A picture containing polygon

Description automatically generated

THE COZY CROISSANT

Security Assessment Findings Report

Business Confidential

Date: November 18, 2022

Project: TCC22

Version 1.0

Table of Contents

[**Confidentiality Statement**](#_heading=h.gjdgxs) **3**

[**Disclaimer**](#_heading=h.30j0zll) **3**

[**Executive Summary**](#_heading=h.35nkun2) **5**

[**Assessment Overview**](#_heading=h.cy0grwmsp8jy) **5**

[**Assessment Components**](#_heading=h.2et92p0) **5**

[Internal Penetration Test](#_heading=h.tyjcwt) 5

[**Compliance Summary**](#_heading=h.3dy6vkm) **6**

[Payment Card Industry (PCI) Data Security Standards (DSS)](#_heading=h.4h766rtvxtpg) 6

[NIST SP 1800-27B](#_heading=h.ghqzp8r1jdeu) 8

[**Finding Severity Ratings**](#_heading=h.ky3yw1pcvygz) **8**

[**Risk Factors**](#_heading=h.1t3h5sf) **9**

[Likelihood](#_heading=h.4d34og8) 9

[Impact](#_heading=h.17dp8vu) 9

[**Scope**](#_heading=h.3rdcrjn) **9**

[Scope Exclusions](#_heading=h.26in1rg) 9

[Client Allowances](#_heading=h.lnxbz9) 10

[**Vulnerability Report Card**](#_heading=h.gbpt2wt26w60) **10**

[**Vulnerability Summary**](#_heading=h.44sinio) **10**

[**Technical Findings**](#_heading=h.2jxsxqh) **11**

[Finding TCC001: [CVE -] Vulnerability Name](#_heading=h.z337ya) 11

[**Appendix A: Network Diagram**](#_heading=h.ujp53937wkd8) **13**

[**Appendix B: Methodologies**](#_heading=h.3fbt71l3ksex) **14**

[**Appendix C: Attack Paths**](#_heading=h.kcoh3crtzwuq) **15**

[**Appendix D: Technical Findings Legend**](#_heading=h.e5veagrke1ww) **16**

# Confidentiality Statement

This document is the property of The Cozy Croissant and Finals-10. This document contains sensitive information including proprietary and confidential information. This document shall not be distributed outside of The Cozy Croissant or the Finals-10 without the express consent of both parties involved.

# Disclaimer

This document contains information regarding the overall network and system security of the Cozy Croissant. While Finals-10 maintains the highest standards of quality in their work, this document should not be construed as an exhaustive list of all possible vulnerabilities. We have intentionally focused on the areas with the highest risk and greatest vulnerability to attack to maximize the value of our services.

Due to the changing nature of the computer systems and networks, security vulnerabilities and risks will change over time; Finals-10 recommends annual testing to maintain a good security posture in response to evolving threats.

# 

# Executive Summary

Very brief summary covering the following information: whose security we were evaluating, the date(s) of the evaluation, and what is to follow in the coming sections. Do not need to summarize every section necessarily, just set the expectation of what follows.

# Assessment Overview

On November 19th, 2022, Finals-10 conducted a penetration test to evaluate the overall security posture of The Cozy Croissant. This test was conducted in accordance with industry standard best practices. The phases of the penetration test are as follows:

* Planning – Customer expectations and rules of engagement are obtained.
* Enumeration – Open-source intelligence, and scanning are done to identify common vulnerabilities and weak areas.
* Exploitation – Confirm vulnerabilities by successfully completing an exploit and then perform more discovery based on new information.
* Reporting – Record all vulnerabilities, findings, successful exploits, and organization strengths and weaknesses.









# Assessment Components

## Internal Penetration Test

The internal penetration test will simulate how an attacker would operate inside of the internal network. One member of the team will enumerate the network for vulnerabilities as well as carry out internal network attacks, such as: kerberoasting, token impersonation, pass-the-hash, golden ticket, web exploitations and more. The team member will gain access to hosts through these exploits. They will move through the network using lateral movement eventually attempting to gain access to the domain controller and domain admin accounts.

# Compliance Summary

## Payment Card Industry (PCI) Data Security Standards (DSS)

Due to the processing of customer payment information The Cozy Croissant must comply with PCI DSS. The PCI DSS are a set of global standards that are used to help protect cardholder data and ensure that companies that accept, process, store, or transmit credit card information are doing so in a secure environment. Failure to comply with PCI DSS can result in large fines, damage to reputation, and loss of customer data for the organization. By following this set of standards, The Cozy Croissant can both avoid these damages to the organization as well as increase security across the board.

Reference:

<https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf>

| PCI Objectives | PCI Requirements | Compliance Violations |
| --- | --- | --- |
| Build and maintain a secure network and systems. | 1. Install and maintain a firewall configuration to protect cardholder data. |  |
| 2. Do not use vendor-supplied defaults for system passwords and other security parameters. |  |
| Protect cardholder data. | 3. Protect stored data. |  |
| 4. Encrypt transmission of cardholder data across open, public networks. |  |
| Maintain a vulnerability management program. | 5. Use and regularly update anti-virus software. |  |
| 6. Develop and maintain secure systems and applications. |  |
| Implement strong access control measures. | 7. Restrict access to cardholder data by business need-to-know. |  |
| 8. Assign a unique ID to each person with computer access. |  |
| 9. Restrict physical access to cardholder data. |  |
| Regularly monitor and test networks. | 10. Track and monitor all access to network resources and cardholder data. |  |
| 11. Regularly test security systems and processes. |  |
| Maintain an information security policy. | 12. Maintain a policy that addresses information security for all personnel. |  |

## NIST SP 1800-27B

The ability to properly comply with governing standards like PCI DSS require strong frameworks set by established organizations. NIST or the National Institute of Standards and Technology is a non-regulatory federal agency that provides cybersecurity guidance. The NIST SP 1800 27B is a NIST special publication that outlines a cybersecurity framework specific to the hospitality industry. The use of this guide will provide The Cozy Croissant with a foundation for securing their infrastructure and complying with important standards such as PCI DSS.

Reference:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-27.pdf>

# Finding Severity Ratings

This section is used to define the severity ratings for any vulnerabilities and measure risk impact. The severity ratings will follow the corresponding CVSS score range.

| Severity | CVSS V3 Score Range | Definition |
| --- | --- | --- |
| Critical | 9.0 – 10.0 | Straightforward exploitation typically results in high level system access. Vulnerabilities of this category should be resolved immediately |
| High | 7.0 – 8.9 | Exploitation may involve more steps but could result in gaining elevated privileges and potentially significant downtime or data loss. Vulnerabilities of this category should be resolved as soon as possible. |
| Medium | 4.0 – 6.9 | Vulnerabilities are present but are not exploitable, involve many extra steps, and/or require social engineering. Vulnerabilities of this category should be resolved after high-priority issues are resolved. |
| Low | 0.1 – 3.9 | Vulnerabilities may be present but are not exploitable. Resolving these vulnerabilities would help to reduce the organization’s attack surface. Vulnerabilities of this category should be resolved during the next period of planned maintenance. |
| Informational | N/A | No vulnerability exists. This category is reserved for findings that do not directly relate to exploitation but may provide an attacker with information that would assist them in an attack. |

# Risk Factors

Risk is measured by two factors: Likelihood and Impact.

## Likelihood

Likelihood measures the probability of a vulnerability being exploited. Severity ratings are used for scoring based on how difficult the attack was, the tools available, skill level of the attacker, and the environment of the client.

## Impact

Impact measures the probability of the vulnerability having an effect on operations in the corporation. This includes the confidentiality, integrity, and availability of client-side systems and data, harm to software and/or hardware, and financial loss.

# Scope

| Assessment | Details |
| --- | --- |
| Corporate Network | 10.0.0.0/24 |
| Guest Network | 10.0.200.0/24 |

## Scope Exclusions

Anything else that is explicitly out of scope

The team will not conduct any testing on any externally facing systems or IP addresses. No disruptive or destructive testing will be allowed on any systems.

Testing will be limited to the assigned subnets; the VPN and Pentest box(es) are out of scope.

## Client Allowances

Anything else that the client gives us for access

The client will provide a Windows and Kali system for each tester; these will be used as an entry point to other systems.

# Reassessment Summary

During the team’s previous assessment, several vulnerabilities were found. These vulnerabilities have been reassessed to test any remediation attempted. This table shows a summary of the status of each previously discovered vulnerability.

| Vulnerability Name | Severity | Remediation Status |
| --- | --- | --- |
| Name of something or other | Critical | Remediated |
| YUHHHHHHHH | Medium | Not Remediated |

# Vulnerability Report Card

| Critical | High | Medium | Low | Informational |
| --- | --- | --- | --- | --- |
| 15 | 32 | 5 | 55 | 21 |

# Vulnerability Summary

| Severity | Vulnerability | Recommendation |
| --- | --- | --- |
| Critical | **TCC001:** XMLRPC Remote Code Execution | Update CMS to latest release |
| High | **TCC002**: Cross site scripting on forum page | Implement input sanitization against user-generated content |
| Medium | **TCC004:** XMLRPC Denial of Service | Update CMS to latest release |
| Low | **TCC006**: Clickjacking against user registration page | Add the ‘X-Frame-Options’ header to site requests and only allow page embeds from the same origin |
| Info | **TCC003**: Regex deficiency in sign up page – does not allow email addresses with capital letters | Review the email matching regex and ensure it includes capital letter matching |

# Technical Findings

## Finding TCC001: [CVE -] Vulnerability Name

| **Affected Hosts** | *<Targets/affected systems>* |
| --- | --- |
| **CVSS:**  *<score> | <rating>* | **Likelihood:**  *<Notes about the likelihood of exploitation, including the difficulty, credentials needed, etc..>*  **Technical Impact:**  *<Notes about the effect on TCC’s systems and infrastructure if this vulnerability is exploited, including access gained, or damage to systems done (****what*** *could be done)>* |
| **Vulnerability Description** | *<A description of how the vulnerability works and what it allows an attacker to do (****how*** *it could be done)>* |
| **Business Impact** | *<A description of the negative effects to TCC from a business standpoint>* |
| **Requirements to exploit** | *<A list of requirements that may include tools, credentials needed, internal access, etc.>* |
| **Remediation** | *<General steps to correct any deficiencies specific to this instance of the exploit (don’t do IT’s job for them though.)>* |
| **References** | *<Optional materials for additional reading>* |

Proof of Concept:

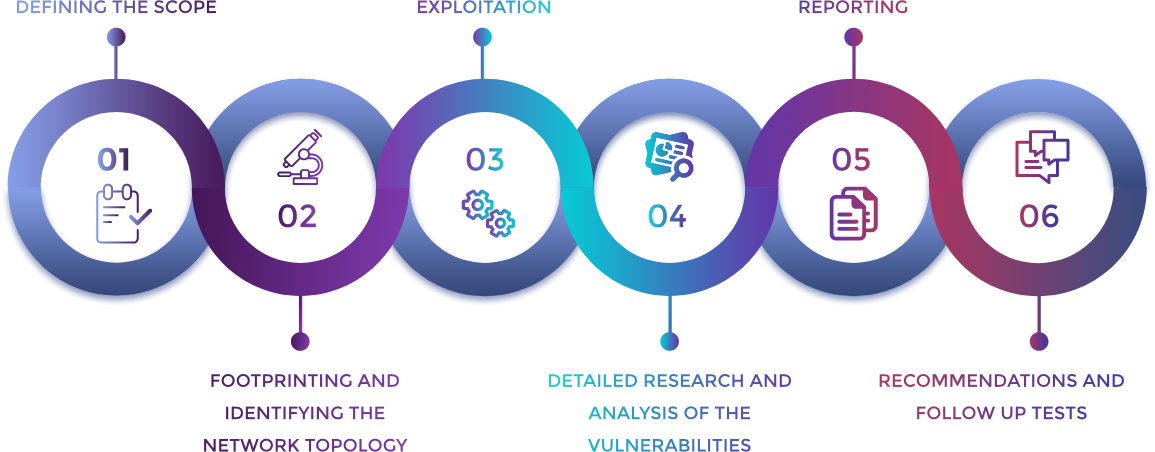
Text

Description automatically generated

# Appendix A: Network Diagram

# Appendix B: Methodologies

## Penetration Testing Phases



## OWASP Top 10

| OWASP Top 10 - 2022 | |
| --- | --- |
| 1. Broken Access Control | 2. Cryptographic Failures |
| 3. Injection | 4. Insecure Design |
| 5. Security Misconfiguration | 6. Vulnerable and Outdated Components |
| 7. Identification and Authentication Failures | 8. Software and Data Integrity Failures |
| 9. Security Logging and Monitoring Failures | 10. Server-Side Request Forgery (SSRF) |

# Appendix C: Attack Paths

# Appendix D: Technical Findings Legend

## Finding *TCC###: [CVE -] Vulnerability Name*

| **Affected Hosts** | *Targets/affected systems* |
| --- | --- |
| **CVSS:**  *score | rating* | **Likelihood:**  *Notes about the likelihood of exploitation, including the difficulty, credentials needed, etc.*  **Technical Impact:**  *Notes about the effect on TCC’s systems and infrastructure if this vulnerability is exploited, including access gained, or damage to systems done* |
| **Vulnerability Description** | *A description of how the vulnerability works and what it allows an attacker to do* |
| **Business Impact** | *A description of the negative effects to TCC from a business standpoint* |
| **Requirements to Exploit** | *A list of requirements that may include tools, credentials needed, internal access, etc.* |
| **Remediation** | *General steps to correct any deficiencies specific to this instance of the exploit* |
| **References** | *Optional materials for additional reading* |

A picture containing polygon

Description automatically generated

**Last Page**