Penetration Test Report

Le Bonbon Croissant

January 9, 2022

[redacted]

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

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

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

Table of Contents

Executive Summary

Purpose and Scope of Evaluation: [redacted] was contracted by Le Bonbon Croissant (LBC) to perform a follow-up security assessment on the company's infrastructure, specifically the enterprise core infrastructure, retail operation and assets, and ICS/SCADA control systems on January 7th - 8th 2022.

For this security assessment, [redacted] conducted a penetration test to assess the remediations from the initial assessment of LBC's environment and to further identify any other existing external/internal security vulnerabilities towards LBC's network resources and services. This test was executed within the scope of 10.0.17.0/24.

The objectives of this test include the following:

- Validate remediations of vulnerabilities from the findings during the initial assessment.
- Identify publicly accessible ports and services that have known information-security vulnerabilities and exposures, which can be exploited by threat actors.
- Discover existing vulnerabilities within LBC's Industrial Control Systems that can provide unauthorized access to sensitive information of the network infrastructure, assets, or disrupt daily operations.
- Compliance to B2B and B2C eCommerce infrastructure, Payment Card Industry Data Security Standards (PCI-DSS), General Data Protection Regulation (GDPR), and NIST-SP-800.

[redacted] assessment identified a total of **14** vulnerabilities, which consisted of **5** critical severity vulnerabilities, that can be classified by severity in the table below:

Severity Rating	Critical	High	Medium	Low	Informational
Vulnerabilities	5 ↑5	4	2 ↓1	2	1 ↓3

Key Findings and Recommendations Response

Since the last security assessment performed on November 13th, 2021, LBC's environment is vulnerable to potential cyber attacks that pose a significant business risk in terms of monetary impact, legal implications, and customer trust. Critical vulnerabilities found within the environment that should be remediated immediately are weak credential policies and API infrastructure problems. These vulnerabilities are not compliant with PCI-DSS, which will result in fines that range from $5,000 to $100,000 per month, in addition to any credit monitoring fees, lawsuits, and actions by state and federal governments until compliant. [redacted] noted LBC's environment implemented security measures that mediate previous vulnerabilities.

[redacted] recommends LBC remediate these findings by implementing stronger credential encryption and managing authentication for all users accessing sensitive information to LBC's resources to further improve the company's implementation of security controls within the company. Failure to mitigate these risks will leave LBC vulnerable to potential future breaches from malicious actors that can affect LBC's retail operations and reputation as a candy and croissant company.

Introduction

Purpose

[redacted] was contracted by LBC to perform a limited-scope penetration test on its network on January 7-9th, 2022. The purpose of the penetration test is to detect vulnerabilities lying within LBC's enterprise network to allow the company to take the appropriate steps towards remediating or mitigating the vulnerabilities found in the network. To further do so, the report not only documents findings in the network, but also outlines recommendations for remediations for each finding, along with a high-level recommended response plan.

As a part of the E-commerce Sector, LBC is part of what is referred to as a B2B and B2C eCommerce.

Consequently, the company must conform to standards such as the Payment Card Industry (PCI) Data Security Standard (hereafter referred to as PCI-DSS or simply PCI). The security assessment performed by [redacted] on LBC's networks takes into account the company's compliances of these PCI-DSS standards along with violations thereof. These findings have also been documented throughout the report.

Scope

The penetration test was of limited scope, only assessing one subnet representative of LBC's main branch. Within this single subnet, the security engineers evaluated the security of API endpoints, marketplace sites, databases, and web services. Additionally, after LBC approved the risk assessment proposal by our security engineers the programmable logic controllers were added to the scope. Although the scope mainly consisted of finding vulnerabilities that can be exploited by external threats, the team also considered internal threats as well.

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

Host Discovery:

In order to seek and maintain an updated list of in-scope targets, [redacted] developed a topology on the LBC network. The graphical topology relies on the Nmap scans for an accurate depiction. During the reconnaissance phase, [redacted] identified several Linux machines and a Programmable Logic Control system on the network.

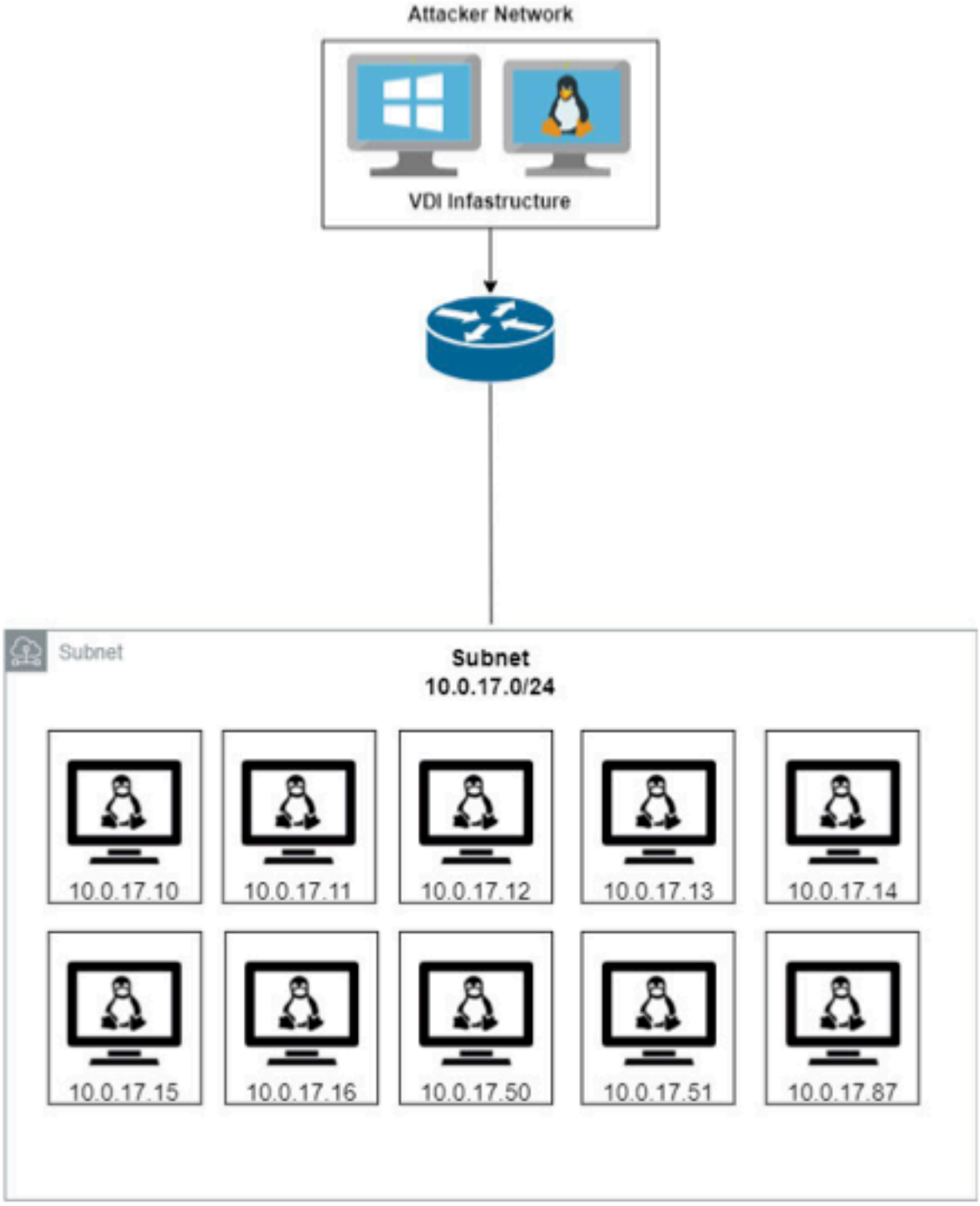

Figure 1.0: LBC Network Topology

Assessment Methodology

In the reconnaissance phase, [redacted]s penetration testers ran a moderate scan of the network in scope. This allowed the testers to find attack vectors such as open ports and provided useful information like the operating system of the machines and the services they provide. After a moderate scan, the penetration testers then ran a slow full port scan to discover potential uncommon attack vectors and ensure the scan does not overload the system.

Next, [redacted]s penetration testers tested any web applications hosted on the client's servers. This assessment ranged from web fuzzing to analyzing HTTP requests and responses. Following the discovery of sensitive credentials such as usernames and passwords, the penetration testers reused these credentials on any application or services that required authentication. After gaining access to the database and being able to read files, the testers checked for misconfigurations, outdated software, and exposed sensitive information. During this process, the testers took extreme caution not to modify the credentials of existing users on the system, so as not to affect LBC's employees and customers.

Lastly, [redacted]s penetration testers gathered evidence of the vulnerabilities found by taking screenshots and recording them, redacting any confidential information found in the recorded evidence. Upon exiting, the testers took the appropriate steps to remove access and artifacts from any vulnerable systems.

Severity and Risk Level Definitions

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

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

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

Severity Level Measures: To measure severity, the CVSS v3.1 standard is used. The Common Vulnerability Scoring System is an open industry standard for assessing the severity of a computer system security vulnerability. The basic score is used as a simple quantitative measure in collaboration with the score-to-rating chart in Fig 2.2A to provide a qualitative measure of the severity. The base vector string is also shown to give a better technical description of the vulnerability. The breakdown of the vector string is shown in Fig 2.2B.

A.) CVSS v3.1 Score-Rating Table

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

B.) CVSS v3.1 Base Vector String Breakdown

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

Fig 2.2. A legend for the usage of CVSS 3.1 metrics. (A) shows the qualitative severity ratings w/ the corresponding color depending on base score. (B) shows the breakdown of the CVSS Base Vector String. The vector string will compose of the field abbreviation (AV for Attack Vector) followed by a colon and the attribute abbreviated (N for Network). Each field is separated by forward slashes.

Risk Level Measures:

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

A.) Probability v Impact, Risk Matrix

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

	Low		m		High

B.) Score-to-Rating Chart

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

Fig 2.3. A legend for the scoring of risk level, probability, and impact. (A) shows the risk matrix for obtaining the qualitative risk level using the qualitative measures of probability and impact. (B) shows the corresponding rating which describes each range of probability, impact, and risk.

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

Key Findings

The 13 vulnerabilities found in LBC's enterprise infrastructure fall under 3 groups of security trends that are commonplace in the network. These four groups are weaknesses (1) Authentication, (2) Authorization, and (3) API.

Authentication:
In the LBC environment, [redacted] found multiple instances of SSH. The SSH users on these systems have strong passwords since none of our brute force attacks lead to the discovery of system credentials. On the other hand, there is no password required to access the MySQL and PostgreSQL database. Through the enumeration of these databases, we found that the LBC marketplace used the same passwords for their users.

Authorization:
While pentesting the LBC network, [redacted] did not discover any credentials related to internal employees. However, [redacted] did notice that the source code and the API key for the LBC marketplace are publicly available. Furthermore, [redacted] was able to compromise a MySQL database on the network to gain access to sensitive customer data.

API:
During the reconnaissance phase, [redacted] is able to find multiple API endpoints. Some API requires authentication to access their endpoints. However, some APIs do not need any authentication to change sensitive customer data. These API endpoints are being used by other web applications; as a result, it poses a serious risk to these web applications.

Recommended Response Plan

[redacted] was able to come up with a recommended response plan, so LBC can have an idea of what areas they need to fix immediately. The immediate fixes that needed to be prioritized are unauthorized access to PLC controls which you do not need a password to access, and little to no encryption in the database. We then

move on to unauthenticated access to API endpoints which can lead to an exhaustion of resources towards LBC.

Within the 30 days scope, [redacted] recommends solving password reuse, denial of service, and etc. Finally, [redacted] is able to provide you with some recommendations that you can do within 90 days or when it's possible. [redacted] recommends fixing anonymous login and adding some kind of password policy.

Potential Risk

Collectively, the 13 identified vulnerabilities expose LBC to a significant degree of business risk. The potential of external fraud exists in the forms of theft and hacking-related damage. Coupled with the possibilities of business disruption and system failures, these vulnerabilities pose a great operational risk to LBC. This compromises the company's ability to ensure confidentiality, availability, and integrity in its operations. Furthermore, the legal risks engendered by violations of PCI-DSS and GDPR regulations constitute a liability to possible significant monetary penalties. Having recently gone public, the same regulatory risks also present the company with reputational risk if investors find these vulnerabilities neglected, and can create further financial risk for the company.

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

Final Notes

Having shown improvement in strengthening their infrastructure's cybersecurity consistent with the recommendations provided during the last assessment, it is evident that LBC is committed to providing candy, croissants, and pastries to the region in a secure and reliable manner. [redacted] and its security engineers are proud to be able to offer their services to LBC and would be proud to further offer their services again to such a client that takes security seriously, should LBC require further evaluation of their network to improve their network security, upon which critical services in the region depend on. The security engineers offer LBC their regards and the best of luck as the company moves forward in its mission.

Compliances

As a part of France's food production and distribution industry, LBC must comply with standards set by national organizations to ensure that the company will be able to withstand attacks set upon it in an attempt to disrupt the company's services. Specifically, LBC must comply with the Payment Card Industry (PCI)
Data Security Standard(PCI-DSS) standards as a Payment Card provider and the General Data Protection Regulation (GDPR) laws as a member of the European Union.

PCI-DSS

As described earlier, the PCI-DSS standards are a set of mandated standards that all credit card handling companies must follow. Violation of these standards holds a company liable to significant monetary penalties of up to $500,000 USD per incident as an enforcement action. More information may be found on ***https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf***, under the "Detailed PCI-DSS Requirements and Security Assessment Procedure" dropdown. Note that the only standards considered by [redacted] were those which are still subject to enforcement on January 09, 2021, and those which could be tested within the time frame and the limited digital access provided. It is recommended LBC also consider those which are subject to future enforcement although they were not included in [redacted]s analysis. The references for each section of the standard which [redacted] uses are as follows:

Title	Reference
PCI-DSS	***https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf***

Req #	Requirements
1.1.7	Install and maintain a firewall configuration to protect cardholder data. Install a firewall at each internet connection(every device). Configure your firewalls with a description of groups responsible for network components and business justifications for all services/protocols/ports in the configuration. Review firewall and router configuration at least every 6 months and confirm all other, non-config traffic (inbound or outbound) is denied.Assign responsibility for someone to check firewall logs daily
2.1	Do not use vendor-supplied defaults for system passwords and other security parameters. Identify a sysadmin to be responsible for system components. Document policies to change vendor-supplied default passwords, default wireless settings and remove default accounts before installing a system on your network. Maintain an inventory list of all system components in scope for PCI-DSS.
2.2.d	Changing of all vendor-supplied defaults and elimination of unnecessary default accounts
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure
3.1	Protect stored cardholder data. Make sure the stored data and data in transit are unreadable. Use a data discovery tool to find misplaced sensitive data in your environment
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse
3.5.3	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data encrypting key, and that is stored separately from the data-encrypting key

	• Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry accepted method
3.6	Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data, as described in 3.6.1 - 3.6.8
3.6.1	Generation of strong cryptographic keys
3.6.2	Secure cryptographic key distribution
3.6.3	Secure cryptographic key storage
3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).
3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.
3.6.6	If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.
3.6.7	Prevention of unauthorized substitution of cryptographic keys.
3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key custodian responsibilities.
4.1	Encrypt transmission of cardholder data across open public networks. Identify where you send cardholder data and ensure your policies are not violated in the journey and only trusted keys or certificates are used.
5.1.1	Protect all systems against malware and regularly update antivirus software or programs. Regularly update anti-virus software on your commonly affected systems and evaluate whether additional systems are at risk of needing an antivirus. Automate anti-virus scans and maintain antivirus audit logs for your systems. Document procedures for protecting against malware
6.2	Develop and maintain secure systems and applications. Establish a process to keep up-to-date with the latest security vulnerabilities and identify the risk level. Use strict development processes and secure coding guidelines (outlined in DSS) when developing software in-house
7.2	Restrict access to cardholder data by business need to know. Create a list of roles with access to the CDE that includes the definition of each role, their privilege level, and what permissions are required for each role to function. Create a least-privilege policy for all employees and a default “deny-all” setting on all access control settings

8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.
8.2	Identify and authenticate access to system components. Define and document procedures for user identification and authentication on all system components. Assign unique IDs to all users, test those privilege controls, and revoke access on inactive/terminated users. Follow best practice guidelines outlined in DSS for password setting – including strong password composition, encrypting credentials, verifying ID before reset, and mandatory resets every 90 days.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.
8.2.3	Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.
8.2.4	Change user passwords/passphrases at least once every 90 days.
8.2.5	Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
8.2.6	Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.
9.1.1	Restrict physical access to cardholder data. Document process for physical access to CDE systems and a list of all devices, limiting access to roles that require it and monitoring all with authorization tokens and surveillance.
10.8	Track and monitor all access to network resources and cardholder data. Track all admin actions, login attempts, account changes, and pauses in the audit trail. Ensure each audit log captures user ID, event type, date and time, event success or failure, where the event originated from, and what resources are affected.
11.1	Regularly test security system and process
12.1	Maintain a policy that addresses information security for all personal

GDPR

The GDPR laws are a set of mandates that all businesses in the European Union must adhere to. Violation of GDPR holds a company liable to significant monetary penalties of up to $20 million euros or 4% of global revenue as an enforcement action. Furthermore, users affected by a breach are permitted to litigate against a non-compliant organization if their security measures have failed or are improper. Additional information on GDPR can be found at ***https://gdpr-info.eu/.*** Note that the only standards considered by [redacted] were those

which are still subject to enforcement on January 09, 2021, and those which could be tested within the time frame and the limited digital access provided. It is recommended LBC also consider mandates which are subject to future enforcement although they were not included in [redacted]s analysis.

In sum, GDPR regulates the handling and processing of PII for organizations within the EU and any external organization conducting business with entities inside the EU. The goal is to enforce a person's right to data privacy and protection by enforcing rules on how to move said data between entities and persons.

The regulation does not exhaustively list specific security measures for organizations to follow, rather it is up to every organization to create a security policy that works best for them while following the guidelines outlined in GDPR. Once a policy is established and roles are distributed, approval must be sought by accredited GDPR institutions to ensure compliance.

Regulations that LBC should specifically pay attention to are as follows:

Title	Reference
GDPR	***https://gdpr-info.eu/***

Article #	Requirements
12	1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.
15	1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: a. The purposes of the processing; b. The categories of personal data concerned; c. The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; d. Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

	e. The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; f. The right to lodge a complaint with a supervisory authority; g. Where the personal data are not collected from the data subject, any available information as to their source; h. The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. 2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
17	1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: a. The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; b. The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; c. The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); d. The personal data have been unlawfully processed; e. The personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; f. The personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
24	1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph shall include the implementation of appropriate data protection policies by the controller. 3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.
32	1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the

	processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: a. The pseudonymisation and encryption of personal data; b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
34	1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
40	1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph shall include the implementation of appropriate data protection policies by the controller. 3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.
78	1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. 2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.
79	1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.
82	1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
83	1. Infringements of the following provisions shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

NIST-SP

The National Institute of Standards and Technology (NIST) is an institution that creates non-regulatory standards that are accepted by a wide range of professional industries around the world. NIST has standards in cybersecurity, but the one most relevant to LBC is NIST-SP-800-82 which deals with ICS infrastructure. Other cybersecurity frameworks can be found at ***https://www.nist.gov/.***

NIST-SP-800-82 outlines the proper security measures for LBC to follow in their ICS environment. The compliance structure is semi-exhaustive, providing recommendations for almost every sector and scenario possible. Due to this, only the most relevant sections to LBC's environment and overarching vulnerabilities and security controls were included from the framework in [redacted]s report. Based on what was found in the environment, section 6.2.7 of the framework is the most relevant to the vulnerabilities and controls associated with LBCs ICS infrastructure.

Section 6.2.7 of NIST-SP-800-82 is as follows:

Title	Reference
NIST-SP-800-82	***https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final***

Section #	Requirements
6.2.7.1	• The length, strength, and complexity of passwords should balance security and operational ease of access within the capabilities of the software and underlying OS. • Passwords should have the appropriate length and complexity for the required security. In particular, they should not be able to be found in a dictionary or contain predictable sequences of numbers or letters. • Passwords should be used with care on operator interface devices such as control consoles on critical processes. Using passwords on these consoles could introduce potential safety issues if operators are locked out or delayed access during critical events. Physical security should supplement operator control consoles when password protection is not feasible. • The keeper of master passwords should be a trusted employee, available during emergencies. Any copies of the master passwords must be stored in a very secure location with limited access. • The passwords of privileged users (such as network technicians, electrical or electronics technicians and management, and network designers/operators) should be most secure and be changed frequently. Authority to change master passwords should be limited to trusted employees. • A password audit record, especially for master passwords, should be maintained separately from the control system. • In environments with a high risk of interception or intrusion (such as remote operator interfaces in a facility that lacks local physical security access controls), organizations should consider supplementing password authentication with other

	forms of authentication such as multi-factor authentication using biometric or physical tokens. • For user authentication purposes, password use is common and generally acceptable for users logging directly into a local device or computer. Passwords should not be sent across any network unless protected by some form of FIPS-approved encryption or salted cryptographic hash specifically designed to prevent replay attacks. It is assumed that the device used to enter a password is connected to the network in a secure manner. • For network service authentication purposes, passwords should not be passed as plain text. There are more secure alternatives available, such as challenge/response or public key authentication.
6.2.7.3	• Multi-factor authentication is an accepted good practice for access to ICS applications from outside the ICS firewall. • Physical/token authentication has the potential for a strong role in ICS environments. An access card or other token can be an effective form of authentication for computer access, as long as the computer is in a secure area (e.g., once the operator has gained access to the room with appropriate secondary authentication, the card alone can be used to enable control actions).
6.2.7.5	• Biometric devices make a useful secondary check versus other forms of authentication that can become lost or borrowed. Using biometric authentication in combination with token-based access control or badge-operated employee time clocks increases the security level. A possible application is in a control room that is environmentally controlled and physically secured. • Biometrics can provide a valuable authentication mechanism, but need to be carefully assessed for industrial applications because physical and environmental issues within the installation environment may need to be restructured for reliable authorized authentication. The exact physical and environmental properties of an installation should be coordinated with a system vendor or manufacturer

Technical Findings

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

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

Overview

Throughout the duration of the penetration test performed on LBC, [redacted] found 13 notable vulnerabilities in the company's network. Of these 13 vulnerabilities: 5 are critical, 4 are high severity, 2 are medium severity, and 2 are low severity. In addition to these, the penetration testers also found 1 informational non-vulnerability findings which warrant discussion and documentation.

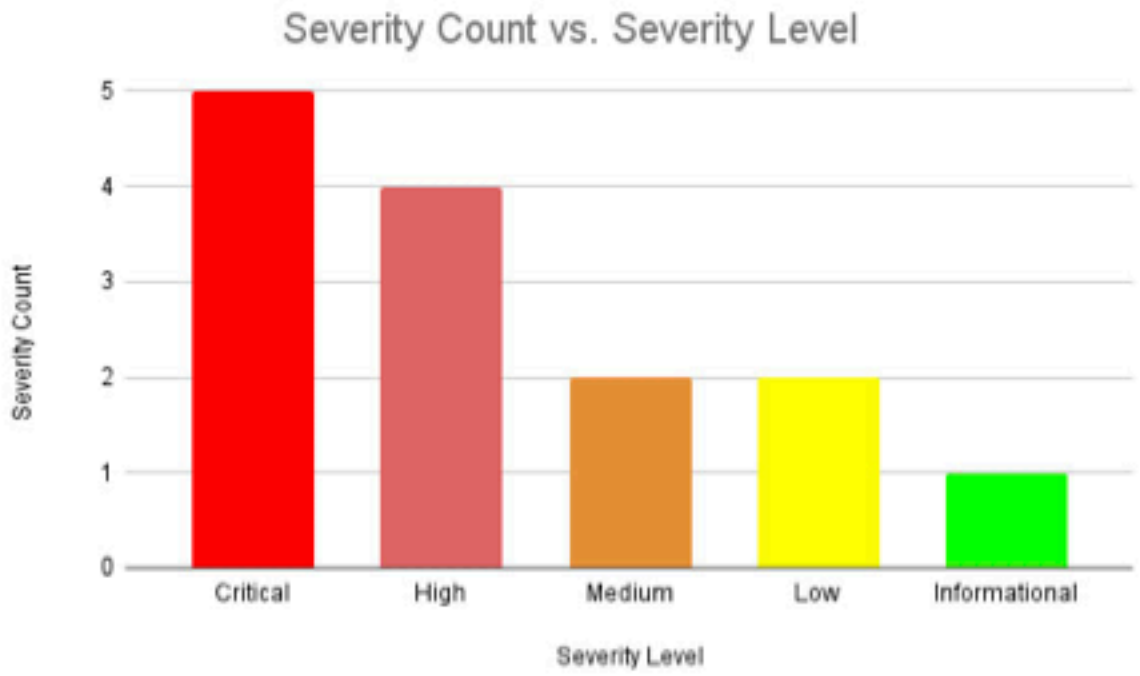

Figure 2.0: Bar graph on severity count vs severity level

Critical Findings:

Unauthenticated Access to Programmable Logic Controller

Affected Systems			
IP Address	Port	Service	Version
10.0.17.51	2001/tcp	PLC	N / A

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Critical	Score	9.9
Vector	AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:L		

Risk Matrix					
Risk Level	Very High	Impact	Very High	Probability	Very High

Details:

During [redacted]s reconnaissance of the SCADA infrastructure, a programmable logic controller (PLC) was detected. Upon further enumeration of the PLC, [redacted] was able to connect without authenticating. Once connected a Guru Meditation error was displayed leading [redacted] to halt testing in order to not disrupt the availability of the critical infrastructure.

Business Impact:

Authentication access to PLC can lead to an attacker bringing the entire LBC supply chain down, costing the companies millions of dollars. Alongside this financial cost, access can cause customers to lose confidence in LBC, potentially costing LBC a huge financial loss in future profits.

Attack Replication:

1. Listen to port 2001: `nc 10.0.17.51 2001`

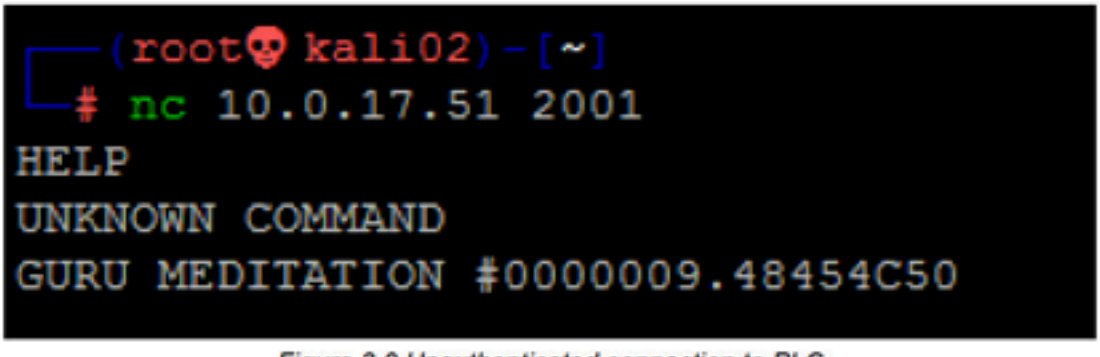

Figure 3.0 Unauthenticated connection to PLC

Recommended Remediation:

Every ICS within the environment needs to have a form of authentication to ensure continued availability and integrity of critical systems. Standard password, physical token, and biometric authentication are measures NIST-SP recommends to properly secure ICS infrastructure. NIST-SP provisions include the following:

- NIST-SP-800-82
    - 6.2.7.1 - Password Authentication
        - The length, strength, and complexity of passwords should balance security and operational ease of access within the capabilities of the software and underlying OS.
        - Passwords should have appropriate length and complexity for the required security. In particular, they should not be able to be found in a dictionary or contain predictable sequences of numbers or letters.
        - Passwords should be used with care on operator interface devices such as control consoles on critical processes. Using passwords on these consoles could introduce potential safety issues if operators are locked out or delayed access during critical events. Physical security should supplement operator control consoles when password protection is not feasible.
        - The keeper of master passwords should be a trusted employee, available during emergencies. Any copies of the master passwords must be stored in a very secure location with limited access.
        - The passwords of privileged users (such as network technicians, electrical or electronics technicians and management, and network designers/operators) should be most secure and be changed frequently. Authority to change master passwords should be limited to trusted employees.
        - A password audit record, especially for master passwords, should be maintained separately from the control system.
        - In environments with a high risk of interception or intrusion (such as remote operator interfaces in a facility that lacks local physical security access controls), organizations should consider supplementing password authentication with other forms of authentication such as multi-factor authentication using biometric or physical tokens.
        - For user authentication purposes, password use is common and generally acceptable for users logging directly into a local device or computer. Passwords should not be sent across any network unless protected by some form of FIPS-approved encryption or salted cryptographic hash specifically designed to prevent replay attacks. It is assumed that the device used to enter a password is connected to the network in a secure manner.
        - For network service authentication purposes, passwords should not be passed as plain text. There are more secure alternatives available, such as challenge/response or public key authentication.
    - 6.2.7.3
        - Multi-factor authentication is an accepted good practice for access to ICS applications from outside the ICS firewall.
        - Physical/token authentication has the potential for a strong role in ICS environments. An access card or other token can be an effective form of authentication for computer

access, as long as the computer is in a secure area (e.g., once the operator has gained access to the room with appropriate secondary authentication, the card alone can be used to enable control actions

- 6.2.7.5
    - Biometric devices make a useful secondary check versus other forms of authentication that can become lost or borrowed. Using biometric authentication in combination with token-based access control or badge-operated employee time clocks increases the security level. A possible application is in a control room that is environmentally controlled and physically secured.
    - Biometrics can provide a valuable authentication mechanism, but need to be carefully assessed for industrial applications because physical and environmental issues within the installation environment may need to be restructured for reliable authorized authentication. The exact physical and environmental properties of an installation should be coordinated with a system vendor or manufacturer

Passwordless Authentication to PostgreSQL Database

Affected Systems			
IP Address	Port	Service	Version
10.0.17.14	5431/tcp	PostgreSQL	12.9

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Critical	Score	9.8
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Risk Matrix					
Risk Level	Very High	Impact	Very High	Probability	Very High

Details:

[redacted] was able to log in to PostgreSQL database with a default username and without a supplied password. A malicious actor could log in to the database and gain access to sensitive customer credit card information and payment information, along with other personal identifiable information (PII). Through the database, an adversary can also read internal system information important to LBC operations.

Business Impact:

All companies that accept, process, store, or transmit credit card information must maintain a secure environment to prevent a data leak. Failure to do so results in loss of trust in confidentiality and integrity of business services.

A malicious actor with access to the database provides access to all Personal Identifiable Information (PII), such as credit card information and names, and other sensitive information hosted on the marketplace. With this information, a malicious actor can cause serious damage to LBC and its loyal customers. Such a compromise leads to loss of confidentiality and integrity of marketplace systems and information, giving LBC a bad public image.

Financially, LBC may be fined thousands of dollars for not complying with PCI-DSS and GDPR security standards, and lawsuits from customers. Additionally, a breach of customer PII may result in loyal customers choosing not to shop with LBC, reducing long and short-term profits.

Attack Replication:

1. Login to PostgreSQL by executing: `psql -h 10.0.17.14 -U postgres`

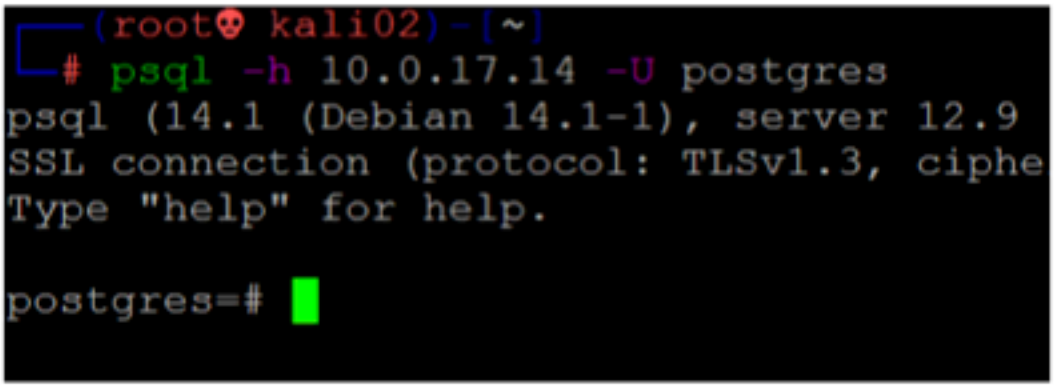

Figure 4.0 Connecting to a confidential PostgreSQL database without supplying a password.

Recommended Remediation:

All services are required to have a form of authentication to prevent adversaries from compromising the confidentiality and integrity of systems and the confidentiality of customer PII, such as credit card information stored on the PostgreSQL database. To comply with PCI-DSS and GDPR, a strong password policy is necessary to secure the service. Compliance implementation involve:

- PCI-DSS
  - 2.2.d Changing of all vendor-supplied defaults and elimination of unnecessary default accounts
  - 8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components
  - 8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.
  - 8.2 Identify and authenticate access to system components
  - 8.2.1 Use strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.
  - 8.2.3 Passwords/passphrases must meet the following:
    - Require a minimum length of at least seven characters.
    - Contain both numeric and alphabetic characters.
  - 8.2.4 Change user passwords/passphrases at least once every 90 days.
  - 8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
  - 8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.
- GDPR
  - Art. 32
    - The pseudonymisation and encryption of personal data;
    - The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
    - The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Passwordless Access to MySQL Database

Affected Systems			
IP Address	Port	Service	Version
10.0.17.14	3306/tcp	MySQL	10.3.32

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Critical	Score	9.4
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L		

Risk Matrix					
Risk Level	Very High	Impact	Very High	Probability	Very High

Details

Authentication is the process of verifying an individual to access a service. [redacted] found that the MySQL database did not require a password to authenticate as the root user. A malicious actor could easily gain operational control over the database, allowing them to read sensitive customer account information and poison the database with malicious data. The malicious actor can also read internal system information that is proprietary to LBC.

Business Impact:

A database compromise on LBC's marketplace carries with it serious reputational and financial repercussions. A malicious actor with access to the database provides access to all Personal Identifiable Information (PII), such as credit card information and names, and other sensitive information hosted on the marketplace. With this information, a malicious actor can cause serious damage to LBC and its loyal customers. Such a compromise leads to loss of confidentiality and integrity of marketplace systems and information, giving LBC a bad public image.

Financially, LBC may be fined thousands of dollars for not complying with PCI-DSS and GDPR security standards, and lawsuits from customers. Additionally, a breach of customer PII may result in loyal customers choosing not to shop with LBC, reducing long and short-term profits.

Attack Replication:

1. Login to MySQL by executing: `mysql -h 10.0.17.14`

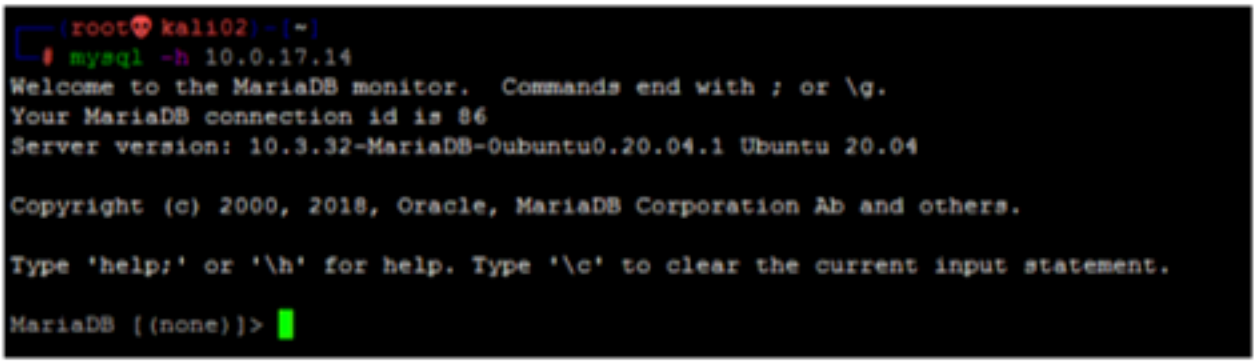

Figure 5.0 Connecting to the MySQL server without supplying a password.

Recommended Remediation:

Authentication is required for every service to prevent unauthorized persons from compromising the confidentiality and integrity of systems and confidentiality of customer PII, such as credit card information stored on the MySQL Database. A strong password policy is needed to prevent attackers from achieving this, while also complying with PCI-DSS and GDPR. Compliance with these frameworks includes:

- PCI-DSS
  - 8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components
  - 8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.
  - 8.2 Identify and authenticate access to system components
  - 8.2.1 Use strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.
  - 8.2.3 Passwords/passphrases must meet the following:
    - Require a minimum length of at least seven characters.
    - Contain both numeric and alphabetic characters.
  - 8.2.4 Change user passwords/passphrases at least once every 90 days.
  - 8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
  - 8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.
- GDPR
  - Art. 32
    - The pseudonymisation and encryption of personal data;
    - The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
    - The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Weak Encryption on Databases

Affected Systems			
IP Address	**Port**	**Service**	**Version**
10.0.17.14	3306/tcp 5432/tcp	MySQL PostgreSQL	10.3.32 12.9

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Critical	Score	9.1
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N		

Risk Matrix					
Risk Level	Very High	Impact	Very High	Probability	High

Details:

Weak encryption on the databases allowed [redacted] to exfiltrate sensitive personal identifiable information on multiple databases. [redacted] obtained credit card information, addresses as well as password information. The weak encryption allows a malicious actor to abuse the information to perform identity theft of customers, hijack LBC marketplace accounts, and much more.

Business Impact:

A weak encryption on LBC's databases finds itself to be in violation of confidentiality. It also can cause serious reputational damage and/or Intellectual Property Theft. LBC's database contained password and payment information due to weak encryption. A malicious actor with access to the database provides them access to all Personal Identifiable Information (PII), such as credit card information and full names as well as other sensitive information that is hosted on the database. It would lead to many violations such as confidentiality, information theft, intellectual property theft, and code theft.

Financially, LBC may be subject to lawsuits from affected customers. They may also be fined thousands of dollars for not complying with PCI-DSS and GDPR security standards. In addition, LBC may take a hit on their reputation as customers may no longer choose to do business with the company.

Attack Replication:

1. Query the customer info on MySQL: `use wmic; SELECT * FROM logins;`

Figure 6.0 Output of MySQL query showing sensitive credentials.

2. Query the PostgreSQL info on pgAdmin:
    a. In pgAdmin, log into PostgreSQL on 10.0.17.14 with the user "postgres" without supplying a password.
    b. Then, query the billing table in the Jawbreaker database to access the confidential information.

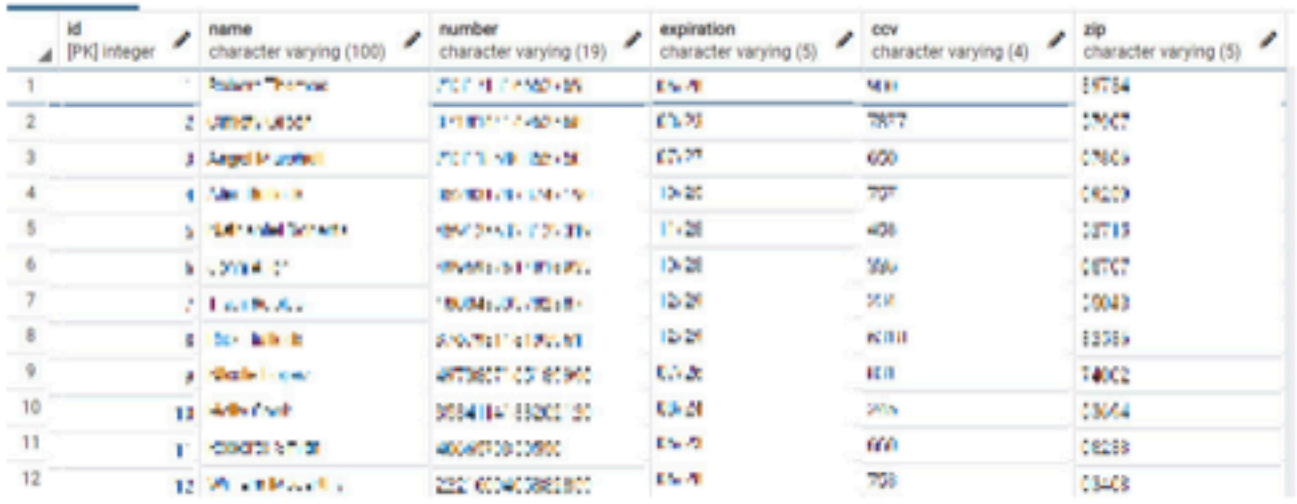

Figure 5.0 Output of PostgreSQL query displaying cardholder information.

Recommended Remediation:

Any and all customer and organization member PII including names, addresses, credit card information, and passwords, must be encrypted. Failure to do so will result in attackers acquiring and using the PII against customers and the organization as a whole. This leads to loss of confidentiality and integrity of business systems. To prevent this, PCI-DSS and GDPR recommend:

- PCI-DSS
    - 3.1 Protect stored cardholder data. Make sure the stored data and data in transit are unreadable. Use a data discovery tool to find misplaced sensitive data in your environment
    - 3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:
        - 3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:
            - Encrypted with a key-encrypting key that is at least as strong as the data encrypting key, and that is stored separately from the data-encrypting key

        - Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device)
        - As at least two full-length key components or key shares, in accordance with an industry accepted method
    - 3.6 Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data, as described in 3.6.1 - 3.6.4 and 3.6.6
        - 3.6.1 Generation of strong cryptographic keys
        - 3.6.2 Secure cryptographic key distribution
        - 3.6.3 Secure cryptographic key storage
        - 3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key
        - owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).
        - 3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.
    - 4.1 Encrypt transmission of cardholder data across open public networks. Identify where you send cardholder data and ensure your policies are not violated in the journey and only trusted keys or certificates are used.
    - 8.2.1 Use strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.
- GDPR
    - Art. 32
        - The pseudonymisation and encryption of personal data

Unauthenticated Access to API Endpoints

Affected Systems			
IP Address	Port	Service	Version
10.0.17.10 10.0.17.11 10.0.17.13	80/tcp 443/tcp	Jawbreaker FastAPI SwaggerAPI	1.0.0 0.1.0 0.0.1

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Critical	Score	9.1
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N		

Risk Matrix					
Risk Level	Very High	Impact	Very High	Probability	High

Details:

During enumeration, [redacted] detected multiple API endpoints that could be queried unauthenticated. These endpoints returned various information regarding invoices, account information, and payment details. Specifically, the Jawbreaker API endpoints output payment information and payment invoices. The FastAPI endpoints could be used to add users and monetary rewards to the gift card platform. Lastly, the SwaggerAPI contains information regarding the type of payment, customer, and invoices. The unauthenticated endpoints can be easily leveraged by a malicious actor to steal from LBC for financial gain.

Business Impact:

The API handles essential business information that contains information subject to regulatory compliances like PCI-DSS. Access to API endpoints leads to exhaustion of resources which would affect user interfaces. In the case of LBC, the APIs found in the network work hand in hand with some of the services found in the network. Such an attack leads to loss of confidentiality, integrity, and availability of all the services available in the network, giving LBC a bad public image.

Financially, LBC may be fined thousands of dollars for not complying with PCI-DSS and GDPR security standards. Furthermore, funds may be stolen from LBC and its customers.

Attack Replication:

1. Visit http://10.0.17.11/docs to execute the unauthenticated API endpoints.
    a. Note: Endpoints with a lock to the right require authentication.

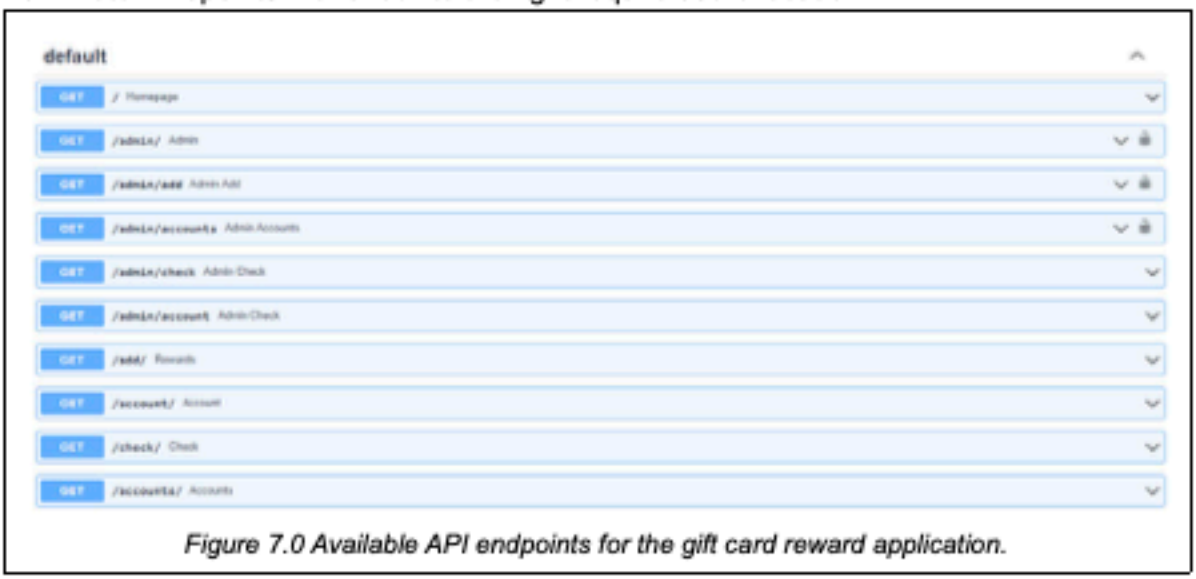

Figure 7.0 Available API endpoints for the gift card reward application.

2. Access http://10.0.17.10/doc to run API endpoints that can return and modify payment information for the marketplace.

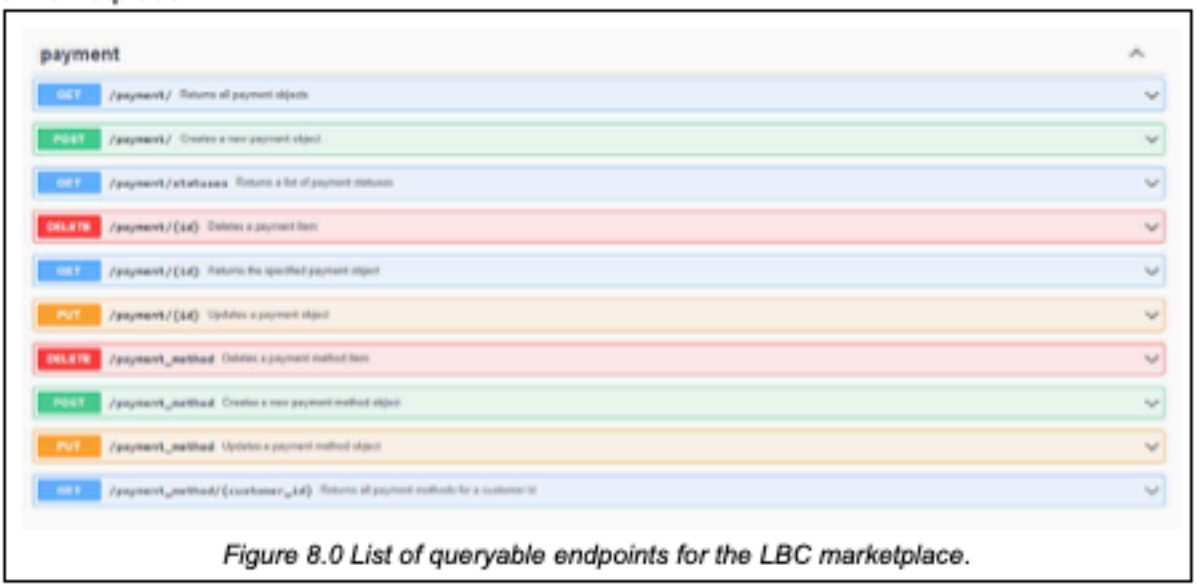

Figure 8.0 List of queryable endpoints for the LBC marketplace.

3. Visit http://10.0.17.13/v1/dt to see a list of endpoints that return payment, invoice, and customer information.

Figure 9.0 More endpoints that are utilized by the LBC marketplace for functionality.

Recommended Remediation:

All services are required to have a form of authentication to prevent adversaries from compromising the confidentiality and integrity of systems and the confidentiality of customer PII, such as credit card information stored on the PostgreSQL database. To comply with PCI-DSS and GDPR, a strong password policy is necessary to secure the service. Compliance implementation involves:

- PCI-DSS
  - 8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components
  - 8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.
  - 8.2 Identify and authenticate access to system components
  - 8.2.3 Passwords/passphrases must meet the following:
    - Require a minimum length of at least seven characters.
    - Contain both numeric and alphabetic characters.
  - 8.2.4 Change user passwords/passphrases at least once every 90 days.
  - 8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
  - 8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.
- GDPR
  - Art. 32
    - The pseudonymisation and encryption of personal data
    - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

High Risk Findings:

Password Reuse

Affected Systems			
IP Address	Port	Service	Version
10.0.17.12	80/tcp	HTTP	N/A

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	High	Score	8.1
Vector	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N		

Risk Matrix					
Risk Level	High	Impact	High	Probability	High

Details:

While enumerating the database, [redacted] discovered that clients' accounts were reusing the same credentials. Recycled credentials leave organizations that handle client data at risk as adversaries can pivot to other services using these credentials and leverage more information on the client, putting them at potential risk of financial loss and/or extortion.

Business Impact:

Reuse of credentials compromises the integrity of systems and confidentiality of customers which can lead to a loss of customers, resources, information, and profits.

Credential reuse can compromise the integrity of systems as a malicious actor could easily guess the correct credentials for a high-ranking company employee and extract and/or destroy information on the network. In either case, customer PII confidentiality is also at risk, potentially leading to lawsuits followed by fines from cyber security compliance violations, costing hundreds of thousands of dollars. These effects will lead to a loss of loyal customers, resources, proprietary information, and potential profits.

Attack Replication:

1. First, authenticate to the MySQL database `mysql -h 10.0.17.14`
2. Query the customer credentials by running `use wmci; SELECT * FROM logins;`
3. The credentials can be decoded in base64 to reveal its plaintext.

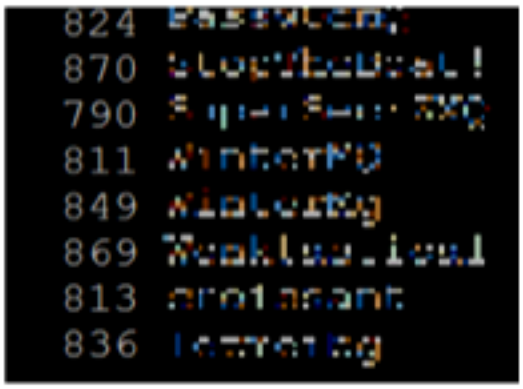

Figure 10.0 Six consistently reused passwords from LBC customers.

Recommended Remediation:

Passwords should never be reused. Failure to uphold a strong password policy consisting of complex and non-reusable passwords will result in loss of customer and organizational confidentiality and business integrity. Implementing PCI-DSS and GDPR controls will secure the information and place the company within compliance. The controls that should be put in place are:

- PCI-DSS
  - 8.2.3 Passwords/passphrases must meet the following:
    - Require a minimum length of at least seven characters.
    - Contain both numeric and alphabetic characters.
  - 8.2.4 Change user passwords/passphrases at least once every 90 days.
  - 8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
  - 8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.
- GDPR
  - Art. 32
    - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

Plain Text Credential in API Token

Affected Systems			
IP Address	Port	Service	Version
10.0.17.14	3306/tcp	MySQL	10.3.32

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	High	Score	8.1
Vector	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H		

Risk Matrix					
Risk Level	Very High	Impact	Very High	Probability	Medium

Details:

[redacted] obtained a hardcoded API key in the website source code. The API key was then decoded to obtain plain text credentials. These credentials could then be used to access the MySQL database and access the customer's confidential information. A malicious actor could easily use the PII to extort LBC customers for financial gain. Damaging the clients' trust in LBC, and resulting in major financial loss.

Business Impact:

The organization has violated integrity by failing to keep API keys secure. Encrypting the credentials in plain text would allow unauthorized access to unwanted users.

It is an organization's responsibility to keep its user information safe. This includes making sure any kind of sensitive data to be encrypted in some kind of way. [redacted] was able to find an API Key in plain text in which an attacker could use it to access API endpoints and be able to exhaust company resources like money and time.

Attack Replication:

1. Decode the API key twice with base64 to reveal the plain text credential.

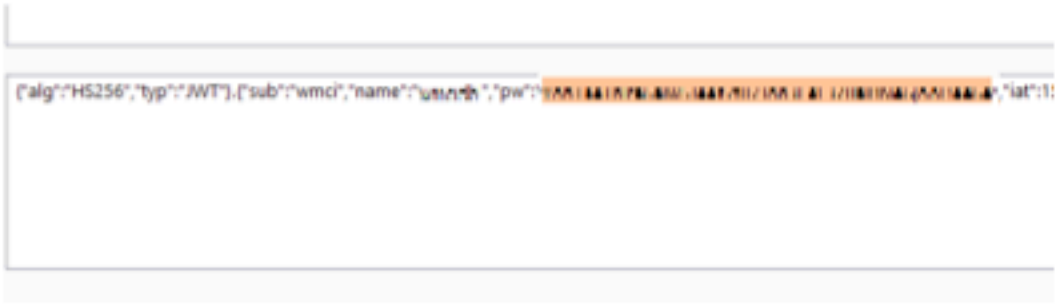

Figure 11.0 Contents of the decrypted API key. Which includes a plaintext database credential.

Recommended Remediation:

All information stored within organizational infrastructure must be either hashed or strongly encrypted to prevent adversaries from compromising customer and business accounts and infrastructure. Additionally, the transmission of these keys should be secure at all times. PCI-DSS and GDPR recommend:

- PCI-DSS
  - 3.6.1 Generation of strong cryptographic keys
  - 3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.
  - 8.2.1 Use strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components..
  - 8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
- GDPR
  - Art. 32
    - The pseudonymisation and encryption of personal data

Denial Of Service on API Infrastructure

Affected Systems			
IP Address	Port	Service	Version
10.0.17.10 10.0.17.11 10.0.17.13	80/tcp	Jawbreaker FastAPI SwaggerAPI	1.0.0 0.1.0 0.0.1

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	High	Score	7.4
Vector	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H		

Risk Matrix					
Risk Level	High	Impact	Very High	Probability	Medium

Details:

During enumeration, [redacted] detected that the API was not stable, and had consistent outages under heavy loads. The APIs are vital in the functionality of LBC's marketplace as they provide the marketplace with customer information, payment status, and more. A malicious actor could utilize the instability to put the API out of commission potentially damaging vital infrastructure. Leading to an overall loss of availability for services utilizing the API.

Business Impact:

If web APIs are out of service, LBC's marketplace can potentially lose thousands in financial loss for every second they are unavailable. Furthermore, LBC's relationship and reputation with their loyal customers will suffer. With the loss of integrity and confidentiality, LBC will struggle to keep their clientele all the while dealing with the financial burden of the unavailable API services.

Attack Replication:

1. Performing any heavy fuzzing or spidering will result in a server error. Putting the API endpoints out of operation.

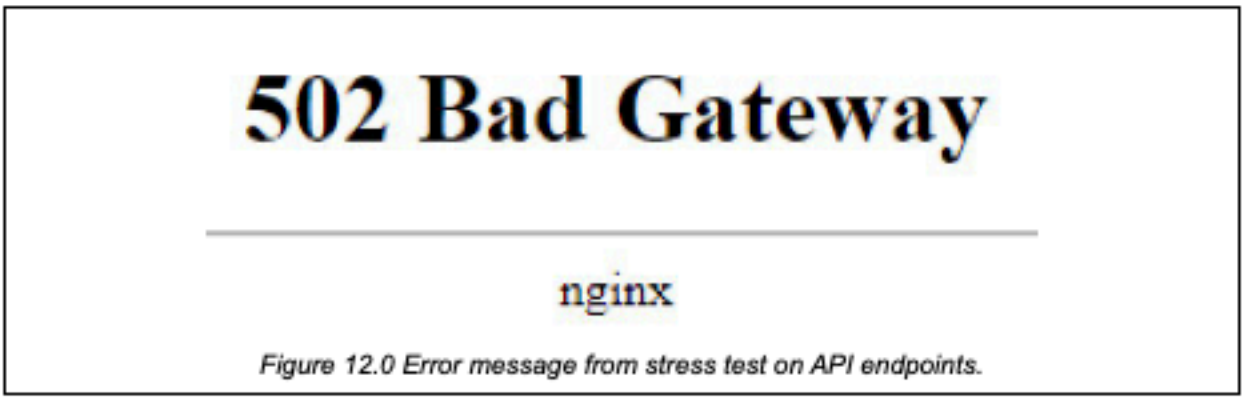

Figure 12.0 Error message from stress test on API endpoints.

Recommended Remediation:

The availability of the API and its subsequent websites is necessary for LBC's daily operations. To prevent potential DoS and DDoS attacks, network monitoring with NIDS software such as Snort must be implemented alongside IP blocking. With this setup, IPs can be automatically blocked for sending too much traffic.

Source Code Disclosure

Affected Systems			
IP Address	Port	Service	Version
10.0.17.12	80/tcp	HTTP	N/A

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	High	Score	7.3
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L		

Risk Matrix					
Risk Level	High	Impact	High	Probability	Medium

Details:

[redacted] found that the backend source code for the LBC's marketplace was publicly accessible to all who visited the site. By allowing the source code to be accessible on the client's browser, LBC is taking on more risks by allowing attackers to utilize the source code to exploit vulnerabilities.

Business Impact:

Public source code can lead to an increase in attacks on a web service. Public source code holds issues and bugs that may still need to be remediated. Attackers with direct access to the source code allows them to find these bugs and exploit them in a faster manner. Public access to source code would cost LBC a lot of resources to continuously patch issues at a fast pace in order to keep data secure. Furthermore, LBC will have difficulty maintaining the availability of the marketplace because of the constant threat of attack due to the source code leak. In this case, LBC's main shopping site would be left vulnerable for an attacker to exploit and gain access to sensitive customer information which can lead to customers losing trust in LBC and losing money. Compliances like GDPR and PCI-DSS would fine LBC thousands of dollars in such a case.

Attack Replication:

1. Visit `http://10.0.17.12`
2. Navigate to `static/js` to find the source code

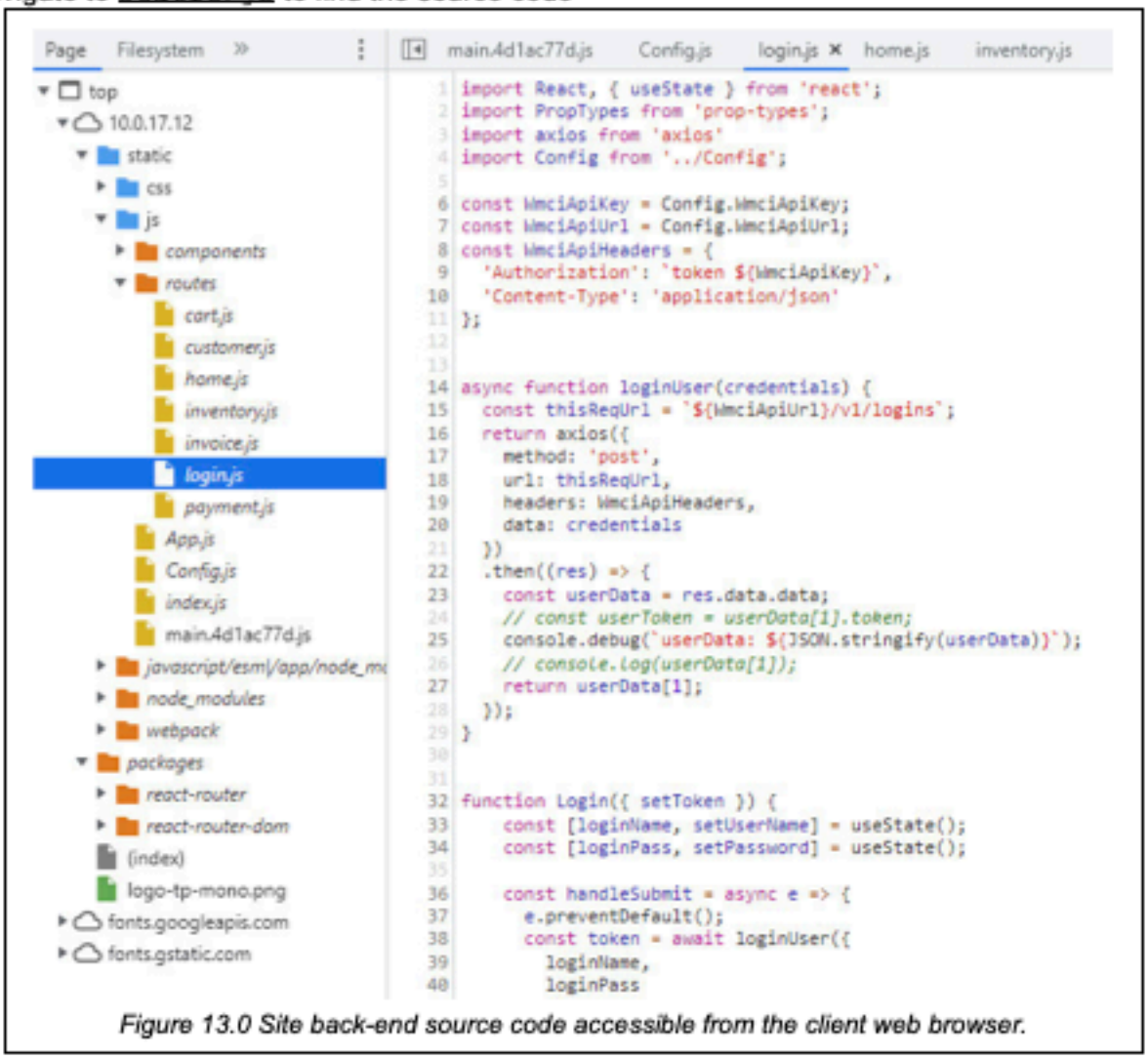

Figure 13.0 Site back-end source code accessible from the client web browser.

Recommended Remediation:

Lack of obfuscation on website code may result in loss of confidentiality, integrity, and availability of the site and the information stored on it. Remediation steps involve obfuscating the source code and/or utilizing HTML templates such as Ajax or jQuery. A template for the website will use the same discovered code, yet all code will be hidden and unavailable to the public, thereby protecting the software and other information utilized.

Medium Risk Findings:

API Key in HTTP Request

Affected Systems			
IP Address	Port	Service	Version
10.0.17.12	80/tcp	HTTP	N/A

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Medium	Score	5.0
Vector	AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L		

Risk Matrix					
Risk Level	Medium	Impact	High	Probability	Low

Details:

The team enumerated through the public source code and discovered that every authenticated user had the API token saved in the HTTP header response. A malicious actor could abuse this lack of confidentiality to access the various resources the API token has permissions to. Furthermore, the attacker could authenticate to the API endpoints and exfiltrate various information along with modifying critical information via the API.

Business Impact:

An API key that is compromised in the LBC network is carried with serious financial and reputational repercussions. In LBC's marketplace website, [redacted] found that an API key was being sent in a web response that is publicly available. A malicious actor with access to the API key is able to access API endpoints and exhaust the company's time and resources. This could lead to unavailable services, money exhaustion, and problems accessing user data. This could potentially cost LBC thousands of dollars in fines and lawsuits for not following compliance like PCI-DSS and GDPR. A breach of a customer PII may also result in loss of customer loyalty and company reputation.

Attack Replication:

1. Visit `http://10.0.17.12`
2. Navigate to `static/js/login.js` to find the source code of how the login works

```
const WmciApiKey = Config.WmciApiKey;
const WmciApiUrl = Config.WmciApiUrl;
const WmciApiHeaders = {
  'Authorization': `token ${WmciApiKey}`,
  'Content-Type': 'application/json'
};


async function loginUser(credentials) {
  const thisReqUrl = `${WmciApiUrl}/v1/logins`;
  return axios({
    method: 'post',
    url: thisReqUrl,
    headers: WmciApiHeaders,
    data: credentials
```

Figure 14.0 API key included in the header of the client's HTTP request.

Recommended Remediation:

All keys should be hidden and unavailable to unauthenticated and unauthorized users. Proper access controls need to be implemented wherein only authorized users can view keys. Additionally, no key should be hardcoded into a system or service, should instead be stored internally, and not present in the HTTP header in order to prevent loss of confidentiality and integrity. Finally, PCI-DSS and GDPR requirements must be followed which are:

- PCI-DSS
    - 3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse
    - 3.6.2 Secure cryptographic key distribution
    - 3.6.3 Secure cryptographic key storage
    - 8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components
    - 8.2.4 Change user passwords/passphrases at least once every 90 days.
    - 8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
- GDPR
    - Art. 32
        - The pseudonymisation and encryption of personal data

Hardcoded Publicly Disclosed API Key

Affected Systems			
IP Address	Port	Service	Version
10.0.17.12	80/tcp	SwaggerAPI	0.0.1

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Medium	Score	4.8
Vector	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N		

Risk Matrix					
Risk Level	Low	Impact	High	Probability	Low

Details:

During the engagement, [redacted] searched the previously obtained source code, and found a hardcoded API key in a configuration file. From the source code, the publicly available API key would allow a malicious actor access to any resources that the API key has permissions to. With the new level of access the attacker can exfiltrate various critical information from the API along with modifying sensitive values compromising the integrity of the system.

Business Impact:

API keys can be incredibly powerful, but must be safeguarded like any other credential. In a situation where an API key is exposed, the consequences can result in major damage to both the company and the data that it holds. In LBC's case, the API key was used to gain access to the system database that holds customer login information. This would have violated some compliances like PCI-DSS and GDPR which can lead to financial fines to the company regarding the safety of public information. Losing the trust of customers and possibility loss of information.

Attack Replication:

1. Navigate to static/js/Config.js in the Sources tab

Figure 15.0: API key is exposed to the public

Recommended Remediation:

All keys should be hidden and unavailable to unauthenticated and unauthorized users. Proper access controls need to be instilled wherein only authorized users can view keys. Additionally, no key should be hardcoded into a system or service, should change between user sessions and not be persistent, and should instead be stored internally. Finally, PCI-DSS and GDPR requirements must be followed which are:

- PCI-DSS
    - 3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse
    - 3.6.2 Secure cryptographic key distribution
    - 3.6.3 Secure cryptographic key storage
    - 8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components
    - 8.2.4 Change user passwords/passphrases at least once every 90 days.
    - 8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
- GDPR
    - Art. 32
        - The pseudonymisation and encryption of personal data

Low Risk Findings:

Memcache Anonymous Login

Affected Systems			
IP Address	Port	Service	Version
10.0.17.15	11211	Memcached	1.5.6

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Low	Score	3.7
Vector	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N		

Risk Matrix					
Risk Level	Medium	Impact	Low	Probability	Low

Details:

After enumerating through the subnet our security engineers detected that Memcache allows for anonymous login. Allowing Memcache to be queried anonymously could lead to an adversary accessing sensitive information within Memcache's keys. Memcache may store user hashes, user credentials, and other confidential information.

Business Impact:

Services that do not have a form of authentication do not comply with compliances like GDPR and PCI-DSS. Memcached, a service that is very popular to use along with web pages and databases, should not have anonymous login. Without any type of authentication, information about services can be dumped which can later lead to access to sensitive information that an attacker should not have. By not following GDPR and PCI-DSS may lead to fines of thousands of dollars alongside reputational loss by clientele.

Attack Replication:

1. Run memcstat and specify the target `memcstat --servers=10.0.7.15`

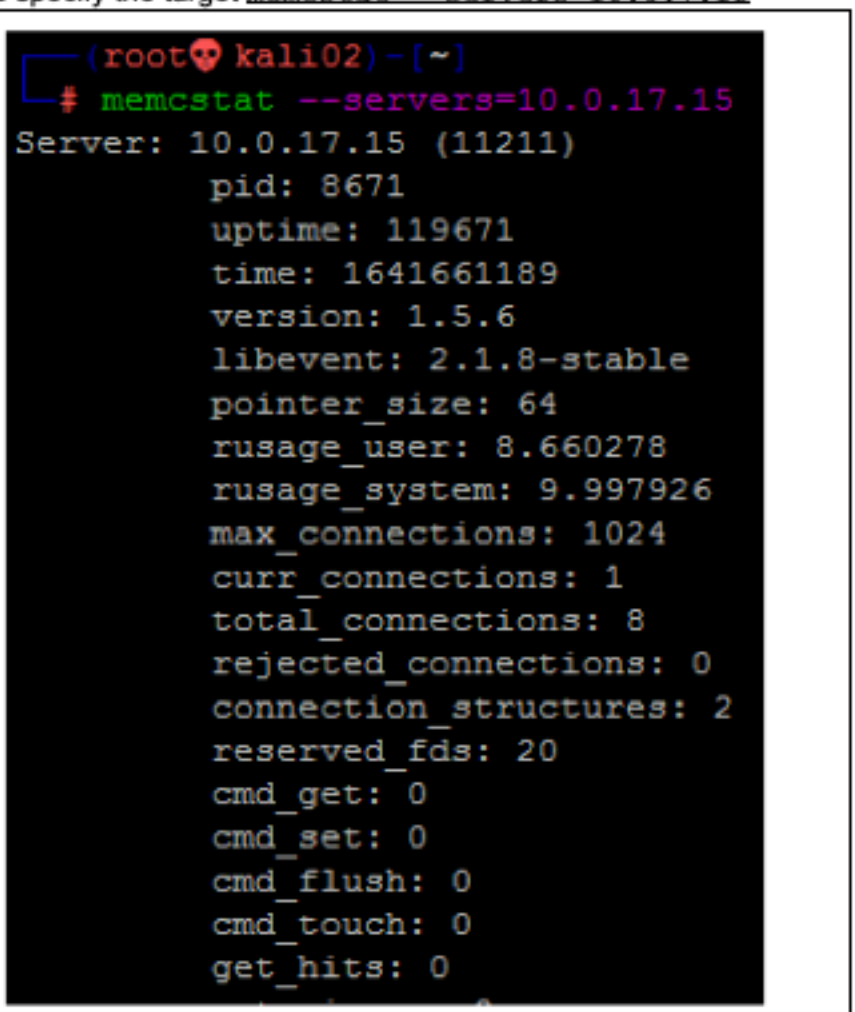

Figure 16.0: Anonymous login on Memcache querying configuration info

Recommended Remediation:

All services are required to have a form of authentication to prevent malicious actors from compromising the confidentiality and integrity of systems. To comply with PCI-DSS and GDPR, a strong password policy is necessary to secure the service. Compliance implementation involves:

- PCI-DSS
  - 8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components
  - 8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.
  - 8.2 Identify and authenticate access to system components
  - 8.2.3 Passwords/passphrases must meet the following:
    - Require a minimum length of at least seven characters.
    - Contain both numeric and alphabetic characters.
  - 8.2.4 Change user passwords/passphrases at least once every 90 days.

- 8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
- 8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.

- GDPR
  - Art. 32
    - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

Music Player Daemon Anonymous Login

Affected Systems			
IP Address	**Port**	**Service**	**Version**
10.0.17.87	**6600/tcp**	**Music Player Daemon**	**0.21.11**

Severity and Risk:

Common Vulnerability Scoring System (CVSS v3.1)			
Severity	Low	Score	3.1
Vector	AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N		

Risk Matrix					
Risk Level	Low	Impact	Low	Probability	Low

Details:

Anonymous login on the Music Player Daemon gives any user access to the service. Even though the daemon has very limited functionality, there should always be some form of authentication, so it prevents a threat from attacking.

Business Impact:

Every service should always have a form of authentication. Without proper authentication to the music player daemon, a malicious actor can influence the player to function in unintended ways or play inappropriate music. Although the effects are limited, the player should still be protected from potential attackers to keep availability high and employees happy as they conduct day-to-day operations.

Attack Replication:

1. Install the MPC client to connect to the music player daemon.
2. Once installed connect via the following command `mpc -h 10.0.17.87 stats`

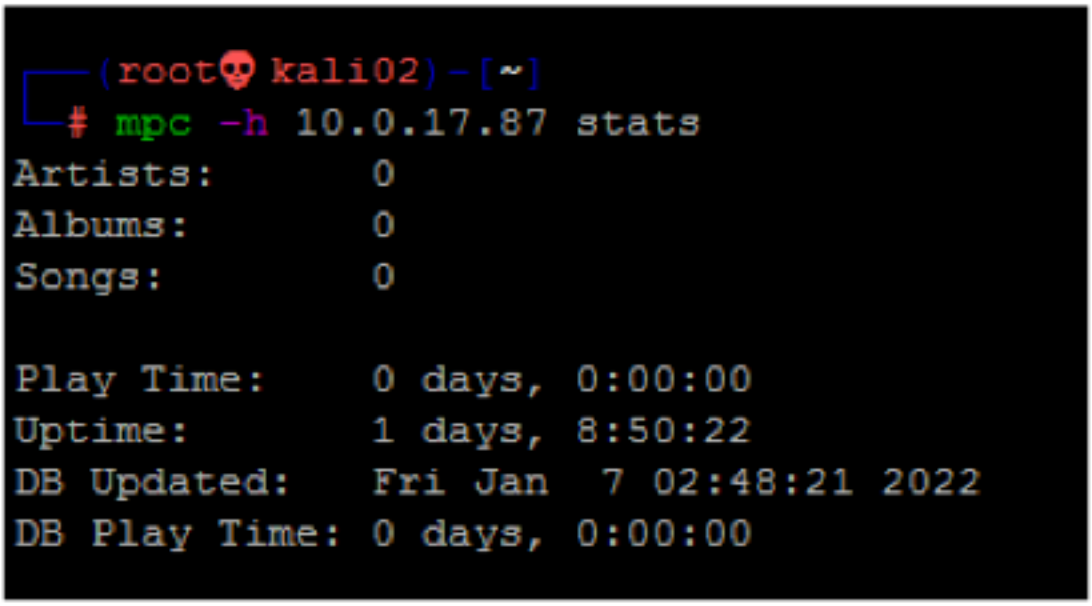

Figure 17.0: Anonymous login on MPD

Recommended Remediation:

All services are required to have a form of authentication to prevent malicious actors from compromising the confidentiality and integrity of systems. To comply with PCI-DSS and GDPR, a strong password and lockout policy are necessary to secure the service. Compliance implementation involves:

- PCI-DSS
  - 8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components
  - 8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.
  - 8.2 Identify and authenticate access to system components
  - 8.2.3 Passwords/passphrases must meet the following:
    - Require a minimum length of at least seven characters.
    - Contain both numeric and alphabetic characters.
  - 8.2.4 Change user passwords/passphrases at least once every 90 days.
  - 8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
  - 8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.
- GDPR
  - Art. 32
    - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

Informational Findings:

Weak Linux Password Policy

Affected Systems			
IP Address	Port	Service	Version
10.0.17.14	22/tcp	SSH	N/A

Details:

During [redacted]s enumeration, the team had discovered a weak password policy on Linux. The team noticed that the maximum number of days a password may be used is 99999 while the minimum is zero and a warning at seven days. Not requiring a periodic password can greatly increase the time window an adversary has to crack a password and gain access to the system.

Business Impact:

LBC, a company that holds user payment information carries with it serious reputational and financial repression by not implementing strong password policies.

Password policy is a set of rules created to improve computer security by motivating users to create dependable, secure passwords so they can be stored and utilized properly. A weak password policy can lead to a wide variety of attacks such as brute force and impersonation. Without a strong password policy, PCI-DSS regulations can demand a fine if LBC cannot protect sensitive payment information.

Attack Replication:

1. Read the /etc/login.defs in PostgreSQL by executing:
   `select pg_read_file('/etc/login.defs' , 0 , 1000000);`

```
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
```

Figure 18.0: Weak password policy

Recommended Remediation:

All systems and services on the network need a strong password policy to prevent loss of confidentiality and integrity. Without a solid policy, customers and organization members can be compromised. PCI-DSS mandates a password policy consisting of:

- PCI-DSS
    - 8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components
    - 8.2.3 Passwords/passphrases must meet the following:
        - Require a minimum length of at least seven characters.
        - Contain both numeric and alphabetic characters.
    - 8.2.4 Change user passwords/passphrases at least once every 90 days.
    - 8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
    - 8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.

Conclusion

As an established company in the candy, croissants, and pastry industry, Le Bonbon Croissant is a part of the food and distribution sector in France. With loyal customers inside and outside the company being dependent on the company's services, it is important that LBC take the security of their infrastructure seriously and comply with PCI-DSS, GDPR, and NIST-SP regulations. By hiring [redacted] to perform a penetration test on their network, along with the improvements in security consistent with the recommendations provided from the last assessment, it is evident that LBC takes security seriously and is committed to providing candy, croissants, and pastries to the people, in a reliable and secure way.

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

Principal Strengths in Security

LBC has made changes to the security of its networks since the last penetration test performed by [redacted] implementing most of the measures recommended in November 2021. These changes greatly reduce the potential attack vectors to which the company's network is vulnerable, and makes LBC much more compliant to the PCI-DSS standard and GDPR mandate.

1. Authorization: Throughout the environment, LBC has effectively implemented proper authorization controls. These controls were primarily seen through a principle of least privilege approach wherein customer and system users only had the authorization to access information and conduct business as intended. This security measure significantly reduces external access to the company's critical infrastructure while depriving potential intruders of the authorization needed to severely compromise the network. The aforementioned security systems are significant as they keep LBC compliant to various points in PCI-DSS, GDPR, and NIST standards, greatly reducing the company's exposure to regulatory risks by avoiding violation fines, as well as operational and financial risks in avoiding compromising the company's services and assets.

2. Authentication: LBC has also enforced strong authentication measures in most of its systems. With secure configurations that strictly require authentication on interfaces and stronger password policies that prevented the team from using basic brute force attacks, the company has truly improved in implementing its authentication systems. As a result, adversaries will certainly have a difficult time executing authentication bypassing attacks and brute force attacks against the company's systems

Principal Trends in Vulnerabilities

Although LBC has improved a few areas of security, vulnerabilities were still persistent. A number of these vulnerabilities were new to the environment compared to the previous engagement in November 2021. These vulnerabilities increase the potential attack vectors LBC's network is vulnerable to, making the company more likely to be attacked by a malicious actor

1. Authentication: In portions of LBC's network, systems and services had poor authentication. Weak password policies, default credentials, recycled credentials, and weak encryption were ever present, especially with customer accounts. Most passwords did not meet PCI-DSS standards, default or no credentials were utilized for critical databases holding sensitive customer information, passwords were reused hundreds of times, and poor encryption of passwords was stored in various places throughout the environment. All of these present significant risks to LBC's business operations as malicious outsiders could take advantage of these to take over accounts and potentially cause harm to LBC operations and its customers.

2. API: One of the largest problems encountered in LBC's primary websites centered around the API. Sensitive information disclosure, currency manipulation, database access, plaintext API keys, and an overall sensitive API system were rampant. These vulnerabilities make LBC susceptible to numerous attacks from adversaries that could compromise the integrity of the entire company.

Resultant Compliance to PCI-DSS

Taking into account both positive security controls as well as the vulnerabilities found within LBC's network, [redacted] has compiled the following compliance checklist. As noted earlier, many points have been omitted from the checklist due to the limited time frame and scope of [redacted]s evaluation, and only takes into account standards in enforcement as of January 09, 2021.

Y/N	Ref #	Requirements
N	1.1.7	Install and maintain a firewall configuration to protect cardholder data. Install a firewall at each internet connection(every device). Configure your firewalls with a description of groups responsible for network components and business justifications for all services/protocols/ports in the configuration. Review firewall and router configuration at least every 6 months and confirm all other, non-config traffic (inbound or outbound) is denied.Assign responsibility for someone to check firewall logs daily
N	2.1	Do not use vendor-supplied defaults for system passwords and other security parameters. Identify a sysadmin to be responsible for system components. Document policies to change vendor-supplied default passwords, default wireless settings and remove default accounts before installing a system on your network. Maintain an inventory list of all system components in scope for PCI-DSS.
N	2.2.d	Changing of all vendor-supplied defaults and elimination of unnecessary default accounts
N	2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure
N	3.1	Protect stored cardholder data. Make sure the stored data and data in transit are unreadable. Use a data discovery tool to find misplaced sensitive data in your environment
N	3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:
N	3.5.3	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:

		• Encrypted with a key-encrypting key that is at least as strong as the data encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry accepted method
N	3.6	Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data, as described in 3.6.1 - 3.6.8
N	3.6.1	Generation of strong cryptographic keys
N	3.6.2	Secure cryptographic key distribution
N	3.6.3	Secure cryptographic key storage
Y/N	3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57)
N	3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.
N	3.6.6	If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.
Y/N	3.6.7	Prevention of unauthorized substitution of cryptographic keys.
Y/n	3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key custodian responsibilities.
Y/N	4.1	Encrypt transmission of cardholder data across open public networks. Identify where you send cardholder data and ensure your policies are not violated in the journey and only trusted keys or certificates are used.
N	5.1.1	Protect all systems against malware and regularly update antivirus software or programs. Regularly update anti-virus software on your commonly affected systems and evaluate whether additional systems are at risk of needing an antivirus. Automate anti-virus scans and maintain antivirus audit logs for your systems. Document procedures for protecting against malware
N	6.2	Develop and maintain secure systems and applications. Establish a process to keep up-to-date with the latest security vulnerabilities and identify the risk level. Use strict development processes and secure coding guidelines (outlined in DSS) when developing software in-house
Y/N	7.2	Restrict access to cardholder data by business need to know. Create a list of roles with access to the CDE that includes the definition of each role, their privilege level, and what

		permissions are required for each role to function. Create a least-privilege policy for all employees and a default "deny-all" setting on all access control settings
N	8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components
	8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.
N	8.2	Identify and authenticate access to system components. Define and document procedures for user identification and authentication on all system components. Assign unique IDs to all users, test those privilege controls, and revoke access on inactive/terminated users. Follow best practice guidelines outlined in DSS for password setting – including strong password composition, encrypting credentials, verifying ID before reset, and mandatory resets every 90 days.
N	8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.
N	8.2.3	Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.
N	8.2.4	Change user passwords/passphrases at least once every 90 days.
N	8.2.5	Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
N	8.2.6	Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.
Y/N	9.1.1	Restrict physical access to cardholder data. Document process for physical access to CDE systems and a list of all devices, limiting access to roles that require it and monitoring all with authorization tokens and surveillance.
Y	10.8	Track and monitor all access to network resources and cardholder data. Track all admin actions, login attempts, account changes, and pauses in the audit trail. Ensure each audit log captures user ID, event type, date and time, event success or failure, where the event originated from, and what resources are affected.
Y	11.1	Regularly test security system and process
N	12.1	Maintain a policy that address information security for all personal

Resultant Compliance to GDPR

Centered on the discovered vulnerabilities and positive security controls found within LBC's network, an assessment was conducted on GDPR compliance. GDPR does not exhaustively list specific security measures

for organizations to follow, rather it is up to every organization to create a security policy that works best for them while following the guidelines outlined in GDPR. Once a policy is established and roles are distributed, approval must be sought by accredited GDPR institutions to ensure compliance. Notwithstanding this fact, there are general guidelines to follow.

Based on [redacted]s testing, LBC is in severe violation of the General Data Protection Regulation. The framework mandates in article 32 the use of encrypted user information, ensuring the confidentiality, integrity, and availability of systems, services, and information at all times, and informing customers of a breach within a timely manner. From the discovered vulnerabilities and the information provided to [redacted] by LBC, the company is in danger of incurring legal and financial penalties from GDPR enforcement.

Although this violation and risk may come as a surprise to LBC, [redacted] would like to reassure LBC that by hiring [redacted] to conduct a penetration test on their systems, LBC is taking the proper steps and procedures to secure their systems and coming into compliance with GDPR, procedures which are also mandated in article 32 of the regulation.

Resultant Compliance to NIST-SP-800-82

NIST-SP-800-82 outlines the proper security measures for LBC to follow in their ICS environment. The compliance structure is semi-exhaustive, providing recommendations for almost every sector and scenario possible. Due to this, only the most relevant sections to LBC's environment and overarching vulnerabilities and security controls were included from the framework in [redacted]s report.

Based on the most relevant section to LBC's environment, section 6.7.2, and its sub-categories, LBC is at risk of violating the NIST standard. Although there are no specific repercussions from violating the framework as it is non-regulatory, NIST is globally recognized and used in frameworks, such as the European Union Agency for Cybersecurity (ENISA), that are relevant to LBC and its operations. These alternative frameworks may have financial implications if violated. As such, the recommendations provided in NIST-SP-800-82 section 6.7.2 should be taken seriously and implemented in LBC's environment to ensure the integrity and availability of their critical infrastructure is undisturbed.

Resultant Risk Analysis

The 14 vulnerabilities detailed within the report exposes LBC to a significant degree of business risk. The first of these is the operational risk brought directly by cyber vulnerabilities. This risk comes in the form of the potential for external fraud, like theft, brought about by the compromise of confidentiality and integrity leading to the theft of intellectual property as well as other assets with obtained credentials. Any damages leading to the compromise of availability of LBC's services caused by the exploitation of these vulnerabilities are also classified as external fraud which poses an operational risk to LBC.

Furthermore, some of the vulnerabilities found may qualify as violations of PCI-DSS. Should such violations be found and remain unmitigated, they may pose regulatory risks to LBC as well as a financial risk due to the

possibility of significant monetary penalties of up to $500,000 per incident. Additionally, if the same violations are publicized through a Notice of Penalty posted on the PCI-DSS website, they may also pose a reputational risk to the company. With the company being well established and continually growing, this risk also amounts to potential financial risk if investors lose trust in the company.

Finally, violations to GDPR were present in a few vulnerabilities. Such violations can lead to regulatory risk and financial risk from fines of up to 20,000,000 euros, or 4% of total global revenue (whichever is higher), along with litigation from disgruntled customers, should these risks remain unmitigated. Similar to PCI-DSS, if a Notice of Penalty is released by GDPR standards, these vulnerabilities may also pose a reputational risk to the company, leading to a tarnished public image and dissatisfied customers and further financial risk from lost investors.

Recommended Improvements

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

Recommended Response Plan		
Time Horizon	**Vulnerability**	**Response**
Urgent Mitigation	Unauthenticated Access to Programmable Logic Controller	PLC needs to have a form of authentication to ensure continued availability and integrity of critical systems while complying with NIST-SP-800-82. Some forms of authentication include password authentication, multi-factor authentication and biometric authentication.
	Weak Encryption on Databases	Implement strong encryption for all PII stored on all databases that comply with both PCI-DSS and GDPR compliance recommendations, such as SHA256
	Passwordless Authentication to MySQL and PostgreSQL	Have authentication for all users accessing the database by removing default or vendor-supplied credentials. Put in place PCI-DSS password recommendations.
	Unauthenticated Access to API Endpoints	All services are required to have a form of authentication to prevent adversaries from compromising the confidentiality and integrity of

		the system. To help comply with GDPR and PCI-DSS we are going to need to define some strong password credentials and encryption
Within 30 days	Plain Text Credential in API Token	All information stored within organizational infrastructure must be either hashed or strongly encrypted to prevent adversaries from compromising customer and business accounts and infrastructure. Additionally, the transmission of these keys should be secure at all times.
	Password Reuse	Implement a strong password policy that complies with both PCI-DSS and GDPR. PCI-DSS and GDPR control will secure the information and place the company in compliance.
	Denial of Service on API Infrastructure	Any type of key should be hidden and unavailable to authenticated and authorized users. Proper access control needs to be placed. The API key should be stored internally.
	Source Code Disclosure	All keys should be hidden and unavailable to unauthenticated and authorized users. Proper access control needs to be placed. The API key should be stored internally and while being stored they should also be encrypted in a form that complies with both PCI-DSS and GDPR.
Within 60 days	API Key in HTTP Request	All keys should be hidden and unavailable to unauthenticated and unauthorized users. Proper access controls need to be implemented wherein only authorized users can view keys.
	Hardcoded Publicly Disclosed API Key	All keys should be hidden and unavailable to unauthenticated and unauthorized users. Proper access controls need to be instilled wherein only authorized users can view keys. Additionally, no key should be hardcoded into a system or service, should change between user sessions and not be persistent, and should instead be stored internally.
Within 90 days	Memcache Anonymous Login	All services are required to have a form of authentication to prevent malicious actors from compromising the confidentiality and integrity of systems. To comply with PCI-DSS and GDPR, a strong password policy is necessary to secure the service
	Music Player Daemon Anonymous Login	All services are required to have a form of authentication to prevent malicious actors from compromising the confidentiality and integrity of

		systems. To comply with PCI-DSS and GDPR, a strong password and lockout policy are necessary to secure the service
When possible	Weak Linux Password Policy	All systems and services on the network need a strong password policy to prevent loss of confidentiality and integrity. Without a solid policy, customers and organization members can be compromised. PCI-DSS mandates a password policy.

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

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

Final Notes

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

While only having recently gained the resources to modernize LBC's network, [redacted] is proud to report that the company is taking steps to improve its network's cybersecurity within a short period of time. [redacted] is especially pleased to see just how serious LBC is about their cybersecurity standing in seeing that recommendations provided during the last engagement have been implemented to some degree by the company.

Despite this improvement, it is important that LBC does not grow complacent and proactively respond to threats by continuously keeping itself updated on the state of its security and continuously improving it. To do so, [redacted] urges LBC to heed the technical findings documented in the report along with the recommended responses provided with it. By paying close attention to the vulnerabilities found within the network and by considering the recommended response plans outlined by [redacted] LBC may find itself to be more able in achieving its security and reliability goals.

The security engineers offer LBC their regards and wish them the best of luck as the company moves forward in modernizing its infrastructure, and in its mission to provide candy, croissants, and pastries reliably, with security and reliability in mind. [redacted] hopes to conduct business with LBC again in the near future, to provide further services in assessing the company's security and help the company become more secure.

Appendix

APPENDIX A: Network Diagram

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

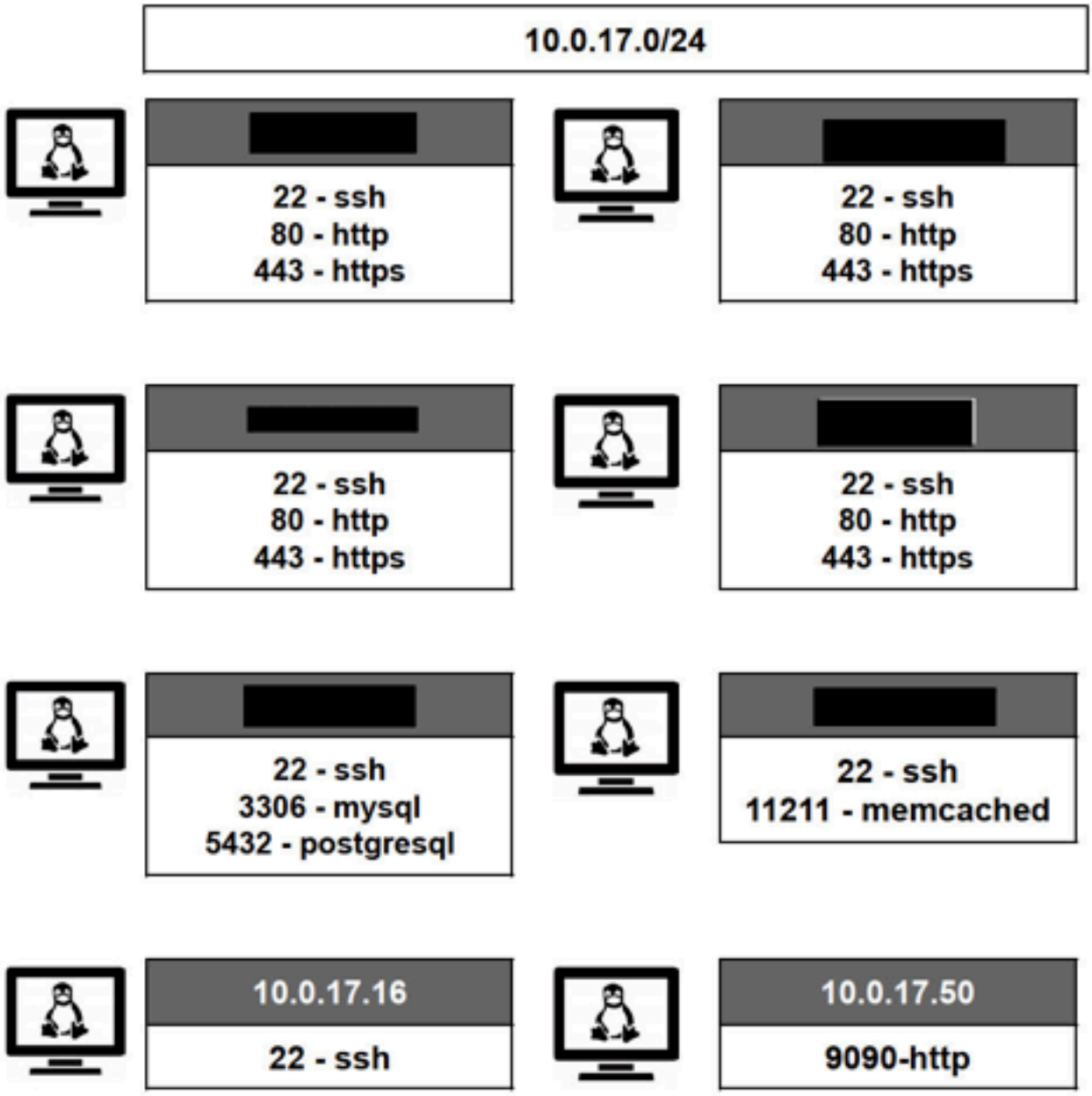

Figure 19: Visualized scan on ports on LBC 10.0.17.0/24 network

Appendix B: Offensive Tools

Tool	Version	Description
Burp Suite	**2021.10.3**	Burp Suite is a set of tools used for penetration testing of web applications developed by the company, Portswigger. *https://portswigger.net/burp*
Hydra	**9.1**	Hydra is a parallelized network login cracker that supports various protocols such as FTP, SSH, Telnet, and more. *https://github.com/vanhauser-thc/thc-hydra*
Metasploit	**6.1.14**	Metasploit is a Ruby-based, open-source framework that is used to find, exploit, and validate system vulnerabilities. *https://www.metasploit.com/*
Netcat	**1.10-47**	Netcat is a computer networking utility for reading from and writing to network connections using TCP or UDP. *http://netcat.sourceforge.net/*
Nmap	**7.92**	Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. *https://nmap.org/download.html*
Seclist	**2021.4**	SecLists is a collection of multiple types of lists used during security assessments. *https://github.com/danielmiessler/SecLists*
Wfuzz	**3.10**	Wfuzz is a tool designed to brute force web applications through various methods. *https://github.com/xmendez/wfuzz*

Appendix C: Additional References for Further Improvement

Industrial Control System Guides:

NIST 800-82 - *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf*

- A guide to Industrial Control Systems (ICS) security, Supervisory Control, and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC).
- Give advice on the structure or topology of ICS systems, such as the utilization of network segmentation and segregation with firewalls and DMZs, as well as advice on risk management and assessment, security program development and deployment, and security controls.

CISA Recommended Practices for ICS - *https://us-cert.cisa.gov/ics/Recommended-Practices*

- A page by the Cybersecurity and Infrastructure Security Agency providing abstracts for existing recommended practices and links to the corresponding sources, along with additional supporting documents which detail various topics for control systems such as cyber vulnerabilities and mitigation therefor. Regularly updated for additional content and arising issues.

The Prioritized Approach to Pursue PCI-DSS Compliance - *https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI-DSS-v3_2_1.pdf*

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

Security Technical Implementation Guides:

Unclassified DISA FSO STIG List - *https://www.stigviewer.com/stigs*

- A listing of unclassified STIGs from the Defense Information Systems Agency (DISA). The list includes STIGs, giving high-quality security technical implementation guides for various operating systems and services running thereon. These standards are not legally required, however they are a great guide to follow in configuring systems and services to be secure.