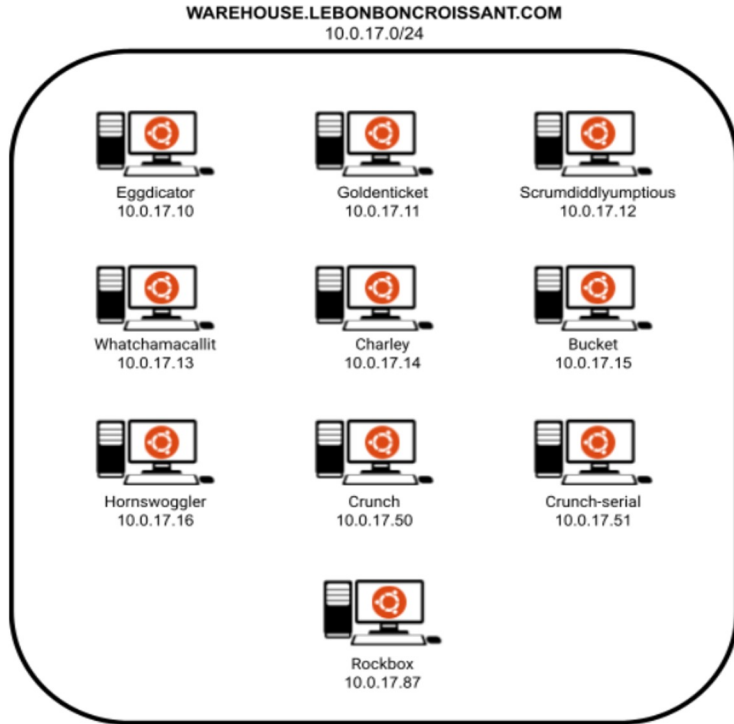


Figure 1: Network Diagram

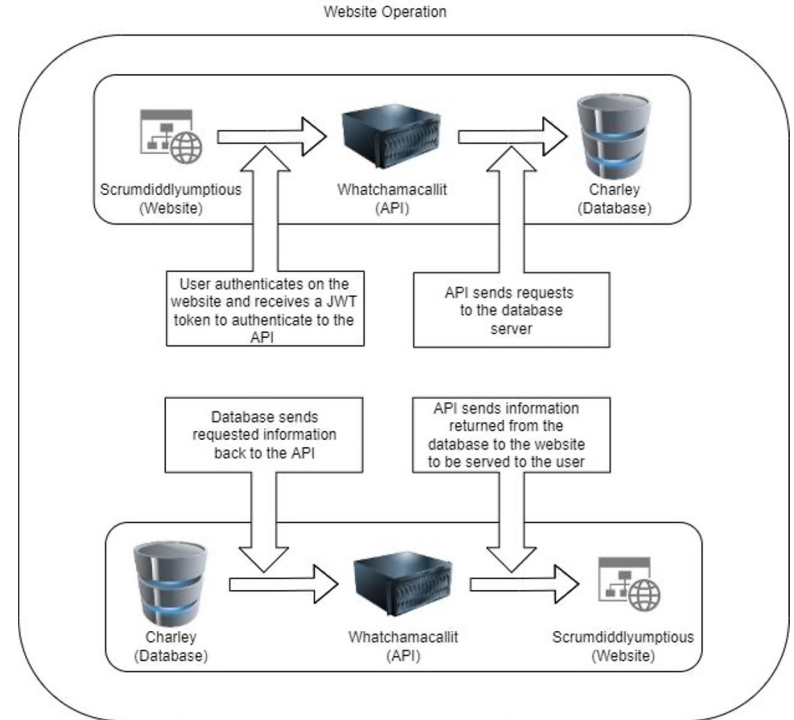


Figure 2: Website Operation



# Summary of Engagement



Number of Findings by severity

Critical	High	Medium	Low	Informational
2	3	3	3	3



# Key Strengths



## Usage of input sanitization on APIs



The implementation of sanitization on API endpoints prevents injection attacks. This was observed during an in-depth testing of the FastAPI server located on 10.0.17.11.



## Up to date software



Much of the software on the Le BonBon Croissant warehouse network was running the latest version available. This helps prevent the exploitation of known vulnerabilities that have patches available.



## Usage of HTTPS on API endpoints



The usage of HTTPS on all API endpoints ensures the identity of the server and maintains secure connections.

# Key Findings

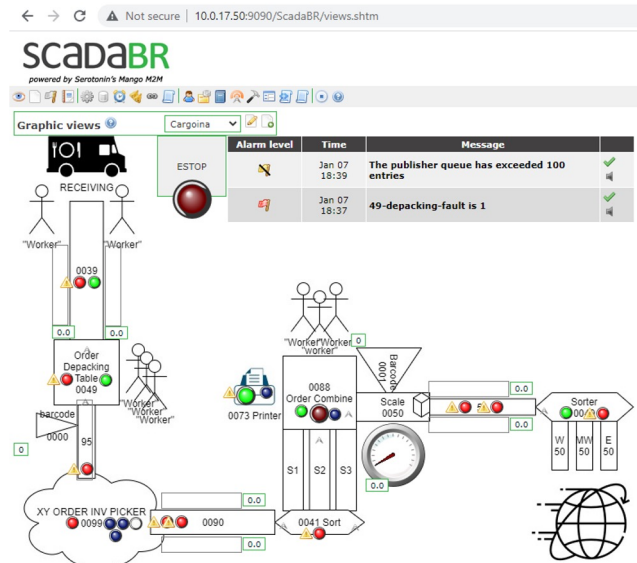


## ScadaBR Authenticated File Upload



ScadaBR located at

'<http://10.0.17.50:9090/ScadaBR/>' is a web-management software that is used to manage Le BonBon Croissant's Programmable Logic Controllers (PLC). These devices measure and control physical machinery in the warehouse. The current version of ScadaBR allows for file upload and remote code execution.





# Key Findings



## PostgreSQL - Default Credentials



- The PostgreSQL database is currently using a default configuration which allows for remote access to the administrative user of the database with no password.

```
COPY billing.credit_cards (id, name, number, expiration, ccv, zip) FROM stdin;
```

```
1 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
2 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
3 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
4 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
5 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
6 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
7 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
8 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
9 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
10 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
```



# Recommendations



## Network Segmentation



The implementation of network segmentation would separate systems that do not need to be connected.



## Authentication



Many API endpoints within the network utilized no authentication, which left the information that they provided accessible to anyone.



## Principle of Least Privilege (PoLP)



Authentication mechanisms should allow only functionality that is required of the user. This can help prevent insider attacks



# Business Impact



Damaged reputation due to unsecure PII and payment information



Non-compliance with Payment Card Industry Data Security Standards (PCI-DSS) can result in fines ranging from \$5,000 to \$100,000 per month



Negative customer experiences caused by website instability may result in decreased revenue



# Questions?