Penetration Testing Agreement

Between:
Pentester: Robert Dzogah
Client: ParoCyber

---

1. Introduction and Purpose

This agreement formalizes the professional relationship between Robert Dzogah and ParoCyber for conducting authorized penetration testing activities. The objective is to identify, assess, and document security vulnerabilities within the defined scope, providing actionable remediation recommendations to enhance ParoCyber's security posture.

---

2. Scope of Work

2.1 In-Scope Assets

- Web applications

- Internal network: 1.1.1.0/24

- API endpoints: api.parocyber.com/v1/

- Mobile application (Android):

2.2 Out-of-Scope Assets

- Social engineering or phishing campaigns

- Denial-of-Service (DoS/DDoS) attacks

- Physical security assessments

- Third-party hosted services not owned by ParoCyber

2.3 Testing Methodology

- OWASP Top 10 (web applications)

- NIST SP 800-115 guidelines

- Industry-standard tools: Burp Suite, Nmap, Metasploit (where applicable)

3. Responsibilities

3.1. Pen tester Responsibilities

- Perform testing within agreed scope and timelines

- Maintain confidentiality of all findings

- Provide detailed report including:

    o Executive summary

    o Technical vulnerability details

    o Proof-of-concept evidence

    o Risk ratings

    o Remediation recommendations

- Coordinate with ParoCyber team for any critical findings

3.2 ParoCyber Responsibilities

- Provide necessary access credentials (if authorized)

- Designate a point of contact for communication

- Maintain system availability during testing windows

- Notify relevant stakeholders of testing activities

4. Timeline and Deliverables

4.1. Project Schedule

- **Start Date:** 01/12/2025

- **Testing Duration:** 5 business days

- **Report Delivery:** Within 3 business days after testing completion

- **Debrief Meeting:** Scheduled within 5 business days of report delivery

4.2 Deliverables

1. **Initial Reconnaissance Report** (Day 1)

2. **Daily Status Updates** (Optional, upon request)

3. **Final Penetration Testing Report** in PDF

4. **Remediation Validation** (Optional follow-up engagement)

---

5. Rules of Engagement

5.1. Authorized Activities

- Vulnerability scanning and exploitation (where explicitly permitted)

- Credential testing with provided accounts only

- Data extraction limited to proof-of-concept requirements

5.2 Prohibited Activities

- Data exfiltration beyond proof-of-concept needs

- Modification or deletion of production data

- Testing outside agreed time windows (8 AM–6 PM GMT)

- Sharing of findings with unauthorized parties

5.3 Emergency Contact Protocol

- Critical/High-risk findings: Immediate phone notification to POC

- Medium/Low findings: Documented in final report only

---

6. Legal and Compliance

6.1. Authorization

This document serves as explicit authorization for the Pen tester to conduct security testing against defined in-scope assets. ParoCyber agrees to hold the Pen tester harmless for activities conducted within this agreement's boundaries.

6.2 Confidentiality

All findings, reports, and communications are classified as **Confidential** and subject to a 12-month non-disclosure period unless otherwise agreed in writing.

6.3 Data Handling

- No sensitive customer data will be retained after engagement

- All collected data will be securely destroyed after 30 days

- Reports will be transmitted via encrypted channels only

6.4 Compliance

Testing activities will comply with:

- Computer Fraud and Abuse Act (CFAA) exemptions

- Relevant data protection regulations (GDPR/CCPA considerations)

- Industry best practices and ethical guidelines

---

7. Payment Terms

- **Total Fee:** GHC 10,000

- **Payment Schedule:** 50% upon signing, 50% upon report delivery

- **Additional Costs:** None unless scope is modified with written consent

---

8. Signatures

Pentester
Name: Robert Dzogah
Signature: D.R.
Date: 01/12/2025

ParoCyber Representative
Name: _____
Signature: _____
Date: _____