Penetration Test Report

The Cozy Croissant

January 14, 2023

[redacted]

Notice of Confidentiality: This document and the contents thereof are provided in strict confidence for the sole usage of The Cozy Croissant. As the contents of the document contain strictly confidential and privileged information regarding the infrastructure of The Cozy Croissant, the document may not be disclosed or redistributed without the sole consent of The Cozy Croissant, as such actions may expose sensitive information regarding the company and put them at risk.

Disclaimer of Warranty and Limitation of Liability: If further professional assistance is required outside the responsibilities of penetration testing, the services of a competent professional person should be sought. Neither the publisher nor the authors shall be liable for damages arising therefrom. The referencing of any external sources or works as a citation or a potential source of further information does not imply the endorsement of the publisher and authors. Further, readers should be aware that standards and practices constantly change within the field of cybersecurity, and that the information in this document is only deemed accurate up to the time the work was written.

Warning: The contents of this report are to be provided to The Cozy Croissant in a format that is not easily modifiable. The customer should not attempt to omit any findings within this report and should take full responsibility in remediating or mitigating any findings herein. The resolution of any of these findings should only be documented once the finding has been remediated and has been validated by another professional competent in the field of cybersecurity, which may be the same as the publishers of this document.

Table of Contents

Executive Summary 05
- Purpose and Scope of Evaluation 05

Introduction 06
- Purpose 06
- Scope 06
- Host Discovery 07
- Assessment Methodology 08
- Severity and Risk Level Definitions 08
- Key Findings 10
- Potential Risk 11
- Final Points 11
- Compliances 11

Technical Findings 13
- Overview 13
- Critical Severity Findings 14
  - Jellyfin Default Admin Access 14
  - Reward System User Broken Access Control 17
  - Reward System Weak Admin Password 20
  - Reward System Admin API Unauthorized Access 22
  - SMB Users Using No Password 24
- High Severity Findings 26
  - WordPress Weak Admin Password 26
  - Invoice System User Broken Access Control 28
- Medium Severity Findings 31
  - Invoice System PostgreSQL Injection 31
  - CVE-2022-3590 33
  - CVE-2021-21311 34
  - Reward System Guest No Password 36
  - Reward System Weak Customer Password 38
- Informational Findings 40
  - Payment API Documentation 40
  - SMB Signing Not Required 42
  - Publicly Exposed Organization Chart 44
  - Outdated WordPress 47
  - Cleartext Windows Password Policies 49
  - Windows Defender Turned Off 51
  - Insecure Safe Model 53

Conclusion **54**
Principal Strengths in Security 54
Principal Trends in Vulnerabilities 54
Resultant Compliance to PCI DSS 55
Resultant Risk Analysis 56
Recommended Improvements 57
Final Notes 58

Appendix **60**
Appendix A: Network Diagram 60
Appendix B: Kill Chain Audit 63
Appendix C: OSINT Discovery 64
Appendix D: Offensive Tools 64
Appendix E: Additional References for Further Improvement 64

Executive Summary

Purpose and Scope of Evaluation: [redacted] was contracted by The Cozy Croissant (TCC) to perform a security assessment on the company's infrastructure, specifically the corporate and guest network infrastructure on January 13th and 14th, 2023.

For this security assessment, [redacted] conducted a penetration test to assess the risk of external/internal security vulnerabilities towards TCC's network resources and services. This test was executed within the scope of two subnets: 10.0.0.0/24, and 10.0.200.0/24.

The objectives of this test include the following:

1. Identify publicly accessible ports and services that have known information-security vulnerabilities and exposures, which can be exploited by threat actors.
2. Discover vulnerabilities within TCC's systems that can provide unauthorized access to sensitive information of the network infrastructure, and assets, or even disrupt daily operations.
3. Compliance with the Payment Card Industry Data Security Standards (PCI DSS) and other related security regulations.

[redacted]s assessment identified a total of **19** vulnerabilities, which consisted of **5** critically severe vulnerabilities, that can be classified by severity in the table below:

Severity Rating	Critical	High	Medium	Low	Informational
Vulnerabilities	5	2	5	0	7

During the assessment, several internal and external vulnerabilities were found within TCC's infrastructure that posed a significant business risk in terms of monetary impact, legal implications, and customer trust. Critical vulnerabilities found within the environment that should be remediated immediately are **Jellyfin Default Admin Access**, **Reward User System Broken Access Control**, **Reward System Weak Admin Password, Unauthorized Reward API Admin Access**, and **SMB Users Using No Password**.

These vulnerabilities are not compliant with PCI DSS and will result in fines that range from $5,000 to $100,000 per month. Additional costs could include credit monitoring fees, lawsuits, and actions by state and federal governments until compliance is met.

[redacted] recommends TCC remediate these findings by **restricting and limiting access to the Jellyfin profile to the proper users, hiding and modifying the rewards source code, enforcing complex password policies, ensuring that each admin has a unique secret key,** and **setting complex passwords for all SMB accounts and also disabling unused accounts**. The Cozy Croissant must take into account

compliance standards when setting policies to ensure that they are compliant with industry standards. Failure to mitigate these risks will leave TCC vulnerable to potential future breaches from malicious actors that can affect TCC's operations and reputation in the hospitality industry.

Introduction

Purpose

[redacted] was contracted by TCC to perform a limited-scope penetration test on its network on January 13th and 14th. The purpose of the penetration test is to detect vulnerabilities lying within TCC's enterprise network, such that TCC is aware of the issues and is able to take the appropriate steps toward remediating or mitigating the vulnerabilities found in the network. This report not only documents findings in the network, but also outlines remediation recommendations and a high-level recommended response plan.

As a part of the hospitality sector, TCC must conform to standards such as the Payment Card Industry (PCI) Data Security Standard (hereafter referred to as PCI DSS or simply PCI) as there are customer transactions involved within the business. The security assessment performed by [redacted] on TCC's networks takes into account the company's compliance with these PCI DSS standards along with violations, which have also been documented throughout the report.

Scope

The penetration test was of limited scope, only assessing two subnetworks representative of TCC's corporate branch network and the guest network. These subnetworks are addressed by two IPv4 CIDR blocks: 10.0.0.0/24, and 10.0.200.0/24, respectively. Within these subnets, the security engineers evaluated the security of endpoint devices as well as the services hosted thereon, such as web services and databases. Although the scope mainly consisted of finding vulnerabilities that can be exploited by external threats, [redacted]s team also considered internal threats as well.

[redacted]s penetration testers remained within the defined scope of the penetration test and ensured that actions taken during the evaluation did not interfere with the company's operations, as the tests took place during the company's operating hours. The team also took precautions to avoid exposing the company to additional risks. Any sensitive information gathered is also held in strict confidence and has been redacted from the report or graphics herein to prevent any potential leaks.

Host Discovery

In order to seek and maintain an updated list of in-scope targets, [redacted] developed a topology on the TCC network. The graphical topology relies on the Nmap scans for an accurate depiction. During the reconnaissance phase, [redacted] was able to identify various systems and interfaces within the company's two subnets, which were the corporate network (10.0.0.0/24) and the guest subnet (10.0.200.0/24). In its corporate network, multiple databases, admin APIs, customer portals, and servers were identified. In the guest subnet, there were several windows workstations. On the other hand, the guest network contained four systems that were used mainly for hosting public-facing information.

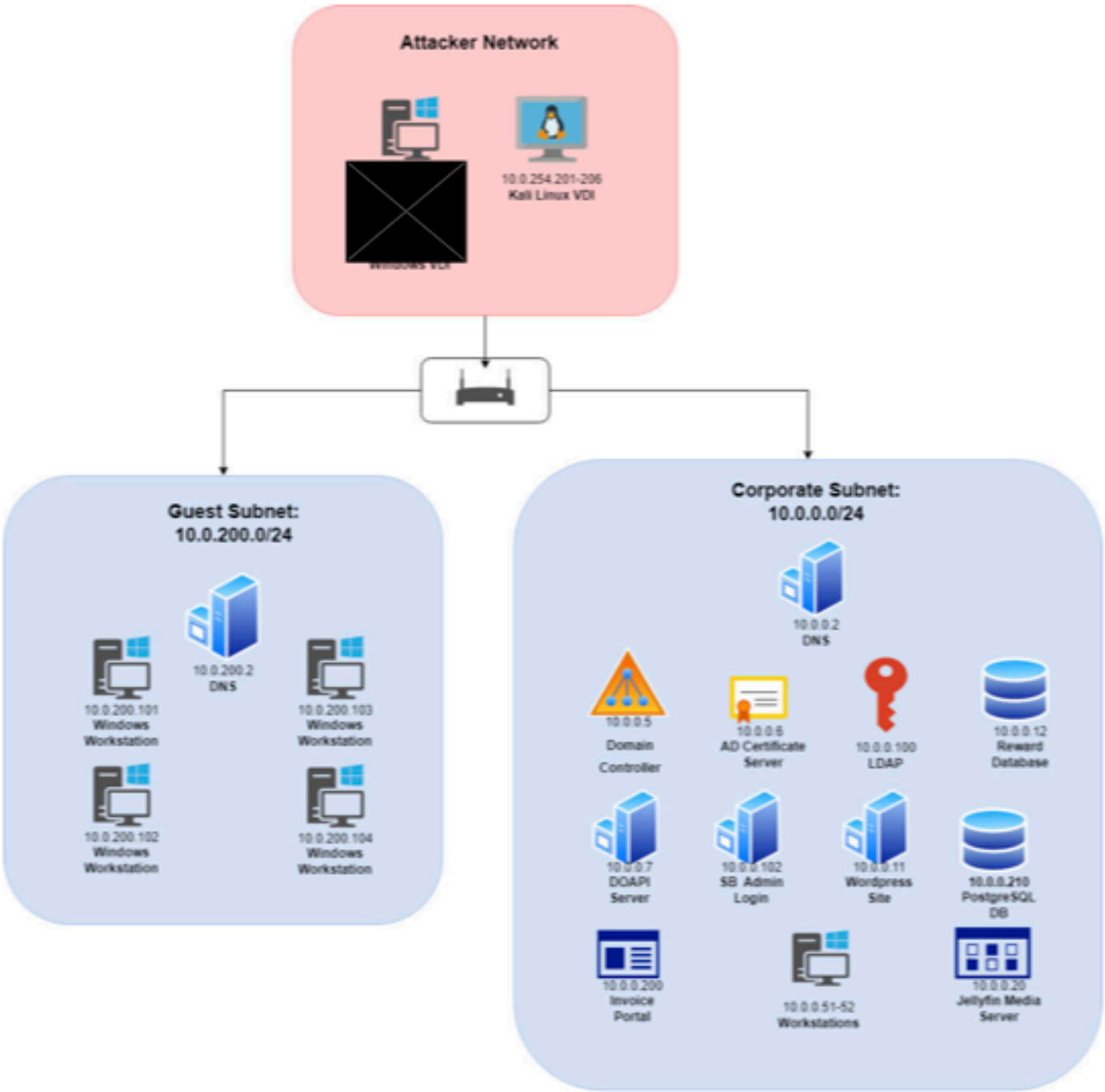


Figure 1.0: TCC Network Topology

Assessment Methodology

In the reconnaissance phase, [redacted]s penetration testers ran a moderate scan of the network in scope. This allowed the testers to find attack vectors such as open ports and provide useful information such as the operating system of the machines and the services they provide. After a moderate scan, the penetration testers then ran a full port scan to discover potential uncommon attack vectors.

Next, [redacted] was asked to conduct a social engineering assessment by joining in a call to gather Personally Identifiable Information (PII) from the TCC staff. The team created a scenario and wrote a script that was used during the call. Our team spoofed a phone number when calling the front desk and questioned the receptionist to collect PII by using previously collected information from the invoice website (10.0.0.200/admin/reservations) to gain the trust of the receptionist. During the call, a team member impersonated an employee from the finance department, emulating a situation where a customer was suspected of fraud based on suspicious credit card activity. The front desk receptionist was pressured by the impersonator using the punishment of authorities and the threat of superiors. The employee revealed the customer's PII, such as credit card information, home address, name, and phone number, under the deception that further verification was needed to protect the safety of the customer and the company.

[redacted]s penetration testers tested any web applications hosted on the client's servers. This assessment ranged from web fuzzing to analyzing HTTP requests and responses. The testers are able to exploit the API and discover sensitive customer information. Following the discovery of sensitive credentials such as usernames and passwords, the penetration testers reused some credentials on any application or service that required authentication. After gaining access to the server shells and establishing Windows RDP sessions, the testers checked for misconfigurations, outdated software, and exposed sensitive information. During this process, the testers took extreme caution to not modify the credentials of existing users on the system, so as not to affect TCC's employees and customers.

Severity and Risk Level Definitions

Within the report, two main measures are used to evaluate the urgency of a vulnerability. The primary measure used is the severity level, which is scored using the Common Vulnerability Scoring System v3.1 (CVSS). The secondary measure used is the risk level, using a risk matrix scoring system.

Though similar, it is important to note that severity and risk are not equivalent. Risk level measures are affected by the likelihood of a vulnerability more than severity levels are. This may lead to negligence of critical severity vulnerabilities of low likelihood. As part of the region's critical infrastructure, the range of potential threat actors anticipated by TCC is not limited to unsophisticated, low-level criminals, but also includes sophisticated, high-caliber, and well-funded threats. Such a threat actor is not limited by low likelihood, as they will search extensively for any vulnerabilities that may compromise the company's systems. Thus, TCC can not afford to ignore any high-impact vulnerability merely because of its lower likelihood.

For this reason, [redacted] has decided to use severity levels as the primary measure to mitigate this issue. Severity levels still take likelihood into consideration in the form of "exploitability", but with reduced effects. However, risk levels are still provided in the report regardless, to give risk analysts and management an alternative measure for evaluating a vulnerability.

Severity Level Measures: To measure severity, the CVSS v3.1 standard is used. The Common Vulnerability Scoring System is an open industry standard for assessing the severity of a computer system security vulnerability. The basic score is used as a simple quantitative measure in collaboration with the score-to-rating chart in Fig 2.0A to provide a qualitative measure of the severity. The base vector string is also shown to give a better technical description of the vulnerability. The breakdown of the vector string is shown in Fig 2.0B.

A.) CVSS v3.1 Score-Rating Table

Severity Rating	Base Score
Critical	9.0-10.0
High	7.0-8.9
Medium	4.0-6.9
Low	0.1-3.9
Informational	0

B.) CVSS v3.1 Base Vector String Breakdown

Exploitability	Scope (S)
Attack Vector (AV)	Unchanged (**U**), Changed (**C**)
Network (**N**), Adjacent (**A**), Local (**L**)	**Impact**
Attack Complexity (AC)	Confidentiality (C)
Low (**L**), High (**H**)	None (**N**), Low (**L**), High (**H**)
Privileged Required (PR)	Integrity (I)
None (**N**), Low (**L**), High (**H**)	None (**N**), Low (**L**), High (**H**)
User Interaction (UI)	Availability (A)
None (**N**), Required (**R**)	None (**N**), Low (**L**), High (**H**)

Fig 2.0 A legend for the usage of CVSS 3.1 metrics. (A) shows the qualitative severity ratings w/ the corresponding color depending on the base score. (B) shows the breakdown of the CVSS Base Vector String. The vector string will compose of the field abbreviation (AV for Attack Vector) followed by a colon and the attribute abbreviated (N for Network). Each field is separated by forward slashes.

Risk Level Measures:
To measure risk levels, a simplistic risk matrix is outlined in Fig 2.3A. The risk matrix will take into account the impact of the vulnerability, along with the probability that it will occur. A base impact score is obtained using the impact subscore provided by the CVSS calculator, along with a base probability using the CVSS exploitability subscore. The two scores are then adjusted by [redacted]s security engineers using their own technical knowledge and contextual judgement. The risk score is then obtained by mapping the adjusted impact score and probability to a risk rating using the Probability v Impact Risk Matrix in Fig 2.3A. Finally, all quantitative scores are converted to qualitative ratings using a score-to-rating scale as described in Fig 2.3B.

A.) Probability v Impact, Risk Matrix

Probability	Risk Level				
Very High	Medium	Medium	High	Very High	Very High
High	Low	Medium	High	High	Very High
Medium	Low	Low	Medium	High	High
Low	Very	Low	Mediu	Mediu	High

	Low		m	m	
Very Low	Very Low	Very Low	Low	Mediu m	Mediu m
Impact	Very Low	Low	Mediu m	High	Very High

B.) Score-to-Rating Chart

Rating	Probability	Impact
Very High	0.9 - 1.00	0.90 - 1.00
High	0.7 - 0.89	0.75 - 0.89
Medium	0.5 - 0.69	0.60 - 0.74
Low	0.3 - 0.49	0.25 - 0.59
Very Low	0.0 - 0.29	0.00 - 0.24

Fig 2.1 A legend for the scoring of risk level, probability, and impact. (A) shows the risk matrix for obtaining the qualitative risk level using the qualitative measures of probability and impact. (B) shows the corresponding rating which describes each range of probability, impact, and risk.

It is important to note that the aforementioned scoring process is done throughout the report using the technical knowledge and professional experience of [redacted]s security engineers. These scores do not reflect the official values found in the National Vulnerability Database (NVD) and should not be treated as such.

Key Findings

The 19 vulnerabilities found in TCC's network infrastructure fall under four groups of security trends that are commonplace in many networks. These four groups are weaknesses (1) Authentication, (2) Authorization, (3) Input / Output Sanitization, and (4) General Misconfigurations.

Authentication:

The PostgreSQL account that manages the billing information cannot be brute-forced. Additionally, [redacted] was unable to find valid credentials through brute forcing SSH. The password policy implemented could be a baseline for securing passwords for user accounts.

Our team found multiple accounts that either had weak passwords or default credentials. Upon gaining access to the vulnerable accounts, customer passwords were not encrypted and left in plaintext. There were more than one instance where critical admin accounts were left with weak password policies leaking customer information and giving black hat hackers the ability to shut off the service.

Authorization:

The WordPress site has a proper authorization setup. There is only a single admin managing the WordPress site.

It is crucial to ensure that only those who are properly authorized would have access to certain services. In many cases, TCC's various hosts seemed to have poor if not any authorization. A lot of accounts were given unauthorized privileges due to password policies.

Input / Output Sanitization:
The input query for Reward System is sanitized and the input validation system has been drastically improved since our last engagement. [redacted] attempted to inject different services and barely succeeded once in comparison to our attempts in the previous engagement.

Lack of input sanitization in HTTP requests and inputs in applications leaves the network vulnerable to remote code execution in the form of SQL injections and server-side request forgeries (SSRF). Our security engineers were able to use and exploit systems that were not sanitizing input, specifically in WordPress systems.

General Misconfigurations:
[redacted] was pleased to see improvements made to the general configurations of the systems. A lot of software and services have been patched since our last engagement and more security measures have been implemented. One particular improvement worth noting is that the invoices would expire upon inactivity or time limit.

It is important to make sure that users are configured appropriately when creating accounts. Our security engineers found vulnerabilities where customers would be given administrative access upon creating an account. Our security engineers also discovered a group of users that are given admin privileges. It is crucial that TCC follows the principle of least privilege and ensures that all users are configured properly. General account misconfigurations can allow newly created customers to wreak havoc with elevated privileges.

Potential Risk

Collectively, the 20 identified vulnerabilities expose TCC to a significant degree of business risk. The potential for external fraud exists in the form of theft and hacking-related damages. Coupled with the possibilities of business disruption and system failures, these vulnerabilities pose a great operational risk to TCC. This compromises the company's ability to ensure confidentiality, integrity, and availability in its operations.

Furthermore, the legal risks engendered by violations of PCI DSS regulations constitute a liability to possible significant monetary penalties.

Considering the great business risk posed by the vulnerabilities found in the report, it is important that TCC shall take note of all technical findings and remediate the vulnerabilities reported. Taking heed to the technical findings as well as the recommended responses provided will allow the company to improve its security posture, able to guarantee the provision of its critical services to the region and the security of its assets. Failure to remediate the reported vulnerabilities may expose the company to great strategic risk as the technical debt accumulates.

Final Notes

Having shown great improvement in strengthening their infrastructure's cybersecurity consistent with the recommendations provided during the last assessment, it is evident that TCC is committed to providing hospitality to the region in a secure and reliable manner. [redacted] and its security engineers are proud to be able to offer their services to TCC and would be proud to further offer their services again to such a client that

takes security seriously. Should TCC require further evaluation of their network to improve their network security, [redacted] is ready to offer its services. The security engineers offer TCC their regards and the best of luck as the company moves forward in its mission.

Compliances

As a part of the region's hospitality service, TCC must comply with standards set by national organizations to ensure that the company will be able to withstand attacks set upon it in an attempt to disrupt the company's operation and protect customer information. Specifically, TCC must comply with the Payment Card Industry (PCI) Data Security Standard(PCI DSS) standards as a Payment Card provider.

As described earlier, the PCI DSS standards are a set of mandated standards that all Hotels in North America must follow as a part of the region's critical infrastructure. Violation of these standards holds a company liable to significant monetary penalties as an enforcement action. More information may be found on ***https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf***, under the "Detailed PCI DSS Requirements and Security Assessment Procedure" dropdown. Note that the only standards considered by [redacted] were those which are still subject to enforcement on January 14th, and those which could be tested within the time frame and the limited digital access provided. It is recommended the TCC also consider those which are subject to future enforcement although they were not included in [redacted]s analysis. The references for each section of the standard that [redacted] uses are as follows:

Title	Reference
PCI DSS	***https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf***

Req #	Requirements
2.2	System components are configured and managed securely.
3.6	Cryptographic keys used to protect stored account data are secured.
4.2	PAN is protected with strong cryptography during transmission.
5.3	Anti-malware mechanisms and processes are active, maintained, and monitored.
6.2	Bespoke and custom software are developed securely.
6.3	Security vulnerabilities are identified and addressed.
7.2	Access to system components and data is appropriately defined and assigned.
8.2	User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.
8.3	Strong authentication for users and administrators is established and managed.

8.5	Multi-factor authentication (MFA) systems are configured to prevent misuse.
8.6	Use of application and system accounts and associated authentication factors is strictly managed
9.1	Processes and mechanisms for restricting physical access to cardholder data are defined and understood
12.7	Personnel are screened to reduce risks from insider threats.

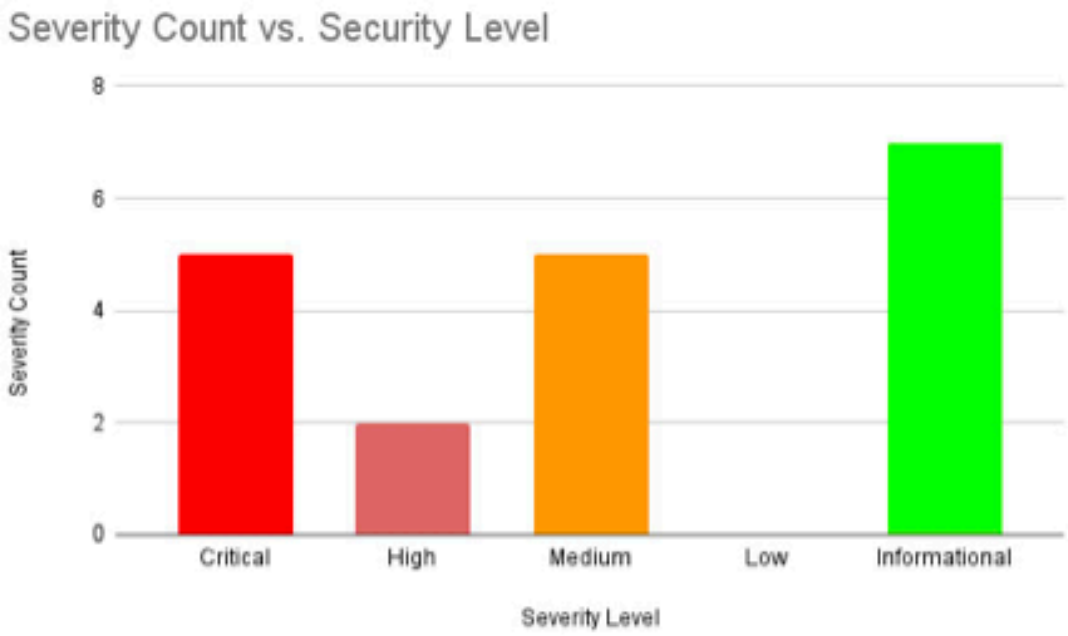
Technical Findings

The following section contains a listing of the main technical findings discovered throughout the security assessment. The section first starts with a summary of findings along with relevant info-graphics to accompany it. Afterward, all notable vulnerabilities are listed in the following subsections, sorted by severity levels as described and justified in the "Severity and Risk Level Definitions" segment above. Specifically, it lists critical severity findings, followed by high severity, medium severity, then low severity findings. Lastly, a listing of notable informational findings then follows the vulnerabilities to discuss any positive security findings or indeterminate findings that are worth mentioning.

Within each technical finding is a descriptive severity and risk level graphic to outline the severity and risk of the vulnerability. A brief description of the vulnerability is provided, followed by a statement of the potential business impacts, then by an attack replication portion outlining how [redacted]s security engineers were able to find the vulnerability, along with a listing of the systems affected by the vulnerability. Finally, a recommended remediation section describes a possible solution for the technical finding for technicians to use, concluded by a list of references for technicians and management alike to look into should they need additional information regarding the technical findings or the recommended remediation proposed therefor.

Overview

Throughout the duration of the penetration test performed on TCC's network infrastructure, [redacted] found 12 notable vulnerabilities in the company's network. Of these 12 vulnerabilities: 5 are critical, 2 are high severity, 5 are medium severity, and 0 are low severity. In addition to these, the penetration testers also found 7 informational non-vulnerability findings which warrant discussion and documentation.



Critical Findings:

Jellyfin Default Admin Access

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Critical		Score	9.4	
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L				
Risk Matrix					
Risk Level	High	Impact	High	Probability	High
Affected Systems					
IP Address		Port	Service	Version	
10.0.0.20		80/tcp	Jellyfin	10.8.8	

Details:

On 10.0.0.20, a "Jellyfin" account can easily be accessed by clicking the sign in button. From there, you gain admin access to Jellyfin without any authentication needed. A malicious attacker can shut down the server from the admin dashboard. They can also edit the admin credentials and lock out the authorized user from accessing the server and its contents.

Business Impact:

If an administrator account can easily be accessed, that means it has a higher chance of being accessed by those who are not authorized to do so, which could lead attackers to use said accounts to negatively impact any system(s) around them. If a malicious attacker has the ability to shut down the server from an easily accessible account, this could adversely affect business continuity. Attackers are also able to mess with the integrity of the data and lock users out of their accounts.

Attack Replication:

First, go to http://10.0.0.20/web/#!/login.html

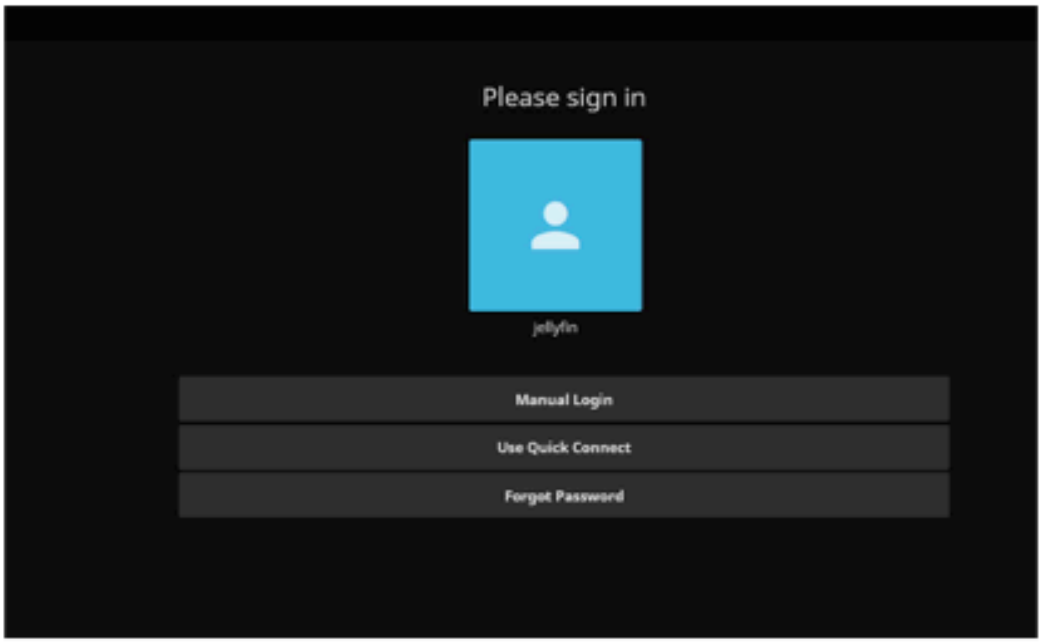


Figure 3.0: The jellyfin account in question

Then, click on the "jellyfin" account icon.

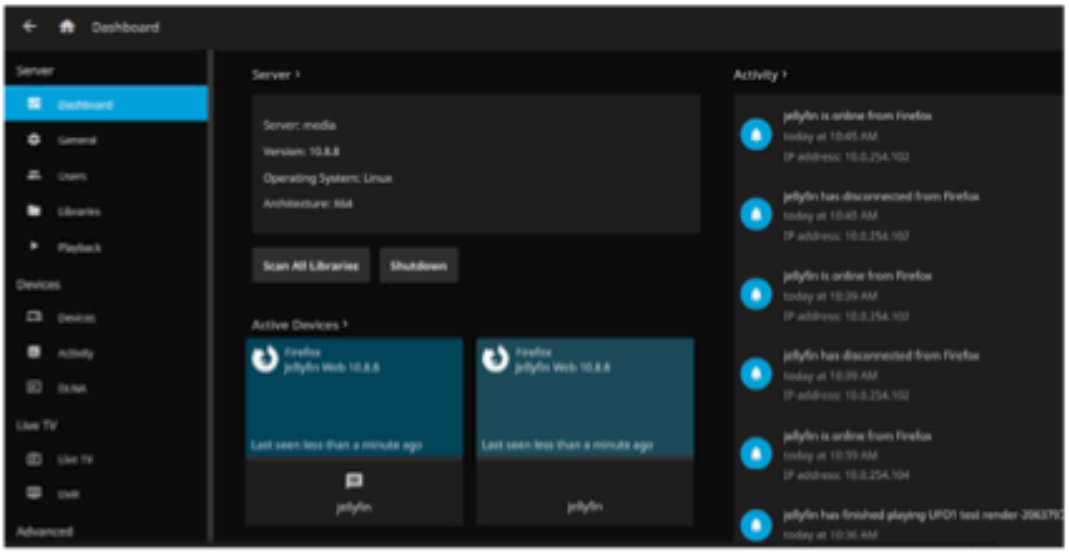


Figure 3.1: Jellyfin account has the ability to shutdown the service

Recommended Remediation:

Remove or restrict the option for users to click on the jellyfin profile to log in without a password. One way to do so is to create a designated administrator account that only a few people have credentials to and disable the default jellyfin account so that it is more difficult for attackers to find it.

PCI DSS Standards:

- 2.2.1 - Configuration standards are developed, implemented, and maintained to address all known security vulnerabilities.
- 8.3.1 - All user access to system components for users and administrators is authenticated via a strong authentication factor.
- 8.3.4 - Lock a user out after no more than 10 invalid attempts.
- 8.3.4 - Set the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.
- 8.3.6 - Passwords shall be a minimum length of 12 characters
- 8.3.6 - Passwords shall contain both numeric and alphabetic characters.
- 8.3.7 - Individuals are not allowed to submit a new password/passphrase that is the same as any of the
- last four passwords/passphrases used
- 8.3.9 - Passwords/passphrases are changed at least once every 90 days.

Reward System User Broken Access Control

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Critical		Score	9.1	
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N				
Risk Matrix					
Risk Level	High	Impact	High	Probability	High
Affected Systems					
IP Address		Port	Service	Version	
10.0.0.12		443/tcp	Nginx	1.23.3	

Details:

The source code of the reward can be found when navigating to https://10.0.0.12/query. In the source code, there are a few lines of code where, whenever a new customer account is created, they are given administrator rights by default. This violates the least privilege principle and gives every user the privilege to edit and delete data. This affects the integrity, authenticity, and confidentiality of the Reward portal.

Business Impact:

As this shows the source code behind the reward query, this can informationally show an attacker how this function works. In addition, if creating new customer accounts grants them administrative privileges, then that is a severe violation of access control as external customers should not have the same privileges as internal administrators, as these users could end up misusing their privileges to harm the system.

In addition, the source code is considered confidential, and having external access to what is otherwise considered company intellectual property is a breach of confidentiality, as rival companies can steal and use and/or modify the code for their own benefit.

Attack Replication:

Attackers fuzzed 10.0.0.12 and found the subfolder /query that contained the source code.

Figure 4.0: Using FFuF to perform a fuzzing attack on 10.0.0.12

After viewing the source code, the User class contains a variable called "is_admin". It is true by default.

```
secret = Column(String, unique=True)
username = Column(String)
fullname = Column(String, nullable=True)
email = Column(String)
password = Column(String, nullable=True)
is_admin = Column(Boolean, unique=False, default=True)
is_active = Column(Boolean, unique=False, default=True)
points = Column(Integer, nullable=True)
#rewards = relationship("Rewards", back_populates = "user")
```

Figure 4.1: Code snippet that shows whenever a new user is created they are given admin rights

Recommended Remediation:

If this source code is not intended to be shown to users outside the organization, restrict access to the source code using role-based access controls (RBACs) such that only those who are authorized to view the source code can do so.

Also, if new customers are not intended to gain administrative privileges, modify the code such that whenever a new customer account is created, then they should not be gaining administrator rights.

PCI DSS Standards:

- 2.2.1 - Configuration standards are developed, implemented, and maintained to address all known security vulnerabilities.
- 4.2 - Primary Account Numbers (PAN) are protected with strong cryptography during transmission.

- 6.2 - Bespoke and custom software are developed securely.
- 6.3 - Security vulnerabilities are identified and addressed.
- 7.2.2 - Access is assigned to users, including privileged users, based on job classification and function and the least privileges necessary to perform job responsibilities.
- 8.3.1 - All user access to system components for users and administrators is authenticated via a strong authentication factor.

Reward System Weak Admin Password

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Critical		Score	9.1	
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N				
Risk Matrix					
Risk Level	High	Impact	High	Probability	Moderate
Affected Systems					
IP Address		Port	Service	Version	
10.0.0.12		443/tcp	Nginx	1.23.3	

Details:

An administrator account found in a Reward System source code can be accessed using a weak password. The administrator account can be used to query customer credentials and modify transaction information. Additionally, the customer credentials are stored in plain text.

Business Impact:

If an administrator account contains weak credentials, this makes them more susceptible to brute-force type of attacks, where an attacker can easily gain unauthorized access to administrator accounts. Having people who are not supposed to be administrators could lead to financial risk, as unauthorized administrative access means that customer sensitive information is exposed, including cardholder data, which also leads to reputational risk as customers will lose trust in a company who is supposed to keep their information safe.

Attack Replication:

Attackers fuzzed the IP 10.0.0.12 and found a /query directory that contained default admin and guest login credentials.

Figure 5.0: Conducting a fuzzing attack on 10.0.0.12

In the initialization of the database, the login credentials for admin and guest is shown in plain text.

```
def initDB():
        db.create_all(bind=engine)
        admin = User(username='[redacted]', password='[redacted]', email='admin@[redacted]')
        guest = User(username='[redacted]', email='guest@[redacted]')
        guest.is_active = False
        guest.is_admin = False
        session.add(admin)
        session.add(guest)
        #session.commit()
        session.flush()
```

Figure 5.1: Admin username and password, and guest username hardcoded in database initiation

By using the credentials, we are able to log in with the username "admin" and the password.

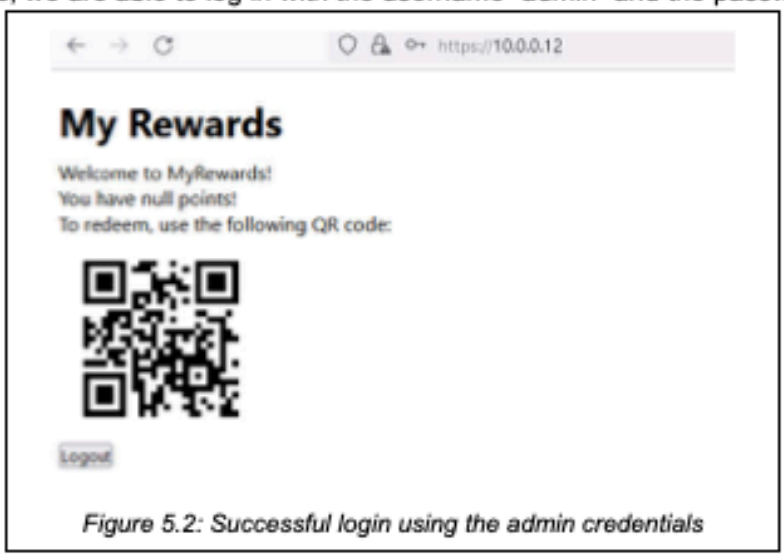


Figure 5.2: Successful login using the admin credentials

Recommended Remediation:

Ensure that the administrator account is using a secure password to mitigate potential password-related attacks targeting that account. Also, ensure that a strong password policy is set to ensure that all users must comply with a having a strong password requirement.

PCI DSS Standards:

- 8.3.4 - Lock a user out after no more than 10 invalid attempts.
- 8.3.4 - Set the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.
- 8.3.6 - Passwords shall be a minimum length of 12 characters
- 8.3.6 - Passwords shall contain both numeric and alphabetic characters.

- 8.3.7 - Individuals are not allowed to submit a new password/passphrase that is the same as any of the
- last four passwords/passphrases used
- 8.3.9 - Passwords/passphrases are changed at least once every 90 days.

Reward System Admin API Unauthorized Access

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Critical	Score	9.1		
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N				
Risk Matrix					
Risk Level	High	Impact	High	Probability	High
Affected Systems					
IP Address		Port	Service	Version	
10.0.0.12		443/tcp	Nginx	1.23.3	

Details:

The Reward admin API does not need a valid secret key in order to gain access to customer rewards information. Any value would work as the secret key value is not empty. A malicious actor can easily leak customer information without any authentication.

Business Impact:

If a secret key value is not properly authenticated, then there are no controls to prevent an attacker from using any secret key value to gain access to sensitive customer information. In addition, without the ability to properly distinguish between a regular and administrator's secret key, then this could lead to an unauthorized regular user gaining access to confidential information normally accessed by a company administrator.

This causes financial risk as data breach can occur from unauthorized access to customer information, including cardholder information such as primary account numbers (PAN). By also having unauthorized access to customer data, causing a potential data breach, this leads to reputational risk as TCC is no longer reliable in storing and protecting sensitive customer information.

Attack Replication:

Go to https://10.0.0.12/adminapi.php?query&;type=all;secret=a

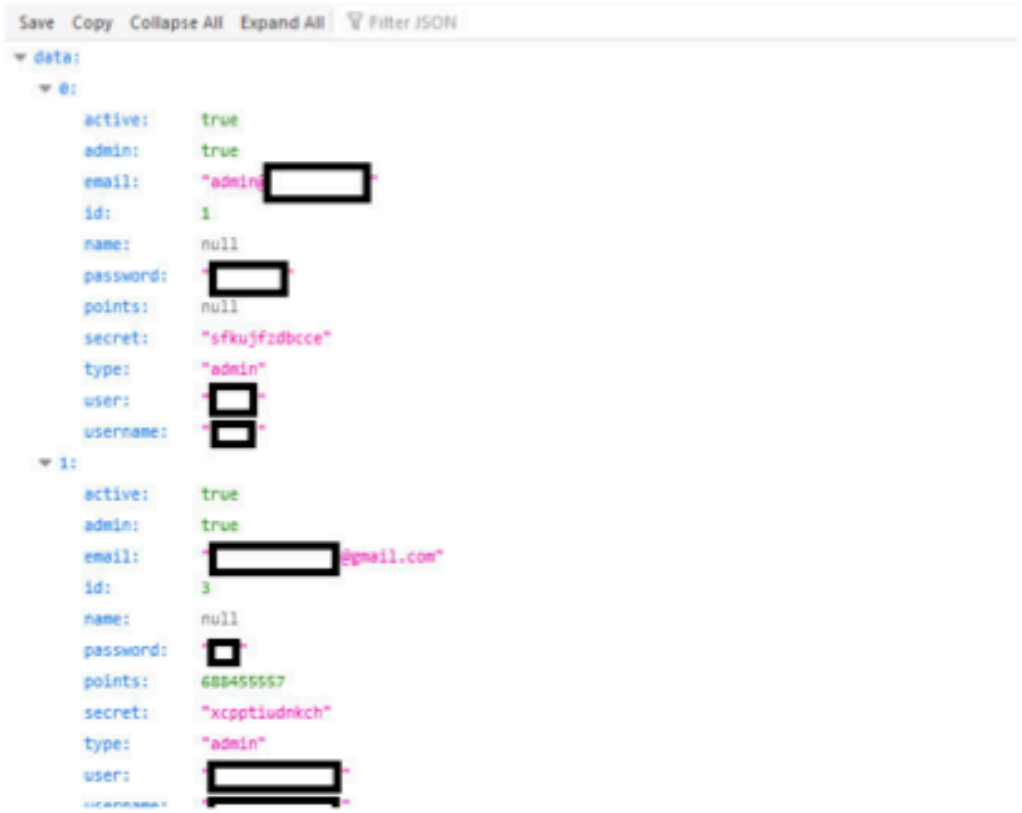


Figure 6.0: Access to admin and customer credentials after inputting any secret

Recommended Remediation:

Ensure that each administrator has a unique secret key that has administrative privileges, as if all administrators have the same secret key then it would make access to the Rewards System much easier. One recommendation for doing so would be to generate a unique secret key for each administrator and add them to a database of administrator secret keys.

PCI DSS Standards:

- 6.3 - Security vulnerabilities are identified and addressed.
- 8.3.1 - All user access to system components for users and administrators is authenticated via a strong authentication factor.

SMB Users Using No Password

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Critical		Score	9.1	
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N				
Risk Matrix					
Risk Level	High	Impact	High	Probability	High
Affected Systems					
IP Address		Port	Service	Version	
10.0.0.51 10.0.0.52 10.0.200.10*		445/tcp	SMB	3.1.1	

Details:

The authentication for SMB users "guest" and "administrator" on certain workstations and kiosks did not require a password. Coincidentally, the workstation accounts came with escalated privileges and utilized the same username and password combo for the workstation through RDP. SMB is crucial for the access of files on remote servers and various resources so passwordless authentication is not ideal.

Business Impact:

In the workstation (10.0.0.51 and 10.0.0.52), SMB has a range of functionality for working with files. An attacker harboring malicious intent has the capability to freely read, write, and adjust any files as they please. Incorrect or missing files can lead to misinformation or a lack of information. A hacker can also easily input malicious code that could lay dormant until opened.

In the kiosks system, the kiosk's main function is to display information. If a Kiosk has weak authentication, an attacker can access the server and display what they want. This can be detrimental for businesses as unauthorized content can lower company reputation and even potentially lead to lawsuits. Imagine New York City's famous Time Square under a cyber attack and all the collective billboards displaying content deemed unsafe for work. News outlets would ensure the story makes the front page and the breach would easily be a household topic of conversation. Kiosk security is important, and it's crucial that an attack of the aforementioned nature never happens in the first place.

Attack Replication:

Run the Nmap script "smb-brute" which tests the most common SMB usernames and passwords. The script returns valid credentials for accessing the SMB client.

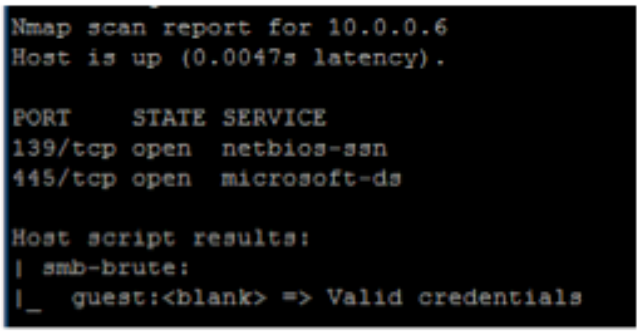


Figure 7.0

Recommended Remediation:

Set complex passwords for all SMB accounts and disable unused accounts.

PCI DSS Standards:

- 8.3.4 - Lock a user out after no more than 10 invalid attempts.
- 8.3.4 - Set the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.
- 8.3.6 - Passwords shall be a minimum length of 12 characters
- 8.3.6 - Passwords shall contain both numeric and alphabetic characters.
- 8.3.7 - Individuals are not allowed to submit a new password/passphrase that is the same as any of the
- last four passwords/passphrases used
- 8.3.9 - Passwords/passphrases are changed at least once every 90 days.

High Risk Findings:

WordPress Weak Admin Password

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	High		Score	8.2	
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N				
Risk Matrix					
Risk Level	Moderate	Impact	Moderate	Probability	High
Affected Systems					
IP Address		Port	Service	Version	
10.0.0.11		80/tcp	Wordpress	4.8.21	

Details:

A brute-force password test using a dictionary list of common passwords revealed that the default admin WordPress account has a weak password assigned to it. A malicious actor can easily guess the admin password and modify the WordPress site. In addition, multiple attempts were made to find and login using different password options, meaning that there are no lockout policies in place set for a number of failed attempts.

Business Impact:

If an administrator account is found using a weak password, attackers will have an easier time accessing that account. This means that the attack could gain administrative privileges for malicious intent, which can be destructive to the WordPress site. Modification to the WordPress site could damage the integrity of TCC if it is displaying incorrect or malicious information. A company's website that has been hacked and altered negatively leads to reputational risk as it shows that a company cannot be trusted to secure sensitive information and display factual information.

Attack Replication:

Used Hydra to run a brute-force password dictionary attack: hydra -l admin -P /usr/share/seclists/Passwords/darkweb2017-top1000.txt 10.0.0.11 -V http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:S=Location'

Figure 8.0: Brute-force password attempts on the admin account

Recommended Remediation:

Ensure that the admin account is using a password that is secure, complex, and adheres to the PCI DSS's password policies. Also, ensure that there is a set lockout policy such that brute-force password attacks are discouraged.

It is also recommended to secure the account using multi-factor authentication (MFA) to add an extra layer of security.

PCI DSS Standards:

- 8.3.4 - Lock a user out after no more than 10 invalid attempts.
- 8.3.4 - Set the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.
- 8.3.6 - Passwords shall be a minimum length of 12 characters
- 8.3.6 - Passwords shall contain both numeric and alphabetic characters.
- 8.3.7 - Individuals are not allowed to submit a new password/passphrase that is the same as any of the
- last four passwords/passphrases used
- 8.3.9 - Passwords/passphrases are changed at least once every 90 days.

Invoice System User Broken Access Control

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	High		Score	7.4	
Vector	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N				
Risk Matrix					
Risk Level	High	Impact	High	Probability	Moderate
Affected Systems					
IP Address		Port	Service	Version	
10.0.0.200		80/tcp	Nginx	1.23.3	

Details:

During the login process for the invoice system, a token is generated that does not contain the role of the user like guest or admin. This allows any user to gain access to customer information that would otherwise be accessed by administrator accounts. A malicious actor could gain access to credit card information which poses a huge financial risk to the company.

Business Impact:

Without any enforcement of role-based access controls, regular users can inadvertently gain access to information or privileges that would otherwise be for administrators only. This is problematic because if an attacker, whether they are internal or external to the business, gains access to the system, they can easily not only view sensitive customer information, but can also potentially cause damage to the system as they are in control of administrative rights. This leads to financial risk as unauthorized administrative access can lead to viewing sensitive customer information, which would also then lead to data breaches.

As a byproduct of potential data breaches, this also leads to reputational risk because it means that customers' sensitive information would be released to the public, lowering general company trust about its integrity and reliability to keep their information safe.

Attack Replication:

After we login to the invoice portal as a customer, our role is "guest" in the JSON response.

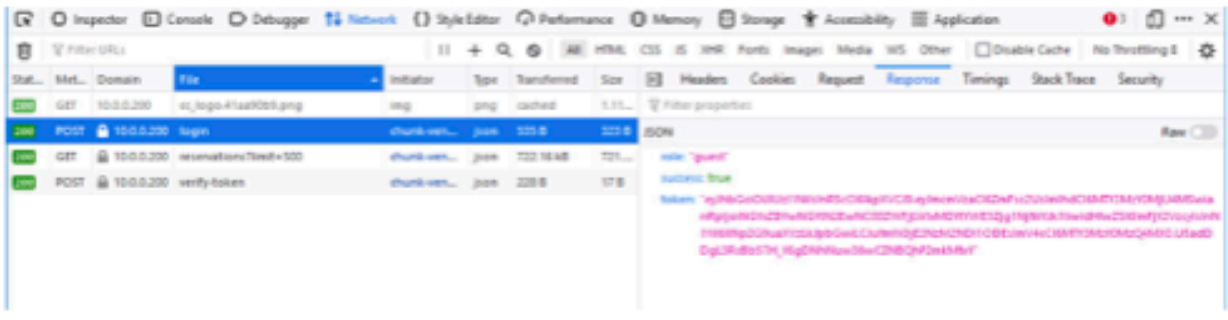


Figure 9.0: Logging in to invoice portal as customer, with role set to "guest"

However, in the JWT token, there is no mention of the role of the user.

Figure 9.1: Decoded JWT token with no mention of user role

As a result, an attacker can query the API with admin access to view sensitive customer data.

Figure 9.2: Using the token in admin API to view sensitive customer data

Recommended Remediation:

Ensure that the token contains the level of access that a user should have during the login process. Validate the role of the user in API calls.

PCI DSS Standards:

- 2.2.1 - Configuration standards are developed, implemented, and maintained to address all known security vulnerabilities.
- 4.2 - Primary Account Numbers (PAN) are protected with strong cryptography during transmission.
- 6.3 - Security vulnerabilities are identified and addressed.

- 7.2.2 - Access is assigned to users, including privileged users, based on job classification and function and least privileges necessary to perform job responsibilities.
- 8.3.1 - All user access to system components for users and administrators is authenticated via a strong authentication factor.
- 9.1 - Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

Medium Risk Findings:

Invoice System PostgreSQL Injection

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Medium		Score	5.9	
Vector	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N				
Risk Matrix					
Risk Level	Moderate	Impact	Moderate	Probability	Moderate
Affected Systems					
IP Address		Port	Service	Version	
10.0.0.200		80/tcp	Nginx	1.23.3	

Details:

In the invoice query page, SQL commands can be injected to the input. In this case, using a SQL injection in the billing database would leak sensitive customer information and allow potential access to the system.

Business Impact:

If an attacker can externally inject commands into the invoice system, not only does it show that whatever the attacker inputs is not properly checked, but this allows them to send commands intended for an internal database administrator to perform, which could include gaining potential unauthorized access to the system.

Attack Replication:

Enumerate the number of columns for UNION SELECT. Then select the version of the database.

Figure 10.0 - The result of injection SQL code in invoice ID query

Recommended Remediation:

Sanitize the input such that SQL injection commands do not work externally, and must be run within the system by users with the appropriate roles.

PCI DSS Standards:

- 2.2.1 - Configuration standards are developed, implemented, and maintained to address all known security vulnerabilities.
- 4.2 - Primary Account Numbers (PAN) are protected with strong cryptography during transmission.

- 6.3 - Security vulnerabilities are identified and addressed.
- 7.2.2 - Access is assigned to users, including privileged users, based on job classification and function and the least privileges necessary to perform job responsibilities.
- 9.1 - Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

References:

SQL injection prevention cheat sheet -
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

CVE-2022-3590 (Wordpress Unauthorized Blind SSRF)

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Medium		Score	5.9	
Vector	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N				
Risk Matrix					
Risk Level	Moderate	Impact	High	Probability	Low
Affected Systems					
IP Address		Port	Service	Version	
10.0.0.11		443/tcp	Wordpress	4.8.21	

Details:

Attackers could exploit the old version of Wordpress, 4.8.21, by taking advantage of the pingback link feature, which involves a url that can lead to an internal server. This issue could be used to bypass logins and their defense mechanisms. This can be used to exploit the internal server that is not accessible to the outside.

Business Impact:

If attackers can exploit this vulnerability, they would be able to view and modify the data in the internal server. This is a breach of confidentiality and can affect customers' safety and trust in the company in the future. Additionally, the attacker can attack the internal server, which can causing more damage and data leak.

Attack Replication:

The proof of concept for this CVE is not yet available.

Recommended Remediation:

Implement a firewall between the WordPress site and the internal server. Make sure the internal server communicates with whitelisted servers.

References:

CVE-2022-3590 NVD entry - https://nvd.nist.gov/vuln/detail/CVE-2022-3590
Details - https://www.sonarsource.com/blog/wordpress-core-unauthenticated-blind-ssrf/

CVE-2021-21311 (Adminer SSRF)

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Medium		Score	5.3	
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N				
Risk Matrix					
Risk Level	Moderate	Impact	Low	Probability	Moderate
Affected Systems					
IP Address		Port	Service	Version	
10.0.0.12		443/tcp	Adminer	4.3.0	

Details:

An outdated version of Adminer is found in 10.0.0.12, as the current version is 4.3.0 while the latest version is 4.8.1. This version of Adminer is vulnerable to a server-side reflection (SSRF) attack. Using an SSRF tool, an attacker can remotely inject commands into a server, which would normally be something that is done by server-side administrators.

Business Impact:

Having an outdated version of Adminer or any program can make it susceptible to attacks pertaining to it. In this case, an attacker can send commands to be remotely executed on the server side, which could allow the attacker to even find information that could be listed in an internal database.

Attack Replication:

First, go to http://10.0.0.12/adminer

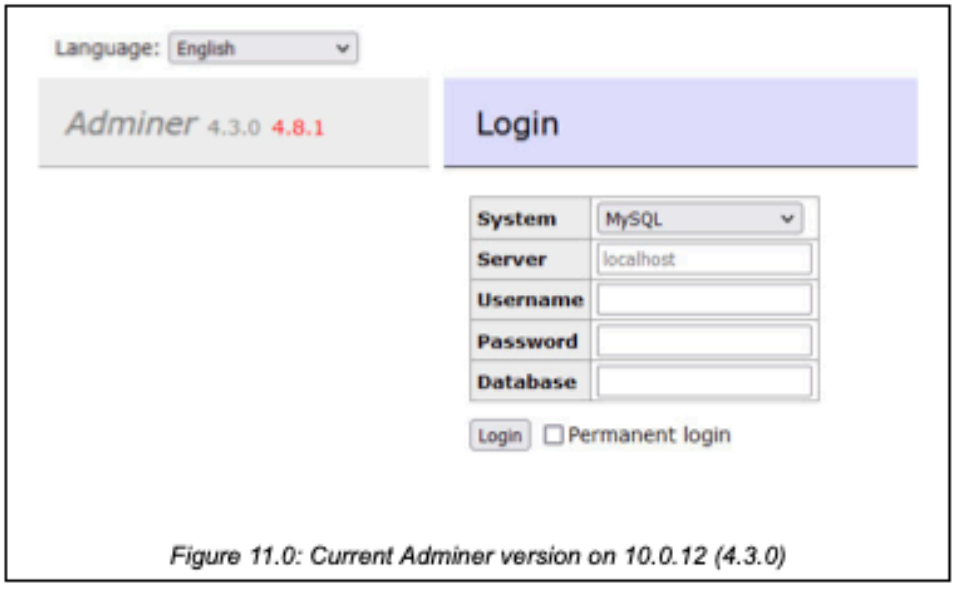


Figure 11.0: Current Adminer version on 10.0.12 (4.3.0)

Run the POC script from exploitDB and enter the following information:

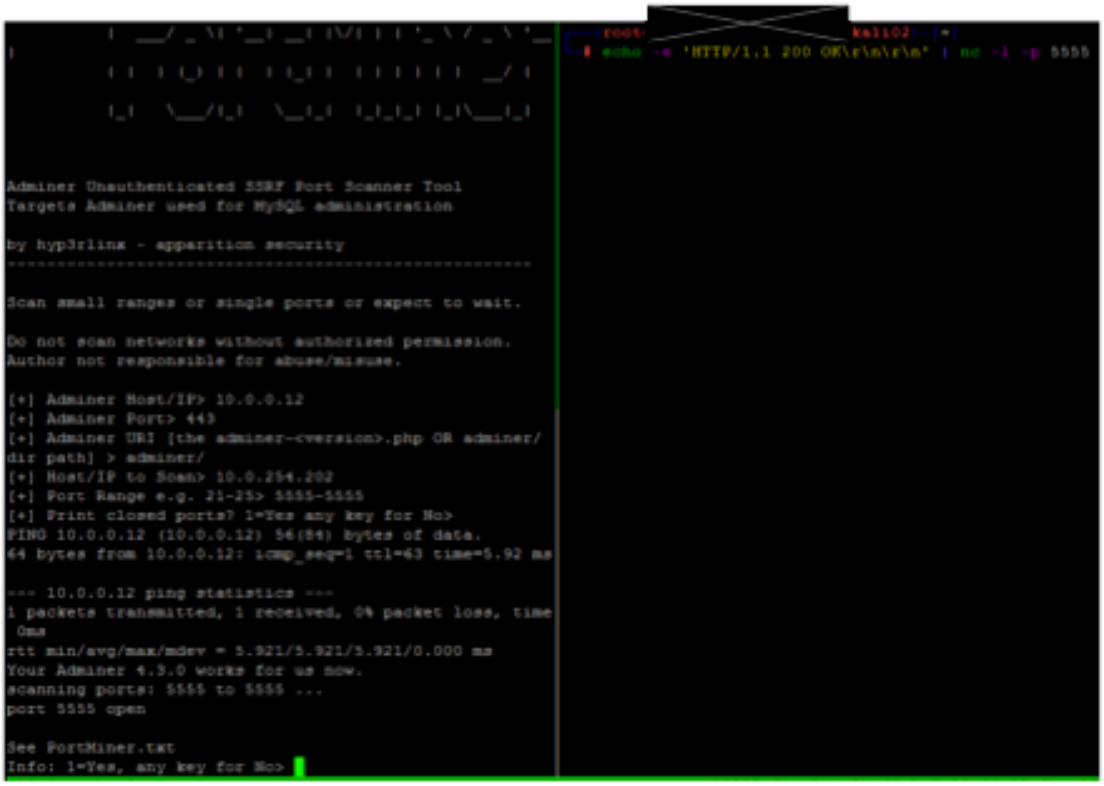


Figure 11.1: Running an SSRF attack on Adminer

Recommended Remediation:

Ensure that the latest, stable version of Adminer is running on the host to mitigate vulnerabilities that come with having an outdated version of the program.

PCI DSS Standards:

- 2.2.1 - Configuration standards are developed, implemented, and maintained to address all known security vulnerabilities.
- 6.3 - Security vulnerabilities are identified and addressed.

References:

CVE-2021-21311 entry - https://nvd.nist.gov/vuln/detail/CVE-2021-21311
Adminer 4.3.1 SSRF vulnerability - https://www.exploit-db.com/exploits/43593

Reward System Guest No Password

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Medium		Score	5.3	
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N				
Risk Matrix					
Risk Level	Moderate	Impact	Low	Probability	Moderate
Affected Systems					
IP Address		Port	Service	Version	
10.0.0.12		443/tcp	Nginx	1.23.3	

Details:

A guest account found in a Reward System can be accessed without using a password. The guest account would then have no special access to the Reward System; however, there is still potential for lateral movement as it is an easily accessible account.

Business Impact:

Guest accounts are easily identifiable if no measures are made to re-label or disable them, as not only is the display name "Guest". An attacker with knowledge of guest accounts can attempt to easily log in as not only passwords are not required to access them, but an attacker can use that account as an entry point to gain further access into the system. It can further compromise the integrity of the reward system.

Attack Replication:

Figure 12.0 Guest login without password parameter

Recommended Remediation:

Disable and rename the guest account accordingly to make it less obvious for attackers to find them.

PCI DSS Standards:

- 8.3.1 - All user access to system components for users and administrators is authenticated via a strong authentication factor.
- 8.3.4 - Lock a user out after no more than 10 invalid attempts.

Reward System Weak Customer Password

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Medium		Score	5.3	
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N				
Risk Matrix					
Risk Level	High	Impact	Moderate	Probability	Moderate
Affected Systems					
IP Address		Port	Service	Version	
10.0.0.12		443/tcp	Nginx	1.23.3	

Details:

Customer accounts have been found using weak passwords. A malicious actor can easily brute-force the customer account and gain access to their rewards. Additionally

Business Impact:

If customer accounts have weak passwords, in the case where either their credentials are breached, or a password-related attack is attempted on them, then there is a higher chance that the attacker can gain access to those accounts as the passwords are not complex enough. Not having a complex password requirement makes it more likely for a malicious actor to steal customer information or any other sensitive data, which could then cause financial risk through the form of information exfiltration and/or data breach.

Attack Replication:

Go to https://10.0.0.12/adminapi.php?query&;type=all;secret=<admin secret>

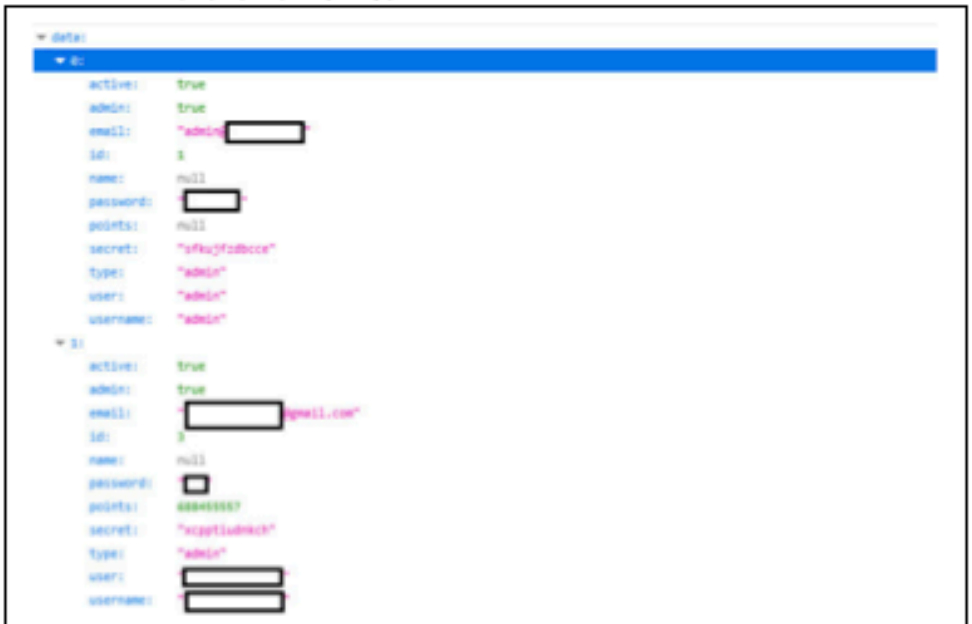


Figure 13.0 Query the users with admin secret

Recommended Remediation:

Ensure that not only users change their passwords to stronger, complex ones, but also enforce a system-wide complex password policy such that future customer accounts must comply with them.

PCI DSS Standards:

- 8.3.4 - Lock a user out after no more than 10 invalid attempts.
- 8.3.4 - Set the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.
- 8.3.6 - Passwords shall be a minimum length of 12 characters
- 8.3.6 - Passwords shall contain both numeric and alphabetic characters.
- 8.3.7 - Individuals are not allowed to submit a new password/passphrase that is the same as any of the
- last four passwords/passphrases used
- 8.3.9 - Passwords/passphrases are changed at least once every 90 days.

Informational Findings:

Payment API Documentation

Affected Systems			
IP Address	Port	Service	Version
`10.0.0.200`	`8000/tcp`	`FastAPI`	`1.0.0`

Details:

The Payment API shows documentation on how to use the API. This gives useful information for a malicious act to exploit API functions.

Business Impact:

As this mainly shows how the API is being used while having sandbox environments to try certain commands, without affecting the main system, this is more of an informational concern as this would tell external users what kind of API is being used within the system. The attacker can compromise the API and gain customer information.

Attack Replication:

Go to http://10.0.0.200/doc

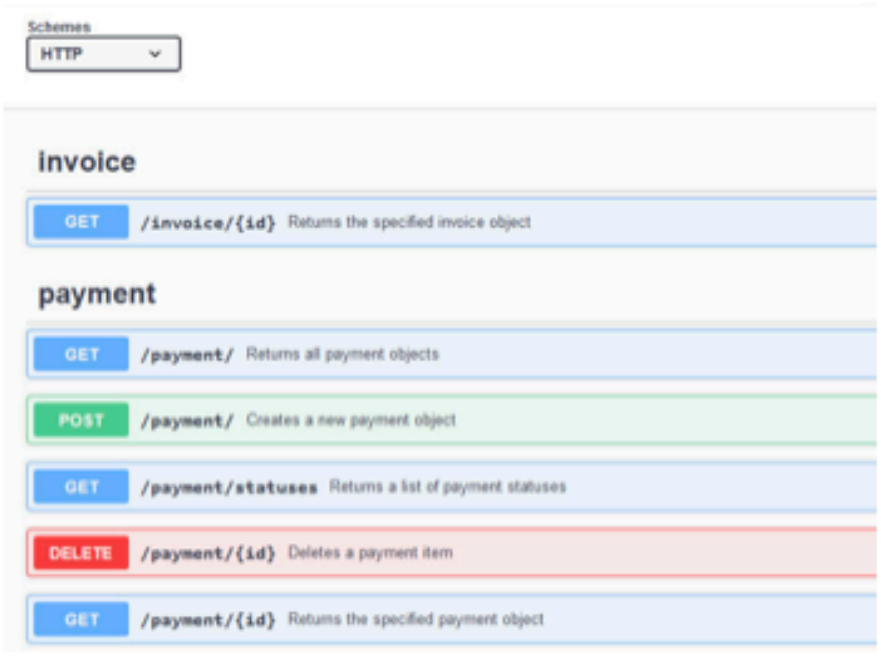


Figure 14.0 Documentation of API function

Recommended Remediation:

Keep the API information private to prevent external users from finding out what kind of API is being used on the system.

PCI DSS Standards:

- 6.2 Bespoke and custom software are developed securely.
- 7.2.2 - Access is assigned to users, including privileged users, based on job classification and function and the least privileges necessary to perform job responsibilities.

SMB Signing Not Required

Affected Systems			
IP Address	Port	Service	Version
10.0.0.6 10.0.0.11 10.0.0.51 10.0.0.52	445/tcp	SMB	3.1.1

Details:

When running a script to discover some SMB security mode settings, Server Media Block (SMB) signing is not required on some servers. This can be dangerous because it can increase the chance of data leak.

Business Impact:

With SMB Message Signing disabled, an attacker who is not authenticated can be in the middle of the SMB process and intercept any sensitive information that gets transmitted. This affects the integrity of an otherwise private conversation between two parties of the SMB process, because that attacker in a man-in-the-middle attack can not only intercept the information or data sent in the process, but they can also modify and tamper with it, causing operational and reputational risk.

Attack Replication:

Run SMB security mode script on port 445

Figure 15.0 Result of the script on 10.0.0.6 and 10.0.0.11

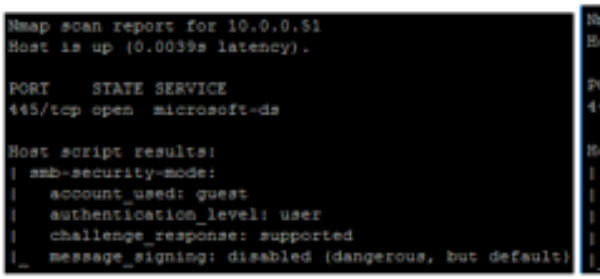


Figure 15.1 Result of the script on 10.0.0.51 and 10.0.0.52

Recommended Remediation:

Enable SMB Message Signing to mitigate potential attacks that could occur as a result of that setting being turned off, specifically man-in-the-middle attacks.

PCI DSS Standards:

- 2.2.1 - Configuration standards are developed, implemented, and maintained to address all known security vulnerabilities.
- 6.3 - Security vulnerabilities are identified and addressed.

References:

Info on SMB Message Signing - https://www.tenable.com/plugins/nessus/57608

Publicly Exposed Organizational Chart

Affected Systems			
IP Address	Port	Service	Version
`www.thecozycroissant.com`	`443/tcp`	`Apache`	`2.4.41`

Details:

An organizational chart can be found when going to https://www.thecozycroissant.com/content. The organization chart shows the employee's name and position in the organization. A malicious actor can use this information to create a username list and brute force organization login pages.

Business Impact:

This is confidential information that can be easily accessed by appending something to a website URL, and this information can be used to phish people in the organization. If attackers can get a hold of the names and the roles of people within the organization, and how these people are connected to each other, they can use other publicly available information to create specific phishing attacks for certain users. For example, an attacker could create a fake email from a manager to scare people into clicking a malicious link, which could actually host a solution that would collect personal information.

Attack Replication:

There is a public Github repository found by searching through Github, that hinted at a directory named /content.

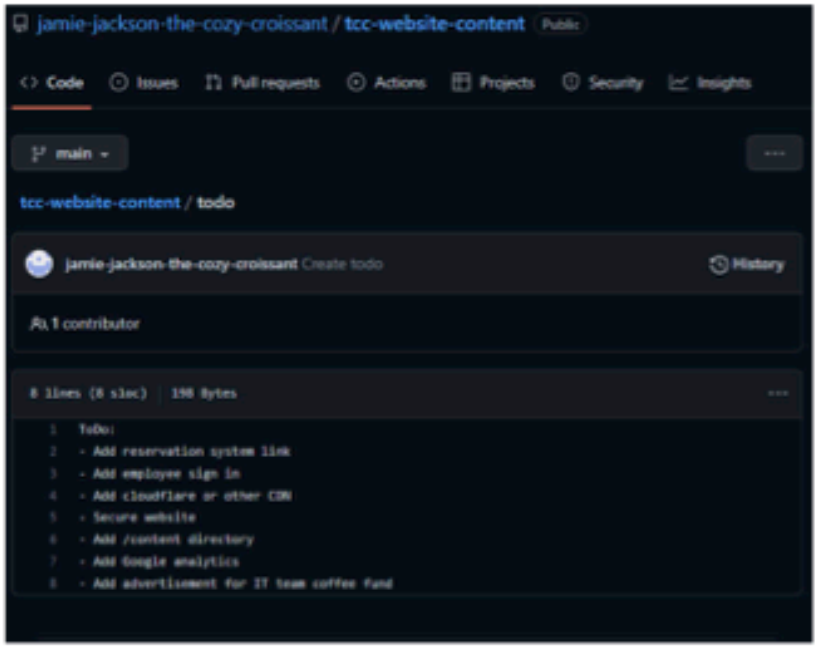


Figure 16.0 screenshot of the public Github repository

The organizational chart can be found by going to https://www.thecozycroissant.com/content.

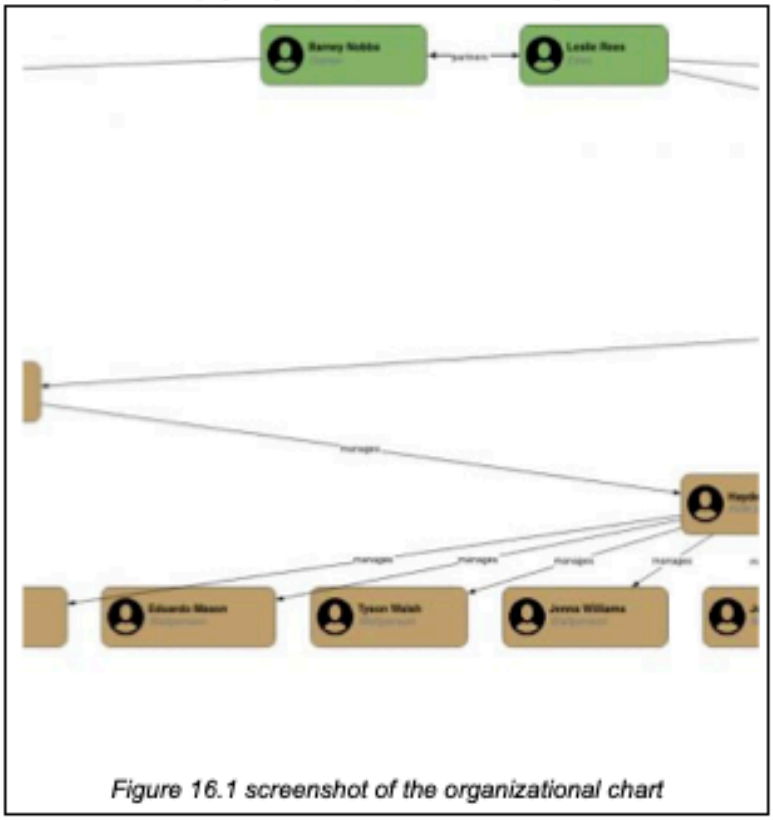


Figure 16.1 screenshot of the organizational chart

Recommended Remediation:

Relocate the organizational chart to an internal drive where personnel with the appropriate privileges have access to them. An ideal example of an internal drive would be using SharePoint as it has the ability to restrict access based on RBACs (role-based access controls).

Take down the /content directory so that it is not easily accessible to the general public.

Lastly, ensure that any Github repositories associated with TCC are not displaying sensitive data or information, such as mentioning that there is a /content directory.

PCI DSS Standards:

- 2.2 - System components are configured and managed securely
- 8.1 - Processes and mechanisms for identifying users and authenticating access to system components are defined and understood
- 8.3.4 - invalid authentication attempts are limited by locking out the user after several failed attempts and setting the duration to a minimum of 30 minutes or until the user's identity is confirmed
- 8.5 - Multi-factor authentication (MFA) is implemented to prevent misuse of internal content
- 8.6 - Use of application and system accounts and associated authentication factors is strictly managed

- 12.6 - Security awareness education is an ongoing activity
- 12.7 - Personnel are screened to reduce risks from insider threats

References:

Jamie Jackson's Github -
https://github.com/jamie-jackson-the-cozy-croissant/tcc-website-content/blob/main/todo
Directory Listing (Apache) -
https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/directory-listing-apache/

Outdated WordPress

Affected Systems			
IP Address	Port	Service	Version
10.0.0.11	**80/tcp**	**WordPress**	**4.8.21**

Details:

A WordPress scan on 10.0.0.11 returned findings on an outdated version of WordPress. It is running version 4.8.21, while the latest version as of January 2023 is 6.1.1. Running an outdated software can increase the chance of being compromised.

Business Impact:

Running outdated versions of software can leave it and its related systems vulnerable to outside attacks pertaining to its version, as current versions of software are patched to mitigate any threats related to its older versions. It can potentially cause data breach, customer information to be exfiltrated for malicious purposes, and ultimately a loss of trust in the way the company is handling sensitive data.

Attack Replication:

Checked the current version of of WordPress on 10.0.0.11 using the vane script

```
[+] URL: http://10.0.0.11/
[+] Started: Sat Jan 14 07:56:37 2023

[+] robots.txt available under: 'http://10.0.0.11/robots.txt'
[!] The WordPress 'http://10.0.0.11/readme.html' file exists exposing a version
number
[!] Full Path Disclosure (FPD) in: 'http://10.0.0.11/wp-includes/rss-functions.p
hp'
[+] Interesting header: SERVER: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.33
[+] Interesting header: SET-COOKIE: wp_sr_session_5c016e8f0f95f039102cbe8366c5c7
f3=663a12d527187e3abd24f40c1f5cbe2b%7C%7C1673884594%7C%7C1673880994%7C%7C2bc6c5e
fa83d2f019a82770ed32a3344; expires=Mon, 16-Jan-2023 15:56:34 GMT; Max-Age=172791
; path=/
[+] Interesting header: X-POWERED-BY: PHP/7.4.33
[+] Registration is enabled: http://10.0.0.11/wp-login.php?action=register
[+] XML-RPC Interface available under: http://10.0.0.11/xmlrpc.php
[!] Upload directory has directory listing enabled: http://10.0.0.11/wp-content/
uploads/

[+] WordPress version 4.8.21 identified from links opml

[+] Enumerating plugins from passive detection ...
[+] No plugins found
```

Figure 17.0 A readme page is available

Go to https://10.0.0.11/readme.html

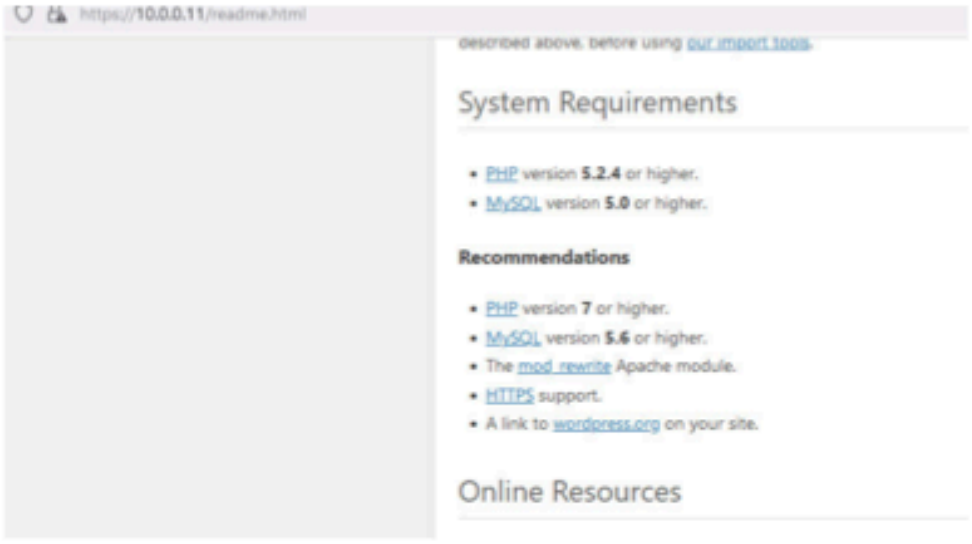


Figure 17.1 Outdated PHP and MySQL

Recommended Remediation:

Ensure that WordPress is running on the latest version to mitigate vulnerabilities.

PCI DSS Standards:

- 2.2.1 - Configuration standards are developed, implemented, and maintained to address all known security vulnerabilities.
- 6.3 - Security vulnerabilities are identified and addressed.

References:

WordPress Releases - https://wordpress.org/news/category/releases/

Cleartext Windows Password Policies

Affected Systems			
IP Address	Port	Service	Version
10.0.0.51 10.0.0.52	135/tcp	RPC	N/A

Details:

On 10.0.0.51, it was discovered that the DOMAIN_PASSWORD_STORE_CLEARTEXT policy was enabled, which means that the directory service is storing all user passwords in cleartext instead of hashing them.

Business Impact:

By storing cleartext passwords, should an attacker ever get access to the directory service, they will have an easier time retrieving passwords without the need to decrypt them. This is a violation of confidentiality as passwords are considered as personally identifiable information (PII), and should only be known to the users of their respective accounts. This makes data breach more damaging.

Attack Replication:

Ran the "enumdomusers" and "getusrdompwinfo" via rpcclient on 10.0.0.51, and discovered the following password policies:

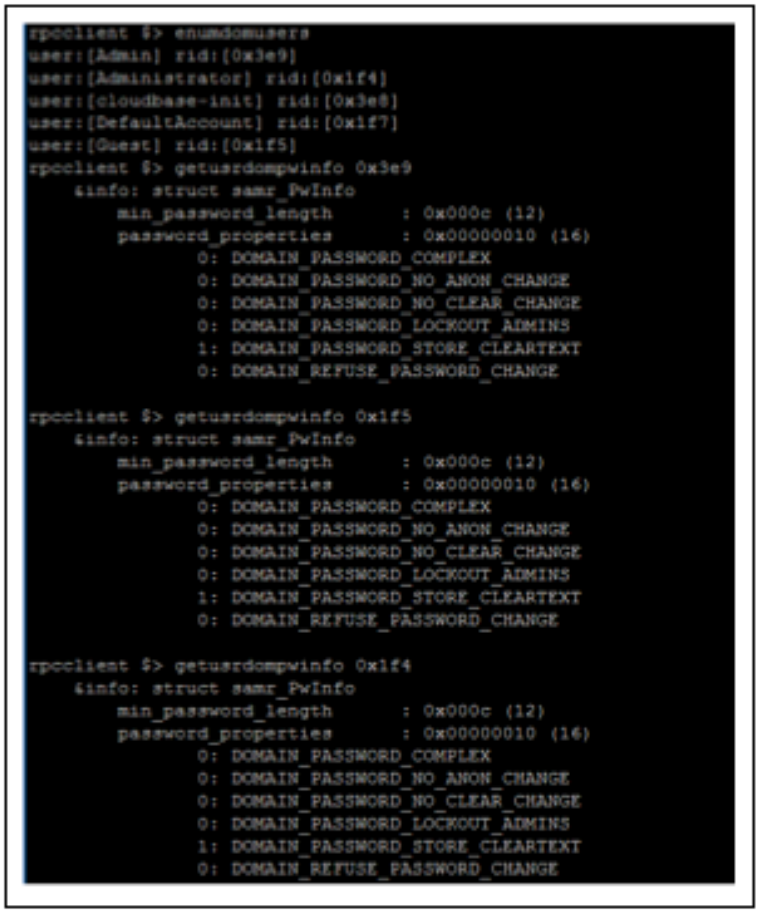


Figure 18.0 Password policy from RPC

Recommended Remediation:

Disable the DOMAIN_PASSWORD_STORE_CLEARTEXT policy so that passwords are encrypted. If that is not possible, then add another layer of security such as one-time passwords (OTPs) or MFA (multi factor authentication).

PCI DSS Standards:

- 3.6 - Cryptographic keys used to protect stored account data are secured.

References:

DOMAIN_PASSWORD_INFORMATION structure -
https://learn.microsoft.com/en-us/windows/win32/api/ntsecapi/ns-ntsecapi-domain_password_information

Windows Defender Turned Off

Affected Systems			
IP Address	Port	Service	Version
10.0.0.52	443/tcp	Windows Defender	N/A

Details:

On 10.0.0.52, it was discovered that Windows Defender service is not enabled and running. By not having a form of antivirus protection, would make a system vulnerable to attacks from viruses or any similar form of malware.

Business Impact:

Malware can have a wide range of impacts on the affected system, ranging from being a nuisance to daily business operations to even being as severe as disrupting the uptime of the device. Regardless of the malware's severity, any form of business operation disruption affects device availability and productivity, which could cause the business to lose time and assets.

Attack Replication:

Upon logging in to the host, and checking to see Windows Defender status, we found that it is not enabled.

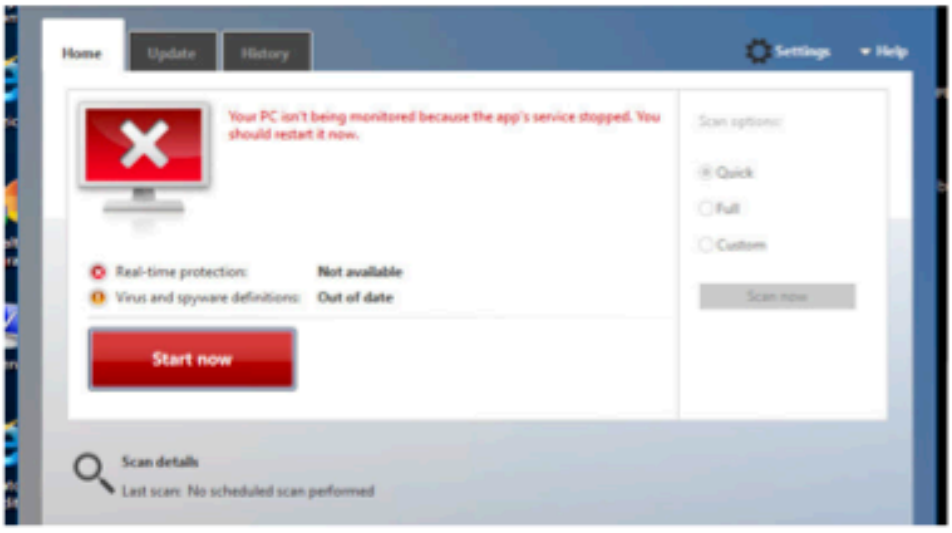


Figure 19.0: Windows Defender is disabled on the host.

Recommended Remediation:

Ensure that Windows Defender or some form of antivirus protection is enabled, as that will add an extra layer of security defense to the host. Also, ensure that the antivirus's definitions are up-to-date to ensure that it is protecting against the latest cyber threats.

PCI DSS Standards:

- 5.3 - Anti-malware mechanisms and processes are active, maintained, and monitored.

Insecure Safe Model

Affected Systems			
IP Address	Port	Service	Version
`Unknown TCC Safe Model`	`N/A`	`N/A`	`N/A`

Details:

When our team was given a safe to investigate, the team was able to study the locking mechanism and manipulate it to open the safe and bypass the code. The team was able to open the safe and reset the password of the safe without knowing the original code or using a key.

Business Impact:

Using this model of safes exposes TCC to physical attacks and risks losing customer belongings as well as important documents left behind the front desk.

Attack Replication:

Put the safe on a stable platform and shake the safe from top to bottom. The locking mechanism of the safe relies on either the code being inputted or a key to press down on a plunger that prevents the knob from turning 90 degrees to the right. The plunger is loose enough to be shaken out of position allowing the knob to be turned while shaking the safe. When timed correctly, the knob should to the right as the plunger is moved out of position unlocking the safe as if a key was used.

Recommended Remediation:

Upon reviewing different options from the same vendor, we recommend changing the manufacturer and opting for different models that have tighter security locking mechanisms.

References:

Visual demonstration of how the locking mechanism works and its exploitation - https://www.youtube.com/watch?v=fWEOvcfVzGE

Conclusion

As The Cozy Croissant continues to grow, it is important that TCC takes the security of its customer information seriously and complies with PCI DSS regulations. By rehiring [redacted] to perform another penetration test on their network, along with the improvements in security consistent with the recommendations provided from the last assessment, it is evident that TCC takes security seriously and is indeed committed to providing a safe place for the people to stay in a reliable and secure way, as a part of their mission to be a family-friendly hotel servicing Reno in the Nevada state.

Following the prior security assessment, TCC's cybersecurity controls have definitely improved. However, even the most secure systems have their vulnerabilities, thus it is important to note the aforementioned vulnerabilities and to remediate them in a timely manner to avoid the various risks they may bring to the company. To aid in this process, [redacted] has provided a layout of the company's security strengths, trends in the vulnerabilities found within, a listing of the company's compliance to the PCI DSS standards, a brief risk analysis, and a listing of recommended responses within the following sections.

Principal Strengths in Security

TCC has greatly improved the security of its networks since the last penetration test performed by [redacted] implementing most of the measures recommended. These improvements greatly reduce the potential attack vectors to which the company's network is vulnerable, and makes TCC much more compliant with the PCI DSS standards.

1. Authorization / Network Security: Since the last security assessment, TCC has effectively implemented firewalls, network access control lists, and network segmentation as recommended. These security measures properly reduce external access to the company's critical infrastructure, and in general, significantly deprives potential intruders of the authorization needed to severely compromise the network. The aforementioned security systems are significant as they greatly reduce the company's exposure to regulatory risks by avoiding violation fines, as well as operational and financial risks in avoiding compromising the company's services and assets.

2. Input / Output Sanitization: As part of the network security improvements, a majority of the malicious network traffic has been sanitized from both inputs and outputs, depriving attackers of something as simple yet vital as a network scan. For example, the debugger in the award server was not susceptible to command injections during this engagement.

Principal Trends in Vulnerabilities

1. Authentication: While the TCC has made efforts since the last assessment to ensure that proper authentication mechanisms are in place to protect sensitive internal information, [redacted] noticed that there is a common trend of poor password policies being used due to the numerous user accounts, especially administrative accounts, containing weak, none, or default passwords being used. This lack of password policy enforcement means that users can set weak passwords for themselves, which also means that attackers will have an easier time trying to discover the passwords of said user accounts. Especially with administrator

accounts, having an easier time attempting to guess passwords would greatly compromise the confidentiality, integrity, and availability of the various systems that are involved in the network.

2. Input / Output Sanitization: While there has been significant improvement in input/output sanitization, Final-08 also discovered a lack of input sanitization in certain systems, which would allow attackers to inject commands into systems as if they had internal access. For instance, the PostgreSQL system is susceptible to SQL injections, which can lead to attackers sending queries to exfiltrate internal information.

3. General Misconfigurations: While TCC has implemented access controls, [redacted] discovered some user misconfigurations in different services. Some of the running services were found to give default admin privileges to customer accounts which can cause major security issues for TCC. We recommend that the remediation plan listed above for the misconfigurations be addressed as TCC should follow the principle of least privilege.

Resultant Compliance to PCI DSS

Taking into account both positive security controls as well as the vulnerabilities found within TCC's network, [redacted] has compiled the following compliance checklist. As noted earlier, many points have been omitted from the checklist due to the limited time frame and scope of [redacted]s evaluation, and only taking into account standards in enforcement as of March 2022. Following the PCI DSS requirements will ensure that TCC remains compliant with PCI standards and avoid fines and penalties.

Ref #	Requirements
2.2.1	Configuration standards are developed, implemented and maintained to: Cover all system components, address all known security vulnerabilities, be consistent with industry-accepted system hardening standards or vendor hardening recommendations, be updated as new vulnerability issues are identified. Standards should be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.
2.2	Vendor default accounts are managed as follows: If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. If the vendor default account(s) will not be used, the account is removed or disabled.
4.2	Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks. Only trusted keys and certificates are accepted. Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. The encryption strength is appropriate for the encryption methodology in use.
5.3	Ensure that anti-malware mechanisms and processes are active, maintained, and deployed, such that they are able to detect and address the latest malware threats.
6.2	Bespoke and custom software are developed securely, as follows: Based on industry standards and/or best practices for secure development. In accordance with PCI DSS

	(for example, secure authentication and logging). Incorporating consideration of information security issues during each stage of the software development lifecycle.
6.3	Security vulnerabilities are identified and managed as follows: New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. Risk rankings identify, at a minimum, all vulnerabilities considered to be high-risk or critical to the environment. Vulnerabilities for bespoke and custom, and third-party software (for example opera
7.2.2	Access is assigned to users, including privileged users, based on: Job classification and function. Follow least privileges necessary to perform job responsibilities.
8.3.1	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: Something you know, such as a password or passphrase. Something you have, such as a token device or smart card. Something you are, such as a biometric element.
8.3.4	Invalid authentication attempts are limited by: Locking out the user ID after not more than 10 attempts. Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.
8.3.6	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). Contain both numeric and alphabetic characters.
8.3.7	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.
8.3.9	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: Passwords/passphrases are changed at least once every 90 days or the security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.

Resultant Risk Analysis

The 19 vulnerabilities detailed within the report expose TCC to a significant degree of business risk. The first of these is the operational risk brought directly by cyber vulnerabilities. This risk comes in the form of the potential for external fraud like theft, brought about by the compromise of confidentiality and integrity leading to the theft of intellectual property as well as other assets with obtained credentials. Any damages leading to the compromise of the availability of TCC's services caused by the exploitation of these vulnerabilities also classify as external fraud which poses an operational risk to TCC.

Furthermore, some of the vulnerabilities found may qualify as violations of PCI DSS. Should such violations be found and remain unmitigated, they may pose regulatory risks to TCC as well as financial risks due to the possibility of significant monetary penalties. Additionally, if the same violations are publicized through a Notice of Penalty posted on the PCI DSS website, they may also pose a reputational risk to the company. With the company only recently having gone public, this risk also amounts to potential financial risk if investors, stakeholders, and customers lose trust in the company.

Recommended Improvements

Considering the vulnerabilities found as well as the risks posed, [redacted] advises TCC to take note of all the technical findings mentioned in the report, as well as the recommended remediations described for the technical findings. To summarize these recommendations and frame them in such a way that should be straightforward for TCC's security engineers to understand, [redacted] has provided the following recommended response plan detailing the time horizon by which the vulnerability should be fixed, the vulnerability in question, along with a summary of the response appropriate when appropriate. Take note that the following summarized response plan is not sufficient alone, and will require greater investigation by the security engineers, or at the least, noting the provided references and detailed response plans in each technical finding.

Recommended Response Plan		
Time Horizon	**Vulnerability**	**Response**
Urgent Mitigation	• Jellyfin Default Admin Access	Remove or restrict the option for users to click on the Jellyfin profile without providing a password.
	• Reward System User Broken Access Control	Hide the source code and modify the code to not allow new customers to gain administrator rights.
	• Reward System Weak Admin Password	Ensure a proper password policy is in place to avoid weak passwords. Follow PCI DSS standards to remain compliant.
	• Reward System Admin API Unauthorized Access	Ensure that each administrator has a unique secret key that has administrative privileges.
	• SMB Users Using No Password	Ensure all SMB accounts have complex passwords and remove or restrict unnecessary accounts.
Within 30 days	• Invoice User Broken Access Control	Ensure that the token contains the level of access that a user should have during the login process.
	• WordPress Weak Admin Password	Ensure that admin accounts are using complex passwords in compliance with PCI DSS standards.
Within 60 days	• Invoice PostgreSQL Injection	Sanitize the input such that SQL injection commands do not work externally.
	• CVE-2021-21311 (Adminer SSRF)	Ensure that the latest, stable version of Adminer is running on the host.
	• Reward Guest No Password	Disable and rename the guest account accordingly.
	• Reward Weak Customer Passwords	Ensure that complex password policies are in place for all users.
When possible	• Payment API Documentation	Keep API information private.
	• SMB Signing Not Required	Enable SMB Message Signing.

	• Publicly Exposed Organizational Chart	Relocate the organizational chart to an internal drive where personnel with the appropriate privileges have access to them.
	• Outdated WordPress Software	Update WordPress to its latest version.
	• Cleartext Windows Password Policies	Disable the policy so that passwords are not stored in cleartext and are encrypted.
	• Windows Defender turned off	Turn on Windows Defender

Aside from the aforementioned recommended responses, [redacted] would also like to add a few more recommendations for strengthening the network security of the company in general. Though the team has not observed the presence or the lack thereof of certain systems, [redacted] recommends the continued implementation of *Single Sign-On (SSO) solutions* for both greater security and convenience to company employees, as well as *Multi-factor Authentication* which would greatly increase the security posture of user accounts and systems involved within TCC's network. Failure to implement multi-factor authentication may expose the company to regulatory risks potentially amounting to significant financial risks.

In moving forward, TCC should also keep its software and services up to date to install the latest security patches. Failure to do so exposes the company to a technical debt amounting to significant strategic risk, as having outdated software and services could potentially evolve into operational risk if exploited.

Final Notes

With TCC being so committed to providing hospitality services to the region in a secure and reliable manner, the regions serviced by TCC may confide in the company to live up to their commitments. [redacted] and its security engineers are proud to offer their services to TCC, and would be glad to offer their services again, should the company require further evaluation of its network after mitigations have been attempted in light of this report.

[redacted] is proud to report that the company has greatly improved its network's cybersecurity within a short period of time. [redacted] is especially pleased to see just how serious TCC is about its cybersecurity standing in seeing that a significant amount of the recommendations provided during the last engagement have been implemented to some degree by the company. [redacted] invested the time to revisit previously exploited vulnerabilities and was pleased to see that the remediation plans have been followed.

Despite this great improvement, it is important that TCC does not grow complacent and, as usual, continue to proactively respond to threats by continuously keeping itself updated on the state of security, and continuing to improve it. To do so, [redacted] urges TCC to heed the technical findings documented in the report along with the recommended responses provided with it. [redacted] is confident in TCC's efforts in applying the remediation plans following the drastic improvements we have seen since our prior engagement. By paying close attention to the vulnerabilities found within the network and by considering the recommended response plans outlined by [redacted] TCC may find itself to be more able in achieving its security and reliability goals.

[redacted] is extremely pleased with TCC's active approach and interest in improving its physical and cyber security measures. The security engineers offer TCC their regards and wish them the best of luck as the company moves forward in securing its infrastructure, and in its mission to provide the best hospitality for its customers, while also keeping security and reliability in mind. [redacted] hopes to conduct business with TCC again in the near future, to provide further services in assessing the company's security and help the company become more secure.

Appendix

APPENDIX A: Network Diagram

During the assessment, the team identified the following hosts, services, and corresponding ports in the TCC internal network, as listed in the figures below:

10.0.0.0/24

10.0.0.2
53 - tcpwrapped

10.0.0.5
53 - domain 88 - kerberos-sec 135 - msrpc 139 - netbios-ssn 389 - ldap 445 - microsoft-ds 464 - kpasswd5 593 - ncacn_http 636 - ldap 3268 - ldap 3269 - ldap 3389 - ms-wbt-server

10.0.0.6
80 - http 135 - msrpc 139 - netbios-ssn 445 - microsoft-ds 3389 - ms-wbt-server

10.0.0.7
22 - ssh 3000 - ppp

10.0.0.11
80 - http 135 - msrpc 139 - netbios-ssn 443 - http 445 - microsoft-ds 3306 - mysql 3389 - ms-wbt-server

10.0.0.12
22 - ssh 80 - http 443 - http 3306 - mysql

10.0.0.20
22 - ssh 80 - http

10.0.0.51
135 - msrpc 139 - netbios-ssn 445 - microsoft-ds 3389 - ms-wbt-server

10.0.0.52
135 - msrpc 139 - netbios-ssn 445 - microsoft-ds 3389 - ms-wbt-server

10.0.0.100
22 - ssh 389 - ldap 636 - ldapssl

10.0.0.52
135 - msrpc 445 - microsoft-ds

10.0.0.100
22 - ssh 80 - http 3306 - mysql

10.0.0.102
22 - ssh 80 - http 443 - http

10.0.0.200
22 - ssh 80 - http 443 - http 8000 - rtsp

10.0.0.210
22 - ssh 5432 - postgresql

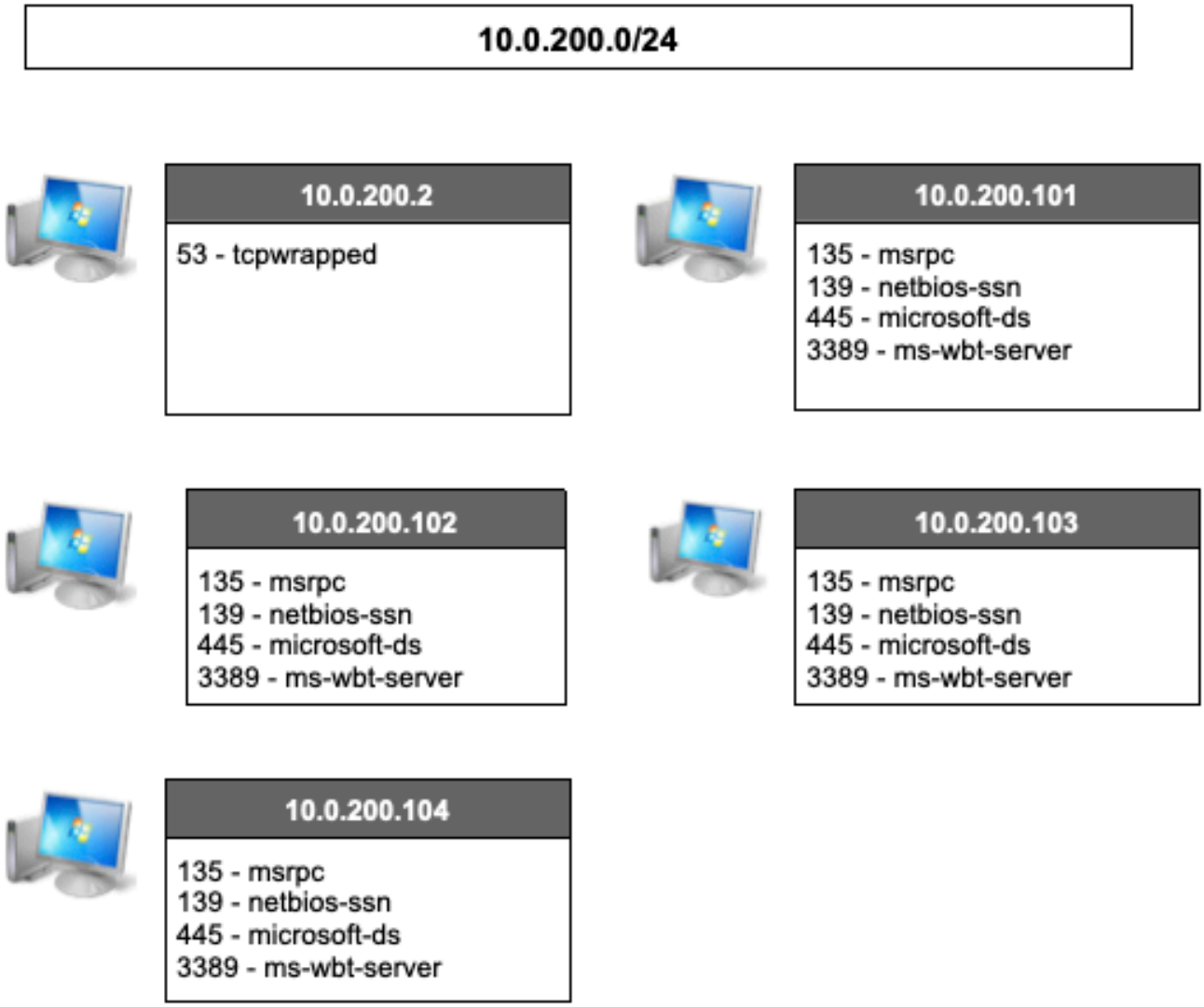
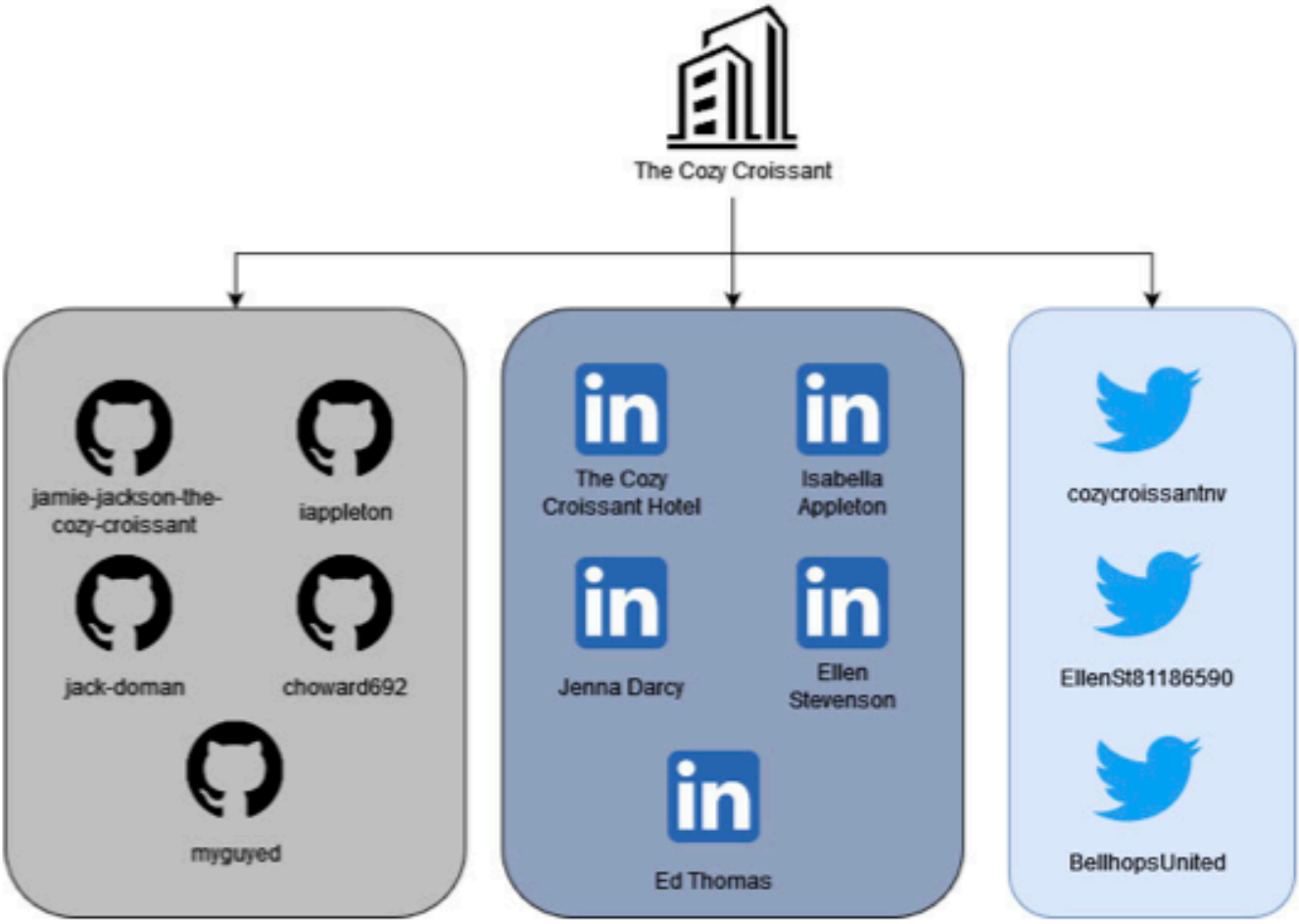


Figure XX: Visualized scan on ports on TCC 10.0.0.0/24 and 10.0.200.0/24 network

Appendix B: Kill Chain Audit

Date	Time	Host(s)	Description
1/13/2022	13:29 EST	10.0.0.12	CVE-2021-21311 (Adminer SSRF)
1/13/2022	13:40 EST	10.0.0.20	Jellyfin Default Admin Access
1/13/2022	14:00 EST	10.0.0.200	Payment API Documentation
1/13/2022	14:30 EST	10.0.0.12	Reward System Weak Admin Password
1/13/2022	14:35 EST	10.0.0.12	Reward System User Broken Access Control
1/13/2022	14:50 EST	10.0.0.12	Reward System Guest No Password
1/13/2022	15:00 EST	10.0.0.12	Reward System Weak Customer Password
1/13/2022	15:41 EST	10.0.0.200	Invoice System User Broken Access Control
1/13/2022	16:00 EST	Unknown TCC Safe Model	Insecure Safe Model
1/13/2022	16:10 EST	10.0.0.200	Invoice PostgreSQL Injection
1/13/2022	16:40 EST	Windows	SMB Signing Not Required
1/14/2022	9:13 EST	10.0.0.12	Reward System Admin API Unauthorized Access
1/14/2022	11:00 EST	10.0.0.11	Outdated WordPress
1/14/2022	11:13 EST	10.0.0.51	Cleartext Windows Password Policies
1/14/2022	11:40 EST	10.0.0.11	WordPress Weak Admin Password
1/14/2022	12:30 EST	10.0.0.51	SMB Users Using No Password
1/14/2022	13:45 EST	Front Desk	Social Engineering Phone Call
1/14/2022	15:02 EST	10.0.0.52	Windows Defender Not Turned On
1/14/2022	15:30 EST	10.0.0.11	CVE-2022-3590 (WordPress Blind SSRF)

Appendix C: OSINT Discovery



Appendix D: Offensive Tools

- Nmap: *https://nmap.org/download.html*
- Burp Suite: *https://portswigger.net/burp*
- Metasploit: *https://www.metasploit.com/*
- Wfuzz: *https://github.com/xmendez/wfuzz*
- CrackMapExec: *https://github.com/byt3bl33d3r/CrackMapExec*
- Hydra: *https://github.com/vanhauser-thc/thc-hydra*
- Seclist: *https://github.com/danielmiessler/SecLists*
- LinPEAS: *https://github.com/carlospolop/PEASS-ng*
- Netcat: Default program
- Impacket *https://github.com/SecureAuthCorp/impacket*

Appendix E: Additional References for Further Improvement

The Prioritized Approach to Pursue PCI DSS Compliance -
https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/Prioritized-Approach-For-PCI-DSS-v4-0.pdf

- The Prioritized Approach provides six security milestones that will help merchants and other organizations incrementally protect against the highest risk factors and escalating threats while on the road to PCI DSS compliance.