
QUICROISSANT PENETRATION TEST



Jan. 18-19 / Team Finals-XX / **CONFIDENTIAL**

TEAM MEMBERS



Team Lead / Captain



Analyst / Member



Analyst / Member



Analyst / Member



Analyst / Member



Analyst / Member

AGENDA

1. Assessment Overview
2. Strengths
3. Key Findings
4. Remediations
5. Business Impact

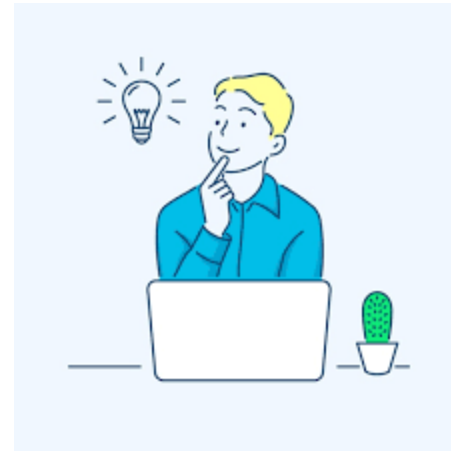
ASSESSMENT OVERVIEW

Our two main goals for this assessment were:

1. A reassessment of previous systems and vulnerabilities
 - Reviewing previously discovered vulnerabilities to see if remediation strategies were implemented
2. Discovering new Vulnerabilities
 - Including testing with OuiCroissant's new social media platform Y
 - Interacting with beta stage AI tools being developed by OuiCroissant

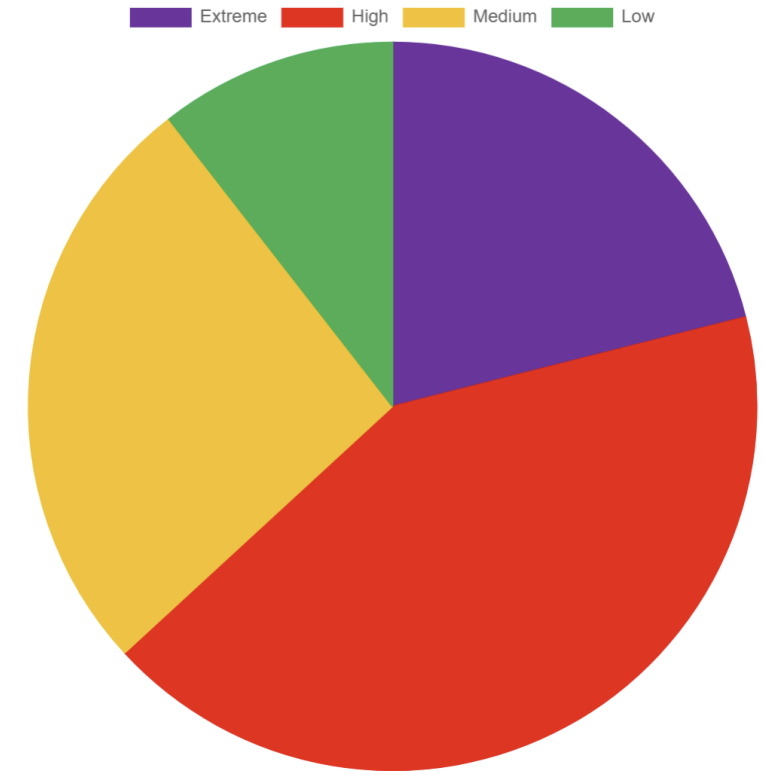
STRENGTHS

1. Most critical vulnerability from initial assessment was remediated
2. Updated software widely used
3. Hardened production servers



KEY FINDINGS

- Blank Local Administrator Password on Desktop Machines
- Arbitrary Remote Code Execution as Root
- Insecure Direct Object Reference Enables Impersonation on Y
- Cross Site Scripting on Y



BUSINESS IMPACT

- Data Modification, Loss, and Exfiltration
- Legal Consequences for PII Data Breach
- Reputational Damage

QUESTIONS?