



# Penetration Test Report

Oui Croissant

November 16, 2024

SoCal Team [TEAM NAME]

CONFIDENTIAL

**Notice of Confidentiality:** This document and the contents thereof are provided in strict confidence for the sole usage of Oui Croissant. As the contents of the document contain strictly confidential and privileged information regarding the infrastructure of Oui Croissant, the document may not be disclosed or redistributed without the sole consent of Oui 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 therefrom. 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 Oui 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 for 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.

**Contact Information:**

**Project lead:**  
**Email:**  
**Phone number:**

**Table of Contents**

**Assessment Overview ..... 5**

**1.1 STATEMENT OF WORK..... 5**

**1.2 SCOPE ..... 5**

**1.3 EXECUTIVE SUMMARY ..... 6**

**1.4 SUMMARY OF FINDINGS ..... 6**

**1.5 RECOMMENDATIONS..... 7**

<b>1.6 FINAL NOTES.....</b>	<b>7</b>
<b><i>Introduction.....</i></b>	<b>8</b>
<b>2.1 METHODOLOGY .....</b>	<b>8</b>
<b>2.2 RISK AND SEVERITY CLASSIFICATION .....</b>	<b>8</b>
2.2.1 RISK.....	9
2.2.2 SEVERITY .....	10
<b>2.3 COMPLIANCE AND REGULATION OVERVIEW .....</b>	<b>11</b>
2.3.1 CHILDREN ONLINE PRIVACY AND PROTECTION ACT (COPPA) .....	12
2.3.2 GENERAL DATA PROTECTION REGULATION (GDPR).....	12
2.3.3 PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI-DSS).....	13
<b><i>Impact and Remediation .....</i></b>	<b>14</b>
<b>3.1 RESULTANT COMPLIANCE .....</b>	<b>14</b>
3.1.x REPLACEMENT EXAMPLE .....	14
<b>3.2 RISK ANALYSIS.....</b>	<b>15</b>
<b>3.3 BUSINESS IMPACT .....</b>	<b>15</b>
<b>3.4 RECOMMENDED REMEDIATION PLAN .....</b>	<b>15</b>
<b><i>Technical Findings.....</i></b>	<b>17</b>
<b>4.1 OVERVIEW .....</b>	<b>17</b>
<b>4.2 CRITICAL .....</b>	<b>18</b>
C-0.....	18
<b>4.3 HIGH .....</b>	<b>20</b>
H-0 .....	20
<b>4.4 MEDIUM .....</b>	<b>22</b>
M-00: .....	22
<b>4.5 LOW .....</b>	<b>24</b>
L-00:.....	24
<b>4.6 INFORMATIONAL .....</b>	<b>26</b>
I-00: .....	26
I-69: Steps to Compromise .....	26
<b><i>Appendix.....</i></b>	<b>28</b>
<b>A: CVSS AND RISK.....</b>	<b>28</b>
<b>B: OFFENSIVE TOOLS.....</b>	<b>34</b>
<b>C: COPPA .....</b>	<b>34</b>
<b>C: HOSTS DISCOVERED .....</b>	<b>36</b>
<b><i>And all that.....</i></b>	<b>35</b>

<b>PASSWORD POLICY .....</b>	<b>36</b>
<b>CLASSIFICATION OF SENSITIVE INFO .....</b>	<b>37</b>
<b><i>Final Checklist.....</i></b>	<b><i>37</i></b>

# Assessment Overview

## 1.1 STATEMENT OF WORK

SoCal Tram **[TEAM NAME]** is contracted by Oui Croissant on Saturday, November 16 at 9:30 am to conduct a penetration test of Flakebook, the new product scheduled for release in January of 2025.

The engagement aims to achieve the following objectives:

1. Identify and exploit vulnerabilities within the agreed-upon scope of the organization's infrastructure.
2. Evaluate compliance with the relevant standards and regulations including GDPR, COPPA, and PCI-DSS.
3. Document the methods used and the results obtained from any vulnerabilities exploited during the assessment
4. Provide recommendations for addressing vulnerabilities and mitigating risks identified from the penetration test.

The assessment simulated an adversarial attack without prior access to the systems and networks within the defined scope. Access to the networks was achieved by emulating techniques employed by adversaries.

## 1.2 SCOPE

The scope for this engagement encompasses all hosts within the following **[Number]** subnets:

- List subnets

Windows Workstations	Windows DC	Linux

1.3 EXECUTIVE SUMMARY

1.4 SUMMARY OF FINDINGS

The chart below illustrates the distribution of identified risks and vulnerabilities.

Severity Rating	Critical	High	Medium	Low	Informational
Vulnerabilities	#	#	#	#	#

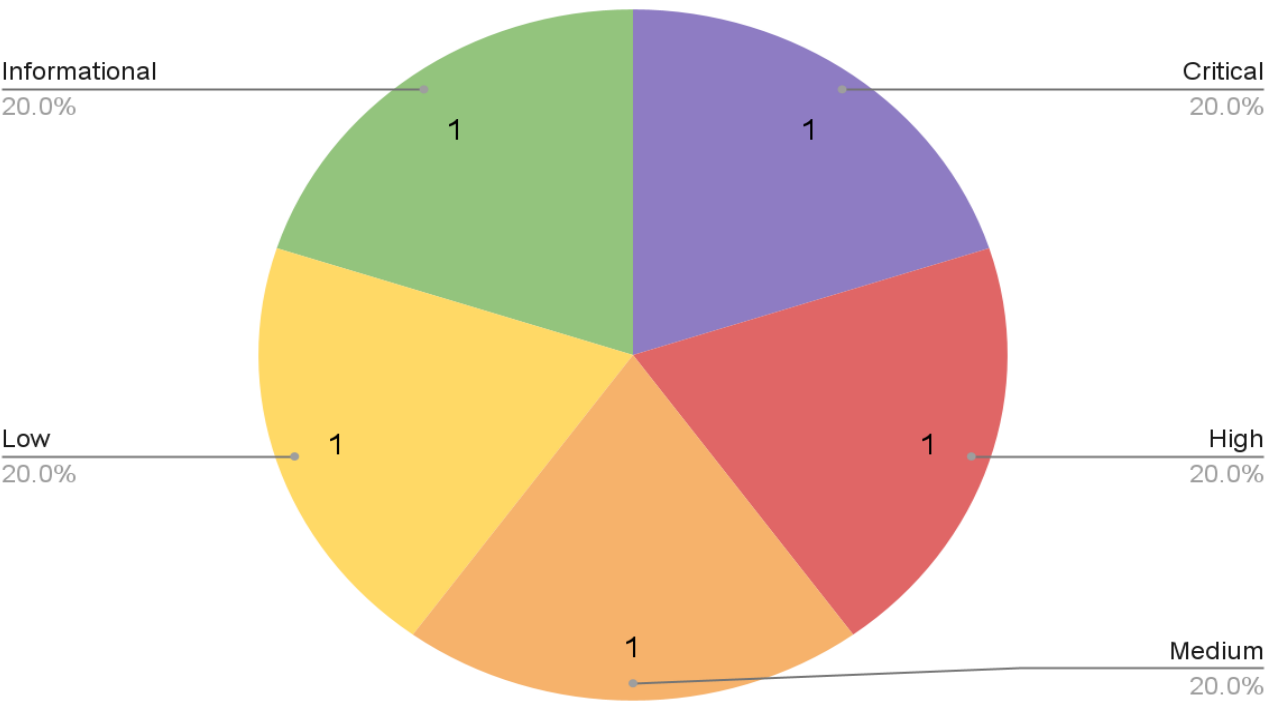


Figure 1

## 1.5 RECOMMENDATIONS

**[TEAM NAME]** recommends the following measures to improve Oui Croissant 's overall security posture and remediate identified vulnerabilities:

### **Password Policy:**

### **Patch Management:**

## 1.6 FINAL NOTES

SoCal Team **[TEAM NAME]** values Oui Croissant's partnership in this journey towards a more secure and innovative social media landscape. Flakebook is a platform designed from the ground up to create secure, engaging, and meaningful experiences for its users. It's been a pleasure working together to ensure that safety and innovation go hand-in-hand as Flakebook becomes ready to launch. The recommendations in this report are here to help Oui Croissant keep raising the bar on security, so users can trust and enjoy everything the platform has to offer. We look forward to continuing this partnership and supporting you as Flakebook grows.

# Introduction

## 2.1 METHODOLOGY

To ensure a thorough evaluation of Oui Croissant security, **[TEAM NAME]** conducted the penetration test in accordance with the following penetration testing methodology. This approach ensures our assessments stay current, thorough, and highly effective against evolving threats.

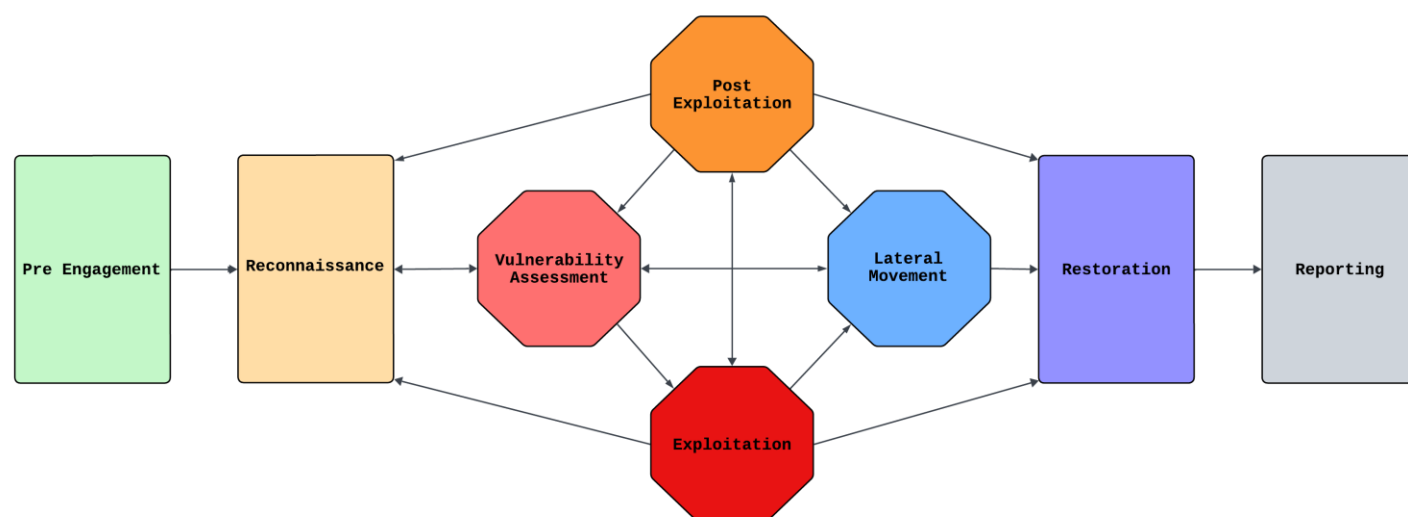


Figure 2

## 2.2 RISK AND SEVERITY CLASSIFICATION

**[TEAM NAME]** assessed each vulnerability based on two factors: severity and risk. Severity indicates the potential impact and exploitability of a vulnerability, while risk reflects the likelihood of loss or damage if that vulnerability is exploited. These assessments help prioritize remediation efforts by evaluating the overall impact on confidentiality, integrity, and availability, as well as potential business consequences like financial loss, reputational harm, and legal exposure.

*Refer to Appendix A for a detailed explanation of risk calculations and CVSS scoring.*



## 2.2.1 RISK

The secondary measure, risk level, ranks vulnerabilities based on their impact and the likelihood of the vulnerability being exploited in the context of the organization, following the approach recommended in NIST SP-800-30.

Risk Level Explanations	
Rating	Explanation
<b>Critical</b>	Vulnerability poses a severe threat with a high probability of exploitation. Potential for severe data breaches, operation disruptions, financial loss, and considerable compromise to the organization's systems and reputation
<b>High</b>	Vulnerability poses a significant threat with a significant probability of exploitation, potentially leading to substantial data exposure, financial risk, or operational disruption.
<b>Medium</b>	Vulnerability has a moderate probability of exploitation, potentially causing moderate disruption or sensitive information exposure
<b>Low</b>	Vulnerability has a lower probability of exploitation and poses minimal risk to operations or security. It has the potential to cause minimal disruption or have little potential for data exposure or system compromise.
<b>Very Low</b>	Vulnerability has an extremely low probability of exploitation with minimal impact if exploited. Poses a negligible risk to operations and security. It is improbable to be exploited or cause any significant disruption or data exposure.

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

### 2.2.2 SEVERITY

The main measure is the severity level, which is scored using the Common Vulnerability Scoring System v3.1 (CVSS), an industry-standard framework for measuring the severity of vulnerabilities that ensures a consistent and reliable approach to assessing their potential impact. CVSS measures severity based on several factors, such as exploitability, extent, impact, and complexity. See Appendix A for a full breakdown of the CVSS factors, and how they are used by [TEAM NAME].

Severity Level Explanations		
Severity Rating	Base Score	Explanation
Critical	9.0-10.0	Vulnerability poses an immediate and significant threat, capable of causing extensive system compromise. Has the potential to lead to significant data breaches and severe operational disruption

<b>High</b>	7.0-8.9	Vulnerability poses a substantial risk, potentially resulting in partial system compromise or significant data exposure, impacting operations and security
<b>Medium</b>	4.0-6.9	Vulnerability has a moderate potential impact, causing moderate disruption or exposing some sensitive information, affecting operational continuity to a certain extent
<b>Low</b>	0.1-3.9	Vulnerability has limited impact or limited potential for exploitation They might lead to minimal disruption or have low potential for data exposure
<b>Informational</b>	0	Finding does not pose an immediate threat, but provides useful information for improving the overall security posture

## 2.3 COMPLIANCE AND REGULATION OVERVIEW

Staying compliant with the following acts and regulations is critical for Oui Croissant to avoid fines, lawsuits, and public scrutiny. **[TEAM NAME]** has done some research on compliances necessary

Confidential - Do not duplicate or distribute without written permission from Oui Croissant

for social media platforms like Facebook. The top three that we would like to highlight are the General Data Protection Regulation (GDPR), the Children Online Privacy and Protection Act (COPPA), and the Payment Card Industry Data Security Standard (PCI-DSS). COPPA is necessary for any social networking platform to monitor and regulate the type of data being collected on minors. GDPR is required for doing business in the European Union. Additionally, due to Oui Croissant **<INSERT WHAT THEY'RE DOING WITH CARDS>** it is essential to be compliant with PCI-DSS in order to continue doing business. Please note that these regulations are not the only standards applicable to Oui Croissant, and the compliance analysis done in this report was using the limited information **[TEAM NAME]** has on the company. Please use our analysis as a guide for further research.

### 2.3.1 CHILDREN ONLINE PRIVACY AND PROTECTION ACT (COPPA)

This act protects the privacy of children under 13 by limiting the type of personal information that can be stored on social media platforms aimed at children. Personal information can include first and last name, home address, phone number, geolocation, audio, video, or photographs. COPPA requires companies to implement specific measures to protect young users' data, including obtaining verifiable parental consent, providing clear privacy notices, and limiting data collection to necessary information only. Compliance with COPPA is essential for Oui Croissant to avoid legal penalties and demonstrate a commitment to safeguarding children's privacy on its platform.

The Federal Trade Commission (FTC) assesses whether a website is directed toward children based on various factors, including the subject matter, visual content, language, and features that appeal to children, such as games, animation, or child-friendly characters. Additionally, the FTC considers whether the website advertises to children or collects information that might be of interest to a younger audience. For Facebook, this means that if it includes content or features that could appeal to users under 13, it may need to comply with COPPA requirements.

### 2.3.2 GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR is a European-based regulation that was designed to incorporate data privacy laws across Europe. GDPR mandates strict requirements for data protection, user consent, and transparency, ensuring that individuals' personal information is handled securely and responsibly. GDPR violations include fines of 2-4% of annual revenue. Compliance with GDPR is crucial for Oui Croissant to avoid significant fines, maintain user trust, and uphold its commitment to privacy, especially if Facebook handles sensitive personal data and connects users across European borders.

### **2.3.3 PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI-DSS)**

PCI DSS ensures entities that store, process, and transmit payment account data keep that data secure. Compliance with this standard is mandatory for any company that handles payment card data. Non-compliance can lead to fines of up to \$100,000 per month. Compliance with PCI DSS is essential to protect customer payment data from breaches and fraud, ensuring that Flakebook and other company services meet industry security standards for handling sensitive financial information. By adhering to PCI DSS, Oui Croissant not only safeguards its customers' payment information but also reinforces trust and reduces legal and financial risks associated with data breaches.

# Impact and Remediation

## 3.1 RESULTANT COMPLIANCE

### 3.1.x REPLACEMENT EXAMPLE

Title	Reference
Reg	<a href="https://xxx.xxx/xxx">https://xxx.xxx/xxx</a>

Applicability	Violation Count	Resultant Compliance with GDPR	
Yes/No	Amount	Ref #	Requirements
Does it apply rn or is it narrative	9	Article 5(1)(f)	Insert general info
	9	Article 24	
	9	Article 25	
	5	Article 29	
	5	Article 30	
	9	Article 32	
	9	Article 33	
	9	Article 34	
	1	Article 44	

## 3.2 RISK ANALYSIS

[TEAM NAME] identified serious risks due to multiple vulnerabilities found within the Flakebook network. [EXPLAIN RISKS OF EACH]. The potential impact comes from unauthorized access to sensitive data, loss of availability, and the potential for malware deployment. [GO THROUGH ATTACK EXAMPLES FOR EACH VULN]. All these vulnerabilities can be exploited using common knowledge, the internet, and publicly available proof of concept scripts.

**Purpose:** Identifies and evaluates potential threats and vulnerabilities within a system.

**Focus:** Assesses the likelihood and impact of various risks, including financial, reputational, regulatory, and operational risks.

**Outcome:** Provides a detailed understanding of the risks associated with specific vulnerabilities, helping organization prioritize remediation efforts based on the severity and likelihood of exploitation

## 3.3 BUSINESS IMPACT

## 3.4 RECOMMENDED REMEDIATION PLAN

To address identified risks and vulnerabilities, [TEAM NAME] presents a strategic response plan designed to address and remediate vulnerabilities, mitigate risks, and strengthen **Oui Croissant's** overall security posture.

The plan prioritizes actions based on urgency and time constraints to ensure a proactive approach to security enhancement. While this outline provides a high-level guide, it is crucial to consult with security engineers for a thorough investigation and implementation of the outlined measures. For further resources, consult the references and comprehensive remediation recommendations provided in each technical finding.

Recommended Response Plan		
Time Horizon	Vulnerability	Response
Urgent Mitigation	•	
Within 30 days	•	
Within 60 days	•	



# Technical Findings

## 4.1 OVERVIEW

This section presents the key technical findings from the security assessment, following a structured approach. Vulnerabilities are categorized by severity levels, presented in order of severity: critical, high, medium, and low, in alignment with predefined definitions. Additionally, informational findings are documented and discussed. Each technical finding includes a risk level assessment, a brief vulnerability overview, a business impact analysis, reproducible attack replication documentation, systems affected, recommended remediation, and references for further information.

Findings Count					
Severity Rating	Critical	High	Medium	Low	Informational
Vulnerabilities	#	#	#	#	#

Findings	Severity Level	Remediation
C-01:	Critical	
H-01:	High	
M-01:	Medium	
L-01:	Low	
I-01:	Informational	

## 4.2 CRITICAL

C-0

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Critical		Score		
Vector	CVSS:3.1/				
OWASP	Don't need				
Risk Matrix					
Risk Level	High	Impact	High	Probability	High
Affected Systems					
IP Address		Port	Service	Version	
Overview					
<p>[Vulnerability] was found on [found location - be specific]. This allows attackers to [attacker capabilities], compromising the [CIA triad]. This attack poses [risk level] as it [explain risk assessment]. This attack carries the potential [attack potential, details on the compromise].</p>					
Business Impact					
<p>The discovery of [identified finding] poses [severity level] risks to [affected area]. An attacker exploiting this vulnerability could potentially [impact description – e.g., disrupt operations, compromise sensitive data, violate compliance standards, etc.].</p> <p>Potential impact scenario:</p> <ul style="list-style-type: none"><li>• Scenario</li></ul>					

These risks could lead to [potential consequences - e.g., legal liabilities, financial losses, reputational damages, etc.], necessitating immediate remediation to safeguard [affected area].

## Steps to Replicate

Target audience: Engineers/Technical

Include screenshots, use codeblocks, don't talk about how to install tools

## Recommended Remediation

[TEAM NAME] recommends that Oui Croissant implement [specific action] to mitigate the risk associated with [identified finding]. This includes [details on recommended actions – e.g., implementing strong authentication methods, changing weak credentials, enforcing strong password policies, etc.]. Additionally, it is advised to [further actions, e.g., implementing access control mechanisms, enforcing encryption protocols, etc.] to enhance the overall security posture of Flakebook.

## Compliance

keep it condensed

## References

4.3 HIGH

H-0

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	High		Score		
Vector	CVSS:3.1/				
OWASP					
Risk Matrix					
Risk Level	High	Impact	High	Probability	High
Affected Systems					
IP Address	Port	Service	Version		
Overview					
<p>[Vulnerability] was found on [found location - be specific]. This allows attackers to [attacker capabilities], compromising the [CIA triad]. This attack poses [risk level] as it [explain risk assessment]. This attack carries the potential [attack potential, details on the compromise].</p>					
Business Impact					
<p>The discovery of [identified finding] poses [severity level] risks to [affected area]. An attacker exploiting this vulnerability could potentially [impact description – e.g., disrupt operations, compromise sensitive data, violate compliance standards, etc.].</p> <p>Potential impact scenario:</p> <ul style="list-style-type: none"><li>Scenario</li></ul>					

These risks could lead to [potential consequences - e.g., legal liabilities, financial losses, reputational damages, etc.], necessitating immediate remediation to safeguard [affected area].

## Steps to Replicate

Target audience: Engineers/Technical

Include screenshots

## Recommended Remediation

[TEAM NAME] recommends that Oui Croissant implement [specific action] to mitigate the risk associated with [identified finding]. This includes [details on recommended actions – e.g., implementing strong authentication methods, changing weak credentials, enforcing strong password policies, etc.]. Additionally, it is advised to [further actions, e.g., implementing access control mechanisms, enforcing encryption protocols, etc.] to enhance the overall security posture of Flakebook.

## Compliance

## References

4.4 MEDIUM

M-00:

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Medium		Score		
Vector	CVSS:3.1/				
OWASP					
Risk Matrix					
Risk Level	Medium	Impact		Probability	
Affected Systems					
IP Address		Port	Service	Version	
Overview					
<p>[Vulnerability] was found on [found location - be specific]. This allows attackers to [attacker capabilities], compromising the [CIA triad]. This attack poses [risk level] as it [explain risk assessment]. This attack carries the potential [attack potential, details on the compromise].</p>					
Business Impact					
<p>The discovery of [identified finding] poses [severity level] risks to [affected area]. An attacker exploiting this vulnerability could potentially [impact description – e.g., disrupt operations, compromise sensitive data, violate compliance standards, etc.].</p> <p>Potential impact scenario:</p>					

- Scenario

These risks could lead to [potential consequences - e.g., legal liabilities, financial losses, reputational damages, etc.], necessitating immediate remediation to safeguard [affected area].

## Steps to Replicate

Target audience: Engineers/Technical

Include screenshots

## Recommended Remediation

[TEAM NAME] recommends that Oui Croissant implement [specific action] to mitigate the risk associated with [identified finding]. This includes [details on recommended actions – e.g., implementing strong authentication methods, changing weak credentials, enforcing strong password policies, etc.]. Additionally, it is advised to [further actions, e.g., implementing access control mechanisms, enforcing encryption protocols, etc.] to enhance the overall security posture of Flakebook.

## Compliance

## References

4.5 LOW

L-00:

Common Vulnerability Scoring System (CVSS v3.1)					
Severity	Low		Score		
Vector	CVSS:3.1/				
OWASP					
Risk Matrix					
Risk Level	Medium	Impact		Probability	
Affected Systems					
IP Address		Port	Service	Version	
Overview					
<p>[Vulnerability] was found on [found location - be specific]. This allows attackers to [attacker capabilities], compromising the [CIA triad]. This attack poses [risk level] as it [explain risk assessment]. This attack carries the potential [attack potential, details on the compromise].</p>					
Business Impact					
<p>The discovery of [identified finding] poses [severity level] risks to [affected area]. An attacker exploiting this vulnerability could potentially [impact description – e.g., disrupt operations, compromise sensitive data, violate compliance standards, etc.].</p> <p>Potential impact scenario:</p> <ul style="list-style-type: none"><li>• Scenario</li></ul>					



These risks could lead to [potential consequences - e.g., legal liabilities, financial losses, reputational damages, etc.], necessitating immediate remediation to safeguard [affected area].

## Steps to Replicate

Target audience: Engineers/Technical

Include screenshots

## Recommended Remediation

[TEAM NAME] recommends that Oui Croissant implement [specific action] to mitigate the risk associated with [identified finding]. This includes [details on recommended actions – e.g., implementing strong authentication methods, changing weak credentials, enforcing strong password policies, etc.]. Additionally, it is advised to [further actions, e.g., implementing access control mechanisms, enforcing encryption protocols, etc.] to enhance the overall security posture of Flakebook.

## Compliance

## References

4.6 INFORMATIONAL

I-00:

Affected Systems			
IP Address	Port	Service	Version
			N/A
Overview			
<p>[Vulnerability] was found on [found location - be specific]. This allows attackers to [attacker capabilities], compromising the [CIA triad]. This attack poses [risk level] as it [explain risk assessment]. This attack carries the potential [attack potential, details on the compromise].</p>			
Business Impact			
<p>The discovery of [identified finding] poses [severity level] risks to [affected area]. An attacker exploiting this vulnerability could potentially [impact description – e.g., disrupt operations, compromise sensitive data, violate compliance standards, etc.].</p> <p>Potential impact scenario:</p> <ul style="list-style-type: none"><li>Scenario</li></ul> <p>These risks could lead to [potential consequences - e.g., legal liabilities, financial losses, reputational damages, etc.], necessitating immediate remediation to safeguard [affected area].</p>			
Steps to Replicate			
<p>Target audience: Engineers/Technical</p>			
Recommended Remediation			

[TEAM NAME] recommends that Oui Croissant implement [specific action] to mitigate the risk associated with [identified finding]. This includes [details on recommended actions – e.g., implementing strong authentication methods, changing weak credentials, enforcing strong password policies, etc.]. Additionally, it is advised to [further actions, e.g., implementing access control mechanisms, enforcing encryption protocols, etc.] to enhance the overall security posture of Flakebook.

## Compliance

## References

## Appendix

### A: CVSS AND RISK

#### CVSS Version 3.1 Features

The Common Vulnerability Scoring System (CVSS) is a framework for communicating the characteristics and severity of vulnerabilities in software. Although CVSS has three metric groups, a risk score is calculated using the base metric only, which includes exploitability and impact on the affected system. Temporal and environmental metrics are not required but do provide additional context on the identified vulnerability.

#### Exploitability

These metrics assess the ease and means by which a vulnerability can be exploited.

- **Attack Vector (AV):** This metric reflects the level of access required to exploit a vulnerability.

Confidential - Do not duplicate or distribute without written permission from Oui Croissant

- **Attack Complexity (AC):** This metric reflects the actions needed by the attacker to evade defensive measures.
- **Privileges Required (PR):** This metric describes the level of privileges to exploit a vulnerability.
- **User Interaction (UI):** This metric describes whether a user is required to participate in a successful exploit.
- **Scope (S):** This metric reflects whether the impact of this vulnerability affects systems beyond its means.

### **System Impact**

These metrics reflect the impact on confidentiality, integrity, and availability of a targeted system after a successful exploit.

- **Confidentiality (C):** This metric describes if an exploit results in the disclosure of sensitive information.
- **Integrity (I):** This metric reflects if protected data is able to be tampered with or changed in any way.
- **Availability (A):** This metric reflects whether an exploit is able to render access to information unavailable.

### **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 Figure A 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 Figure B.

#### **A) CVSS 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 ( <b>U</b> ), Changed ( <b>C</b> )
Network ( <b>N</b> ), Adjacent ( <b>A</b> ), Local ( <b>L</b> )	Impact
Attack Complexity (AC)	Confidentiality (C)
Low ( <b>L</b> ), High ( <b>H</b> )	None ( <b>N</b> ), Low ( <b>L</b> ), High ( <b>H</b> )
Privileged Required (PR)	Integrity (I)
None ( <b>N</b> ), Low ( <b>L</b> ), High ( <b>H</b> )	None ( <b>N</b> ), Low ( <b>L</b> ), High ( <b>H</b> )
User Interaction (UI)	Availability (A)
None ( <b>N</b> ), Required ( <b>R</b> )	None ( <b>N</b> ), Low ( <b>L</b> ), High ( <b>H</b> )

Figures A and B:

Legends 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. The full breakdown of Supplemental, Environmental, and Threat Metrics is not included.

## Risk Analysis Features

Confidential - Do not duplicate or distribute without written permission from Oui Croissant

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 a budding social media platform, the range of potential threat actors anticipated by Flakebook is not limited to unsophisticated, low-level criminals but includes sophisticated, high-caliber, and well-funded threats. This is because social media platforms like Flakebook collect and process a significant amount of personal, behavioral, and financial data, making them attractive targets for a range of attackers. 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, Oui Croissant cannot afford to ignore any high-impact vulnerability merely because of its lower likelihood.

For this reason, [TEAM NAME] 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.

The following outlines the criteria used to assess and score both probability and impact.

### **Probability**

**Very High:** The exploit is easily achievable, requiring minimal technical knowledge, and likely has a publicly available, detailed guide or walkthrough.

**High:** No specific privileges are required for exploitation, and a proof-of-concept (PoC) is available, though some technical skill or troubleshooting might be necessary.

**Medium:** Exploitation does not require privileges, but a PoC is not publicly available, meaning it may take additional time or expertise to exploit.

**Low:** Exploitation requires the attacker to already have some low-level privileges, restricting access to those who can gain such access.

**Very Low:** The exploit requires high-level privileges, making it feasible only if the attacker has significant access beforehand.

### **Impact**

**Very High:** An attacker would gain full control of critical systems, potentially locking out administrators or compromising all accounts.

**High:** The attacker gains access to a significant part of the system, though further actions would be required to fully compromise or control it.

**Medium:** The attacker can access sensitive parts of the system, potentially disrupting operations but without full system compromise.

**Low:** Limited impact on operations or data exposure, potentially causing minor disruptions without significant damage.

**Very Low:** The impact is minimal, possibly causing minor annoyance or inconvenience without affecting critical operations.

### **Risk Level Measures:**

Alternatively, to measure risk levels, a simplistic risk matrix is used as defined in Figure C. 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 sub score provided by the CVSS calculator, along with a base probability using the CVSS exploitability sub score. The two scores are then adjusted by Offensive Security Society'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 Figure C. Finally, all quantitative scores are converted to qualitative ratings using a score-to-rating scale as described in Figure D.

### **C) Probability vs Impact Risk Matrix**

Probability	Risk Level
-------------	------------



Very High (9.0-10.0)	Medium	Medium	High	Critical	Critical
High (7.0-8.9)	Low	Medium	High	High	Critical
Medium (4.0-6.9)	Low	Low	Medium	High	High
Low (2.0-3.9)	Very Low	Low	Medium	Medium	High
Very Low (0-1.9)	Very Low	Very Low	Low	Medium	Medium
<b>Impact</b>	Very Low (0-1.9)	Low (2.0-3.9)	Medium (4.0-6.9)	High (7.0-8.9)	Very High (9.0-10.0)

**D) Score-to-Rating Chart**

Rating	Probability	Impact
Critical	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	0.0 - 0.49	0.00 - 0.59

Figures C and D:

Legends for the scoring of risk level, probability, and impact. (C) shows the risk matrix for obtaining the qualitative risk level using the qualitative measures of probability and impact. (D) shows the corresponding rating which describes each range of probability, impact, and risk.

It is important to note that the scoring process is done throughout the report using the technical knowledge and professional experience of [TEAM NAME]'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.

## B: OFFENSIVE TOOLS

Tool	Link
<b>nmap</b>	<a href="https://nmap.org/download.html">https://nmap.org/download.html</a>
<b>metasploit</b>	<a href="https://www.metasploit.com">https://www.metasploit.com</a>
<b>hashcat</b>	<a href="https://hashcat.net/hashcat/">https://hashcat.net/hashcat/</a>
<b>ffuf</b>	<a href="https://github.com/ffuf/ffuf">https://github.com/ffuf/ffuf</a>
<b>seclists</b>	<a href="https://github.com/danielmiessler/SecLists">https://github.com/danielmiessler/SecLists</a>
<b>netcat</b>	<a href="https://nmap.org/ncat/">https://nmap.org/ncat/</a>
<b>impacket</b>	<a href="https://github.com/SecureAuthCorp/impacket">https://github.com/SecureAuthCorp/impacket</a>
<b>evil-winrm</b>	<a href="https://github.com/Hackplayers/evil-winrm">https://github.com/Hackplayers/evil-winrm</a>
<b>mimikatz</b>	<a href="https://github.com/ParrotSec/mimikatz">https://github.com/ParrotSec/mimikatz</a>
<b>smbmap</b>	<a href="https://github.com/ShawnDEvans/smbmap">https://github.com/ShawnDEvans/smbmap</a>
<b>proxychains</b>	<a href="https://github.com/haad/proxychains">https://github.com/haad/proxychains</a>
<b>enum4linux</b>	<a href="https://github.com/CiscoCXSecurity/enum4linux">https://github.com/CiscoCXSecurity/enum4linux</a>
<b>gobuster</b>	<a href="https://github.com/OJ/gobuster">https://github.com/OJ/gobuster</a>
<b>dirsearch</b>	<a href="https://github.com/maurosoria/dirsearch">https://github.com/maurosoria/dirsearch</a>
<b>crackmapexec</b>	<a href="https://github.com/byt3bl33d3r/CrackMapExec">https://github.com/byt3bl33d3r/CrackMapExec</a>




C: HOSTS DISCOVERED

<begin of template>

<Subnet#>
-----------


<large window instance>




<ip>		

</>

<window and linux instance>



<ip>



<ip>

</>

<single linux instance>



<ip>

</>

<end of template>

E: Steps to Compromise

Step #	Action	Version
		N/A
Overview		
<p>[Vulnerability] was found on [found location - be specific]. This allows attackers to [attacker capabilities], compromising the [CIA triad]. This attack poses [risk level] as it [explain risk assessment]. This attack carries the potential [attack potential, details on the compromise].</p>		

## Final Checklist

Remove [TK]

Page break in between findings

Professionalism:

- Proofread !!! (if possible)
- Use professional tone, use 3rd ppov (avoid 1st and 2nd ppov).
  - Don't be too technical.
  - Check for spelling and grammar to improve credibility and professionalism.
- Remove / redact all sensitive information.
- Make sure all hyperlinks have the full URI in text for printing.

Friendly Nature with Company

- Did the report start off with the positives before the negatives?
- Does any negative point note / complement the efforts of the company
- Does the report directly blame anyone for mistakes?

Confidential - Do not duplicate or distribute without written permission from Oui Croissant

Presentability:

- Avoid too much whitespace, but also avoid very dense and text-heavy appearance,
  - (Attempt to distribute whitespace evenly throughout page)
  - Use justify alignment instead of left align (unless the paragraph width is too small, in which case large amounts of awkward white space will appear, so use left align instead)
- Use color coding for vulnerabilities and risks
- Use different sizings and notations to clearly show a different section.

Final Notes:

- Export in file format that is not easily edited (pdf)
- Deliver the report through safe channels.

END OF FINAL CHECKLIST - <REMOVE WHEN REPORT IS FINISHED>