OuiCroissant: Y Social Media Platform

Security Assessment Executive Briefing

Finals-XX CPTC

OUR TEAM

Member
Web Services

Captain
Penetration Testing Lead

Member
Linux Engineer

Member
Active Directory Lead

Member
Windows Specialist

Member
Project Manager

OVERVIEW

01
Executive Summary

02
Methodology

03
Key Weaknesses

04
Recommendations

01

Executive Summary

Executive Summary

Secure

Infrastructure
Security

Application
Security

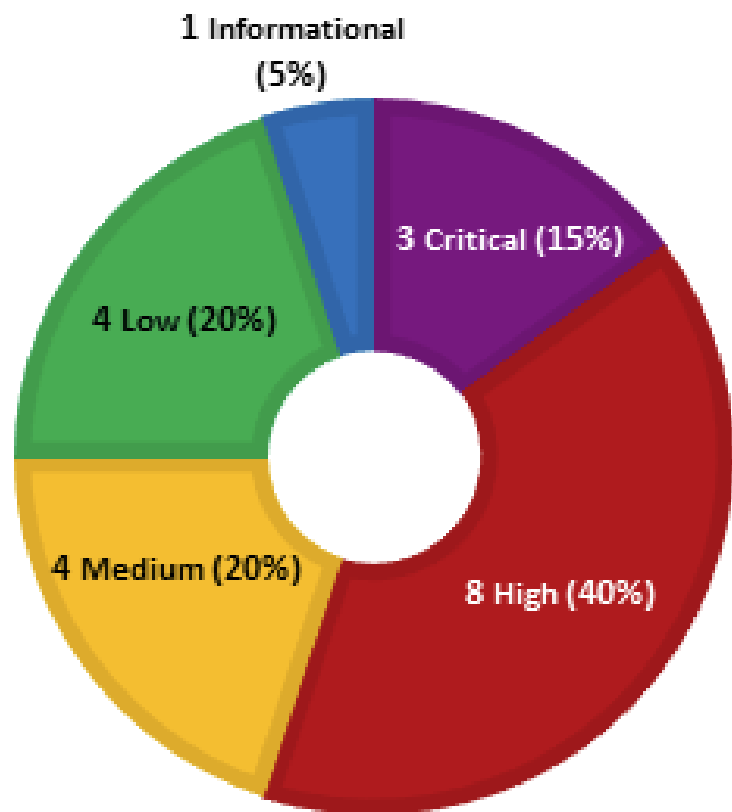**Critical**

1000+

Users with
Breached Data

Impact

1) Application
   Downtime
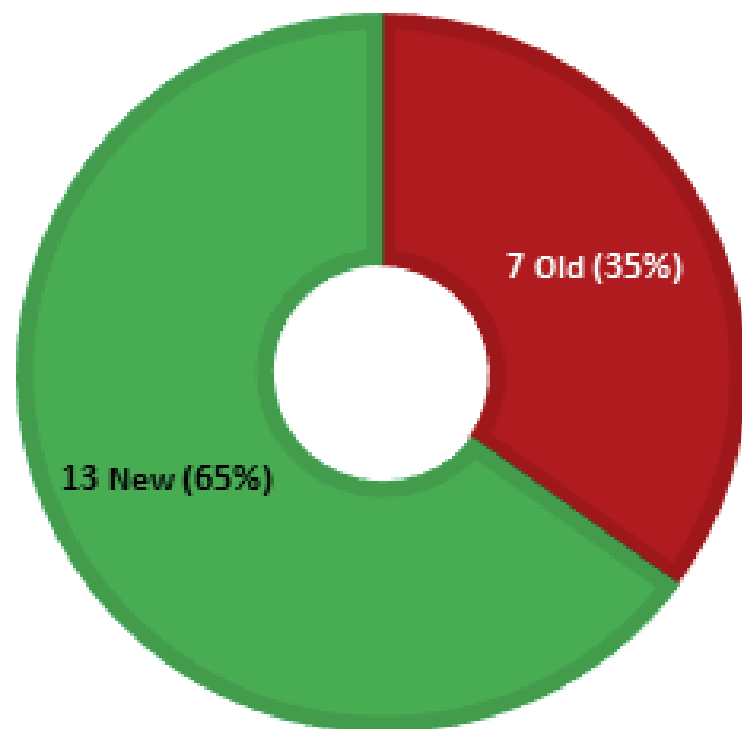2) Reputation
   Damage
3) Financial Loss

VULNERABILITIES BY SEVERITY

Legend: ■Critical ■High ■Medium ■Low ■Informational

1 Informational (5%)

3 Critical (15%)

4 Low (20%)

4 Medium (20%)

8 High (40%)

OLD VS NEW VULNERABILITIES

Legend: ■Old ■New

7 Old (35%)

13 New (65%)

AI Integration

Prompt Injection

Overwriting instructions of the AI

Vishing Call

Social engineering IT helpdesk

02

Methodology

Methodology

DEFINING THE SCOPE

EXPLOITATION

REPORTING

01

02

03

04

05

06

FOOTPRINTING AND IDENTIFYING THE NETWORK TOPOLOGY

DETAILED RESEARCH AND ANALYSIS OF THE VULNERABILITIES

RECOMMENDATIONS AND FOLLOW UP TESTS
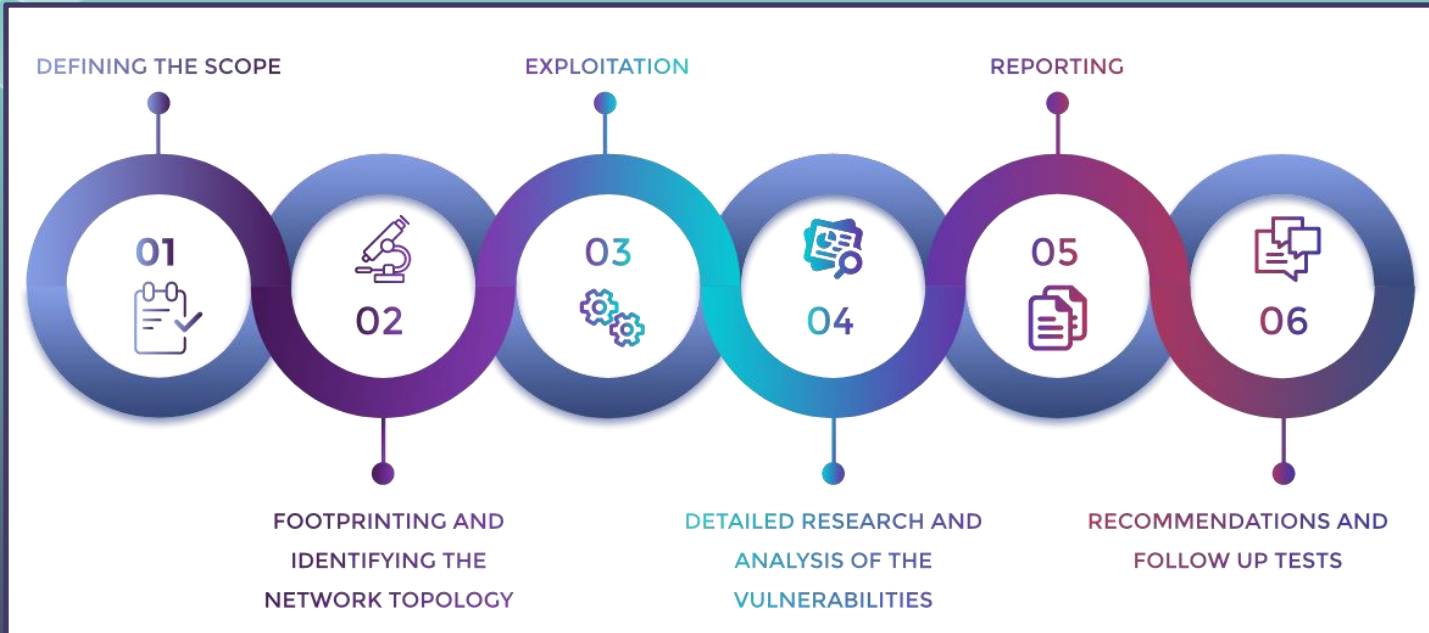
Methodology

Severity

The overall damage

Degree of Exposure

How exposed the finding is

Ease of Exploitation

How easy it is to exploit the finding

Business Impact

The direct impact on operations

Effort to Fix

The effort needed to remediate

Technical Impact

Effect on application and infrastructure

Objectives

Evaluate Product Security

Retest Previous Observations

Assess Overall Security Posture

03

Key Strengths

Key Strengths

1 Remediating Past Observations

2 Hardening Active Directory

3 Incident Response

Key Security Flaws

1 Potential Denial of Service

2 Unauthenticated SMTP Relay

3 Unauthenticated User Management

04

Recommendations

Recommendations

1 Rate limit & disable error broadcasting

2 Require authentication for SMTP relay

3 Secure user management resources

4 Do not hard code admin credentials

Summary

Findings

20 Discovered
Vulnerabilities

Key Weaknesses

Critical Vulnerabilities
Preventing Launch

Remediations

Advised safeguards
for each vulnerability

Questions?

Please don't hesitate to contact us at

cptc10-finals-xx@cptc.team