Penetration Testing Agreement

Between:
Pentester: HAKIZIMANA Jean D'Amour
Client: ParoCyber
Date: 04/12/2025

1. Introduction

This Penetration Testing Agreement ("Agreement") outlines the terms and conditions under which the Pentester will conduct an authorized security assessment for ParoCyber ("Client"). The objective of this engagement is to identify security vulnerabilities, assess the Client's security posture, and provide actionable remediation recommendations.

The testing will be conducted in a controlled, ethical, and legally compliant manner, in accordance with recognized cybersecurity and responsible disclosure standards.

2. Scope of Work

2.1 In Scope Assets

The Pentester is authorized to perform penetration testing on the following systems:

- **Web Applications**
- **Network Infrastructure**
- **APIs**
- **Cloud / Virtual Assets**
- **Authentication & Access Control Systems**

2.2 Out of Scope Assets

The following systems are explicitly excluded from testing unless separately authorized in writing by the Client:

- Production databases containing live customer or sensitive data
- Third party systems or assets not owned or controlled by ParoCyber
- Physical security controls and facilities
- Social engineering activities (phishing, impersonation, onsite tests) unless pre-approved

2.3 Allowed Testing Activities

The Pentester may perform the following activities:

- Vulnerability assessment and scanning
- Web application testing based on **OWASP Top 10**
- Network penetration testing
- API security testing
- Authentication, authorization, and session management testing
- Configuration and policy review
- Controlled exploitation of discovered vulnerabilities within safety limits

2.4 Prohibited Actions

The Pentester shall not perform any of the following:

- Denial of Service (DoS/DDoS) attacks
- Intentional data deletion, corruption, or unauthorized modification
- Extraction or exfiltration of sensitive personal information
- Any activities that may cause major service disruption or operational impact

---

3. Rules of Engagement

3.1 Testing Window

Testing will be conducted during the following period:
Start: 04/12/2025
End: 30/12/2025

Testing may take place during business or non-business hours as mutually agreed.

3.2 Communication Protocol

- The Pentester will provide daily or weekly progress updates to the Client's appointed security representative.
- Critical vulnerabilities or high-risk findings will be reported immediately upon discovery.
- Both parties will provide 24/7 emergency contacts for incident escalation, if needed.

3.3 Methodology

The Pentester will follow industry accepted methodologies, including:

- **OWASP Testing Guide**
- **NIST SP 800-115 (Technical Guide to Information Security Testing)**
- **PTES (Penetration Testing Execution Standard)**
- **MITRE ATT&CK Framework** (as a reference)

4. Legal Authorization

ParoCyber grants explicit written authorization for the Pentester to perform penetration testing on all assets listed as in scope in Section 2.

The Pentester agrees to:

- Perform all testing ethically, professionally, and lawfully
- Strictly adhere to the defined scope
- Immediately halt testing if discovered actions pose unanticipated risk to systems or data

This authorization protects the Pentester from legal liability arising from approved testing activities conducted within scope.

5. Confidentiality

Both parties agree to maintain strict confidentiality regarding all aspects of the engagement, including but not limited to:

- Identified vulnerabilities
- System or network configurations
- Sensitive data encountered during testing
- Final reports and supporting documentation

All collected data will be securely stored and permanently deleted within **30 days** after report delivery unless otherwise requested by the Client.

6. Deliverables

6.1 Penetration Testing Report

The Pentester will provide a comprehensive report including:

- Executive summary for management
- Detailed list of identified vulnerabilities with severity ratings
- Technical analysis and root cause of each issue
- Screenshots, logs, and evidence supporting the findings
- Risk assessment
- Recommended remediation actions

6.2 Review Presentation

The Pentester will conduct a walkthrough session with the Client to explain findings, discuss risks, and support remediation planning.

7. Liability & Responsibility

The Pentester shall not be held responsible for:

- Pre-existing vulnerabilities or misconfigurations
- System failures not directly caused by testing activities
- Losses arising from inadequate backups or poor system maintenance

The Client is responsible for ensuring that full system backups are created before the testing engagement begins.

8. Payment Terms

- **Total Fee:** $10,000
- **Payment Schedule:** (e.g., 50% upfront, 50% upon final report delivery)

9. Termination

Either party may terminate this Agreement by providing written notice. In the event of termination:

- All testing activities will cease immediately
- The Client will be invoiced for completed work to date
- All collected data will be securely deleted

10. Signatures

By signing below, both parties acknowledge that they have read, understood, and agreed to all terms stated in this Penetration Testing Agreement.

Pentester

Name: HAKIZIMANA Jean D’amour
Signature: 
Date:4/12/2025

Client (ParoCyber)

Representative Name: **ParoCyber**
Signature:
Date: 4/12/2025