CONFIDENTIAL - DO NOT DISTRIBUTE

The Cozy Croissant

Penetration Testing Report

January 13 - 14, 2023

Xxxxxx-xx

Table of Contents

Document Control Information

Document Details	
Company:	The Cozy Croissant
Version:	1.0
Date Last Edited:	January 14, 2023
Authors:	Xxxxxx-xx
Penetration Testers:	Xxxxxx-xx
Classification:	Confidential

Recipients	
Name:	Title:

Jamie Jackson	Technology Director

Executive Summary

Xxxxxx-xx performed a follow-up penetration test on The Cozy Croissant's corporate and guest networks on January 13 - 14, 2023. The penetration test simulated an attack of an internal threat actor attempting to gain access to The Cozy Croissant corporate and guest network systems. The purpose of the penetration test was to discover network strengths, vulnerabilities, and suggest remediation to improve The Cozy Croissant's cybersecurity posture. The consultants also reevaluated the vulnerabilities found during the initial penetration test to help determine the effectiveness of The Cozy Croissant's remediation efforts.

Xxxxxx-xx identified strengths including the use of docker containers, network segmentation, and an updated password policy. These strengths significantly improve security across multiple points of the tested networks. After reevaluating previous findings from the initial penetration test, we identified 1 remediated finding and 3 partially remediated findings.

Xxxxxx-xx identified a total of 22 findings within the scope of engagement, which are broken down by severity in the table below:

Critical	High	Medium	Low	Informational
4	7	5	5	1

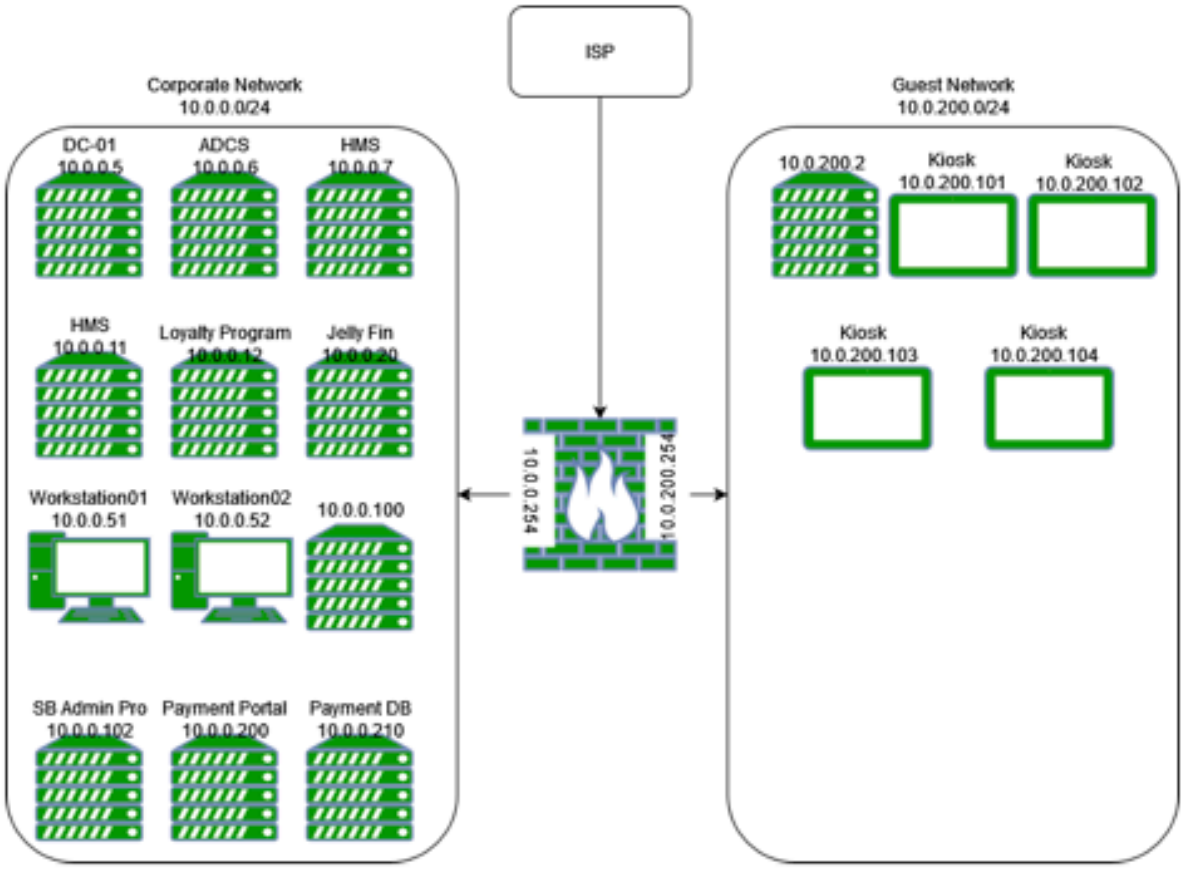
Additionally, Xxxxxx-xx was able to access personally identifiable information (PII) of TCC customers on the Hotel Management System, My Rewards system, and the Payment Portal. The consultants were also able to access payment card information on the Hotel Management System and Payment database. The PII and payment card information found on TCC's networks could be used with malicious intent and lead to reputational damage if it becomes widely known that the information is accessible. The Cozy Croissant could also be found in non-compliance of the General Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI DSS). GDPR non-compliance can result in fines up to €20 million or 4% of TCC's annual revenue and PCI DSS non-compliance can result in fines ranging from $5,000 to $100,000 per month.

Technical Overview

Scope

The scope of this penetration test included The Cozy Croissant's corporate and guest networks. The IP address range of the corporate network was 10.0.0.0/24 and the IP address range of the guest network was 10.0.200.0/24. The scope also included any publicly available information including websites, social media profiles, and GitHub repositories that pertain to The Cozy Croissant.

Network Topology



Key Strengths

I. Docker Containers

- Most applications and services hosted on the linux based services were hosted using Docker containers. This prevents code execution on the applications from affecting underlying systems.

II. Corporate and Guest Network Segmentation

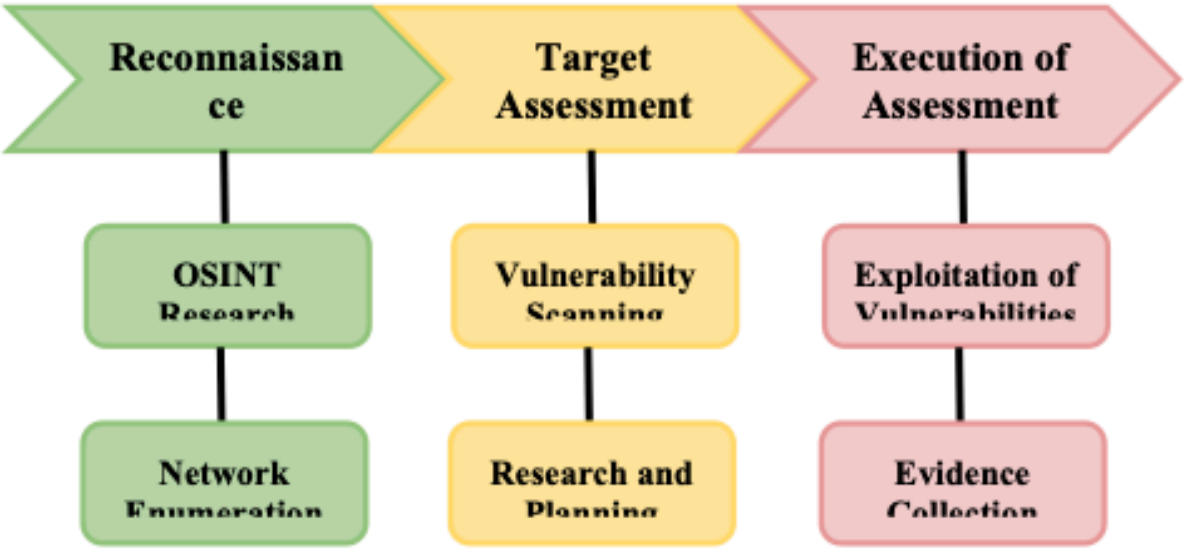
- During Xxxxxx-xx's initial penetration test, the corporate and guest networks were not segmented so users on the guest network could access corporate resources. After the consultants conducted the follow-up penetration test the implementation of network segmentation between the corporate and guest networks was confirmed. Separating the two networks is a beneficial first step in improving the overall security of TCC's networks. Additional network segmentation could be implemented by creating a Kiosk segment and Payment card segment.

III. Updated Domain Password Policies

- During [redacted] initial penetration test, the consultants discovered that there was a weak password policy in place permitting weak passwords. During this retest the domain users' passwords adhered to a much stronger password policy requiring longer, more complex passwords.

Testing Methodology

Xxxxxx-xx's testing methodology had three main phases - reconnaissance, target assessment, and execution of assessment. Reconnaissance involved conducting Open-Source Intelligence (OSINT) research to gather publicly available information about The Cozy Croissant and network enumeration scans to gather information on available hosts and the network topology. The consultants used tools such as Nmap to identify systems and service versions of hosts and applications on the networks. Manual vulnerability scans were also conducted during the target assessment phase. For execution of assessment, the consultants used tools such as Burp Suite, Metasploit, and Hydra. . to find and exploit vulnerabilities. The diagram below shows a visual representation of the testing methodology the consultants followed throughout the penetration test.



Compliance

While conducting the follow-up penetration test of The Cozy Croissant corporate and guest networks, Xxxxxx-xx discovered findings that result in regulatory non-compliance or go against cybersecurity best practices. Some of the findings were found during the consultants initial penetration test, and upon re-evaluation had not yet been remediated. Complying with regulations is crucial to avoid legal and/or financial repercussions and it will help improve the overall security of TCC's networks.

General Data Protection Regulation (GDPR)

During [redacted] initial penetration test, customer's personally identifiable information (PII) was discovered on the Hotel Management System software. After conducting the follow-up penetration test, the consultants found PII on the Hotel Management System, Payment Portal and "My Rewards" database. These systems are accessible on the TCC corporate network at the IP addresses 10.0.0.11, 10.0.0.12, and 10.0.0.200, respectively. The information about customers that was accessible includes: full name, address, postal code, phone number, and email address.

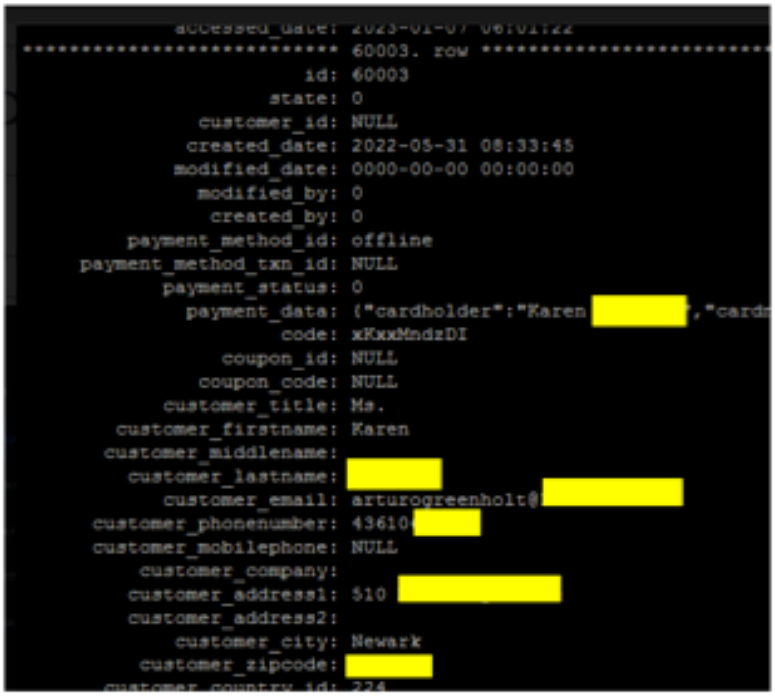


Image Description: PII on Hotel Management System (10.0.0.11)

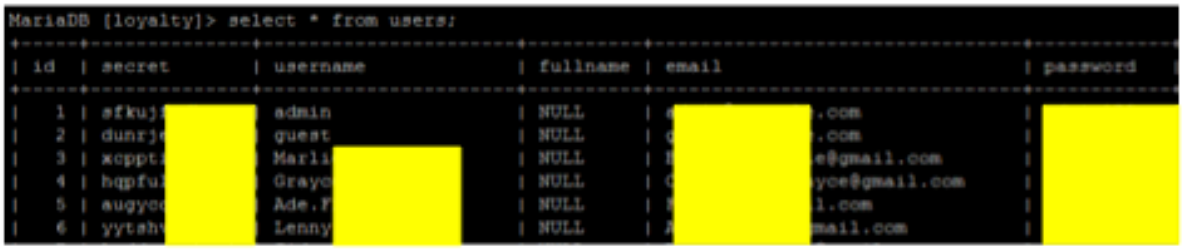


Image Description: PII from TCC My Rewards Database (10.0.0.12)

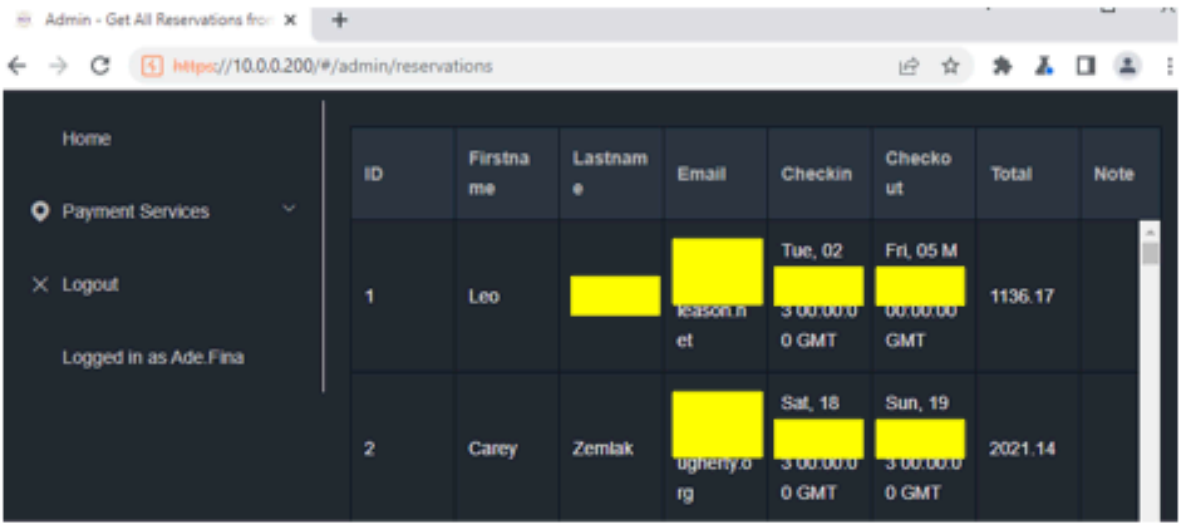


Image Description: PII from TCC Payment Portal (10.0.0.200)

While there are currently not any privacy protection laws in place in the United States, The Cozy Croissant will need to be in compliance with the General Data Protection Regulation (GDPR) created by the European Union (EU) if TCC collects, stores, or processes any personal data about an EU citizen as defined in Article 3 of the GDPR. For example, if an EU citizen travels to Reno, NV and stays at The Cozy Croissant and the company collects, stores, and/or processes their information, then TCC is subject to the GDPR and may face penalties if found in non-compliance. Credit card data was also discovered on the TCC network and is identified as personal data under GDPR. Further information about the credit card data that was found will be discussed in the Payment Card Industry Data Security Standard section.

Less severe GDPR infringements can result in a fine of up to €10 million, or 2% of TCC's annual revenue from the preceding financial year, whichever amount is higher. More serious GDPR infringements can result in a fine of up to €20 million, or 4% of TCC's annual revenue from the preceding financial year, whichever amount is higher. Technically, TCC would only need to comply with GDPR in regards to EU citizen personal data, but it is best practice to apply

the regulation requirements to all personal data collected about any customer. Compliance with GDPR will also help prepare TCC for any privacy laws/regulations that may be passed in the United States in the future. For detailed information about GDPR and the requirements TCC needs to implement, the consultants recommend visiting this site, https://gdpr-info.edu/, to learn more. For a brief overview of the GDPR key requirements found in Article 5, see the table below:

GDPR Key Requirements
Lawfulness, fairness, and transparency
Purpose limitation
Data minimization
Accuracy
Storage limitation
Integrity and Confidentiality
Accountability

References:

GDPR Document - https://gdpr-info.eu/
GDPR Fines - https://gdpr.eu/fines/
GDPR Principles - https://gdpr-info.eu/art-5-gdpr/

Payment Card Industry Data Security Standard (PCI DSS)

During Xxxxxx-xx's initial penetration test, we discovered a PostgreSQL database on the Payment-db host at IP address 10.0.0.210 that was formatted to contain payment information in plaintext. After re-evaluating the network the same PostgreSQL database was discovered to have plaintext credit card information stored on it. Xxxxxx-xx also discovered a second database on the TCC corporate network that contains plaintext credit card information. The second database with credit card information is the MySQL database on the Hotel Management System (HMS) host at IP address 10.0.0.11.

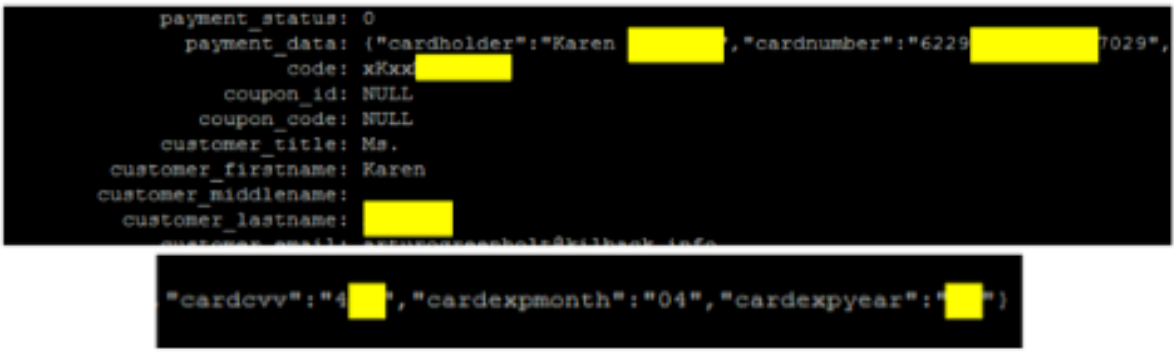


Image Description: Credit Card information on Hotel Management System (10.0.0.11)

Image Description: Credit Card information on Payment Database (10.0.0.210)

The Payment Card Industry Data Security Standard (PCI DSS) is a global standard that is applicable to all entities that store, process, or transmit cardholder data and/or sensitive authentication data. Cardholder data includes the Primary Account Number (PAN), cardholder name, expiration date, and service code. Sensitive authentication data includes full track data (magnetic-stripe data or chip data), card verification code, and PINs/PIN blocks. Since TCC handles credit card information, certain requirements will need to be met to be compliant with PCI DSS. Below are tables outlining the Principal PCI DSS Requirements and PCI DSS account data storage requirements:

Principal PCI DSS Requirements	
1.	Install and Maintain Network Security Controls
2.	Apply Secure Configurations to All System Components
3.	Protect Stored Account Data
4.	Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
5.	Protect All Systems and Networks from Malicious Software
6.	Develop and Maintain Secure Systems and Software
7.	Restrict Access to System Components and Cardholder Data by Business Need to Know
8.	Identify Users and Authenticate Access to System Components
9.	Restrict Physical Access to Cardholder Data
10.	Log and Monitor All Access to System Components and Cardholder Data
11.	Test Security of Systems and Networks Regularly
12.	Support Information Security with Organizational Policies and Programs

PCI DSS Account Data Storage Requirements

	Data Elements	Storage Restrictions	Required to Render Stored Data Unreadable
Cardholder Data	Primary Account Number (PAN)	Storage is kept to a minimum as defined in Requirement 3.2	Yes, as defined in Requirement 3.5
	Cardholder Name	Storage is kept to a minimum as defined in Requirement 3.2	No
	Service Code		
	Expiration Date		
Sensitive Authentication Data	Full track Data	Cannot be stored after authorization as defined in Requirement 3.3.1	Yes, data stored until authorization is complete must be protected with strong cryptography as defined in Requirement 3.3.2
	Card Verification Code		
	PIN/PIN Block		

The network segmentation TCC implemented after [redacted] initial penetration test is a beneficial first step towards improving payment card security. According to PCI DSS, network segmentation/isolation of the Cardholder Data Environment (CDE) from the remainder of an entity's network is not a requirement but it is strongly recommended. Further network segmentation within TCC's corporate network to separate the cardholder data from other corporate resources would improve security of the cardholder data. Segmentation of CDE may reduce the following:

- Scope of the PCI DSS assessment
- Cost of the PCI DSS assessment
- Cost and difficulty of implementing and maintaining PCI DSS controls
- Risk to an organization relative to payment card account data (reduced by consolidating the data into fewer, more controlled locations)

The storage of plaintext Primary Account Numbers (PANs) and Card Verification Codes (CVVs) and the storage of CVVs after authorization in the Hotel Management System database and Payment database is not compliant with PCI DSS storage requirements. The use of acceptable

encryption techniques as outlined in section PCI DSS Requirement 3.5 should be implemented and CVV information should be destroyed after payment authorization. Also, all payment card information should be kept to a minimum to minimize security risks and as part of PCI DSS compliance requirements.

PCI DSS non-compliance can result in fines ranging from $5,000 to $100,000 per month. Therefore, Xxxxxx-xx recommends that TCC ensures the storage, transmission, and/or processing of payment card information anywhere on the TCC network is compliant with PCI DSS. It is important to note that as previously mentioned credit card data is considered personal data under GDPR, therefore the credit card data found on the TCC networks could also be found in non-compliance with GDPR and the fines associated with that could be imposed in addition to PCI DSS fines.

Although PCI DSS is a mandatory regulation, compliance will improve the overall security of TCC's network systems. For detailed information about PCI DSS and the requirements TCC needs to implement, the consultants recommends visiting this site, https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI DSS-v4_0.pdf, to learn more.

References:

PCI DSS v4 - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI DSS-v4_0.pdf
PCI DSS Security Penalties - https://financial.ucsc.edu/pages/security_penalties.aspx
PCI DSS Compliance Guide - https://www.pcicomplianceguide.org/faq/

Social Engineering Assessment

At the request of The Cozy Croissant, Xxxxxx-xx conducted a vishing social engineering assessment. Vishing is the practice of making fraudulent phone calls in an attempt to gain personal or sensitive information. The consultants called the front desk at The Cozy Croissant and pretended to be someone named “John” from the accounting department at Croissant Holdings, LLP. The consultants claimed to be conducting an audit of discrepancies identified in a guest’s account. The target was asked to provide information on the individuals from two different rooms, after giving the target false information regarding the rooms in question, the consultants were provided with the correct guest name. From here the consultants requested the guest credit card information, which the target declined to provide. After which the consultants were able to successfully elicit the guest mailing addresses. The consultants were able to gather the following information about 2 TCC customers from the vishing assessment: first name, last name, phone number, address, and the amount owed to TCC. The information obtained by the consultants is personally identifiable information (PII) and should not be given to anyone unless the individual requesting the information can be properly identified and authenticated and they have authorization to obtain the information. A successful attack could potentially result in monetary and reputational damages.

To help mitigate against similar attacks such as this, users that have access to PII can receive additional training in order to recognize common techniques utilized by attackers, such as vishing, smshing, and phishing. Management should implement policy regarding when and how guest information can be disclosed.

Physical Security Assessment

On January 13, 2023, Xxxxxx-xx was provided a small safe that is under consideration for use behind the front desks and in hotel rooms at TCC. The consultants were tasked with trying to gain access to the safe in as many non-destructive ways as possible. Xxxxxx-xx was provided with a limited set of tools and resources to complete this assessment. On January 13 - 14, 2023 the consultants were able to successfully open the safe using three different methods.

Method 1: Brute Force the Keypad
The keypad had wear markings on the buttons 8, 2 and "Enter". The consultants entered combinations of three numbers containing 8 and 2. On the third input attempt the combination "822" resulted in the safe opening.

Method 2: Reset the Keypad
This safe model includes a red keypad reset button on the door near the hinge. The consultants used a customized tool consisting of a pen cap and a tension wrench to press the reset button through one of the mounting holes on the back of the safe. A review of the safe on Amazon provided information about the reset button. Pictured below is an image containing tools that can be purchased for less than $5 that can be used to perform this attack efficiently.

Image Description: Low cost lockpicking tools.

Method 3: Latch Bypass

After conducting online research about the safe and methods to open it, Xxxxxx-xx found a video demonstrating how bouncing the safe would cause the locking mechanism to fail and the safe to open. To test this, the consultants sat in a chair and bounced the safe on a leg and successfully opened the safe..

Image Description: Yuanshikj Electronic Deluxe Digital Security Safe Box

References:

Safe Box on Amazon (Method 2) - https://www.amazon.com/Yuanshikj-Electronic-Security-Fireproof-Business/dp/B078MYJYD5/ref=asc_df_B078MYJYD5/?tag=hyprod-20&linkCode=df0&hvadid=312060853864&hvpos=&hvnetw=g&hvrand=10990357311933972104&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=2840&hvtargid=pla-568693134129&th=1

Youtube Video of Safe Opening Technique (Method 3) - https://youtu.be/fjrTTlxWTIY

Initial Penetration Test

The January 13 - 14, 2023 penetration test was a follow-up engagement to Xxxxxx-xx's initial penetration test conducted for The Cozy Croissant. The consultants re-evaluated all of the vulnerabilities found during the initial penetration test to provide detailed information about The Cozy Croissant's remediation efforts. Out of the 16 previous findings, 1 finding has been successfully remediated, 3 findings were partially remediated, 7 findings need to be remediated, and 5 findings were not applicable. The table below indicates the remediation status of each vulnerability from the initial engagement. The hosts that were associated with the vulnerabilities classified with the status "Not Applicable" were unavailable during the retest of the network or the service associated with the finding was no longer in use, so the consultants was unable to confirm whether or not the findings had been remediated on The Cozy Croissant networks.

Finding Name	Status	Comments
PostgreSQL Default Credentials	Remediated	Requires password change
Weak Password Policy	Partially Remediated	Domain policy has been modified
Sensitive Data Served Through HTTP	Partially Remediated	N/A
MySQL Passwordless Local Root Login	Partially Remediated	N/A
Username Enumeration	Not Remediated	N/A
Insecure Domain Credential Storage	Not Remediated	N/A
Client Side Authentication and Data Exposure	Not Remediated	N/A

SMB Signing Disabled	Not Remediated	N/A
LM LAN Manager Network Authentication is Enabled	Not Remediated	N/A
PetitPotam to ADCS Relay Attack Vector	Not Remediated	N/A
Windows Systems Missing Critical Security Updates	Not Remediated	N/A
phpLDAPadmin LDAP Injection Vulnerability CVE-2018-12689	Not Applicable	N/A
Unauthenticated Access to Client Credit Card Webpage	Not Applicable	N/A
Unauthenticated Access to Hotel Management System	Not Applicable	The HMS software that was in use during [redacted] initial engagement was replaced with a different software.
Weak or Default Credentials on phpLDAPadmin Page	Not Applicable	The 10.0.0.101 IP address that the findings was on during [redacted] initial engagement was no longer accessible.
Verbose Error Page Versioning	Not Applicable	The HMS software on 10.0.0.11 was no longer accessible by web browser.

Technical Assessment Findings

Classification definitions and scales for risk score, exploitation likelihood, business impact, and remediation difficulty can be found in Appendix A.

Summary of Findings

Critical	High	Medium	Low	Informational
4	7	5	5	1

Number	Finding	Risk Level
1	Default / Weak Credentials	Critical
2	PetitPotam to ADCS Relay Attack Vector	Critical
3	Unsecure Credential Storage Method on Domain Controller	Critical

4	SQL Injection	Critical
5	Global Administrative User Password Reuse	High
6	Client Side Data Disclosure in LPS Service	High
7	Privilege Escalation	High
8	Authenticated Remote Code Execution	High
9	SMB Signing Disabled	High
10	Insecure Direct Object Reference	Medium
11	Verbose Error Disclosure	Medium
12	Network Segmentation	Medium
13	Broken Web Access Control	Medium
15	LPS API Cross Client Enumeration	Medium
16	Publicly Available Configs and Logs	Medium
17	Web server does not use HTTPS	Low
18	Unauthenticated Environment Variable Disclosure	Low
19	Source Code Disclosure	Low
20	Self Signed Certificates	Low
21	Username Enumeration	Low
22	Payment Portal Password Policy	Informational

Critical Findings

1. Default / Weak Credentials

Affected Host(s) Information:

Host Name	IP Address	Port	Service
kiosk01	10.0.200.101	445	smb
kiosk02	10.0.200.102	445	smb
kiosk03	10.0.200.103	445	smb
kiosk04	10.0.200.104	445	smb
hms	10.0.0.11	80, 443, 3306	http, mysql
lps	10.0.0.12	80, 443, 3306	http, mysql
profiler	10.0.0.102	80, 443	http
payment-db	10.0.0.210	5432	postgresql
media	10.0.0.20	80, 8096	http

Classifications:

Risk Score	10/10
Exploitation Likelihood	High
Business Impact	Severe
Remediation Difficulty	Easy

Description:
Default / weak credentials were found in the environment. This includes cases where the default password has not been changed or has been changed but is still weak. The passwords found could also have been found in lists of commonly used / breached passwords.

Affected accounts:
kiosk01-04:

- Administrator (Windows)

hms

- Admin (WordPress)
- Root (mysql)

lps

- Admin (My Rewards)
- Root (mysql)

profiler

- cn=admin,dc=cozycroissant,dc=com (ldap)

payment-db

- Postgres (postgresql)

media

- Jellyfin (Jellyfin)

Steps To Reproduce:
The services listed were sprayed with common passwords using tools like Hydra and Crackmapexec. The red team was able to log in to accounts with weak / default passwords.

Remediation Recommendation(s):
Change weak / default passwords for affected accounts.

Business Impact:

If the accounts affected are used for management or administrative purposes, malicious attackers can disrupt business operations, exfiltrate sensitive data, and/or gain complete control over systems. In the cases where the accounts are users, attackers can gain a foothold to systems.

References:
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/02-Testing_for_Default_Credentials

2. PetitPotam to ADCS Relay Attack Vector

Affected Host(s) Information:

Host Name	IP Address	Port	Service
DC01, ADCS	10.0.0.5, 10.0.0.6	N/A	Windows Server 2016

Classifications:

Risk Score	9/10
Exploitation Likelihood	Possible
Business Impact	Severe
Remediation Difficulty	Hard

Description:
This attack vector allows an attacker to abuse Windows encrypted storage services to provoke the domain machine account DC01$ to authenticate to an attacker controlled computer. The attacker will then relay the authentication attempt to the ADCS server to register a certificate for the account, which can be used to impersonate the DC01$ account to extract sensitive domain credentials from the domain controller.

Steps To Reproduce:
Using the Petitpotam tool (https://github.com/topotam/PetitPotam) it is possible to provoke an authentication attempt from the DC01 to a computer. Then using the impacket ntlmrelayx tool it is possible to request a certificate from the ADCS server. After obtaining the certificate, using the tool PKINITtools (https://github.com/dirkjanm/PKINITtools) it is possible to request a TGT ticket for DC01$ and exfiltrate secrets from the domain controller.

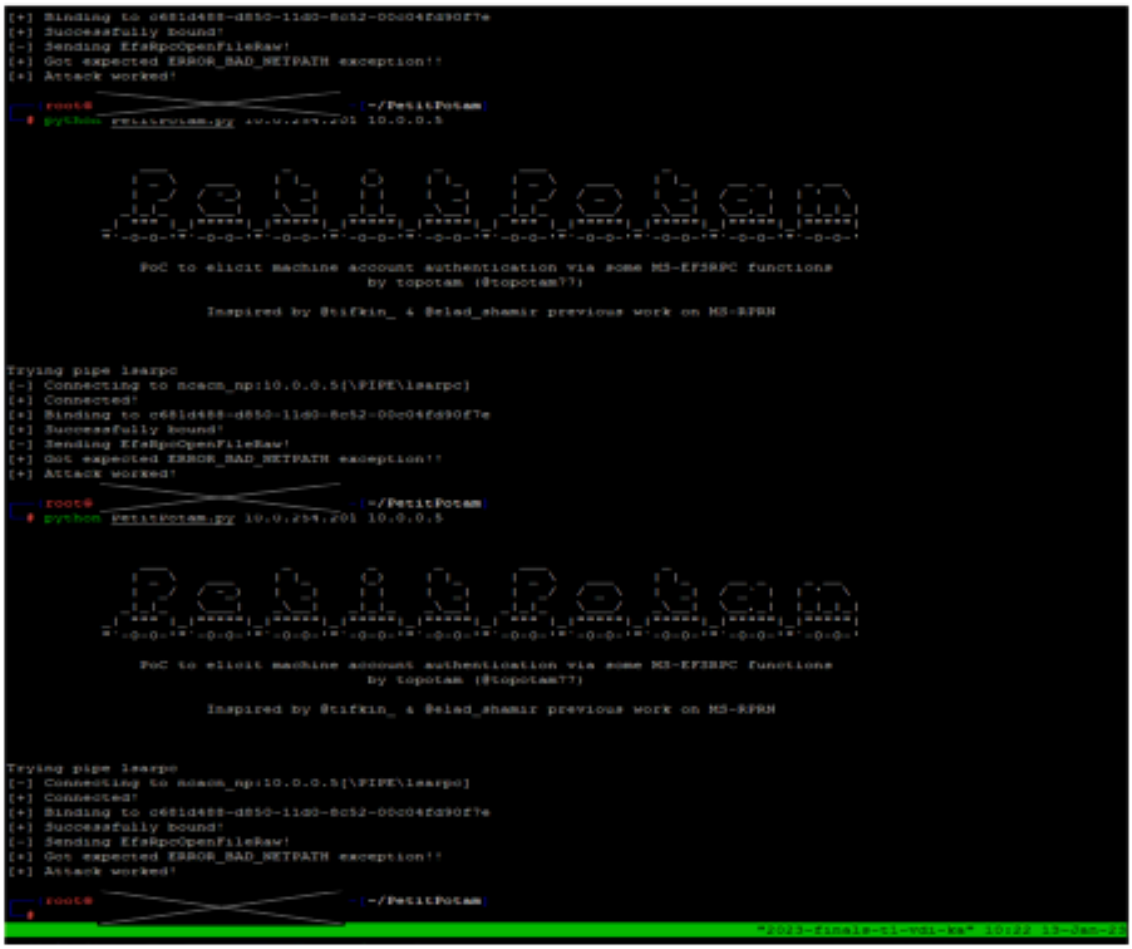


Image Description: Successfully exploiting the PetitPotam attack vector on DC01.

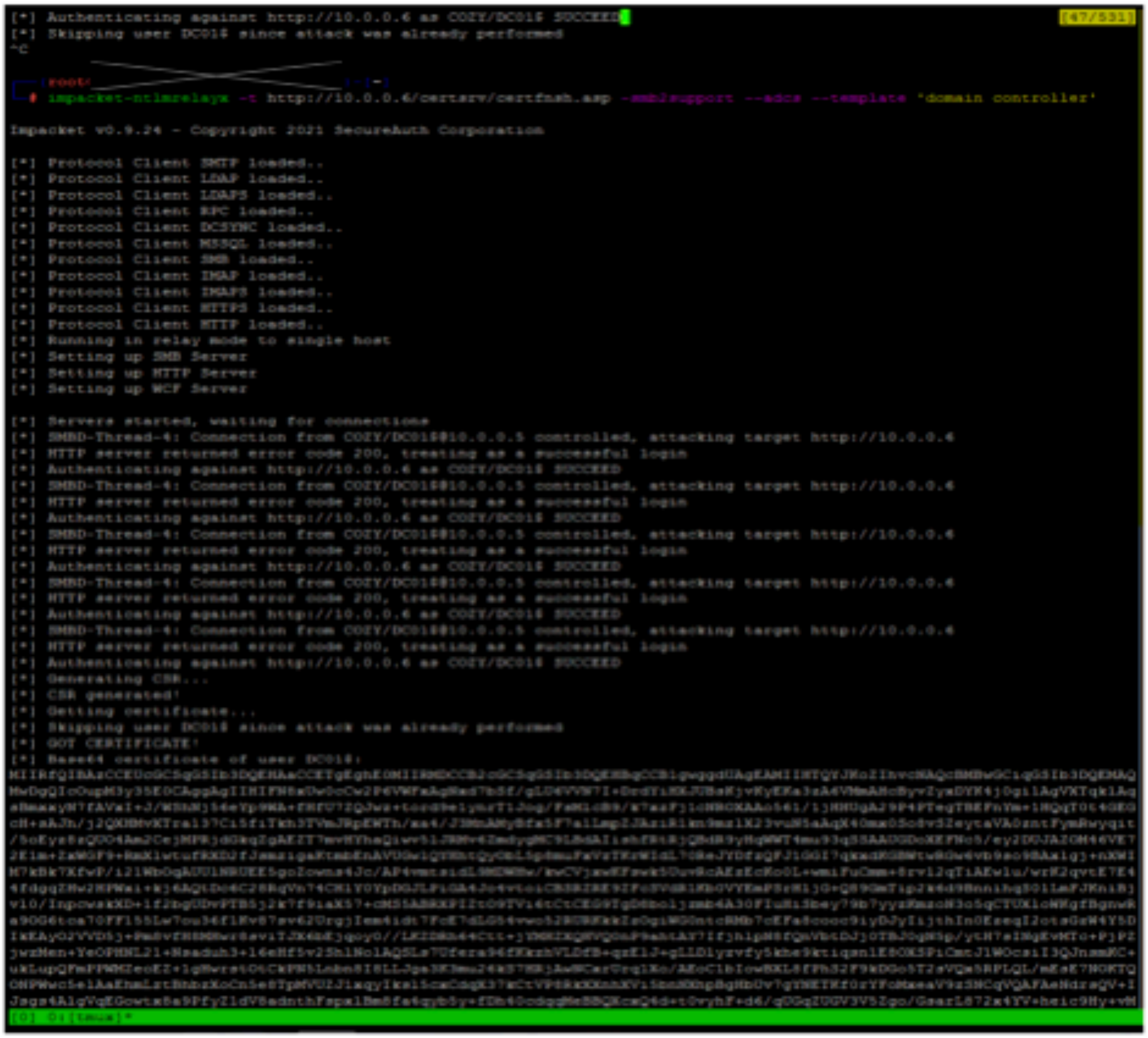


Image Description: Relaying the DC01$ account authentication to ADCS to register for a certificate.

Remediation Recommendation(s):

It is recommended to disable the "Encrypting File System Remote Protocol" if it is not required on the domain controller. Additionally, require SMB signing and https on the ADCS server to prevent authentication forwarding. This can be done by enabling the SMB signing option in the windows administrative tools panel and generating a certificate and enabling HTTPS in the Windows Admin Center for the ADCS service.

Business Impact:

In the event an attacker extracts all domain credentials from the domain controller, The Cozy Croissant could experience widespread issues throughout the network. An attacker may be able

to gain access to PII including credit card information, and guest information by impersonating employees with their credentials.

References:

https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429
https://learn.microsoft.com/en-us/security-updates/SecurityAdvisories/2009/974926

3. Unsecure Credential Storage Method on Domain Controller

Affected Host(s) Information:

Host Name	IP Address	Port	Service
DC01	10.0.0.5	N/A	Windows Server 2016

Classifications:

Risk Score	9/10
Exploitation Likelihood	Possible
Business Impact	Severe
Remediation Difficulty	Medium

Description:

1) The corporation's user credentials are stored in cleartext on the domain controller.
2) The corporation's user credentials are stored using a cryptographically broken hashing algorithm (LANMAN) which is always crackable with modern technology.
3) The corporation's user credentials are stored in the user description exposing the password to anyone with access to their description.

Steps To Reproduce:

1-2) Using a tool such as crackmapexec it is possible to extract domain credentials.

"crackmapexec smb 10.0.0.6 -u 'admin-user' -p 'password' --ntds"

This command will extract domain credentials in the format LANMAN:NTLM. If the LANMAN portion is populated with a value other than "aad3b435b51404eeaad3b435b51404ee", then that account is vulnerable to having their password exposed. If the account's password is present in cleartext, then their password is stored in cleartext separate from the hash.
3) To check the user descriptions you can navigate to the user administration panel on DC01's server administration panel. Then it is possible to view each user's description by opening their properties menu.

Remediation Recommendation(s):

To remediate this vulnerability, the domain policy will have to be modified to prevent LM hashing.

1. Start Registry Editor (Regedt32.exe).

2. Locate and then select the following key:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`

3. On the **Edit** menu, click **Add Key**, type `NoLMHash`, and then press Enter.

4. Exit Registry Editor.

5. Restart the computer, and then change your password to make the setting active.

Image Description: Instructions for LM hashing remediation.

Key Location: "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa"
Value: "NoLMHash"

Run "gpedit.msc".

Navigate to Local Computer Policy >> Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy.

If the value for "Store password using reversible encryption" is not set to "Disabled", this is a finding.

Business Impact:
Storing passwords in clear text or with LM hashing allows an attacker to further compromise the users and services in the network by reusing the passwords to masquerade as each user.

References:
https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/prevent-windows-store-lm-hash-password
https://www.stigviewer.com/stig/windows_10/2019-01-04/finding/V-63429

4. SQL Injection

Affected Host(s) Information:

Host Name	IP Address	Port	Service

payment-web	10.0.0.200	80, 443	http

Classifications:

Risk Score	10/10
Exploitation Likelihood	Likely
Business Impact	Severe
Remediation Difficulty	Medium

Description:

The affected host is vulnerable to SQL injection. SQL injection enables an attacker to insert unchecked or poorly checked SQL code into various user-controlled inputs in the application. This can allow attackers to view and tamper with the underlying database and potentially execute code and compromise systems.

Steps To Reproduce:

The following HTTP request to the payment API endpoint resulted in credit card and PII data exfiltration from the backend database:

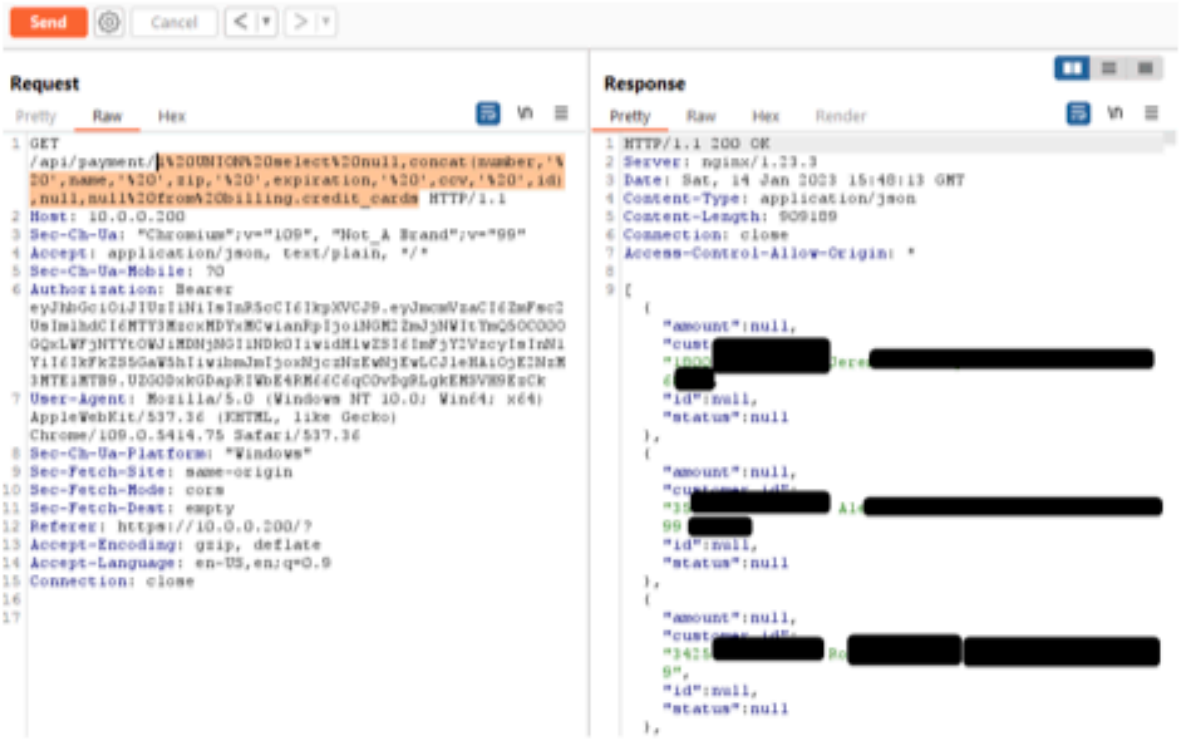


Image Description: Burp showing SQL injection on /api/payment

Remediation Recommendation(s):
SQL injection can be mitigated by using prepared statements, parameterized queries, or stored procedures. These methods ensure that user-supplied input is properly sanitized and cannot be used to modify the intended SQL query. Additionally, using the latest version of a database management system that has built-in protection against SQL injection can also help.

Business Impact:
SQL injection can enable attackers to exfiltrate sensitive information, including personal data and / or financial information. Attackers can also potentially execute statements that allow unauthorized access to the system, causing disruptions.

References:
https://owasp.org/www-community/attacks/SQL_Injection
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

High Findings

5. Global Administrative User Password Reuse

Affected Host(s) Information:

Host Name	IP Address	Port	Service
DC01	10.0.0.5	445	SMB
ADCS	10.0.0.6	445	SSH
DOAPI	10.0.0.7	22	SSH
HMS	10.0.0.11	22	SSH
LPS	10.0.0.12	22	SSH
MEDIA	10.0.0.20	22	SSH
WORKSTATION01	10.0.0.51	445	SMB
WORKSTATION02	10.0.0.52	445	SMB
LDAP	10.0.0.100	22	SSH
PROFILER	10.0.0.102	22	SMB

PAYMENT-WEB	10.0.0.200	22	SMB
PAYMENT-DB	10.0.0.210	22	SMB
KIOSK01	10.0.200.101	445	SMB
KIOSK02	10.0.200.102	445	SMB
KIOSK03	10.0.200.103	445	SMB
KIOSK04	10.0.200.104	445	SMB

Classifications:

Risk Score	8/10
Exploitation Likelihood	Likely
Business Impact	Severe
Remediation Difficulty	Easy

Description:
A sensitive cleartext password was found stored in the lsass process on the ADCS server due to its use in authenticating as a service. In the guest network, the Administrative password was discovered to be blank.

Affected Users: “corp.cc.local\Administrator”, Administrator (Local) for all kiosks “corp.cc.local\Administrator” is reused for the root account on linux hosts, 10.0.0.12, 10.0.0.20, 10.0.0.100, 10.0.0.102, 10.0.0.200, 10.0.0.210

Steps To Reproduce:
Using a tool such as crackmapexec, it is possible to extract credentials stored in memory with a command such as "crackmapexec smb 10.0.0.6 -u 'admin-user' -p 'password' --lsa". This credential pair can be used to authenticate to multiple hosts locally across the domain and in the linux server systems.

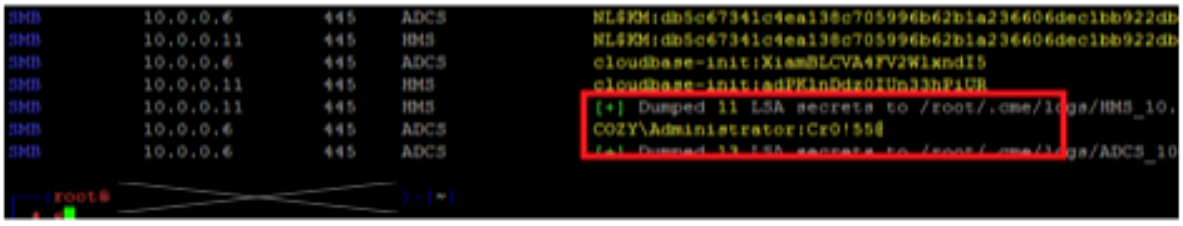


Image Description: Administrator account credentials are stored in clear-text.

Remediation Recommendation(s):
It is recommended that local administrative passwords be unique for each machine to limit the impact of a leaked or compromised administrative password on the company. In order to keep track of these local passwords it is important to use a secure password manager to generate and store credentials.

For the linux machines listed above it is recommended that the root account password be changed to be unique.

"passwd root"

Business Impact:
If the credentials for the "corp.cc.local\Administrator" account is compromised in the domain the attacker will also have access to all of the other systems in the environment that reuse that password.

References:
https://blog.1password.com/how-to-protect-yourself-from-password-reuse-attacks/

6. Client Side Data Disclosure in LPS Service

Affected Host(s) Information:

Host Name	IP Address	Port	Service
lps.corps.cc.local	10.0.0.12	80	My Rewards

Classifications:

Risk Score	7/10
Exploitation Likelihood	Likely
Business Impact	Moderate
Remediation Difficulty	Hard

Description:
This vulnerability allows an attacker to view login information for multiple users in The Cozy Croissant's "My Rewards" program. In its current implementation, this page insecurely handles

authentication and allows an unauthenticated user to view login information from registered users.

Steps To Reproduce:

Intercept a login request using a known username through Burp Suite and send it to Repeater. The response to this request will contain the correct login information of the user regardless of the accuracy of the login password initially provided.

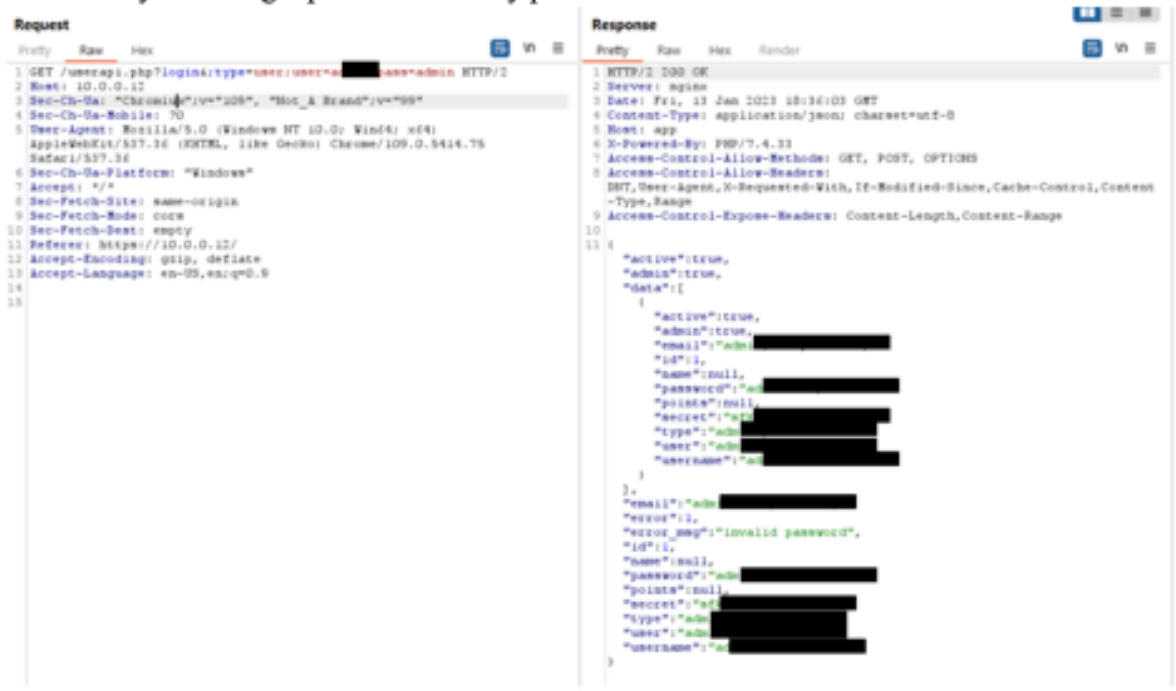


Image Description: Burp Suite proxy request and response capture

After logging in, the default query to the user API returns a JSON containing sensitive data for all users in the system.

Image Description: Burp Suite proxy request and response capture

Remediation Recommendation(s):
Do not send data containing sensitive information to the client in the responses, where Burp Suite or similar proxy tools can intercept them. Instead, process the data only on the server side to prevent information leaks.

Business Impact:
A malicious user could gain access to all the information from the site, including the login information/credentials of other users. Therefore, a malicious user could impersonate other users within the My Rewards program. This could lead to customers not being able to trust the program and stop using it.

References:
https://portswigger.net/web-security/information-disclosure

7. Privilege Escalation

Affected Host(s) Information:

Host Name	IP Address	Port	Service
payment-web	10.0.0.200	443	Nginx Web Server

Classifications:

Risk Score	8/10
Exploitation Likelihood	Likely
Business Impact	Moderate
Remediation Difficulty	Medium

Description:
An attacker can modify the user cookie to set their role as admin which allows the attacker to view all reservations, room details, and other PII. This is because the server trusts the cookie that the user can modify without validating no tampering has occurred.

Steps To Reproduce:
Navigate to the Login page on 10.0.0.200, then log in to a regular user account. Then open the browser developer tools. From there find the browser cookie located in the local storage section and modify the value of the role field to 'admin'. Refresh the page and from here the low privileged user now has access to the administrative section of the payment portal.

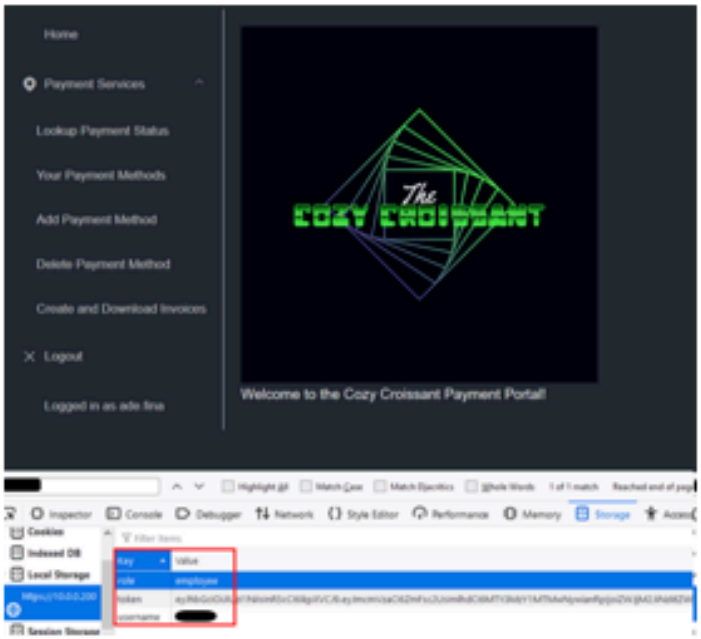


Image Description: user cookie at default value

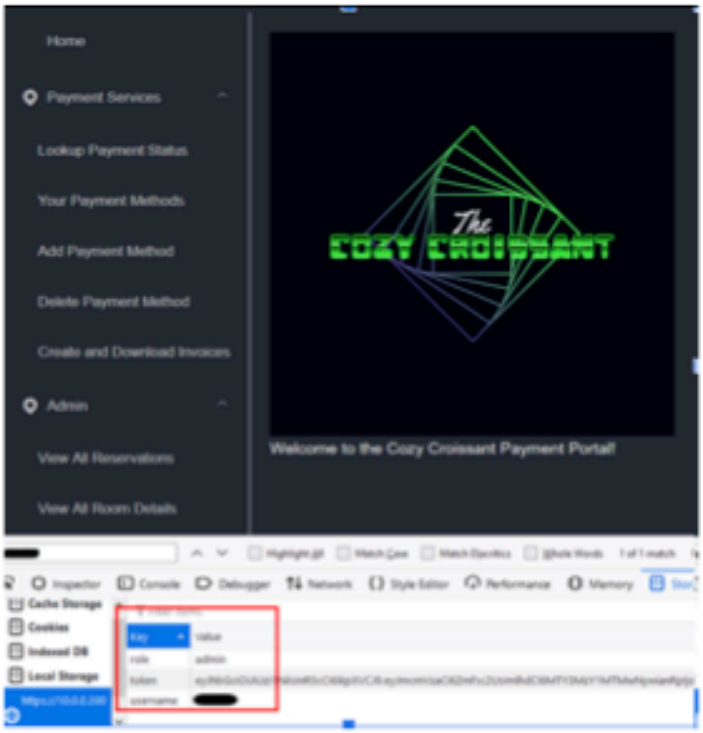


Image Description: Modified cookie value with admin panel

Remediation Recommendation(s):
Implement signed cookies to allow the server to verify that authorization cookies have not been tampered with. Another alternative is to implement Json Web Tokens(JWT). This would prevent an attacker from modifying a cookie in order to escalate privileges in the payment portal.

Business Impact:
Cookie tampering can lead to an attacker gaining admin privileges to the payment portal. Since this portal contains significant amounts of PII, an attacker gaining access to the payment portal and stealing the information could lead to significant financial and reputational damage.

References:
https://knowledge.broadcom.com/external/article/166142/how-do-i-prevent-cookie-modifications-fr.html

8. Authenticated Remote Code Execution in get_output() Function

Affected Host(s) Information:

Host Name	IP Address	Port	Service
LPS	10.0.0.12	80, 443	http

Classifications:

Risk Score	8/10
Exploitation Likelihood	Possible
Business Impact	Moderate
Remediation Difficulty	Medium

Description:
The internal functionality of the website allows for a malicious user to execute commands on the underlying system by specially crafting a web request to the API.

Steps To Reproduce:
It is possible to reproduce this exploit using a tool like Burpsuite. By crafting a request with the following parameters:

"GET /userapi.php?update&;type=user;user=<user>;secret=<secret>;a=$(whoami)"

The resulting response will be a "200 ok" and the command will be injected into the get_output() function parameter in the "$args" variable.

Image Description: Request sent to the server with the modified parameter.

Image Description: Server response, 200 ok.

```
alty
 -s sfkujfzdbcc'
alty
in -k action=update type=user username=admin user=admin secret=sfkujfzdbcc a='
alty
 -s sfkujfzdbcc'
alty
in -k action=update type=user username=admin user=admin secret=sfkujfzdbcc a=root'
```

Image Description: Code execution achieved on “a” parameter.

```php
function update_user($username,$fields){
    $args = "";
    foreach($fields as $field=>$value){
        $args=$args . $field . "=" . $value . " ";
    }
    //echo($args);
    $res = get_output("update -u $username -k $args");
}
```

Image Description: Injection point in $args

```
function get_output($cmd){
    $cmd = COREBIN . " " . $cmd;
    if(stristr($_SERVER['QUERY_STRING'],"debug")){
        echo("<br><pre>\n\r\n\r\n\r\n\r\n");
        echo($cmd);
        echo("\n\r\n\r\n\r\n\r\n</pre><br>");
    }
    ob_start();
    passthru($cmd);
    $var = ob_get_contents();
    ob_end_clean();
    return $var;
}

```

Image Description: passthru() function executes the user input.

Remediation Recommendation(s):

Implement sanitization on user provided variables such as $fields and $args.

Business Impact:
Code execution on the API host could result in compromised user data and passwords as well as modification to the loyalty program services.

References:
https://owasp.org/www-community/attacks/Command_Injection

9. SMB Signing Disabled

Affected Host(s) Information:

Host Name	IP Address	Port	Service
adcs	10.0.0.6	445	smb
hms	10.0.0.11	445	smb
workstation01	10.0.0.51	445	smb
workstation02	10.0.0.52	445	smb

kiosk01	10.0.200.101	445	smb
kiosk02	10.0.200.102	445	smb
kiosk03	10.0.200.103	445	smb
kiosk04	10.0.200.104	445	smb

Classifications:

Risk Score	7/10
Exploitation Likelihood	Possible
Business Impact	Moderate
Remediation Difficulty	Medium

Description:

The SMB service is used to transfer files and execute management commands on windows endpoints. If a machine does not require SMB signing, it has no way of verifying the identity of the system attempting to connect or the connection's message integrity. This could allow an attacker to capture and redirect valid authentication attempts and modify them to gain initial access and perform malicious actions on vulnerable hosts.

Steps To Reproduce:

Using the following command, you can enumerate the system's signing status:

crackmapexec smb <ip/subnet>

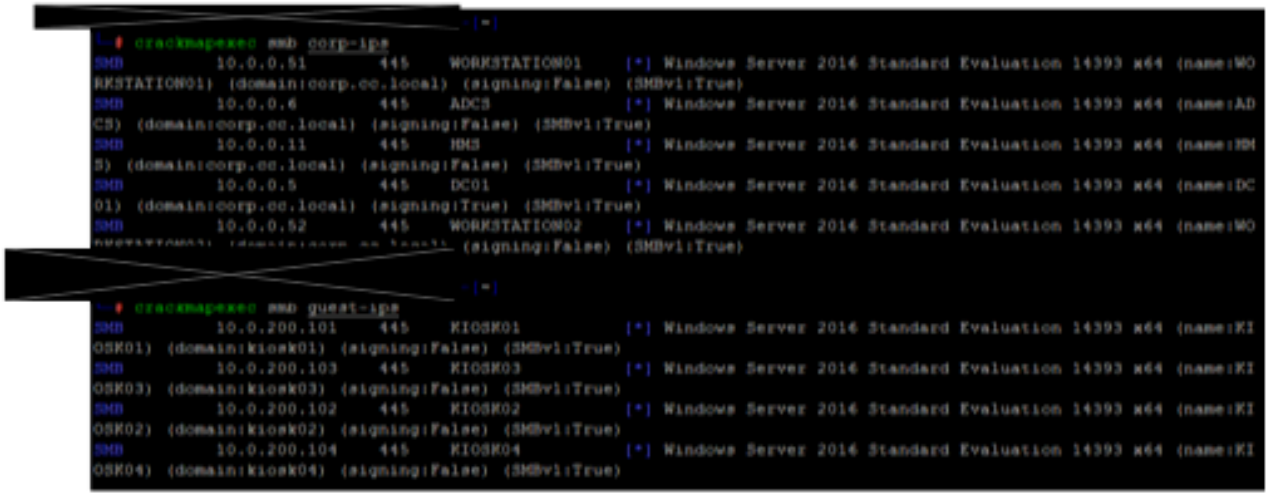


Image Description: Crackmapexec command output

Remediation Recommendation(s):
Enable SMB signing in the group policy for the domain and its connected hosts. If the host is not connected to a domain, SMB signing can be locally configured.

Business Impact:
An attacker could impersonate any user on the network, potentially causing business disruption or compromise of business infrastructure.

References:
https://www.rapid7.com/db/vulnerabilities/cifs-smb-signing-disabled/

9. Plaintext Credentials in LDAP

Affected Host(s) Information:

Host Name	IP Address	Port	Service
dc01	10.0.0.5	389	ldap

Classifications:

Risk Score	8/10
Exploitation Likelihood	Moderate
Business Impact	Severe
Remediation Difficulty	Easy

Description:
An authenticated query to the LDAP server was used to dump the contents of the database. Plaintext credentials were found in the description field of select users in the database. Credentials and other sensitive information should not be stored in plaintext fields in the database as this can lead to accidental disclosure of such information.

Steps To Reproduce:
Tools like Ldapdomaindump can be used to quickly dump an LDAP database using known credentials for authentication:

```
ldapdomaindump -u example\user -p pass <target>
```

Domain Users

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
[redacted]			01/10/23 14:04:27	01/10/23 14:04:27	01/01/01 00:00:00	NORMAL_ACCOUNT	01/10/23 14:04:27	1166	lov[redacted]
[redacted]			01/10/23 14:04:27	01/10/23 14:04:27	01/01/01 00:00:00	NORMAL_ACCOUNT	01/10/23 14:04:27	1165	

Image Description: Dump output showing credentials in description field

Remediation Recommendation(s):
Do not store sensitive information in plaintext fields like description in the LDAP database.

Business Impact:
This issue increases the risk of attackers gaining access to accounts in the networked environment. If attackers can gain access to systems, it might increase the risk of system compromise and business interruptions.

References:
https://improsec.com/tech-blog/storing-sensitive-data-in-active-directory

10. Insecure Direct Object Reference

Affected Host(s) Information:

Host Name	IP Address	Port	Service
payment-web	10.0.0.200	80, 443	http

Classifications:

Risk Score	8/10
Exploitation Likelihood	Likely
Business Impact	Severe
Remediation Difficulty	Hard

Description:
Multiple insecure direct object reference (IDOR) vulnerabilities were found in the tested environment. IDOR vulnerabilities happen when an application exposes a direct reference to an object element in the backend. This can be an object ID and / or some identifier with a format or pattern. Because of this pattern, attackers can extrapolate identifiers and potentially enumerate or directly access objects that should not be accessible.

Steps To Reproduce:

The payment API has multiple IDOR vulnerabilities, including some in the /api/payment and /api/payment_method endpoints. The IDs associated with these endpoints can be easily inferred based on a basic numeric pattern.

Image Description: Burp showing IDOR vulnerabilities

Remediation Recommendation(s):

Use hashes to replace the direct identifiers. The best practice is to also apply a salt to the hash to make it unpredictable and hard to guess.

Business Impact:

Attackers can exploit IDOR vulnerabilities to gain access to and exfiltrate sensitive data on the application.

References:
https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

Medium Findings

11. Verbose Error Disclosure

Affected Host(s) Information:

Host Name	IP Address	Port	Service
profiler	10.0.0.102	80, 443	http
payment-web	10.0.0.200	80. 443	http

Classifications:

Risk Score	6/10
Exploitation Likelihood	Likely
Business Impact	Moderate
Remediation Difficulty	Medium

Description:
When verbose error disclosure is enabled, detailed error messages are displayed to users when an error occurs. This can be helpful for developers, but it can also be a security risk if the information is displayed to an attacker. An attacker who sees a detailed error message can use the information to learn about the system's architecture and potentially exploit vulnerabilities.

Steps To Reproduce:

Image Description: LDAP profiler error disclosure

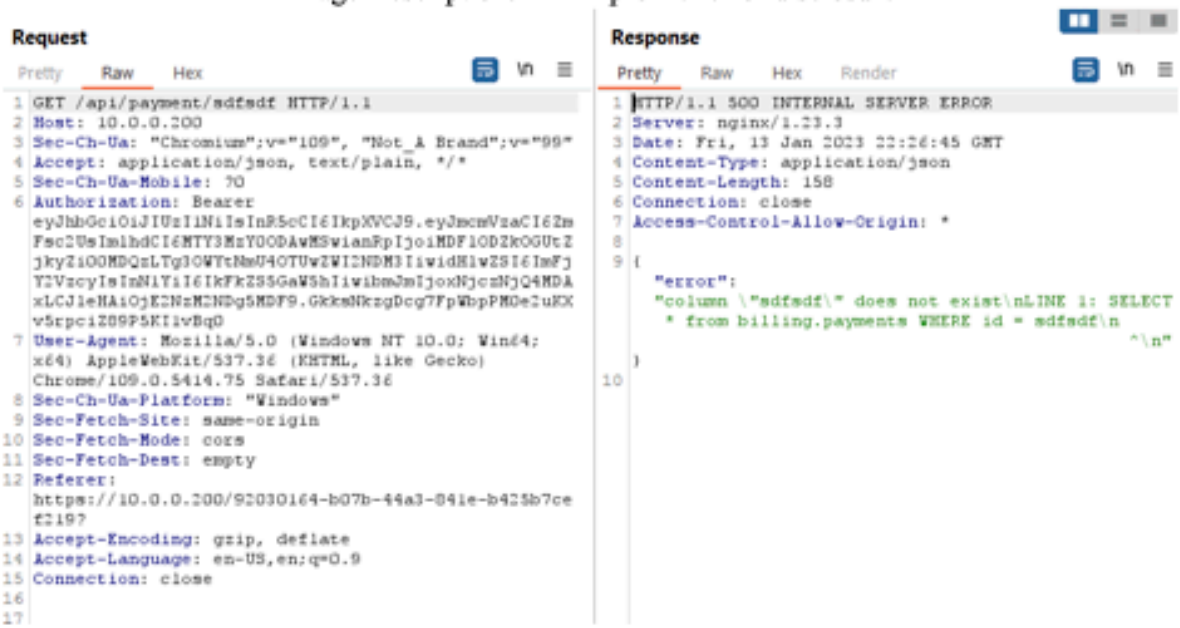


Image Description: SQL error disclosure

Remediation Recommendation(s):

Suppress and disable verbose error messages in the application. Use a local logging mechanism and handle errors properly instead of displaying the errors to the user.

Business Impact:

Verbose errors can aid attackers in performing more complicated attacks on systems. These attacks can potentially lead to the compromise of business-critical applications and systems, causing disruption and potential data loss.

References:
https://owasp.org/www-community/Improper_Error_Handling
https://cwe.mitre.org/data/definitions/209.html

12. Network Segmentation Controls Insufficient

Affected Host(s) Information:

Host Name	IP Address	Port	Service
kiosk01	10.0.200.101		
kiosk02	10.0.200.102		
kiosk03	10.0.200.103		
kiosk04	10.0.200.104		

Classifications:

Risk Score	5/10
Exploitation Likelihood	Possible
Business Impact	Severe
Remediation Difficulty	Hard

Description:
If an attacker can compromise one of the kiosk devices, an attacker can utilize this device as a pivot point to access the corporate network.

Steps To Reproduce:
A meterpreter shell is opened on the compromised device, and from there tools such as crackmapexec are proxied through meterpreter proxychains.

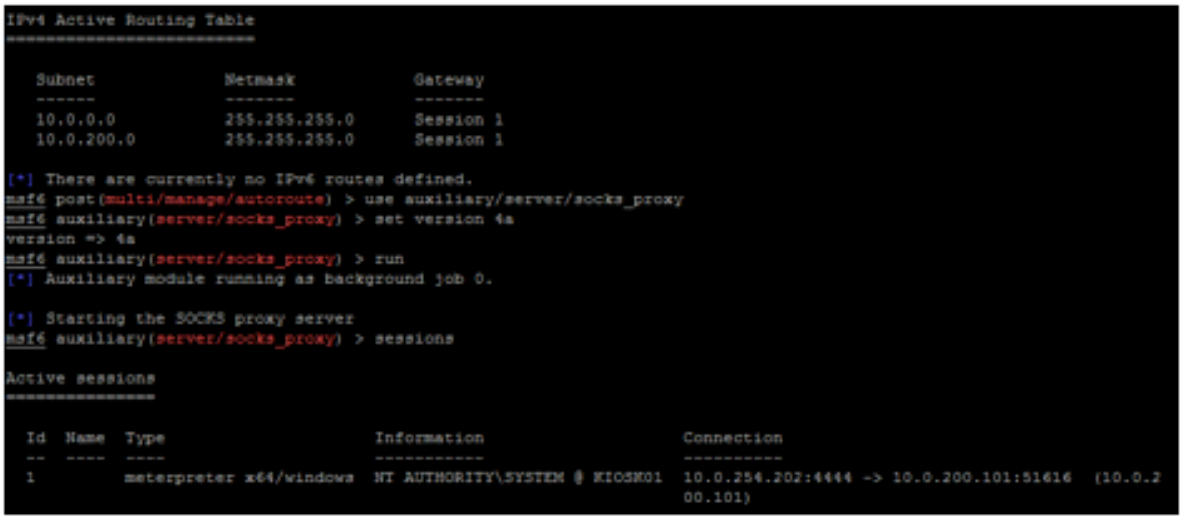


Image Description: Meterpreter Shell on a kiosk

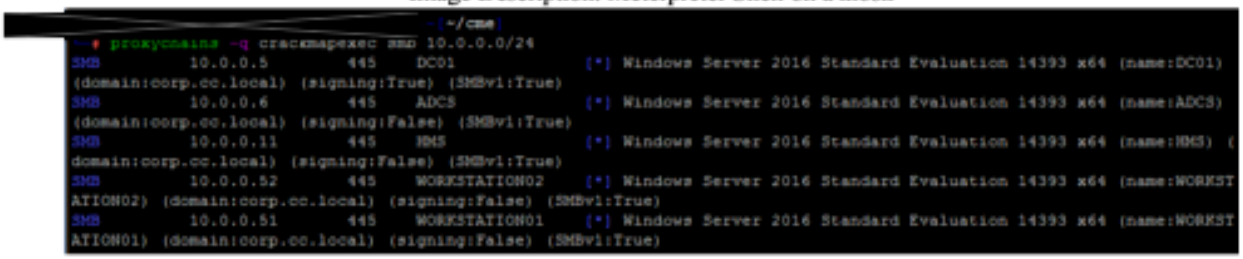


Image Description: Crackmapexec begins proxied into the corporate network network through a kiosk.

Remediation Recommendation(s):

Implement granular access controls between the kiosks and corporate network, limiting access from the kiosks to only required IP addresses and Ports for the given services being accessed. This will limit the ability of the kiosks to be used as a pivot point in the event of compromise.

Business Impact:

If the kiosks are compromised, the potential lost business due to loss of functionality is low to medium. While if an attacker gains access to the kiosk and pivots into the corporate network, they then have the potential to impact mission critical software and applications, which could result in reputation loss, or loss of functional time for the business.

13. Broken Web Access Control

Affected Host(s) Information:

Host Name	IP Address	Port	Service
payment-web	10.0.0.200	80, 443	http

Classifications:

Risk Score	4/10
Exploitation Likelihood	Moderate
Business Impact	Mild
Remediation Difficulty	Medium

Description:
Access control is how a web application grants access to certain content and functionality to certain users. When access control is not implemented properly, it can allow unauthorized users to gain access to sensitive information or perform actions that they should not be able to. For example, an attacker may be able to bypass authentication or authorization checks to access restricted areas of a website or manipulate data without proper permission.

Steps To Reproduce:
An unauthenticated user can browse directly to admin functionality on the web application.

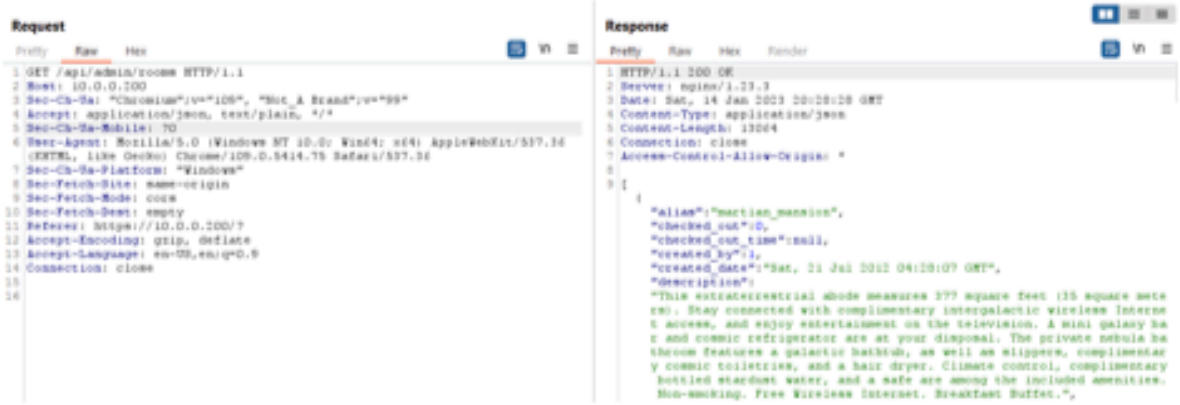


Image Description: Burp showing unauthenticated user accessing admin functionality

Remediation Recommendation(s):
Ensure that authorization is put in place for protected functionality and paths in the web application. Check for a valid access token (like a JWT) before granting access to such functions.

Business Impact:
This vulnerability increases the risk for data loss, as it can enable attackers to gain access to information they should not be able to access.

References:
https://owasp.org/www-community/Broken_Access_Control

14. LPS API Cross Client Enumeration

Affected Host(s) Information:

Host Name	IP Address	Port	Service
LPS	10.0.0.12	80, 443	http

Classifications:

Risk Score	6/10
Exploitation Likelihood	Possible
Business Impact	Moderate
Remediation Difficulty	Medium

Description:
Multiple request endpoints allow modification of parameters to access other users' data.

Steps To Reproduce:
By manipulating the parameters in the url it is possible to access arbitrary client data on the adminapi.php endpoint even if the user is not an administrator. For example a low privilege user can browse to "https://10.0.0.12/adminapi.php?query&;type=all;secret=<users-secret>" to view all other clients data

Remediation Recommendation(s):

Implement user authentication checks to ensure that the user is only able to interact with their data when querying the API.

Business Impact:

The impact of this vulnerability being exploited would result in sensitive user data being exposed to a malicious actor.

References:
https://csrc.nist.gov/Projects/Access-Control-Policy-and-Implementation-Guides

15. Publicly Available Configs and Logs

Affected Host(s) Information:

Host Name	IP Address	Port	Service
LPS	10.0.0.12	80, 443	http

Classifications:

Risk Score	6/10
Exploitation Likelihood	Likely
Business Impact	Mild
Remediation Difficulty	Easy

Description:
Logs on this service disclose sensitive user information publicly such as user authentication tokens and usernames/passwords/query logs. This information can be used for authentication as any account on the website. Other files are also accessible publicly, potentially exposing internal source code.

Steps To Reproduce:
To reproduce this vulnerability browse to "https://10.0.0.12/query.log" other files in the root directory of the website can also be accessed through this method replacing "query.log" with the relative path.

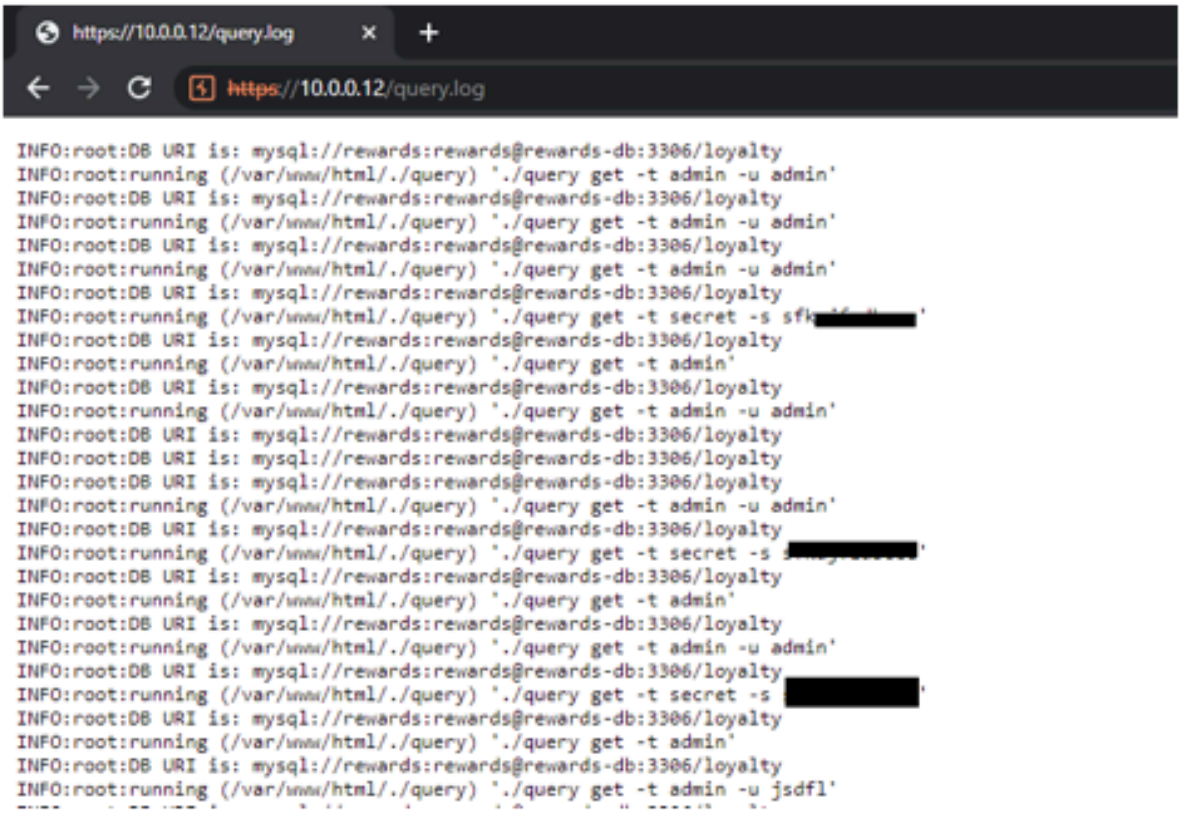


Image Description: Query.log output containing user secrets.

Remediation Recommendation(s):
Restrict access to sensitive files paths from unauthenticated, and unprivileged users.

Business Impact:
An attacker could capture and potentially log in as any user. This could result in loss of service to the loyalty program, as well as the potential loss of customer PII.

Low Findings

16. Web server does not use HTTPS

Affected Host(s) Information:

Host Name	IP Address	Port	Service
media	10.0.0.20	80	http

adcs	10.0.0.6	80	http
profiler	10.0.0.102	80	http

Classifications:

Risk Score	3/10
Exploitation Likelihood	Unlikely
Business Impact	Moderate
Remediation Difficulty	Easy

Description:

The hosts media (10.0.0.20), adcs (10.0.0.6), and profiler (10.0.0.102) all utilize HTTP instead of HTTPS. This leads to requests and responses being unencrypted.

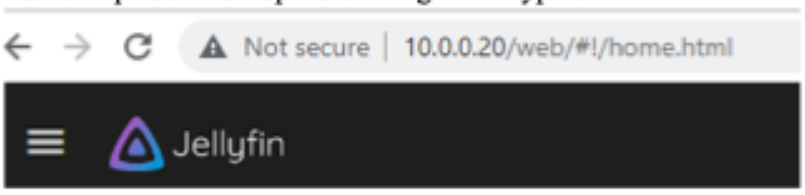


Image Description: Media Server being accessed over an unencrypted connection

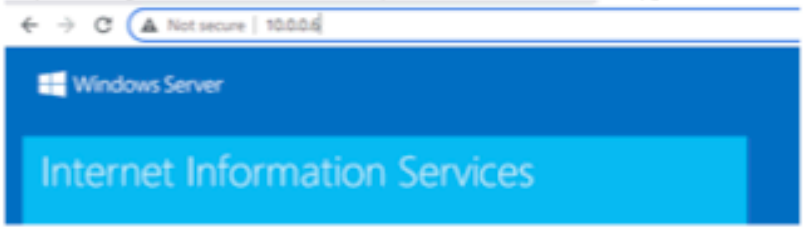


Image Description: adcs being accessed over an unencrypted connection.

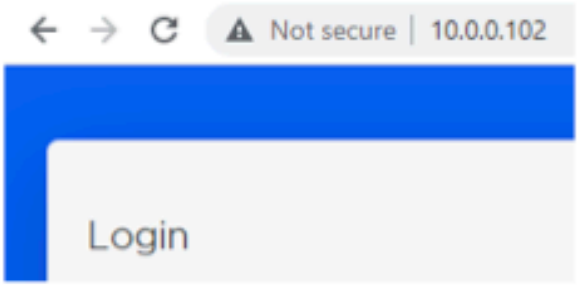


Image Description: Profiler being accessed over an unencrypted connection.

Steps To Reproduce:

Navigate to media (10.0.0.20), and view the “Not secure” notification in the browser.
Navigate to adcs(10.0.0.6), and view the “Not secure” notification in the browser.
Navigate to profiler (10.0.0.102), and view the “Not secure” notification in the browser.

Remediation Recommendation(s):
Enable HTTPS on the server and redirect HTTP traffic to HTTPS.

Business Impact:
These sites are vulnerable to man-in-the-middle attacks, confidentiality and integrity are at risk from unauthorized users.

References:
https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/

17. Unauthenticated Environment Variable Disclosure

Affected Host(s) Information:

Host Name	IP Address	Port	Service
HMS	10.0.0.11	80	xampp

Classifications:

Risk Score	3/10
Exploitation Likelihood	Unlikely
Business Impact	Moderate
Remediation Difficulty	Easy

Description:
System environment variables can store sensitive information such as credentials or authentication tokens as well as disclose system configuration and layout.

Steps To Reproduce:
By browsing to "http://10.0.0.11/cgi-bin/printenv.pl" the website discloses this information publically.

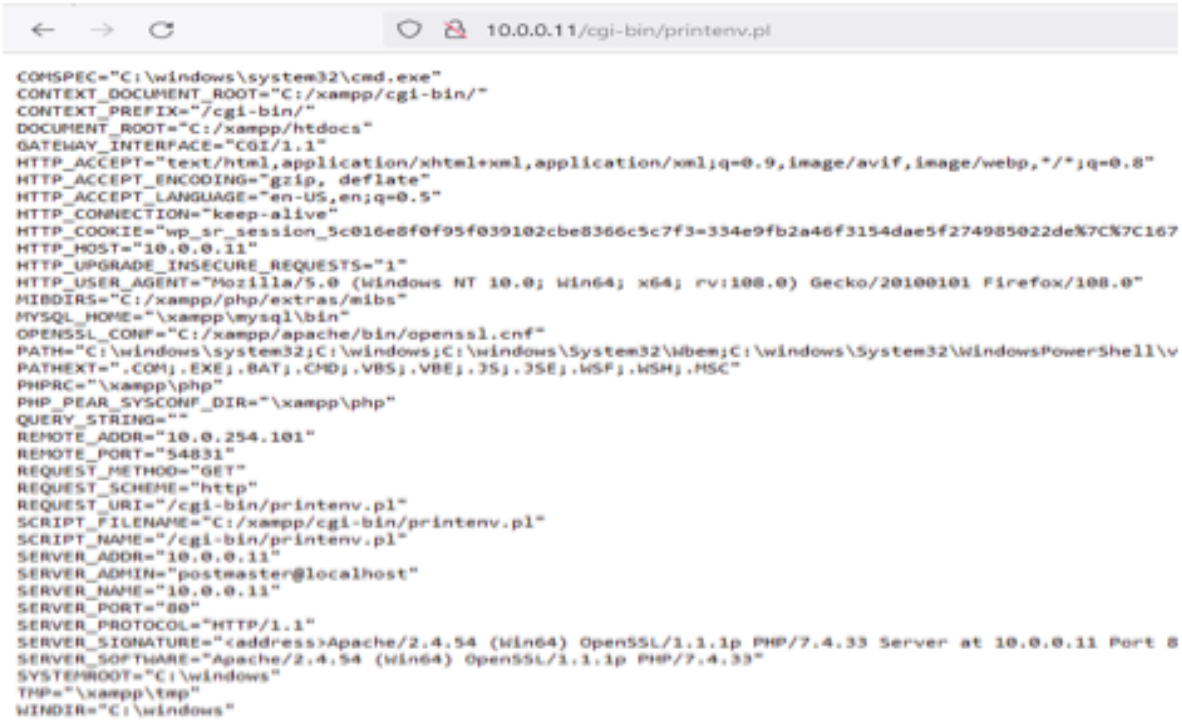


Image Description: Output of the HMS systems local environment variables.

Remediation Recommendation(s):
This vulnerability can be remediated by removing the printenv.pl script or disallowing external access to the cgi-bin directory.

Business Impact:
Token and credential leaks have the potential to cause damage to the local system by allowing an unauthorized user to access sensitive services.

References:
https://community.apachefriends.org/f/viewtopic.php?p=157144

18. Source Code Disclosure

Affected Host(s) Information:

Host Name	IP Address	Port	Service
payment-web	10.0.0.200	80	http

Classifications:

Risk Score	3/10
Exploitation Likelihood	Unlikely
Business Impact	Moderate
Remediation Difficulty	Medium

Description:

The host 10.0.0.200 hosts the Payment Portal on the Cozy Croissant's corporate network. When the src folder is accessed from Inspect it allows users to see all pathways the site offers to both clients and admin.

Steps To Reproduce:

Navigate to the Payment Portal page (10.0.0.200), then access Inspect. Next, navigate to Sources, then look under the src folder to access the router.js file and view pathways.

Image Description: View of webpage home screen and developer tools

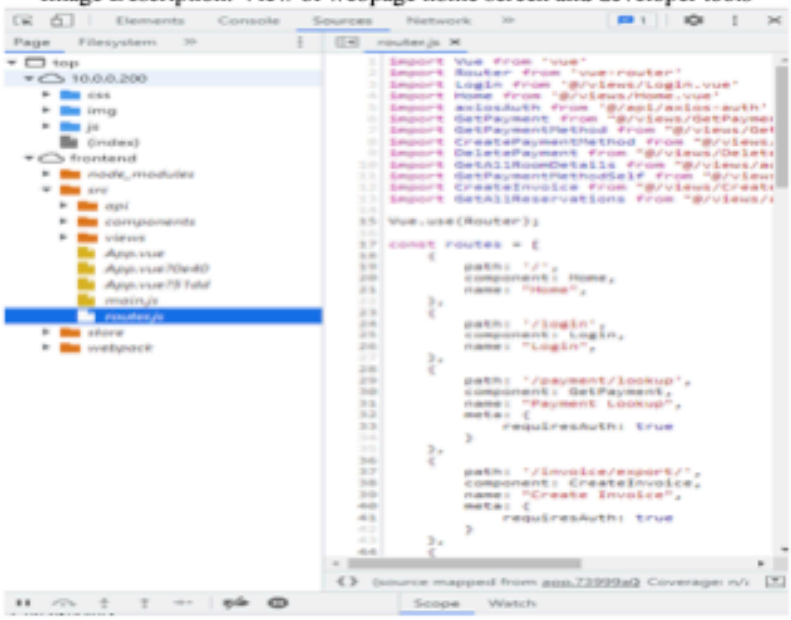


Image Description: View of available paths from webpage source.

Remediation Recommendation(s):

Separate admin functionality from general client-side scripts.

Business Impact:
If admin is accessed by an attacker and coupled with this knowledge of the pathways, they are able to directly access customer PII. This will lead to reputational loss of the company and potential financial loss of both customer and company.

References:
https://portswigger.net/web-security/information-disclosure

19. Self-signed certificates

Affected Host(s) Information:

Host Name	IP Address	Port	Service
Payment-web	10.0.0.200	80	Payment Portal
LPS	10.0.0.12	80	My Rewards

Classifications:

Risk Score	2/10
Exploitation Likelihood	Unlikely
Business Impact	Mild
Remediation Difficulty	Easy

Description:
The hosts 10.0.0.200 and 10.0.0.12 are the Payment Portal and the My Rewards page on the Cozy Croissant's corporate network, respectively. When either site is reached the browser indicates the pages are not secure due to self-signed certificates.

Steps To Reproduce:
Navigate to the Payment Portal (10.0.0.200), then to certificates by clicking the 'Not secure' notice in the browser.

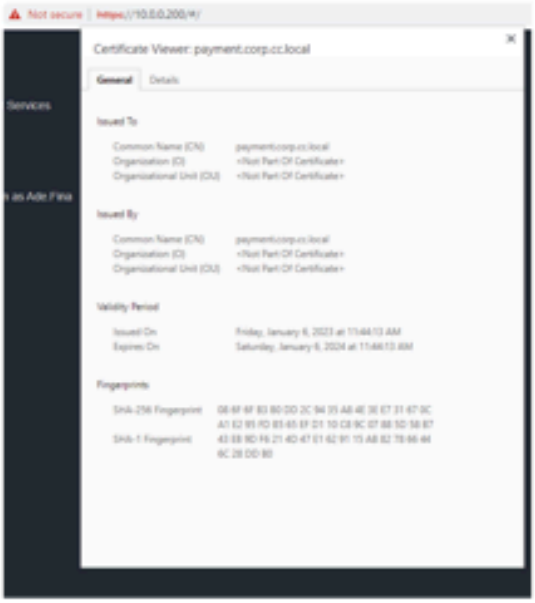


Image description: Self Signed certificate for the Payment Portal.

Navigate to My Rewards (10.0.0.12), then to certificates by clicking the 'Not secure' notice in the browser.

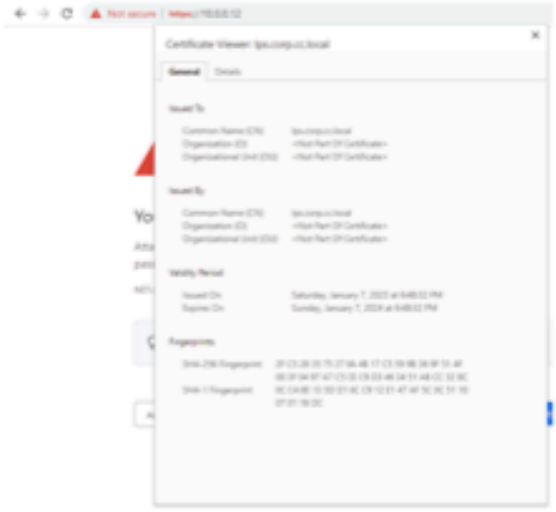


Image description: Self Signed certificate for the Rewards Page

Remediation Recommendation(s):

Replace the self-signed certificate with a certificate signed by a trusted Certificate Authority.

Business Impact:

Self-signed certificates can lead to a loss of trust from the clients, resulting in less website engagement and therefore financial loss.

https://www.ibm.com/docs/en/i/7.2?topic=concepts-certificate-authority
https://www.globalsign.com/en/ssl-information-center/dangers-self-signed-certificates

20. Username Enumeration

Affected Host(s) Information:

Host Name	IP Address	Port	Service
lps.corp.cc.local	10.0.0.12	80	My Rewards

Classifications:

Risk Score	3/10
Exploitation Likelihood	Likely
Business Impact	Mild
Remediation Difficulty	Hard

Description:
This vulnerability allows an attacker to discover valid usernames on The Cozy Croissant's "My Rewards" page. This is done by analyzing the verbose error messages presented on the application during failed login attempts.

Steps To Reproduce:
From the login page, enter an incorrect username and password combination, such as test:test that yields the error "user not found". However, the output given by entering a registered username with any password, which yields the error "invalid password".

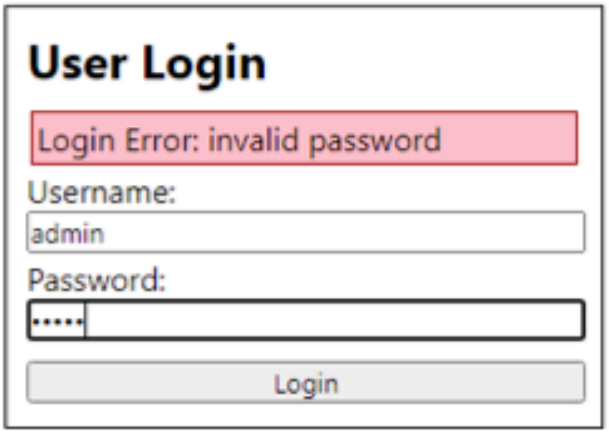


Image Description: User not found error

Remediation Recommendation(s):
Implement obscured errors such as “Login Error” or “Login failed”.

Business Impact:
Username enumeration through verbose error messaging would aid an attacker in finding valid user accounts and could lead to future account compromise.

References:
https://www.rapid7.com/blog/post/2017/06/15/about-user-enumeration/

Informational Findings

21. Payment Portal Password Policy

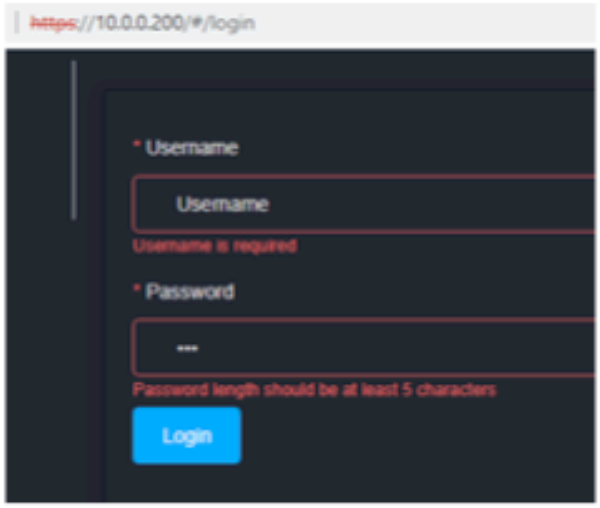
Affected Host(s) Information:

Host Name	IP Address	Port	Service
	10.0.0.200		Nginx Web Server

Classifications:

Risk Score	0/10
Exploitation Likelihood	Not Applicable
Business Impact	Not Applicable
Remediation Difficulty	Easy

Description:
The host 10.0.0.200 hosts The Cozy Croissant’s payment portal on their corporate network. On the login page the password field will return the alert “Password length should be at least 5 characters” when less than 5 characters are typed into the input field. This indicates that the password policy for the web page is set to a minimum of 5.



Steps To Reproduce:
Navigate to the Login page on 10.0.0.200 and type less than 5 characters into the password input field and then click "Enter" or outside of the input field and the alert will be displayed.

Remediation Recommendation(s):
Update the password policy on the Payment Portal on 10.0.0.200 to a minimum of 8 characters to be in accordance with the National Institute of Standards and Technology (NIST) minimum password recommendation.

Business Impact:
Short passwords are easier to compromise by guessing, brute force, password cracking, and other commonly used techniques. A malicious user could potentially gain access to user accounts with short passwords in a relatively short period of time. If payment accounts become compromised sensitive or confidential information could be revealed and TCC reputation may be damaged resulting in customers choosing to do business with other hotels. Therefore, raising the minimum password requirement would improve account security.

References:
NIST Special Publication 800-63B - https://pages.nist.gov/800-63-3/sp800-63b.html

Appendix A: Classification Definitions

Risk Classifications

LEVEL	SCORE	DESCRIPTION
Critical	9 - 10	The vulnerability poses an immediate threat to the organization, and exploitation may permanently affect the organization. Remediation should be performed immediately.
High	7 - 8	The vulnerability poses an urgent threat to the organization. Recovery from exploitation impacts may be difficult. Remediation should be prioritized.
Medium	4 - 6	The exploitation of the vulnerability may result in a notable disruption of business functionality. Remediation should be performed when feasible.
Low	1 - 3	The vulnerability poses a minimal threat to the organization. The presence of the vulnerability should be noted and remediated if possible.
Informational	0	These findings have no clear threat to the organization, but may cause business processes to function undesirably or reveal sensitive company information.

Exploitation Likelihood Classifications

LEVEL	DESCRIPTION
Likely	Exploitation methods are well-known anc can be performed with minimal

	difficulty using publicly available tools.
Possible	Exploitation methods are well-known and may be performed using public tools with configuration changes. Understanding of the underlying system is required for successful exploitation.
Unlikely	Exploitation requires deep understanding of the underlying system or advanced technical skills. Precise conditions may be required for successful exploitation.

Business Impact Classifications

LEVEL	DESCRIPTION
Severe	Successful exploitation of the vulnerability may result in wide-spread disruption of critical business functions and significant financial damage.
Moderate	Successful exploitation of the vulnerability may cause significant disruptions to non-critical business functions.
Mild	Successful exploitation of the vulnerability may affect a few users, without causing much disruption to routine functions.

Remediation Difficulty Classifications

LEVEL	DESCRIPTION
Hard	Remediation may require extensive reconfiguration of the underlying systems and disruption of normal business functions.
Medium	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
Easy	Remediation may be accomplished within a short amount of time and with little difficulty.

Appendix B: Network Information

Corporate Network - 10.0.0.0/24

IP Address	Host Name	Service(s)	Open Ports
10.0.0.2			53
10.0.0.5	DC01		53, 88, 135, 139, 389, 445, 464, 593, 636, 3268, 3269, 3389
10.0.0.6	ADCS	IIS 10.0	80, 135, 139, 445, 3389
10.0.0.7	doapi	OpenSSH 8.2p1	22, 3000, 27017
10.0.0.11	hms	WordPress 4.8.21	80, 135, 139, 446, 445, 3306, 3389
10.0.0.12	lps	NGINX, OpenSSH 8.2p1	22, 80, 443, 3306
10.0.0.20	media	NGINX 1.18, OpenSSH 8.2p1	22, 80, 8096
10.0.0.51	Workstation01		135, 139, 445, 3389
10.0.0.52	Workstation02		135, 139, 445, 3389
10.0.0.100	ldap	OpenSSH 8.2p1, OpenLDAP	22, 389, 636

10.0.0.102	profiler	Apache 2.4.38, PHP 7.2.34, OpenSSH 8.2p1	22, 80, 443
10.0.0.200	payment-web	NGINX 1.23.3, OpenSSH 8.2p1	22, 80, 443, 8000
10.0.0.210	payment-db	PostgreSQL 15.1, OpenSSH 8.2p1	22, 5432
10.0.0.254			

Guest Network - 10.0.200.0/24

IP Address	Host Name	Service(s)	Open Ports
10.0.200.2			53
10.0.200.101	kiosk01	Kiosk	135, 139, 445, 369
10.0.200.102	kiosk02	Kiosk	
10.0.200.103	kiosk03	Kiosk	
10.0.200.104	kiosk04	Kiosk	
10.0.200.254			

Appendix C: Tools Used

Tool Name	Tool Description
Burp Suite	A Java based Web Penetration Testing framework that is an integrated platform for performing security testing of web applications.
CrackMapExec	CME is a wrapper tool for the windows offensive security tool suite Impacket and is used to enumerate and escalate privileges in a domain.
Hashcat	Hashcat is a password cracking tool used for password recovery.
Hydra	Hydra is used for credential stuffing and password spraying against SSH.
Impacket	Impacket is a python based Windows protocol suite used for offensive security testing in Windows domains.
ldapdomaindump	ldapdomaindump collects and parses information available via LDAP and outputs it in a human readable format.
Metasploit	Metasploit is an offensive security tool database used for exploiting known or common vulnerabilities in outdated software.
Nmap	Nmap enumerates devices and services on a network using a variety of techniques such as TCP SYN-scanning, ICMP echo scanning, and reverse name resolution.
PetitPotam	PetitPotam is both the name of a vulnerability and tool used to coerce a Windows server to authenticate to an attacker controlled computer.
PKINITtools	PKINITtools is tools for Kerberos Public Key Cryptography for Initial Authentication (PKINIT) and relaying to AD CS.
Responder	Responder an Link-Local Multicast Name Resolution (LLMNR), NetBIOS Name Service (NBT-NS) and Multicast Domain Name System (MDNS) poisoner.
SSL Scan	SSL Scan tests SSL/TLS enabled IP or web address to gather details of the certificate that is being used.
Wappalyzer	Wappalyzer is a technology profiler that shows what websites are built with.

Appendix D: References

GDPR Document - https://gdpr-info.eu/
GDPR Fines - https://gdpr.eu/fines/
GDPR Principles - https://gdpr-info.eu/art-5-gdpr/
NIST Special Publication 800-63B - https://pages.nist.gov/800-63-3/sp800-63b.html

Youtube Video of Safe Opening Technique - https://youtu.be/fjrTTlxWTIY
Safe Box on Amazon - https://www.amazon.com/Yuanshikj-Electronic-Security-Fireproof-Business/dp/B078MYJYD5/ref=asc_df_B078MYJYD5/?tag=hyprod-20&linkCode=df0&hvadid=312060853864&hvpos=&hvnetw=g&hvrand=10990357311933972104&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=2840&hvtargid=pla-568693134129&th=1
PCI DSS v4 - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI DSS-v4_0.pdf
PCI DSS Security Penalties - https://financial.ucsc.edu/pages/security_penalties.aspx
PCI DSS Compliance Guide - https://www.pcicomplianceguide.org/faq/

Technical References

https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429
https://learn.microsoft.com/en-us/security-updates/SecurityAdvisories/2009/974926
https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/prevent-windows-store-lm-hash-password
https://www.stigviewer.com/stig/windows_10/2019-01-04/finding/V-63429
https://community.apachefriends.org/f/viewtopic.php?p=157144
https://portswigger.net/web-security/information-disclosure
https://pages.nist.gov/800-63-3/sp800-63b.html
https://www.rapid7.com/blog/post/2017/06/15/about-user-enumeration/
https://knowledge.broadcom.com/external/article/166142/how-do-i-prevent-cookie-modifications-fr.html
https://www.ibm.com/docs/en/i/7.2?topic=concepts-certificate-authority
https://www.globalsign.com/en/ssl-information-center/dangers-self-signed-certificates
https://portswigger.net/web-security/information-disclosure
https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/02-Testing_for_Default_Credentials
https://www.rapid7.com/db/vulnerabilities/cifs-smb-signing-disabled/
https://improsec.com/tech-blog/storing-sensitive-data-in-active-directory
https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html
https://owasp.org/www-community/attacks/SQL_Injection
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
https://owasp.org/www-community/Improper_Error_Handling
https://cwe.mitre.org/data/definitions/209.html
https://owasp.org/www-community/Broken_Access_Control