

CONFIDENTIAL



THE COZY CROISSANT

PENETRATION TEST REPORT

XXXXXXX-X

January 13-14, 2023

CONFIDENTIAL - TLP : RED

Table of Contents

Table of Contents	1 Confidentiality and Privacy Statement
	2
1. Report Overview	3
1.1. Executive Summary	3
1.2. Assessment Summary	4
1.2.1. Impact findings	4
1.2.2. Vulnerability Source Findings	5
1.2.3. Vulnerability findings summary	5
1.2.4. Remediation Assessment	6
1.2.5. Vulnerability Response Plan	7
1.2.6. Key Security Strengths	8
2. Engagement Overview	9
2.1. Objectives	9
2.2. Scope	10
2.3. Penetration Testing Methodology	14
2.4. Technical Impact Metric	15
2.5. Business Impact Metric	16
2.6. Response Plan	17
3. Attack Narrative	18
3.1. Critical Vulnerabilities	18
3.1.1. JellyFin Media server susceptible to crash and DoS	18
3.2. High Vulnerabilities	20
3.2.1. Exposed Payment API	20
3.2.2. Password reuse of compromised password leading to data breach	22
3.3. Medium Vulnerabilities	24
3.3.1. Insecure PHP Cookies	24
3.3.2. Weak TLS encryption ciphers	25
3.3.3. Logs and Information Exposure	27
3.4. Low Vulnerabilities	28
3.4.1. Hardcoded credentials in exposed source code	28
3.5. Informational Issues	30
3.5.1. Legacy MariaDB version	30
3.5.2. Outdated OpenSSH	30
3.5.3. Expired SSL certificate	30
3.5.4. Exposed X-Powered-By header	30
3.5.5. Unauthenticated Blind SSRF via DNS Rebinding (CVE-2022-3590)	31
3.5.6. LDAP server registration form reveal	31
4. Physical Security Assessment	32
5. Tools and Services	33
5.1. Tools Utilized	34

Confidentiality and Privacy Statement

This document is the exclusive property of The Cozy croissant and XXXXXX-X. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both parties.

- In no event shall XXXXXX-X be liable for the incidental, collateral, or consequential damages that occur out of the use of this information.
- This document and all the information contained within are confidential and proprietary to XXXXXX-X and The Cozy Croissant.

This document contains sensitive information about the computer security environment, practices and current vulnerabilities and weaknesses for the client's security infrastructure. Reproduction or distribution of this document must be approved in writing from the client or from XXXXXX-X.

Legal disclaimer

All information presented throughout this document is provided as-is and without warranty. A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. XXXXXX-X prioritized the assessment to identify the weakest security controls an attacker would exploit. XXXXXX-X recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

1. Report Overview

1.1. Executive Summary

XXXXXX-X was contracted by The Cozy Croissant to conduct a penetration test in order to determine The Cozy Croissant's Exposure and risk to a targeted attack. This assessment was performed on January 13-14, 2023 as a continuation of the initial security assessment performed on [REDACTED]. The scope of engagement encompassed the Network of 10.0.0.0/24 and 10.0.200.0/24. This report documents security evaluation of TCC security infrastructure and the remediations in response to the uncovered vulnerabilities in the initial penetration test. The document also includes steps for remediation of each finding as well as overall business strategies to help improve overall security posture. The figure below summarizes the number of vulnerabilities found and their respective severity risk level.

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
1	2	3	1	6

Many security issues outlined in this report are in violation of the NIST-1800-27, and PIC DSS requirements which establish security baseline and standards for hospitality, consumer personal information and payment operations. **Failing to meet the security requirements specified by NIST-1800-27, PCI DSS could result in incurred fines.**

The Cozy Croissant is a hotel business which employs many public access devices as well as handling customer confidential and private information, as such, it is crucial that The Cozy Croissant operates with vigilance to ensure compliance with NIST-1800-2, PCI DSS as well as maintaining its operations.

Considering the importance of the infrastructure to perform business operations, our offensive security team was careful to adhere to the provided scope with strict standards to avoid disrupting any business operations.

Immediate action to be taken towards critical findings to reduce the possibility of a network compromise that can result in data breach or outage of services.

1.2. Assessment Summary

1.2.1. Impact findings

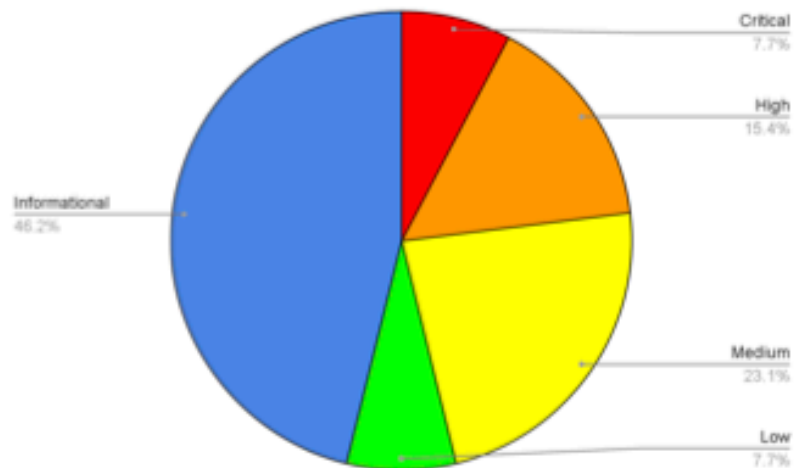


Figure 1 - Composition of impact levels of vulnerabilities

Exposure of private data through compromised machines or networks will not only harm the company's status as an upcoming competitor in the hospitality industry, but incur fines and loss of customer trust. It is vital that high and critical level security threats are dealt with in a timely appropriate manner and urgency.

1.2.2. Vulnerability Source Findings

TCC Penetration Test

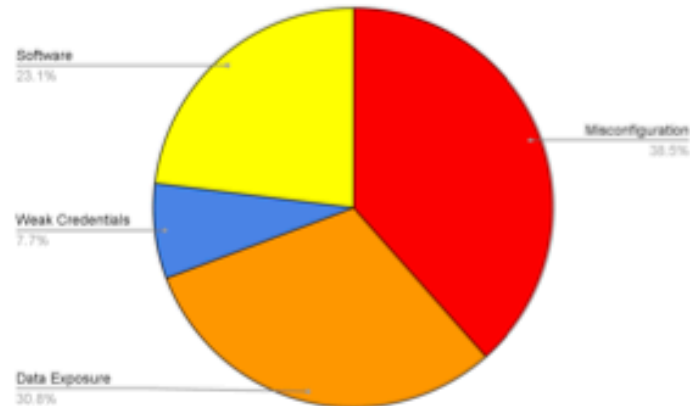


Figure 2 - Composition of source findings

XXXXXX-X defines vulnerability sources across a criteria of 6 categories. Based on the engagement and respective vulnerability findings each vulnerability was categorized to provide further in depth analysis of where security risks lie in TCC infrastructure.

1.2.3. Vulnerability findings summary

The following table summarizes vulnerability findings in the engagement scope of the TCC infrastructure in the two networks.

No.	Description	Host	CVSS	Risk Level
1	JellyFin Media server susceptible to crash and DoS	10.0.0.20	9.5	Critical
2	Exposed Payment API	10.0.0.200	8.3	High
3	Password reuse of compromised password leading to data breach	10.0.0.200	7.5	High
4	Insecure PHP cookies	10.0.0.12	4.2	Medium
5	Weak TLS encryption ciphers	10.0.0.11	4.3	Medium
6	Logs and Information exposure	10.0.0.11, 10.0.0.12	5.3	Medium

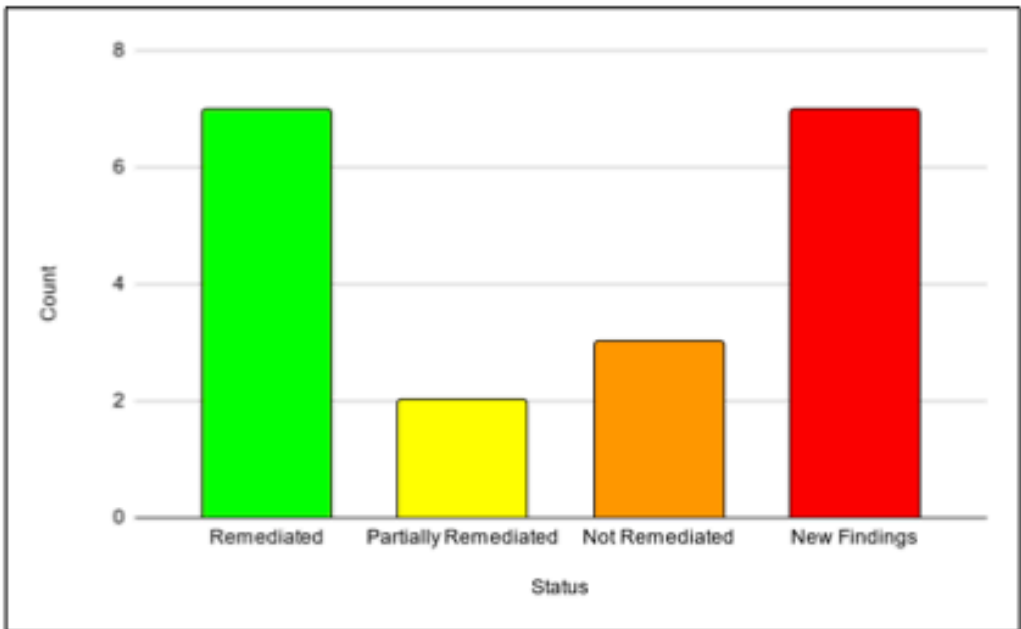
TCC Penetration Test

7	Hardcoded credentials in exposed source code	10.0.0.12	3.9	Low
8	Legacy MariaDB version	10.0.0.11	-	Info.
9	Outdated OpenSSH	10.0.0.12	-	Info.
10	Expired SSL Certificate	10.0.0.11	-	Info.
11	Exposed X-Powered-By Header	10.0.0.12	-	Info.
12	Unauthenticated Blind SSRF via DNS Rebinding (CVE-2022-3590)	10.0.0.11	-	Info.
13	LDAP server registration form reveal	10.0.0.102	-	Info.

1.2.4. Remediation Assessment

XXXXXX-X conducted a retest of the vulnerabilities identified in our initial assessment conducted in [REDACTED]. The above bar graph depicts at a high level the status of

TCC Penetration Test



remediations made based on our previous assessment. In addition to the retest we identified 7 new vulnerabilities.

1.2.5. Vulnerability Response Plan

Based on the prioritization matrix, XXXXXX-X recommends the following response priority plan. The response plan presents a categorized table of which vulnerabilities should be placed as a priority and addressed first based on their technical impact on business operations and likelihood of occurrence. This response plan is the professional opinion based on the varied experience of XXXXXX-X and not a definitive solution.

Mitigation Priority level	Vulnerability
CAT-4	<ul style="list-style-type: none">JellyFin Media server susceptible to crash and DoSExposed Payment APIPassword reuse of compromised password leading to data breach

TCC Penetration Test

CAT-3	<ul style="list-style-type: none">• Insecure PHP Cookies• Weak TLS encryption ciphers• Logs and Information Exposure
CAT-2	<ul style="list-style-type: none">• Hardcoded credentials in exposed source code
CAT-1	<ul style="list-style-type: none">• Legacy MariaDB version• Outdated openSSH• Expired SSL certificate• Exposed X-Powered-By header• Unauthenticated Blind SSRF via DNS Rebinding• LDAP server registration form reveal

1.2.6. Key Security Strengths

Throughout the assessment, XXXXXX-X identified several strong security controls within The Cozy Croissant. These controls should be continually regulated and updated in conjunction with resolving the identified weaknesses in order to bolster the overall security posture of The Cozy Croissant.

Security Control	Description
Network Segmentation	Network segmentation across both tests proved to be efficient. No obvious pivoting opportunities were observed

CONFIDENTIAL - DO NOT DISTRIBUTE

TCC Penetration Test

Strong SSH Security	All ssh services operated with a secure version and standard bruteforcing did not provide access
DNS Zone Security	DNS was configured to refuse DNS zone transfer requests which can be used to obtain additional addresses the DNS points to
Firewall Security and ACL	Very strong configuration of ACL was observed. All services and ports were obfuscated and various scanning techniques proved futile.

2. Engagement Overview

2.1. Objectives

The penetration test was performed on January 13th-14th as a followup assessment to verify security remediations by TCC. In line with the highlighted areas of security interest, XXXXXX-X focused on the following security evaluations:

- Validation of remediation measures by TCC security team in accordance with the previous security assessment and provided remediations for findings.

CONFIDENTIAL - DO NOT DISTRIBUTE

TCC Penetration Test

- Assessment of commercial-of-the-shelf and internally developed application and software packages.
- Assessment of surveillance systems.
- Evaluation of Hotel Management Software Implementation.
- Assessment of Active Directory Environment security controls, policies and configurations.
- Assessment of customer loyalty programs.
- Verification of network segmentation and network pivoting.
- Assessment of public access computing environments.
- Validating Social Engineering training of employees through various phishing techniques and data extraction methods.
- Assessing data privacy and integrity control of customer data.

TCC Penetration Test

2.2. Scope

In accordance with the provided rules of engagement, the scope of the operation consisted of two type-C networks:

10.0.0.0/24 and 10.0.200.0/24 for corporate and guests respectively.

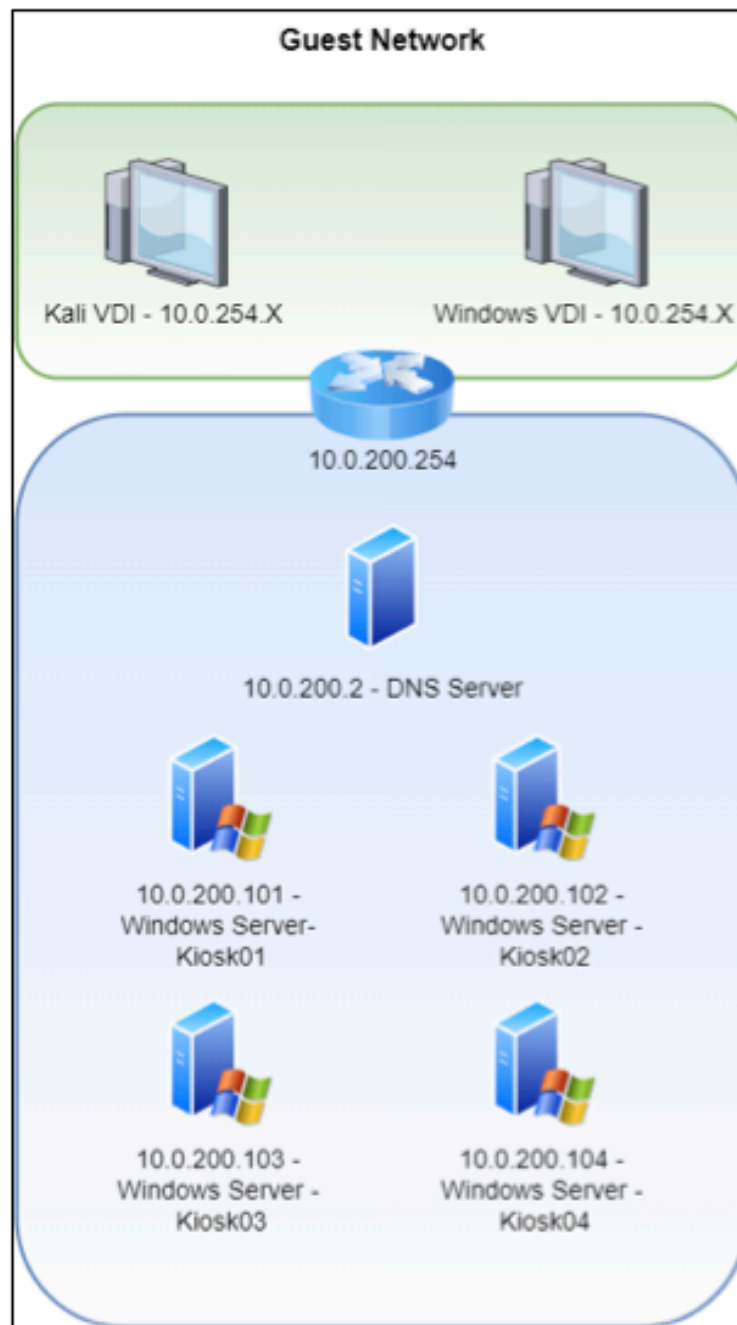
Network Scope	
Network	Type
Corporate 10.0.0.0/24	Type C - Corporate
Guest 10.0.200.0/24	Type C - Guest

Identified hosts in the Corporate Network (10.0.0.0/24)	
10.0.00.2	10.0.00.7
10.0.00.5	10.0.00.11
10.0.00.6	10.0.00.12
10.0.0.20	10.0.0.51
10.0.0.52	10.0.0.100
10.0.0.102	10.0.0.200
10.0.0.210	10.0.0.254

Identified hosts in the Guest Network (10.0.200.0/24)	
10.0.200.2	10.0.200.101
10.0.200.102	10.0.200.103
10.0.200.104	10.0.200.254

2.2.1. Network Topology

The following represents the network topologies of the two provided scopes based on assessment scans.

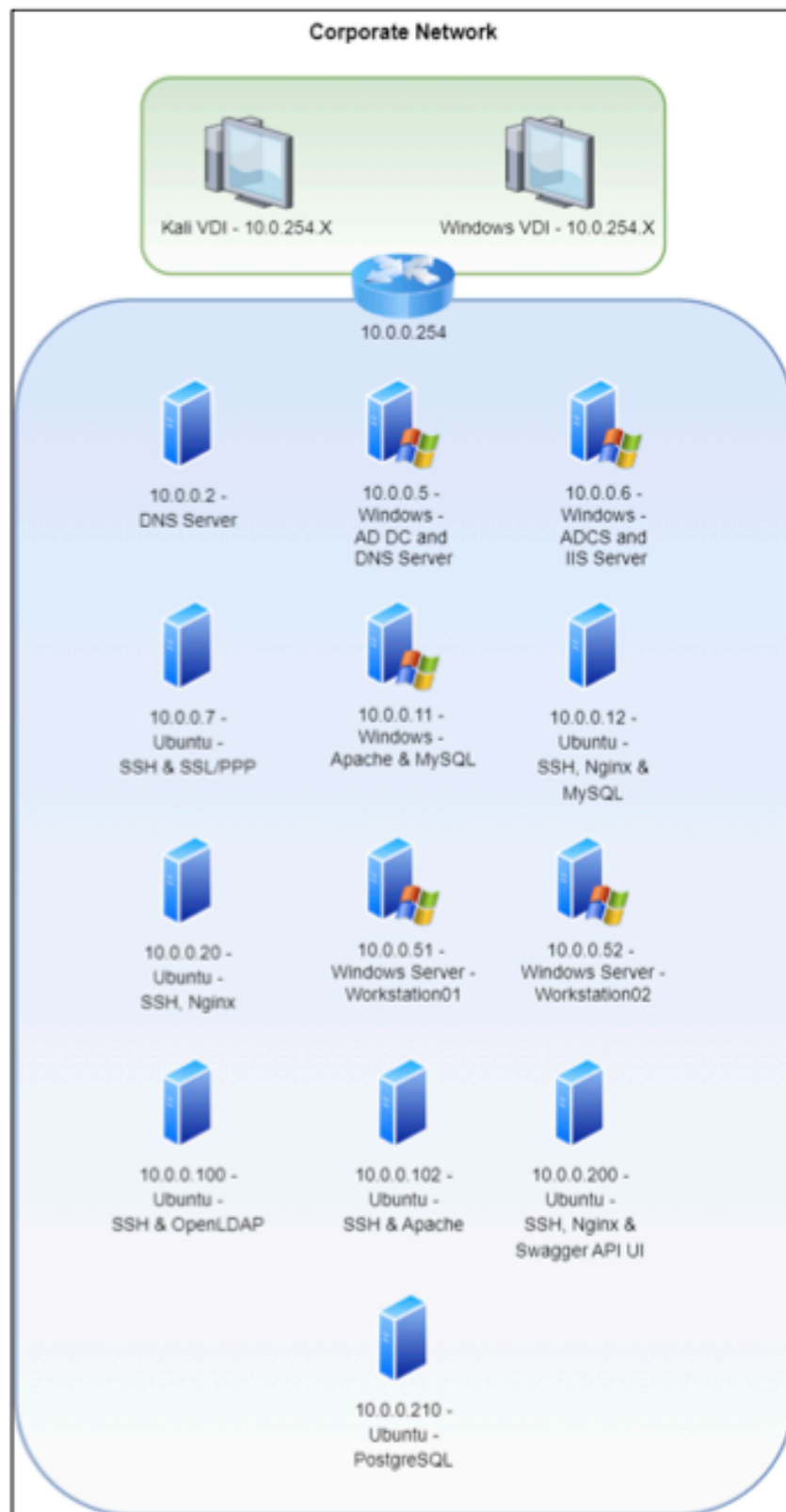


CONFIDENTIAL - DO NOT DISTRIBUTE

TCC Penetration Test

Figure 4 - Mapped Topology for the scope of assessment

TCC Penetration Test



CONFIDENTIAL - DO NOT DISTRIBUTE

TCC Penetration Test

Figure 5 - Mapped Topology for the scope of assessment

2.3. Penetration Testing Methodology

XXXXXX-X will execute the penetration test in accordance with the [National Institute of Standards and Technology \(NIST\) Special Publication 800-115](#). Under the United States Department of Commerce, NIST guides organizations through providing various standard guidelines to follow such as the Information Security Testing and Assessment guide.

NIST 800-115 presents a five step approach for penetration tests: Planning, Discovery, Attack, Additional Discovery and Reporting.

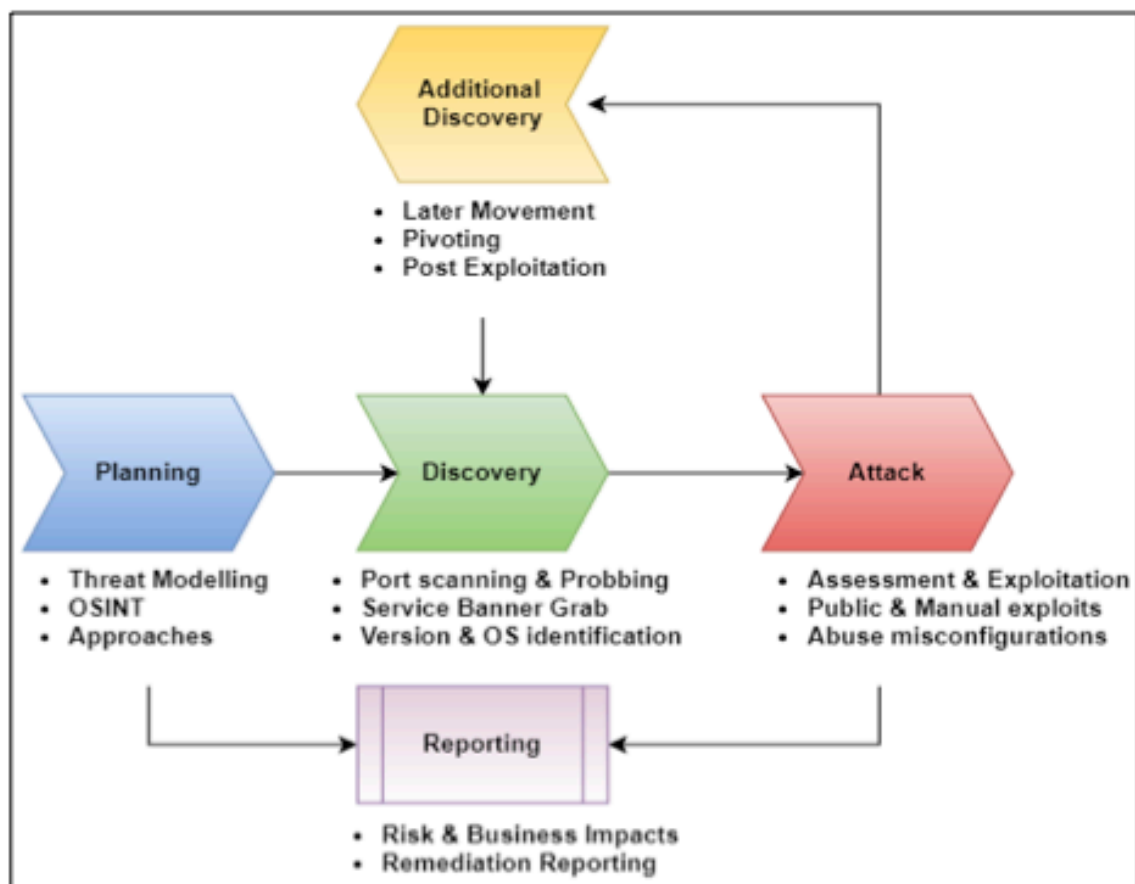


Figure 6 - NIST 800-115, five step approach for penetration tests.

2.4. Technical Impact Metric

For Evaluation of technical impact of discovered vulnerabilities or misconfigurations, XXXXXX-X will utilize the Common Vulnerability Scoring System Version 3.1 which is a universally accepted open NIST standard for evaluation of vulnerability impacts to provide qualitative risk ratings. CVSS measures a vulnerability's impact through accessing the Attack Vector, Complexity, Privileges. User Interaction, Scope, and CIA impact.

The translation of Base Score Rating to a specified Impact level is based upon the NVD NIST guidelines. A CVE string will be provided to its respective vulnerability to provide TCC with further technical context and how the vulnerability was rated. CVSS ratings assigned are based on the collective experience of XXXXXX-X and may not reflect the official assigned score in the NVD.

CVSS Scoring to Impact Severity Level	
Base Score Rating	Impact Level
9.0 - 10.0	Critical
7.0 - 8.9	High
4.0 - 6.9	Medium
0.1 - 3.9	Low
0.0	Informational

2.5. Business Impact Metric

Technical impacts from vulnerabilities translate to business impacts and most often costs. The risk matrix is an industry standard method to determine the risk level from exploiting a given vulnerability and. By considering the likelihood that the exploit occurs and the impact resulting from the exploitation, a severity level can be determined.

In accordance with NIST guidelines for risk assessment specified in NIST Special Publication 800-30 , table I-2 provides a standard for risk matrix evaluation based on likelihood and associated impact from a risk.

LIKELIHOOD	THREAT IMPACT				
	<i>Very Low</i>	<i>Low</i>	<i>Moderate</i>	<i>High</i>	<i>Very High</i>
<i>Very High</i>	V. Low	Low	Moderate	High	Critical
<i>High</i>	V. Low	Low	Moderate	High	Critical
<i>Moderate</i>	V. Low	Low	Moderate	Moderate	High
<i>Low</i>	V. Low	Low	Low	Low	Moderate
<i>Very Low</i>	V. Low	V. Low	V. Low	Low	Low

<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>

2.6. Response Plan

The prioritization metric table provides a simplified outline for clients to prioritize reported vulnerabilities based on several factors. Technical and business impacts are factors for categorization of vulnerabilities and following the priority order in terms of remediation is the most efficient approach.

Remediation Priority	Potential Factors
Category-4 (CAT-4)	<ul style="list-style-type: none"> • High business impact in terms of likelihood and threat impact. • Allows disruption of business operations • Provides access to system or device • Involves private customer information • High CIA factor damage • Data leak or database exposure
Category-3 (CAT-3)	<ul style="list-style-type: none"> • Moderate business impact in terms of likelihood and threat impact. • High tampering with business operations • Partial access to system user • Involves confidential information • Moderate CIA factor damage
Category-2 (CAT-2)	<ul style="list-style-type: none"> • Low business impact in terms of likelihood and threat impact. • Misconfiguration in system which can potentially escalate • Weak passwords, User and device enumeration • Reveal of technical data and system users • Low CIA factor damage
Category-1 (CAT-1)	<ul style="list-style-type: none"> • Very low business impact in terms of likelihood and threat impact. • System secure, but not utilizing latest software versions • No services running, but ports open • Not following best security practices • Unintentional bug or interaction with minor or no security implication

3. Attack Narrative

3.1. Critical Vulnerabilities

3.1.1. JellyFin Media server susceptible to crash and DoS

Status: New Finding		CVSS SCORE	PRIORITIZATION
Risk	Critical	9.5 Critical	CAT-4
Impact	Very High		
Likelihood	High		
CVSS String	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		
Affected Host(s)	10.0.0.20		

Business Impact:

The host 10.0.0.20 maintains the movie service for guests which is essential for the entertainment of the guests. This service contributes heavily to the rating of the establishment and thus, crucial for customer satisfaction and revenue generation. An exploit was discovered where specifying an enormous folder, such as the root of the entire system will overload the server and take it down. This will affect customers, TCC ratings, revenues and overall impact the reputation of TCC at maintaining customer satisfaction.

Details:

TCC Penetration Test

The JellyFin server allows users to provide paths for directories movies are in. While it will only display .MP4 extension files, it still requires scanning the entire directory provided. Given a regular directory with several movies is not an issue. However, attackers can provide the entire filesystem ('/') on the server itself which overloads the service and causes indefinite downtime in a matter of seconds for all users.

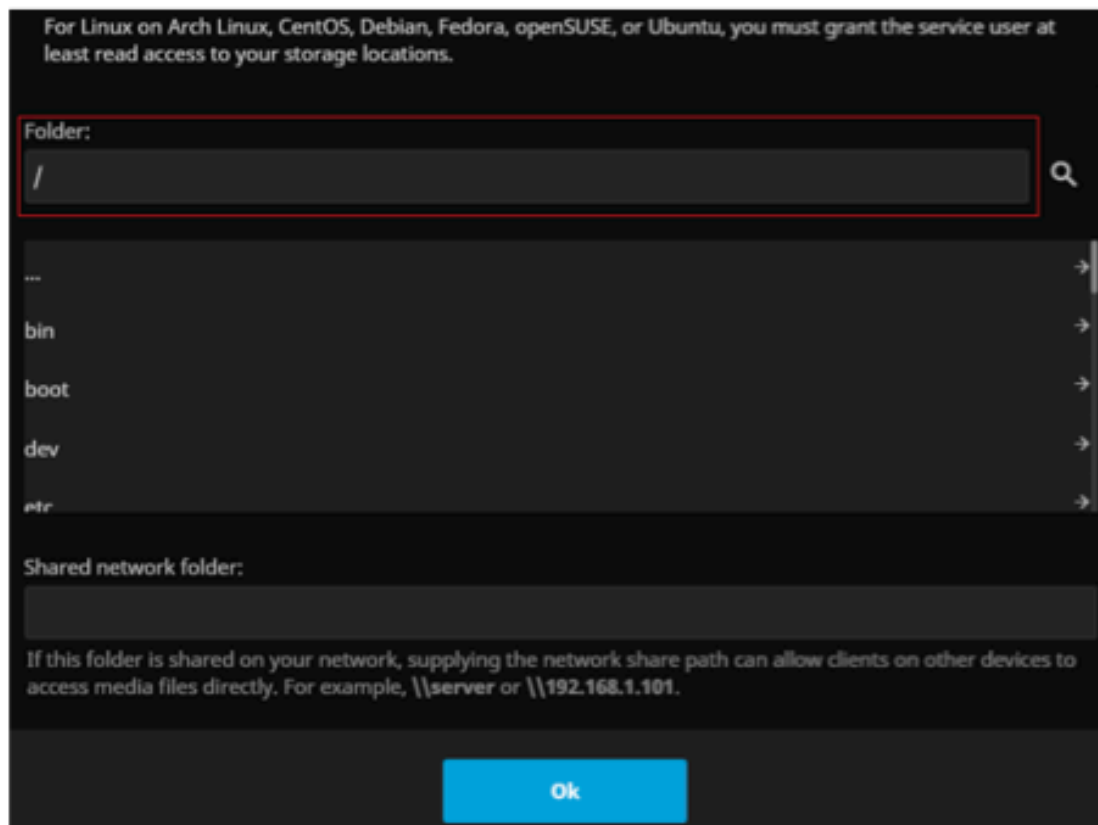


Figure 7 - Dialog box that takes the filesystem to add as a library in the client

Remediation:

1 - Access for JellyFin should be limited to specific immediate directories such that users are not able to specify directories outside the usage scope.

TCC Penetration Test

2 - A size check mechanism can be implemented such that the service will verify the specified directory is within acceptable size in order to avoid overloading.

3 - Upgrade to JellyFin infrastructure to handle DoS situations in order to maintain high availability.

3.2. High Vulnerabilities

3.2.1. Exposed Payment API

Status: New finding		CVSS SCORE	PRIORITIZATION
Risk	Critical	8.3 High	CAT-4
Impact	Very High		
Likelihood	Very High		
CVSS String	AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L		
Affected Host(s)	10.0.0.200		

Business Impact:

The payment API defines the commands that are used to interact with payment data such as billing. For instance, it defines actions such as retrieving all bills, deleting a bill, adding a bill etc. Given this, adversary access to such an API essentially provides them with an instruction set on how to manipulate payment information. Various business impacts can be considered such as disruption of the financial department activities, loss of records, and disclosure of payment information of customers which violates PCI-DSS.

Details:

Directory enumeration of the host 10.0.0.200 revealed the site page /doc#/ on port 8000 run by swagger. The page reveals the payment API which provides REST

CONFIDENTIAL - DO NOT DISTRIBUTE

TCC Penetration Test

commands to interact with the backend. Requests sent can be intercepted and modified to perform various changes to the payment information.

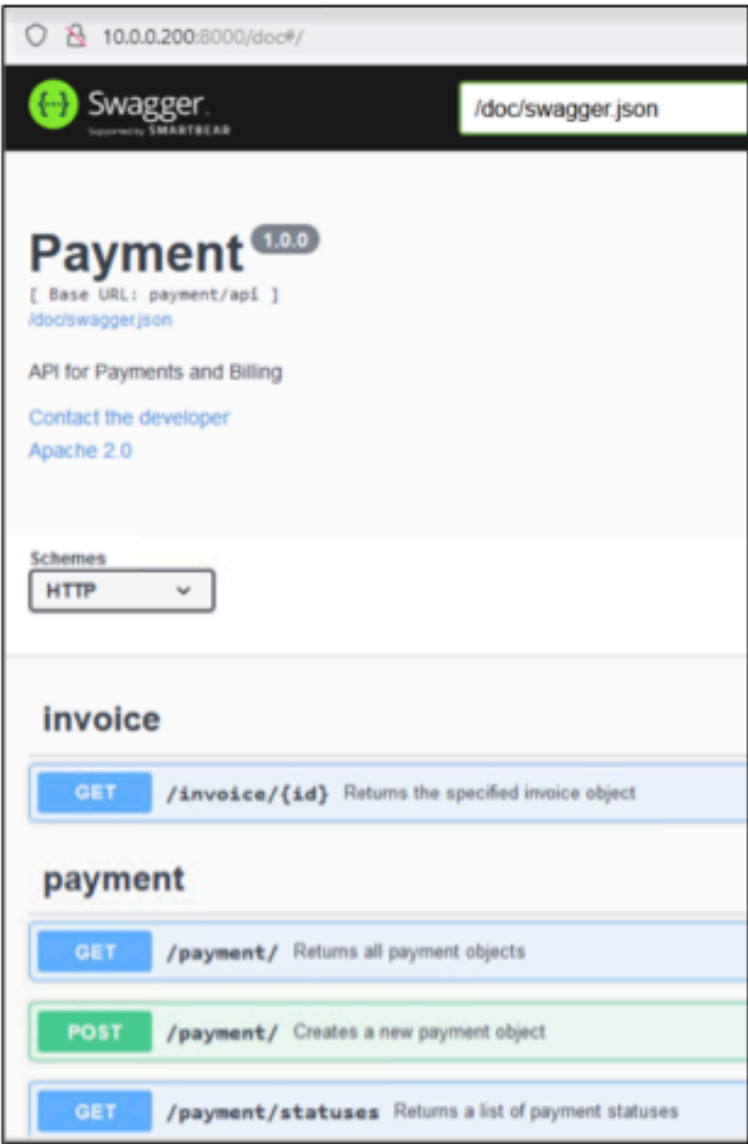


Figure 8 - The API functions observed

CONFIDENTIAL - DO NOT DISTRIBUTE

TCC Penetration Test

Remediations:

1 - Access to swagger UI should be blocked after a web application enters production.

2 - Robots.txt can additionally be used to stop web crawlers from accessing private resources, such as a swagger instance.

3.2.2. Password reuse of compromised password leading to data breach

Status: Partially Remediated		CVSS SCORE	PRIORITIZATION
Risk	Critical	7.5 High	CAT-4
Impact	Very High		
Likelihood	Very High		
CVSS String	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N		
Affected Host(s)	10.0.0.200		

Business Impact:

The host system of 10.0.0.200 maintains various information regarding payments, bookings and reservations, and customer information. Attackers will often reuse compromised passwords as administrators and users don't always change their passwords. Absolute breach of customer privacy is proven in this vulnerability where adversaries are able to view private information about customers. Overall, this results in leak in various data which can result in PCI-DSS violations, fines, as well as legal complications and irreparable reputational damage.

CONFIDENTIAL - DO NOT DISTRIBUTE

TCC Penetration Test

Details:

Social engineering from the previous assessment allowed phishing of the operational manager Aiden Booth. The phishing attempt provided a password which was used to gain admin privileges in the domain controller and various pivoting opportunities. The password was reused again to verify remediation of compromised passwords.

Payment information has become obfuscated since the last engagement. Attackers can no longer view and modify credit card information. However, confidential information including rooms and emails is still visible.

Home	ID	Firstname	Lastname	Email	Checkin	Checkout	Total
Payment Services	1	Leo			Tue, 02 May 2023 00:00:00 GMT	Fri, 05 May 2023 00:00:00 GMT	1136.17
Lookup Payment Status	2	Garry			Sat, 18 Mar 2023 00:00:00 GMT	Sun, 19 Mar 2023 00:00:00 GMT	2021.14
Your Payment Methods	3	Berla			Fri, 26 May 2023 00:00:00 GMT	Thu, 01 Jun 2023 00:00:00 GMT	2388.08
Add Payment Method	4	Israhim			Mon, 12 Jun 2023 00:00:00 GMT	Sat, 17 Jun 2023 00:00:00 GMT	2632.81
Delete Payment Method	5	Barlon			Wed, 31 May 2023 00:00:00 GMT	Mon, 05 Jun 2023 00:00:00 GMT	1871.50
Create and Download Invoices	6	Jennifer			Tue, 15 Aug 2023 00:00:00 GMT	Fri, 18 Aug 2023 00:00:00 GMT	3633.73
Admin							
View All Reservations							
View All Room Details							
Lookup Payment Method							
Logout							

Figure 9 - Using Aiden Booth's login revealed sensitive information of customers

While the operational manager's password was used, it can be assumed that other compromised passwords also face the same issue of remaining unchanged.

Remediations :

TCC Penetration Test

- 1 - Strict password policy must be implemented where the following is applied:
 - Passwords must be at least 8 digits consisting of alphanumerics and special characters.
 - Password change policy must be applied where passwords must be changed every 3 months.
 - Compromised passwords must be changed immediately following any compromise or suspicion of credential leak.
- 2 - Two factor authentication is recommended for additional authentication.

3.3. Medium Vulnerabilities

3.3.1. Insecure PHP Cookies

Status: Unremediated Finding		CVSS SCORE	PRIORITIZATION
Risk	Low	4.2 Medium	CAT-3
Impact	Low		
Likelihood	Medium		
CVSS String	AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N		
Affected Host(s)	10.0.0.12/24		

Business Impact:

Cookies are pieces of information which identify a session between a customer and the TCC hotel websites and web-applications. Cookies are important for session management for users also. Insecure cookies could lead to various attacks including

TCC Penetration Test

XSS which can make the website insecure for usage, thus, having customers opt for other websites which can lead to financial losses and loss of customer loyalty.

Details:

Analysis of communication packets between the VDI and the myRewards site revealed use of insecure cookies which are missing HttpOnly and Secure flags. This means that cookies can be sent over insecure communication which allows interception and inspection of cookies using server side scripts.



Figure 10 - Chrome DevTools shows missing HttpOnly and secure flags

Remediations:

- 1 - Set cookie HttpOnly attribute to prevent JavaScript Document.cookie API accessibility.
- 2 - Set secure attributes to prevent MITM attacks and enable cookies only over encryption.

3.3.2. Weak TLS encryption ciphers

Status: New finding		CVSS SCORE	PRIORITIZATION
Risk	Medium	4.3 Medium	CAT-3
Impact	Medium		
Likelihood	Medium		
CVSS String	AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N		
Affected Host(s)	10.0.0.11		

TCC Penetration Test

Business Impact:

Encryption keys are used to maintain a secure communication line between hosts to preserve confidentiality during transmission. This is especially important when considering rewards, payment, and other financial transactions. Weak encryption could mean adversaries can break the encryption and view financial transactions which can cause financial losses or legal consequences.

Details:

Each ciphersuite is shown with a letter grade (A through F) indicating the strength of the connection. The grade is based on the cryptographic strength of the key exchange and of the stream cipher. Weak ciphers are prone to being attacked by adversaries.

```
(root@ ~)
# nmap -p 443 --script ssl-enum-ciphers 10.0.0.11
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-14 08:26 PST
Nmap scan report for 10.0.0.11
Host is up (0.0052s latency).

PORT      STATE SERVICE
443/tcp   open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - F
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - F
|       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 1024) - F
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - F
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - F
|       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 1024) - F
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 1024) - F
|       TLS_DHE_RSA_WITH_SEED_CBC_SHA (dh 1024) - F
|       TLS_RSA_WITH_SEED_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_IDEA_CBC_SHA (rsa 1024) - F
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher IDEA vulnerable to SWEET32 attack
|       Insecure certificate signature (SHA1), score capped at F
```

Figure 11 - TLS Cipher Key Grading using Nmap

Remediations:

CONFIDENTIAL - DO NOT DISTRIBUTE

TCC Penetration Test

1 - TLS 1.0 and 1.1 maintain very weak cipher keys, as such, clients with connections using TLS 1.0 and 1.1 should not be supported and forced over TLS 1.3 which maintains a cipher key grade of A.

3.3.3. Logs and Information Exposure

Status: Partially Remediated		CVSS SCORE	PRIORITIZATION
Risk	Low	5.3 Medium	CAT-3
Impact	Low		
Likelihood	Very High		
CVSS String	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Affected Host(s)	10.0.0.11, 10.0.12		

Business Impact:

Logs define events and changes of the system which can provide numerous information for administrators to fix the system, but for attackers, can provide information to exploit the system and define its behavior. This may potentially provide enough information for attackers to disrupt business operations and cause monetary loss.

Details:

Web directory scanning revealed several directories open for access. The /doc revealed an index directory which contained various system logs in addition to a to do which defines future implementations to be performed. Such information might be very severe, depending on the information provided in the logs.

CONFIDENTIAL - DO NOT DISTRIBUTE



Figure 12 - Expired Certificate

Remediations:

- 1 - Implementations of access controls on web pages using code based or robots.txt

3.4. Low Vulnerabilities

3.4.1. Hardcoded credentials in exposed source code

Status: Partially Remediated		CVSS SCORE	PRIORITIZATION
Risk	Low	3.9 Low	CAT-2
Impact	Low		
Likelihood	Very High		
CVSS String	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N		
Affected Host(s)	10.0.0.12/24		

Business Impact:

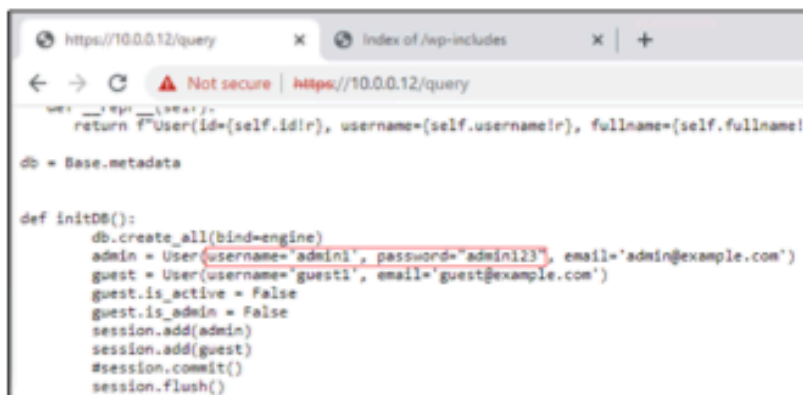
Rewards programs are a great incentive for customers and to maintain a growing loyalty relation between the customer and an organization. The team has identified a rewards portal which allows a customer to scan a QR card to redeem points. An admin/test account was identified in the /query page. If the admin/test account contains a custom amount of points for testing, such as 9999, then an attacker can

TCC Penetration Test

redeem the points to use in various booking which can cause financial loss. This extends even further if many individuals exploited this.

Details:

Web directory enumeration revealed an accessible page /query which contains python source code. Analysis of the code revealed hardcoded default parameters of username and password. The username was then found out to be 'admin' instead of 'admin1' from the previous engagement.



```
return f'User(id={self.id}, username={self.username}, fullname={self.fullname})\n\ndb = Base.metadata\n\ndef initDB():\n    db.create_all(bind=engine)\n    admin = User(username='admin1', password='admin123', email='admin@example.com')\n    guest = User(username='guest1', email='guest@example.com')\n    guest.is_active = False\n    guest.is_admin = False\n    session.add(admin)\n    session.add(guest)\n    session.commit()\n    session.flush()
```

Figure 13a - Admin password leaked in source code.

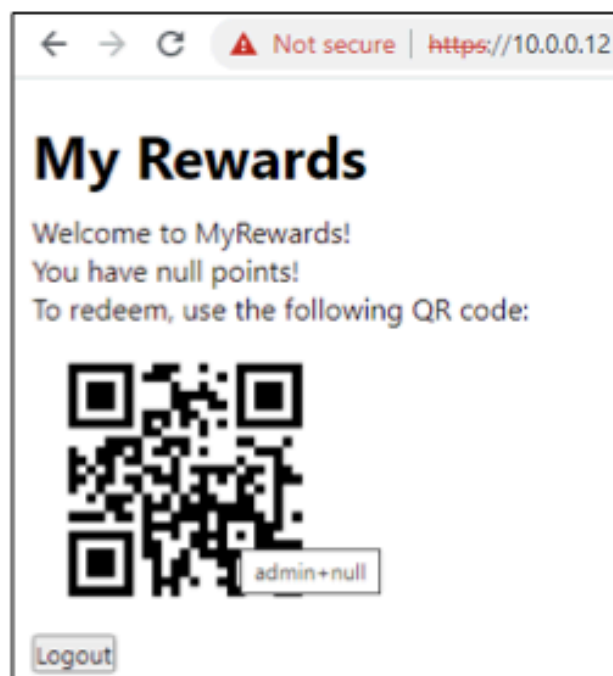


Figure 13b - Access to admin account at MyRewards

TCC Penetration Test

It was found that hovering the QR code does not display the password anymore which protects the account after the login. However, a default admin account is still highly vulnerable.

Remediations:

- 1 - Using any suitable web security measure, such as robots.txt, the /query page which contains the source code should be locked from visitors.
- 2 - Admin account must consist of a much more complex password, preferably 8 alphanumeric characters and inclusion of special characters.
- 3 - Credentials stored as default parameters or variables should be removed from the source code. Use of environment variables can be used instead if default parameters are required to provide code obfuscation.

3.5. Informational Issues

The following highlights issues that do not propose a definite threat, but fall under bugs, non-impactful configurations or cases of not following best security practices

3.5.1. Legacy MariaDB version

MariaDB was identified running on port 3306 on 10.0.0.11 in the corporate network utilizing a non-supported legacy version. We recommended updating to the latest 10.9 release to avoid security implications associated with this release.

3.5.2. Outdated OpenSSH

openSSH version 7.6p1 was identified running on port 22 on 10.0.0.12 with a lower version than the instances running on the other servers which had the version . It is

CONFIDENTIAL - DO NOT DISTRIBUTE

TCC Penetration Test

recommended to update the openSSH in question in order to avoid known potential vulnerabilities associated with this version and maintain consistent version control of software across the system.

3.5.3. Expired SSL certificate

Security certificate in the host 10.0.0.11 has expired since 2018 which results in an insecure connection between the customer and the host machine which can place the customer at possible risk.

3.5.4. Exposed X-Powered-By header

X-powered-by-header is revealed which allows anyone to view what technology the web server is using in terms of a specific PHP version which can be useful for an adversary. It can be disabled by setting `expose_php` to off.

3.5.5. Unauthenticated Blind SSRF via DNS Rebinding (CVE-2022-3590)

The Wordpress website on server 10.0.0.11 is affected by an unauthenticated blind SSRF in the pingback feature. Because of the Time-of-check-to-time-of-use race condition between the validation checks and the HTTP request, attackers can reach internal hosts that are explicitly forbidden. While the version is vulnerable, the exploit may not always execute.

3.5.6. LDAP server registration form reveal

The 10.0.0.102 host machine features a bug where after attempting any login, adding a '?' to the url after receiving a `ldap_bind()` error reveals the registration form.

4. Physical Security Assessment

XXXXXX-X was tasked with performing a physical exploitation of the TCC safes to review the security stature of the safes which will contain valuable items of guests. XXXXXX-X Uncovered two distinct methods to unlock the safe viably.

4.1. Physical Force

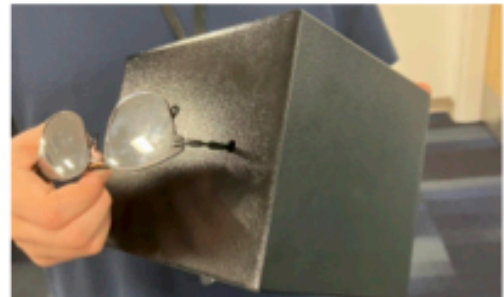
Banging the top of the safe repeatedly while twisting the lock will eventually loosen it up to the point of unlocking the safe without damaging the actual lock mechanism.



TCC Penetration Test

4.2. Reset button backreach

Bottom back of the safe door features a red reset button which allows a user to reset the pin of the lock. While it is conventionally accessible only by having the safe unlocked, two small holes in the back of the safe allow for small objects to pass through. This allows a burglar to reach in and click it to reset the lock, then simply creating a new pin. This provides access to the contents of the safe and also locks out the guest. This was done using sunglasses handles.



5. Tools and Services

In compliance with the Request for Proposal, all tools and services utilized in this engagement were open source, freely available and/or free tier respectively. The following summarized the tools and services used for TCC penetration test assessment.

5.1. Tools Utilized

Tool	Description
nmap	Free and open source utility for network discovery and security auditing.
msfconsole	All-in-one centralized console and allows you efficient access to virtually all of the options available in the MSF

TCC Penetration Test

meterpreter	Meterpreter is a Metasploit attack payload that provides an interactive shell to target a machine and execute code
gobuster	Gobuster is a tool used to brute-force: URIs (directories and files) in web sites.
hydra	Used to brute-force username and password to different services such as ftp, ssh, telnet, MS-SQL
smbclient	Smbclient is a command line tool that is used to communicate with SMB/CIFS servers.
Burp Suite	Used to intercept HTTP traffic and requests to bypass login access
Postman	Api platform used to handle and test functionality of API calls to check the integrity of the backend calls
Chrome DevTools	Inspect webpage source code and web application stored data (eg. cookies)
SQLmap	Automated process to detect and exploit SQL injection
nikto	Comprehensive web server scanning utility for vulnerabilities
nbtscan	Scanning IP networks for NetBIOS name information