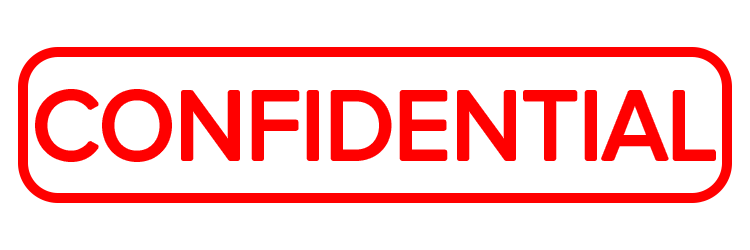
  
The Cozy Croissant (TCC) Penetration Test Report

Prepared by:  
TEAM-IDENTIFIER  
DAY MONTH, YEAR  


# Confidentiality

This document and all the information contained within are confidential and proprietary to TEAM-IDENTIFIER and The Cozy Croissant. Utmost care should be exercised when handling, referring to, or copying this document. TEAM-IDENTIFIER authorizes The Cozy Croissant to view and communicate this document as they see fit in accordance with The Cozy Croissant’s data handling policies.

# Legal Disclaimer

No warranties are provided by TEAM-IDENTIFIER for this penetration test report with respect to the accuracy, reliability, or correctness of the information in this document. This report is delivered “as is” with findings and recommendations reflecting only the information obtained during the assessment. TEAM-IDENTIFIER does not assume liability from any damages, indirectly or directly, related to the reliance of information provided in this report, and it is highly recommended to thoroughly evaluate the business impact of changes before the implementation of them.

# Table of Contents

[**Confidentiality**](#_1qiqsh7lpvnw) **1**

[**Legal Disclaimer**](#_ygqp24wrm4s6) **1**

[**Table of Contents**](#_1kcot8g0rs81) **2**

[**Executive Summary**](#_h1zkjlt68k1r) **4**

[Synopsis](#_8mg6ucwim7mt) 4

[Findings Overview](#_x3cc0idhnsh2) 4

[Strategic Recommendations](#_3h6x36s7qyxz) 4

[**Overall Risks**](#_p34zenyobm78) **5**

[**Strategic Remediations**](#_q70tfnd2lpk6) **6**

[Security Strengths](#_qieu94glpslk) 6

[Areas For Improvement](#_rg43ve2asfag) 6

[**Governance and Regulatory Compliance**](#_snltuabjttll) **7**

[Payment Card Industry Data Security Standard (PCI DSS)](#_scfq3pkovdel) 7

[Nevada Revised Statutes Chapter 603A (NRS 603A)](#_v0n8e3q5vmph) 7

[**Scope**](#_hm1ur2kazely) **8**

[Authorized Assets](#_iy2s1qcwlccq) 8

[Approach](#_t9aw3o3ch2i3) 8

[Timeframe](#_ot7qiez1vktd) 8

[Network Topology](#_kucd63uftx06) 9

[**Testing Methodology**](#_n0qkwr8x5dhk) **10**

[**Assessment Findings**](#_lp4hvt2a09x2) **11**

[Classifications](#_c2226msygc1c) 11

[Findings Summary](#_mrk4eo983nqf) 12

[Critical Risk Findings](#_95ii8bz1c6gc) 13

[High Risk Findings](#_xh2rwxwq5su1) 13

[Moderate Risk Findings](#_fqymnmq40b4r) 13

[Low Risk Findings](#_ur7pe4oxj83e) 13

[Informational Findings](#_mrotplayzx9h) 13

[**Comparison to Previous Engagement**](#_65atxtzghtfc) **14**

[**Conclusion**](#_je94cdjfe2e0) **15**

[**Appendix A: Tools Used**](#_jd36zqplxwa0) **16**

[**Appendix B: Network Reconnaissance**](#_yppgldqj60o3) **17**

# Executive Summary

## Synopsis

TEAM-IDENTIFIER was contracted by The Cozy Croissant (hereafter referred to as TCC) to conduct a penetration test on their network. The penetration test simulated an attack starting within TCC’s network system with [INSERT-DATA]. The purpose of the penetration test was to discover vulnerabilities and suggest recommendations. In total, TEAM-IDENTIFIER found [INSERT-DATA] vulnerabilities during the assessment. It is recommended that TCC takes the provided Strategic Recommendations (detailed below) to resolve these vulnerabilities immediately. If these vulnerabilities are not resolved TCC could face fines up to an estimated amount of $[INSERT-DATA] or <list major vuln then legal, financial, etc consequences in detail along with likelihood>.

## Findings Overview

| **Critical** | **High** | **Moderate** | **Low** | **Informational** |
| --- | --- | --- | --- | --- |
| [INSERT-DATA] | [INSERT-DATA] | [INSERT-DATA] | [INSERT-DATA] | [INSERT-DATA] |

List top 3 findings w/ brief high-level explanation w/ risks

## Strategic Recommendations

List overarching strategic recommendations w/ emphasis on costs (most will be free)

# Overall Risks

Upon conclusion of TEAM-IDENTIFIER’s assessment of TCC’s network, numerous findings were discovered that could result in possible legal issues and drastic adverse effects to business operations.

* Discuss 2-3 significant findings
* Discuss general topics of other findings
* Include estimates for financial & legal implications

Due to the large risk of legal issues, business functionality, and overall reputation, it is imperative that the proper remediation techniques are implemented in order to create a more secure digital environment for TCC and its customers for the future.

# Strategic Remediations

## Security Strengths

Throughout the assessment, TEAM-IDENTIFIER identified several security controls implemented by TCC, especially after re-testing. TEAM-IDENTIFIER recommends TCC to continue maintaining and integrating these controls to improve its overall security posture.

* STRENGTH #1
* STRENGTH #2

## Areas For Improvement

TEAM-IDENTIFIER identified several areas where TCC should improve throughout the current assessment and future assessments. These findings were critical in their impact of the attacks conducted in this assessment. The most significant findings shown below.

* WEAKNESS #1
* WEAKNESS #2

# Governance and Regulatory Compliance

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

Because TCC processes customer credit card data in the normal operations of their business TCC must follow the PCI DSS standard in order to provide a safe and secure environment for customers to utilize their credit and debit cards. As the Cardholder Data Environment (CDE) encompasses networked systems that process, store, and/or transmit cardholder data, as well as any additional components that may directly interact with these systems, TEAM-IDENTIFIER has taken any potential findings that may impact the CDE into consideration when classifying them.

## Nevada Revised Statutes Chapter 603A (NRS 603A)

As TCC is located in Reno, Nevada, it is under the jurisdiction of Nevada state law which includes NRS 603A. This law requires any entity that collects personal data to notify Nevada residents whose personal information has been accessed by an unauthorized person in the event of a data breach as well as to maintain reasonable security measures. In regards to the penetration test, TEAM-IDENTIFIER took this legal requirement into consideration for classifying potential findings due to the financial and legal implications of a data breach on applicable systems.

# Scope

## Authorized Assets

TEAM-IDENTIFIER was authorized by TCC to assess the following assets during the requested penetration test:

* [INSERT-DATA]
* [INSERT-DATA]
* [INSERT-DATA]

## Approach

TEAM-IDENTIFIER’s penetration test was performed with initial internal network access from provided [INSERT-DATA] virtual machines under a “gray-box” penetration testing approach where penetration testers had limited knowledge of network assets from the initial RFP posted from TCC, the network scope provided, and additional information supplied from TCC throughout the penetration testing period.

## Timeframe

TEAM-IDENTIFIER was allotted [INSERT-DATA] hours on [INSERT-DATA] to perform a penetration test on the specified scope with an additional [INSERT-DATA] hours to create a report on said penetration test.

## 

## Network Topology

## 

# Testing Methodology

For the assessment of TCC’s internal network, TEAM-IDENTIFIER utilized the Penetration Testing Execution Standard (PTES) due to its coherency and extensive coverage of all stages encountered throughout an internal penetration test. The PTES methodology separates each penetration test into 7 uniques phases:

**1. Pre-Engagement Interactions:** The first step of the methodology involves all communication relating to the objectives and goals of the client, as well as finalizing all matters related to the scope and details of the assessment.

**2. Intelligence Gathering:** Once pre-engagement interactions have concluded, the next phase of the methodology consists of the collection of all publicly available information on the target, commonly referred to as open-source intelligence (OSINT), in order to identify any potential attack vectors and vulnerabilities.

**3. Threat Modeling:** The primary goal of this stage is identifying and categorizing a business’s critical assets, mapping each asset to all possible and probable attack vectors that may be encountered during the assessment, as well as identifying and modeling the appropriate threat actors based on the nature of the assets.

**4. Vulnerability Analysis:** Next, the methodology then calls for an in-depth analysis of the client’s network with the goal of identifying and taking note of any security vulnerabilities for use in the subsequent phases.

**5. Exploitation:** This stage involves revisiting all vulnerabilities gathered during the previous phases of the methodology, with the primary goal of exploiting these targets and gaining access to the client’s assets.

**6. Post-Exploitation:** Upon gaining access, the next step is evaluating the importance of the compromised asset and the risk that it poses, as well as searching for additional vulnerabilities such as privilege escalation or moving laterally within the client’s network.

**7. Reporting:** The final step of this methodology involves gathering all findings from the previous phases and generating a professional report for the client. The main purpose of the report is to convey all findings from the penetration test, as well as remediation techniques so that security is hardened as a result of the assessment.

# Assessment Findings

## Classifications

TEAM-IDENTIFIER utilized a two-dimensional matrix, see below, consisting of the business impact and CVSS score of each finding to categorize it within one of five overall security risk categories: critical, high, medium, low, and informational. These categories were organized to prioritize the remediation of findings that would cause TCC financial loss, non-compliance with governance requirements, and reputational impact.

|  | **Business Impact** | | | | |
| --- | --- | --- | --- | --- | --- |
| **CVSS Score** | Insignificant (a) | Low (b) | Moderate (c) | High (d) | Critical (e) |
| Critical (5) | 5a | 5b | 5c | 5d | 5e |
| High (4) | 4a | 4b | 4c | 4d | 4e |
| Medium (3) | 3a | 3b | 3c | 3d | 3e |
| Low (2) | 2a | 2b | 2c | 2d | 2e |
| None (1) | 1a | 1b | 1c | 1d | 1e |

**Overall Risk = Business Impact x CVSS**

**Business Impact**

The business impact score on TCC’s assets and operations is based on the potential for a finding to interrupt or impact TCC’s ability to conduct business, protect customer information, or stay in compliance with government regulations and business standards. As TEAM-IDENTIFIER is operating under limited knowledge of the business operations of TCC, we would recommend TCC to recategorize these findings to provide a better understanding of the overall risk of these findings.

**CVSS Score**

The Common Vulnerability Scoring System v3.1 (CVSS)[[1]](#footnote-0) standard was used to measure the severity and attack complexity of each finding. This metric is a commonly utilized open industry standard used to assess security vulnerabilities both quantitatively and qualitatively.

## Findings Summary

| **Critical Risk Findings** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Unique ID** | **Vulnerability Name** | | | **CVSS Score** | **Page Number** |
|  |  | | |  |  |

| **High Risk Findings** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Unique ID** | **Vulnerability Name** | | | **CVSS Score** | **Page Number** |
|  |  | | |  |  |

| **Moderate Risk Findings** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Unique ID** | **Vulnerability Name** | | | **CVSS Score** | **Page Number** |
|  |  | | |  |  |

| **Low Risk Findings** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Unique ID** | **Vulnerability Name** | | | **CVSS Score** | **Page Number** |
|  |  | | |  |  |

| **Informational Findings** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Unique ID** | **Vulnerability Name** | | | **CVSS Score** | **Page Number** |
|  |  | | |  |  |

## Critical Risk Findings

## High Risk Findings

## Moderate Risk Findings

## Low Risk Findings

## Informational Findings

# Comparison to Previous Engagement

* Summarize how many findings were addressed compared to the previous engagement
* Create a table to visualize how many findings were fixed

# Conclusion

* Thank TCC for the opportunity to perform the penetration test
* Give a summary/focus on general areas to resolve based on strategic recommendations

# Appendix A: Tools Used

# Appendix B: Network Reconnaissance

* Create a table for each subnet in scope to include the following for each IP address:
  + Hostname
  + Role
  + Key services/ports

1. <https://www.first.org/cvss/specification-document> [↑](#footnote-ref-0)