

OuiCroissant

Security Assessment Findings Report

Business Confidential

Date: 11/14/2024

Project: OC24

Version 1.0



Table of Contents

[Confidentiality Statement 4](#_Toc179821793)

[Disclaimer 4](#_Toc179821794)

[Executive Summary 5](#_Toc179821795)

[**Purpose** 5](#_Toc179821796)

[**Findings** 5](#_Toc179821797)

[**Compliance** 6](#_Toc179821798)

[Assessment Overview 7](#_Toc179821799)

[Assessment Components 7](#_Toc179821800)

[Open-Source Intelligence 7](#_Toc179821801)

[Internal Penetration Test 7](#_Toc179821802)

[<Last Part> 8](#_Toc179821803)

[Scope 8](#_Toc179821804)

[Scope Exclusions 8](#_Toc179821805)

[Client Allowances 8](#_Toc179821806)

[Network Diagram 9](#_Toc179821807)

[Risk Factors 10](#_Toc179821808)

[Likelihood 10](#_Toc179821809)

[Impact 10](#_Toc179821810)

[Compliance Summary 10](#_Toc179821811)

[Payment Card Industry (PCI) Data Security Standards (DSS) 10](#_Toc179821812)

[NIST SP 1800-27B 13](#_Toc179821813)

[Finding Severity Ratings 14](#_Toc179821814)

[Vulnerability Report Card 15](#_Toc179821815)

[Technical Findings 17](#_Toc179821816)

[Finding OCXXX: Vulnerability Name 17](#_Toc179821817)

[Appendix A: Social Engineering Overview 19](#_Toc179821818)

[Appendix B: Methodologies 20](#_Toc179821819)

[Penetration Testing Phases 20](#_Toc179821820)

[OWASP Top 10 20](#_Toc179821821)

[Appendix C: Attack Paths 21](#_Toc179821822)

[Appendix D: Technical Findings Legend 22](#_Toc179821823)

# Confidentiality Statement

This document is the property of OuiCroissant and <Team-#>. This document contains sensitive information including proprietary and confidential information. This document shall not be distributed outside of OuiCroissant or the <Team-#> without the express consent of both parties involved.

# Disclaimer

This document contains information regarding the overall network and system security of OuiCroissant. While <Team-#> maintains the highest standards of quality in their work, this document should not be construed as an exhaustive list of all possible vulnerabilities. We have intentionally focused on the areas with the highest risk and greatest vulnerability to attack to maximize the value of our services.

Due to the changing nature of the computer systems and networks, security vulnerabilities and risks will change over time; <Team-#> recommends annual testing to maintain a good security posture in response to evolving threats.

# Executive Summary

## **Purpose**

OuiCroissant enlisted the help of <<REGIONALS/FINALS-#>>’s penetration testing services to evaluate their <<NETWORK1NAME>>, <<NETWORK2NAME>>, <<ETC>> networks. <<MENTION ANY ADDITIONAL ASPECTS LIKE AWS HERE>> This test was a reassessment of previous vulnerabilities as well as an assessment for new vulnerabilities present in OuiCroissant’s networks. The penetration test encompassed one workday.

## **Findings**

Among the findings from our assessment, a few were particularly noteworthy due to their significant risk to OuiCroissant’s airport operations safety. <<Finding 1 business impact>> (Finding OCXXX), <<Finding 2 business impact>> (Finding OCXXX), and <<Finding 3 business impact>> (Finding OCXXX), are detrimental consequences from the reported vulnerabilities. It is imperative to remediate these vulnerabilities in this report to mitigate risk to customer privacy. This will help protect the company from disruptions to business operations, damage to business reputation, and an erosion of trust between the business and the consumer.

Figure 1: Chart of Found Vulnerabilities

While this test was designed to find system and business process vulnerabilities, it was also a test of the security posture of OuiCroissant’s networks. Based on our testing, we found OC excelled in the areas of <<AREA1, AREA2, AREA3>>. <<Details for Area 1 explaining why they did well>>. <<Details for Area 2 explaining why they did well>>. <<Details for Area 3 explaining why they did well>>. We commend the OC staff for excelling in these areas of the business’ security posture.

## **Compliance**

Understanding that OuiCroissant falls under the United States PCI DSS, the three highest priority standards requiring re-evaluation are the <<LISTOFCOMPLIANCEAREAS>> areas of security compliance. As understood by OC, a failure to meet these standards can result in safety violations, legal fees and fines, reputational damage, loss of consumer trust, operational disruption, and more. Our firm recommends analyzing the following findings and correcting them and the vulnerabilities described earlier: <<FINDING1COMPLIANCE and details, etc.>>. Following the recommendations will assist OC in maintaining security compliance standards and the business will improve the airport operations safety and information security posture critical to protecting consumer data.

# Assessment Overview

On 11/14/2024, <Team-#> conducted a penetration test to evaluate the overall security posture of OuiCroissant. This test was conducted in accordance with industry standard best practices. The phases of the penetration test are as follows:

* Planning – Customer expectations and rules of engagement are obtained.
* Enumeration – Open-source intelligence and scanning are done to identify common vulnerabilities and weak areas.
* Exploitation – Confirm vulnerabilities by successfully completing an exploit and then perform more discovery based on new information.
* Reporting – Record all vulnerabilities, findings, successful exploits, and organizational strengths and weaknesses.

A diagram of an enumeration

Description automatically generated

# Assessment Components

## Open-Source Intelligence

Before the beginning of the internal penetration test, Open-Source Intelligence on OC will be performed. As much information about the company will be gathered using only public facing and freely accessible sources. This will both give our team more insight and context for performing the rest of the engagement as well as give valuable information on how well OC is protecting the data about their company that gets out on the internet.

## Internal Penetration Test

The internal penetration test will simulate how an attacker would operate inside of the internal network. Members of the team will enumerate the network for vulnerabilities as well as carry out internal network attacks. The goal of this portion of the engagement is to find as many vulnerabilities as possible across OC for the purposes of reporting. The hope is that with the help of our team, OC can remediate much of their technical risk. The team will also assess the business risk each vulnerability possesses so that OC can accurately decide what risk is acceptable and which is not. This will be a large portion of the assessment and will utilize information found during the Open-Source Intelligence part.

## <Last Part>

<fill in later>

# Scope

|  |  |
| --- | --- |
| Assessment | Details |
| Network 1 | 10.0.0.0/24 |

## Scope Exclusions

The team will not conduct any testing on any externally facing systems or IP addresses. No disruptive or destructive testing will be allowed on any systems. Social engineering will not be permitted except in a specific scenario designated directly by OC. Any other social engineering is strictly prohibited.

Testing will be limited to the assigned subnets. The VPN client as well as all computers provided to the testers for the engagement will be out of scope for security testing.

## 

## Client Allowances

The client will provide a Windows and Kali Linux system for each tester; these will be used as an entry point to other systems.

## Network Diagram

Insert network diagram here

# Risk Factors

Risk is measured by two factors, likelihood and impact, with impact being further categorized into technical impact and business impact.

## Likelihood

Likelihood measures the probability of a vulnerability being exploited. Severity ratings are used for scoring based on how difficult the attack was, the tools available, the skill level of the attacker, and the environment of the client.

## Impact

Technical impact measures the potential damage a vulnerability could have on operations in the corporation. This includes the confidentiality, integrity, and availability of client-side systems and data, harm to software and/or hardware.

Business impact is a measure of the overall impact to the business, including financial loss, operational impact in potential downtimes, loss of reputation, and compliance violations.

# Compliance Summary

## Payment Card Industry (PCI) Data Security Standards (DSS)

Due to the processing of customer payment information OuiCroissant must comply with PCI DSS. The PCI DSS are a set of global standards that are used to help protect cardholder data and ensure that companies who accept, process, store, or transmit credit card information are doing so in a secure environment. Failure to comply with PCI DSS can result in large fines, damage to reputation, and loss of customer data for the organization. By following this set of standards, OuiCroissant can both avoid these damages to the organization as well as increase security across the board.

Reference: <https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf>

## General Data Protection Regulation (GDPR)

As OuiCroissant processes and stores personally identifiable information (PII) of consumers, the company must adhere to GDPR. GDPR is an European Union (EU) data compliance standard that all companies which handle PII of EU citizens must comply with. This standard ensures that all user information is stored in a secure manner, protected against unauthorized access and tampering, and remains available to the user upon request. Failure to comply with GDPR can result in fines up to 20 million EUR, or 4% of the company’s total worldwide annual turnover, as well as damage to reputation and loss of customer data for the organization. Adhering to GDPR will allow OuiCrossant to have confidence in their security measures, avoiding any such damages.

The tables below include overall security objectives as well as the actions required to maintain compliance. Any vulnerabilities discovered during the assessment will be mapped to specific requirements if applicable. While all aspects of the security directives are important and mandatory, there are some that our team is unable to test due to the nature of the engagement. These directives should still be carefully tested to ensure full compliance. The table will not include these untestable portions.

Reference: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

|  |  |  |  |
| --- | --- | --- | --- |
| PCI Objectives | PCI Requirements | Compliance Violation Findings | Compliance Fine Amounts |
| Build and Maintain a Secure Network and Systems | 1. Install and maintain a firewall configuration to protect cardholder data | * OCXXX | $###.## |
| 1. Do not use vendor supplied defaults for system passwords and other security | * OCXXX | $###.## |
| Protect Cardholder Data | 1. Protect stored data |  | $###.## |
| 1. Encrypt transmission of cardholder data across open, public networks |  | $###.## |
| Maintain a Vulnerability Management Program | 5. Protect all systems against malware and regularly update anti-virus software or programs | - | $###.## |
| 6. Develop and maintain secure systems and applications | - |  |
| Implement Strong Access Control Measures | 7. Restrict access to cardholder data by business need-to-know |  |  |
| 8. Identify and authenticate access to system components |  |  |
| 9. Restrict physical access to cardholders’ data |  |  |
| Regularly Monitor and Test Networks | 10. Track and monitor all access to network resources and cardholder data. |  |  |
| 11. Regularly test security systems and processes. |  |  |
| Maintain an Information Security Policy | 12. Maintain a policy that addresses information security for all personnel. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| GDPR Objectives | GDPR Requirements | Compliance Violation Findings | Compliance Fine Amounts |
| Security of processing | 1. Implement strong access controls | * OCXXX | $###.## |
| 1. Ensure confidentiality integrity and availability of systems |  | $###.## |
| 1. Implement appropriate technical and organizational measures for data protection |  | $###.## |
| Personal Data storage | 1. Protect data against deletion loss or damage |  |  |
| 1. Encrypt personal data |  |  |
| 1. Adhere to principles of data minimization |  |  |
| 1. Data is accurate and kept up to date |  |  |

## NIST SP 1800-27B

## Properly complying with governing standards like PCI DSS and GDPR requires strong frameworks set by established organizations. NIST, or the National Institute of Standards and Technology, is a non-regulatory federal agency that provides cybersecurity guidance. The NIST SP 1800 27B is a NIST special publication that outlines a cybersecurity framework specific to the hospitality industry. The use NIST guide will provide OuiCroissant with a foundation for securing its infrastructure and complying with important standards such as PCI DSS.

Reference: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-27.pdf>

# Finding Severity Ratings

This section is used to define the severity ratings for any vulnerabilities and measure risk. The severity ratings will follow the corresponding CVSS score range.

|  |  |  |
| --- | --- | --- |
| Severity | CVSS V4.0  Score Range | Definition |
| Critical | 9.0 – 10.0 | Straightforward exploitation typically results in high-level system access. Vulnerabilities of this category should be  resolved immediately |
| High | 7.0 – 8.9 | Exploitation may involve more steps but could result in gaining elevated privileges and potentially significant downtime or data loss. Vulnerabilities in this category should be resolved as soon  as possible. |
| Medium | 4.0 – 6.9 | Vulnerabilities are present but are not exploitable, involve many extra steps, and/or require social engineering. Vulnerabilities in this category should be resolved after high-priority issues are  resolved. |
| Low | 0.1 – 3.9 | Vulnerabilities may be present but are not exploitable. Resolving these vulnerabilities would help to reduce the organization’s attack surface. Vulnerabilities in this category should be resolved during the next period of planned  maintenance. |
| Informational | N/A | No vulnerability exists. This category is reserved for findings  that do not directly relate to exploitation but may provide an attacker with information that would assist them in an attack. |

# Vulnerability Report Card

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Critical | High | Medium | Low | Informational |
| 2 | 13 | 14 | 2 | 7 |

Vulnerability Summary

|  |  |  |
| --- | --- | --- |
| Severity | Vulnerability | Recommendation |
| Critical | **OCXXX:** Lorum Ipsum | Lorum Ipsum |
| High |  |  |
| Medium |  |  |
| Low |  |  |
| Info |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

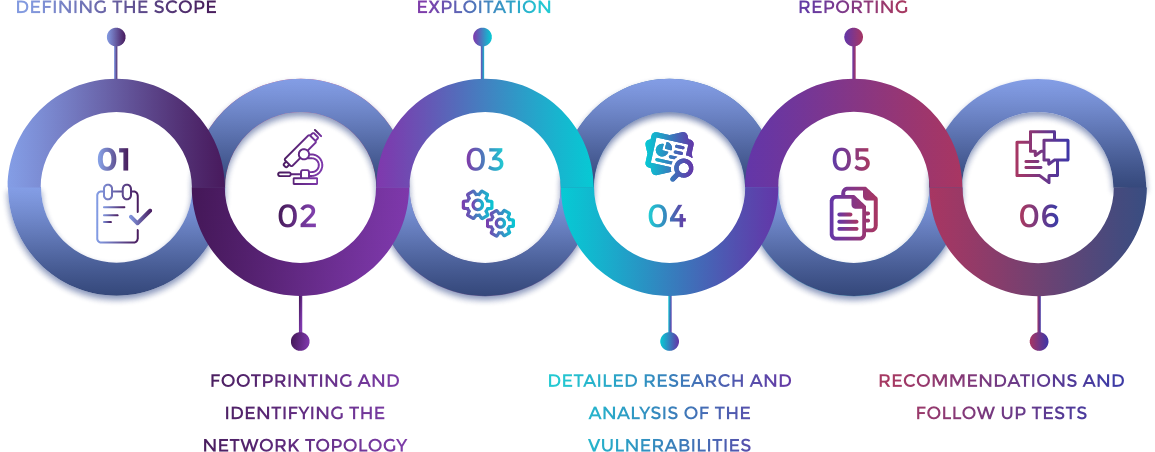
# Technical Findings

|  |  |
| --- | --- |
| Finding OCXXX: Vulnerability Name | |
| **Affected Hosts** | IP Range (Hostname) |
| **CVSS:** #.# | Low, Medium, High, Critical | **Likelihood: Low | Medium | High**  Notes about the likelihood of exploitation, including the difficulty, credentials needed, etc.  **Technical Impact: Low | Medium | High**  Notes about the effect on OC’s systems and infrastructure if this vulnerability is exploited, including access gained, or damage to systems done |
| **Vulnerability Description** | A description of how the vulnerability works and what it allows an attacker to do |
| **Business Impact** | A description of the **direct** negative effects to OC from a business standpoint |
| **Requirements to exploit** | A list of requirements that may include tools, credentials needed, internal access, etc. |
| **Remediation** | General steps to correct any deficiencies specific to this instance of the exploit |
| **References** | Optional materials for additional reading |
| **Proof of Concept**  An explanation of what steps were taken as well as what the screenshots are indicating. Be concise while still giving enough details for replication.    Figure 1: The tester runs a “whoami” command to discover they are the “jbcam”  Ensure there is a newline before and after a screenshot and that the screenshot is centered and the text is left aligned. In addition, use Blue Accent 1 with 2 ¼ pt thickness for the border and try to leave room around the edges of the screenshot. | |

# Appendix A: Social Engineering Overview

# Appendix B: Methodologies

## Penetration Testing Phases

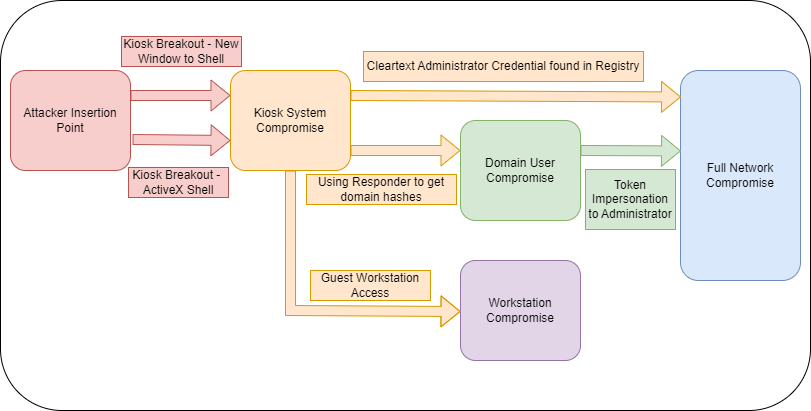
These six phases are the model by which we conduct our penetration tests. They provide accountability and robustness in testing procedures. This ensures that the highest cost to value ratio is achieved while providing an excellent product to the client.

## OWASP Top 10

The OWASP Top 10 are the ten most commonly found vulnerabilities found in web applications. All web applications are tested against these vulnerabilities at a minimum to ensure that the most vulnerabilities are discovered on each system.

|  |  |
| --- | --- |
| OWASP Top 10 - 2022 | |
| 1. Broken Access Control | 2. Cryptographic Failures |
| 3. Injection | 4. Insecure Design |
| 5. Security Misconfiguration | 6. Vulnerable and Outdated Components |
| 7. Identification and Authentication Failures | 8. Software and Data Integrity Failures |
| 9. Security Logging and Monitoring Failures | 10. Server-Side Request Forgery (SSRF) |

# Appendix C: Attack Paths

The following chart shows the most likely attack paths for an adversary based on our findings report. There are two paths discovered to completely compromise the network and another separate vector to compromise the corporate workstations.

# Appendix D: Technical Findings Legend

|  |  |
| --- | --- |
| Finding OCXXX: Vulnerability Name | |
| **Affected Hosts** | *Targets/affected systems* |
| **CVSS:** *#.#* | *Rating* | **Likelihood: *Low | Medium | High***  *Notes about the likelihood of exploitation, including the difficulty, credentials needed, etc.*  **Technical Impact: Low | Medium | High**  *Notes about the effect on OC’s systems and infrastructure if this vulnerability is exploited, including access gained, or damage to systems done.* |
| **Vulnerability Description** | *A description of how the vulnerability works and what it allows an attacker to do.* |
| **Business Impact** | *A description of the direct negative effects to OC from a business standpoint.* |
| **Requirements to exploit** | *A list of requirements that may include tools, credentials needed, internal access, etc.* |
| **Remediation** | *General steps to correct any deficiencies specific to this instance of the exploit.* |
| **References** | *Optional materials for additional reading.* |
| **Proof of Concept**  *A detailed, concise set of steps to reproduce the vulnerability as proof of exploitation.*  *\*Screenshots go here\** | |



**Last Page**