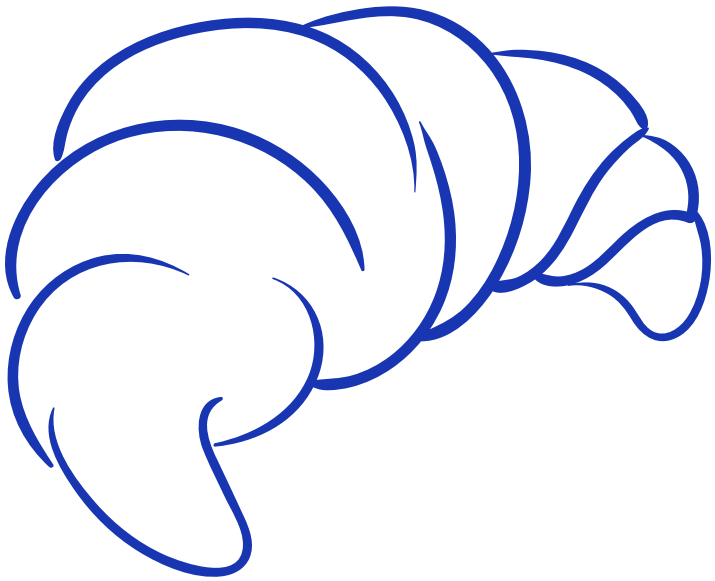
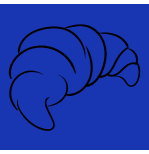


OuiCroissant Security Assessment Report

PREPARED BY: WEST-## PREPARED FOR: OUICROISSANT DATE: 11/16/2024

Contents

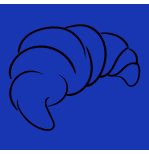


Confidentiality Statement

This penetration testing report has been prepared by the West-## team for OuiCroissant. It contains proprietary information and is intended solely for the internal use of OuiCroissant. Any unauthorized distribution, disclosure, or reproduction of this document or any part of its contents is strictly prohibited. By accepting and reviewing this report, the recipient agrees to maintain the confidentiality of the information provided, ensuring that all findings, recommendations, and details remain within OuiCroissant's security, compliance, or executive teams unless explicit written permission is granted.

Disclaimer

This penetration test and the results outlined in this report were conducted under the conditions and scope agreed upon with OuiCroissant at the time of the assessment. The findings and recommendations are based on the information available during the testing period and do not account for future changes in systems or configurations. While the West-## team has made every effort to identify and assess vulnerabilities, this report does not guarantee complete security and is not an endorsement of the tested systems as immune to all cyber threats. OuiCroissant is advised to implement continual monitoring and regular security assessments to maintain optimal security postures. West-## disclaims any liability for actions taken by third parties or for incidents occurring after the completion of the penetration test.

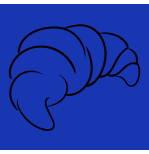


Executive Summary

Findings Summary

OuiCroissant
West-##

CONFIDENTIAL



Strategic Recommendations

Governance and Compliance

To align with the compliance requirements that govern payment card transactions and data protection for customers in the EU, West-## has evaluated OuiCroissant's systems and processes in accordance with PCI-DSS and GDPR standards. OuiCroissant's adherence to these standards is essential for maintaining the ability to process payments, protect customer data, and avoid substantial fines and legal actions associated with non-compliance. Below is an updated breakdown of the findings where OuiCroissant was found to be out of compliance with PCI-DSS and GDPR.

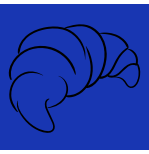
Payment Card Industry Data Security Standard (PCI-DSS):

Required for organizations that handle cardholder data, PCI-DSS mandates annual evaluations to ensure compliance with data protection protocols around storing, transmitting, and securing customer financial information. Violations can lead to fines up to $100,000 per month, additional audits, and other financial or legal repercussions. Non-compliance impacts OuiCroissant's ability to accept card payments.

General Data Protection Regulation (GDPR):

Enforced by the European Union, GDPR applies to companies with customers in the EU and emphasizes data protection, transparency, and customer rights. Violations can incur fines up to 20 million euros or 4% of global revenue, whichever is higher, and may lead to suspension of operations. Compliance with GDPR is crucial for managing OuiCroissant's EU customer base and mitigating legal risks.

Violation	Standard	Relevant Requirement
	PCI-DSS	
	GDPR	



Penetration Test Methodology

West=## followed a custom methodology framework incorporating aspects of Penetration Testing Execution Standard (PTES) and NIST 800-115. The final framework had four phases incorporating the seven phases of PTES into the NIST framework. The four phases are shown, which spanned the pre-assessment and assessment phases of the engagement.

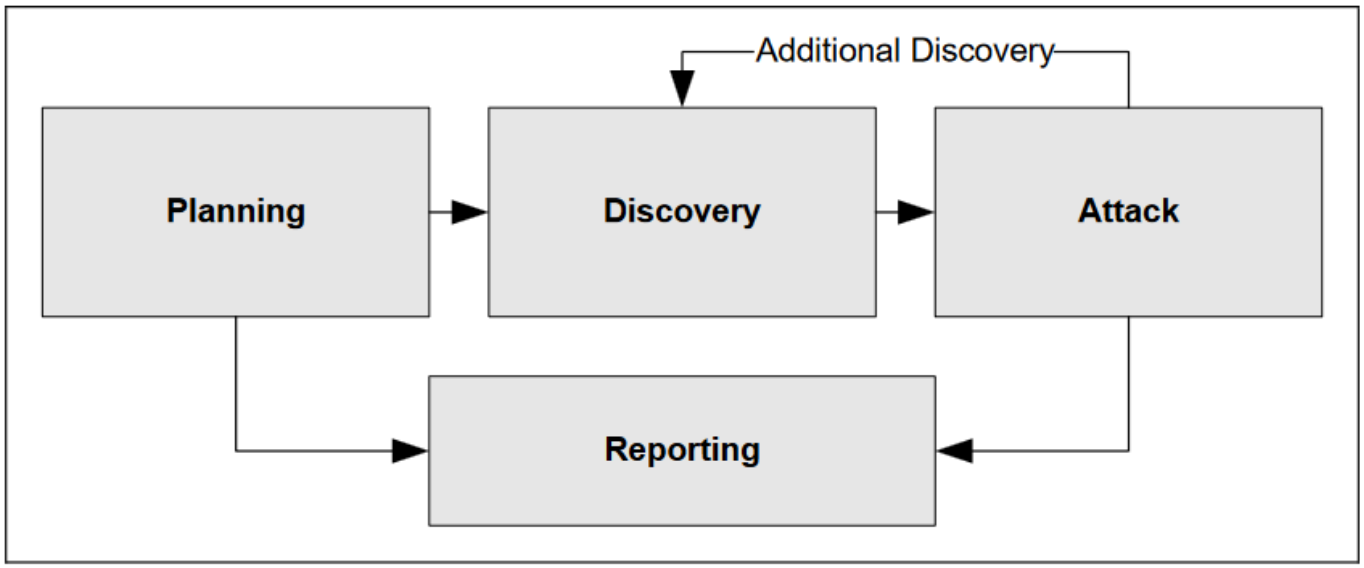


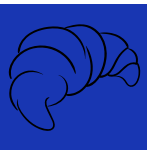
Figure 5-1. Four-Stage Penetration Testing Methodology

Phases of testing adapted from NIST 800 - 115

The approach began with the team conducting open-source research prior to starting the engagement on OuiCroissant's network and forming a plan of attack based upon information discovered. When the engagement began on the network, the team began a discovery phase which had the goal of gathering information and mapping the network of OuiCroissant. When information was gathered, the team proceeded to the attack phase based on the information gathered. The discovery and attack phases were repeated as more information was collected and leveraged for exploitation. All results were logged from the attack and planning phase to have complied during the final reporting phase. The report phase consolidated all the information into a report for OuiCroissant.

Attack Narrative

Vulnerability Report Card



Risk Classification

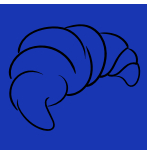
The team evaluated findings during the engagement using a custom risk/impact matrix-based loosely on the Penetration Execution standard and the CVSS scoring matrix. The team sought to give a rating that reflected the potential damage to the business if the vulnerability was exploited. This possibility was multiplied with the skill level required and the likelihood of an incident occurring not overly to alarm the IT team of OuiCroissant. The result is a composite impact/risk score used to rank all finds from the engagement, with the most severe score being 25 and the lowest being 1. The impact score for the first half of the composite score is from 1 to 5, with 1 having little to no impact on business operations and 5 being catastrophic failures. The likelihood score is also on a scale from 1 to 5, with 1 being a very little or accidental chance of exploitation, where 5 would be a high likelihood or requiring almost no skill to exploit. These sub-scores result in the composite risk/impact score used throughout the assessment.

CVSS scores were used to determine the difficulty and, therefore, likelihood score for the matrix. The CVSS scores are still included within the technical findings section for the engineering team to reference. The main components of a CVSS score are the impact on the CIA triad, the level of access required, the attack vector, and the complexity of the vulnerability.

Components are informative to the remediation team but give little insight to business operation and therefore are left within the technical findings section. The risk matrix above determines the team's business impact score to rate the vulnerabilities risk.

	1- Negligible *Insignificant disruption to operations. Or disruption of less than 2 hours.*	**2 - Minor** *Minimal disruption to operations. Or between 2 and 5 hours of disruption.*	**3 - Moderate** *Noticeable disruption to operations. Or between 5 and 10 hours of disruption.*	**4 - Major** *Operations are severely impacted. Or between and 24 hours of disruption.*	**5 - Catastrophic** *Operations are completed halted or multiple days of disruption.*
5 - Very Likely *Above 80% chance of exploitation. Or would require no-skill to exploit.*					
4 - Likely *Between 79% and 60% chance of exploitation. Or would require minimal skill to exploit.*					
3 - Moderate *Between 59% and 30% chance of exploitation. Or would require some skill to exploit.*					
2- Unlikely *Between 29% and 10% chance of exploitation. Or would require expert skills to exploit.*					

1 - Incidental *Less than a 9% change of exploitation. Would only be exploited through accidental means.*					



Business Impact Classification

Severe (>20):

Customers or company data are being exfiltrated or significantly altered. Business is not operational. Staff is working 24/7 to remediate the impact. There is catastrophic financial and reputational impact to OuiCroissant.

High (15-19):

Customer or company data are affected in all ways. Systems or data may be unavailable, and customers cannot complete business due to disruptions. Staff needs to be called in past business hours to remediate the impact. There are significant financial or reputational impacts on OuiCroissant.

Moderate (10-14):

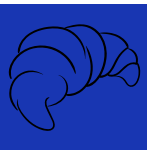
Customer or company data may be unavailable but not exfiltrated or altered. Production systems are affected, and customers are affected by the disruption. Staff may be required to work past business hours to remediate the impact. There is a noticeable financial or reputational impact to OuiCroissant.

Low (5-9):

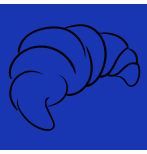
Customer and company data are not affected. Production systems may be impacted, but the disruptions do not impact customers. Day to say staff should be able to remediate any disruptions within the workday. There is a minimal financial or reputational impact to OuiCroissant.

Minimal (<5):

Customer data, company data, and production systems are not affected. Day-to-day staff can remediate the disruptions within their regular work duties without extra time allocated. There is little to no financial or reputational impact to OuiCroissant.



Network Map



Technical Findings

Severe

Issue
Description
Impact
Tactical Remediation
Strategic Remediation
Sub Optimal Recommendation

High

Issue
Description
Impact
Tactical Remediation
Strategic Remediation
Sub Optimal Recommendation

Moderate

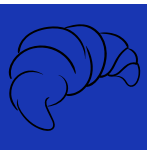
Issue
Description
Impact
Tactical Remediation
Strategic Remediation
Sub Optimal Recommendation

Low

Issue
Description
Impact
Tactical Remediation
Strategic Remediation
Sub Optimal Recommendation

Minimal

Issue
Description
Impact
Tactical Remediation
Strategic Remediation
Sub Optimal Recommendation



Appendix