PENTESTING AGREEMENT — ParoCyber & [Allen Chikwenya]

Penetration Testing Agreement
Between:
Pentester: *Allen Archbold Chikwenya*
Client: *ParoCyber*
Date: *02 December 2025*

---

1. Introduction

This Penetration Testing Agreement (“Agreement”) defines the terms under which the Pentester will conduct authorized security testing activities for ParoCyber (“Client”). The purpose of this engagement is to identify, analyze, and report security vulnerabilities affecting the Client’s systems, networks, and digital assets in a legal, controlled, and ethical manner.

This document establishes the permissions, scope, responsibilities, liabilities, deliverables, and limitations associated with the penetration test.

---

2. Objectives of the Engagement

The primary objectives are:

- To assess the security posture of ParoCyber’s systems.
- To identify vulnerabilities arising from misconfigurations, insecure design, weak authentication, and other security weaknesses.
- To demonstrate real-world attack paths without disrupting business operations.
- To provide actionable remediation guidance to improve the Client’s cybersecurity maturity.

The engagement is **strictly for defensive and assessment purposes**.

---

3. Scope of Work

The penetration test will include (only approved areas):

3.1 In-Scope Assets

- Web applications owned and managed by ParoCyber
- Internal and external network infrastructure
- APIs and cloud-hosted services
- Authentication and access control mechanisms
- Employee-facing systems (with explicit authorization)
- Security policies and configurations

A finalized asset list will be validated before testing begins.

3.2 Out-of-Scope Activities

- Social engineering (unless explicitly authorized)
- Physical security penetration tests
- Denial-of-Service (DoS) or stress testing
- Attacks that may cause system unavailability
- Third-party systems not owned by ParoCyber

---

4. Authorization to Test

The Client grants explicit permission for the Pentester to:

- Perform security assessments on all in-scope assets.
- Use tools, scripts, and exploitation frameworks to identify vulnerabilities.
- Access systems strictly within the agreed scope.
- Collect and analyze data necessary for testing.

All testing will comply with legal standards and ethical codes of conduct.

The Pentester will not exceed authorized access under any circumstances.

---

5. Methodology

Testing will follow industry-recognized frameworks including:

- OWASP Testing Guide
- NIST SP 800-115
- PTES (Penetration Testing Execution Standard)
- MITRE ATT&CK Techniques (for threat modeling)

The engagement includes:

- Reconnaissance (Passive & Active)
- Vulnerability identification
- Exploitation (non-destructive)
- Privilege escalation
- Post-exploitation analysis
- Risk rating and documentation (CVSS scoring)

---

6. Pentester Responsibilities

The Pentester agrees to:

- Maintain confidentiality of all client data.
- Avoid unnecessary damage to systems.
- Stop testing immediately if severe issues arise.
- Document all findings accurately and professionally.
- Store data securely and destroy all client data after handover.
- Report high-risk vulnerabilities immediately to the Client.
- Follow professional ethics codes (e.g., EC-Council, ISC², ISACA).

---

7. Client Responsibilities

The Client agrees to:

- Provide written authorization to conduct the assessment.
- Provide test accounts, credentials, or required access.
- Ensure systems are backed up before testing.
- Inform relevant internal teams about the engagement.
- Communicate any system instability or maintenance schedules.

---

8. Confidentiality & Data Handling

- All data collected during testing is confidential.
- No data will be shared with third parties without written approval.
- The Pentester will securely erase all testing data after report delivery.
- The Client will treat the Pentester’s methodology and tools as confidential.

---

9. Liability Limitations

The Pentester:

- Will not be held liable for unintentional downtime, data corruption, or instability resulting from authorized testing, provided actions remain within the agreed scope.
- Will not be responsible for pre-existing vulnerabilities or misconfigurations.
- Provides no guarantee that all vulnerabilities will be identified.

The Client:

- Assumes responsibility for applying remediation recommendations.

---

10. Deliverables

The Pentester will deliver:

10.1 Final Report (PDF)

Including:

- Executive summary
- Methodology
- Detailed findings (with screenshots & evidence)
- Severity ratings (CVSS)
- Impact analysis
- Recommendations and mitigation guidance

10.2 Debrief Meeting

A walkthrough session explaining:

- Attack paths
- Key risks
- Remediation strategy

---

11. Testing Schedule

Start Date: *03 December 2025*
End Date: *05 December 2025*
Testing will occur within the agreed time window to minimize business impact.

---

12. Payment Terms

- All payments shall be made according to the agreed quotation or invoice.
- Any out-of-scope work or retesting will be charged separately.

---

13. Termination Clause

Either party may terminate the engagement with written notice.
Upon termination, the Pentester must return or destroy all collected data.

---

14. Legal Compliance

Both parties agree to comply with:

- Local and international cybersecurity laws
- Anti-hacking regulations
- Data protection standards (GDPR, ISO 27001 principles)

Unauthorized testing outside this agreement is strictly prohibited.

---

15. Agreement Signatures

Client — ParoCyber
Name: ___________________________
Signature: _______________________
Date: ____________________________

Pentester — Allen Archbold Chikwenya
Name: **Allen Archbold Chikwenya**
Signature:
Date: 02/12/25
