PENETRATION TESTING AGREEMENT

This Penetration Testing Agreement (“Agreement”) is made between:

Client: Paro Cyber
Address: McCarthy Hill, Accra, Ghana.

Pentester: Umoru Martha Nkem (Fumi Nkem)
Address: Mainland, Lagos State, Nigeria

---

1. Purpose of the Agreement

The purpose of this Agreement is to define the scope, rules of engagement, authorization, deliverables, and responsibilities for conducting a controlled and ethical penetration test on the Client’s systems.
All activities will be performed to identify security weaknesses and improve the security posture of the Client.

---

2. Scope of Testing

2.1 In-Scope Systems / Assets

The following systems/assets, applications, and infrastructure are authorized for testing:

- ParoCyber web applications
- Network infrastructure systems
- Cloud resources (if approved)
- Provided test accounts or credentials
- Public-facing services
- Any specific systems listed in the written authorization

2.2 Out-of-Scope Activities

The following are strictly prohibited unless explicitly approved in writing:

- Denial-of-Service (DoS/DDoS) tests
- Physical penetration testing
- Attacks against third-party systems
- Social engineering (phishing, vishing, impersonation)
- Data deletion or modification
- Uploading malware outside controlled testing

Any testing outside the defined scope is strictly prohibited unless written authorization is provided.

---

3. Authorized Activities

The Client (Paro Cyber) grants explicit permission for the Tester to perform the following types of testing:

- Network vulnerability scanning
- Web application penetration testing
- Social engineering (if approved)
- Wireless security testing
- API testing
- Cloud security testing
- Physical security assessment (if included)
- Exploitation of discovered vulnerabilities

The Tester agrees **NOT** to perform destructive or disruptive actions unless explicitly approved.

---

4. Rules of Engagement

4.1 Testing Window

Testing will be conducted during:
Days: determined collaboratively between ParoCyber and Pentester
Times: determined collaboratively between ParoCyber and Pentester

4.2 Required Notifications

The Tester must notify the Client:

- Immediately if a critical vulnerability is discovered
- Immediately in case of accidental service disruption
- Upon completion of each testing phase

4.3 Prohibited Actions

Unless expressly approved in writing, the Tester shall NOT:

- Perform Denial-of-Service (DoS or DDoS) attacks
- Alter or delete client data
- Access employee personal data
- Breach legal or regulatory requirements
- Sell or disclose findings to third parties

4.4 Data Handling

All data obtained during testing:

- Must be stored securely
- Must not be shared with unauthorized parties
- Must be destroyed within **30 days** after project completion unless otherwise agreed

---

5. Client Responsibilities

The Client agrees to:

- Provide written authorization for testing
- Ensure all necessary approvals (internal/legal) are in place
- Provide network diagrams, credentials, or supporting documents as needed
- Notify internal teams to avoid false alarms
- Ensure the systems being tested are backed up

6. Tester Responsibilities

The Tester agrees to:

- Conduct all activities professionally and ethically
- Protect Client data at all times
- Minimize disruptions to Client systems
- Report vulnerabilities accurately and responsibly
- Maintain confidentiality

The Tester will comply with relevant laws and frameworks such as:

- OWASP Testing Guide
- NIST SP 800-115
- ISO/IEC 27001 & 27002
- EC-Council & Offensive Security ethical codes
- OSSTMM

7. Deliverables

Upon completion, the Tester will provide:

7.1 Final Report Including:

- Executive summary
- Methodology
- Detailed findings
- Evidence (screenshots/logs)
- Risk ratings (CVSS or agreed metric)
- Recommended remediations

8. Liability Limitations

The Tester will not be held liable for:

- Pre-existing vulnerabilities
- Crashes or outages resulting from normal testing activities
- Data loss if Client neglected to create backups

The Client (ParoCyber) acknowledges that testing may introduce unintended risk, despite all care taken.

---

9. Confidentiality & Non-Disclosure

Both parties agree to maintain strict confidentiality regarding:

- Any vulnerabilities discovered
- Sensitive data observed
- Report contents
- Client business information

This obligation remains in effect even after termination of this Agreement.

---

10. Payment Terms

(This is to be defined by ParoCyber and the Pentester)

Possible billing structures:

- Fixed engagement fee

- Hourly rate

- Retainer / ongoing partnership

- Milestone-based payment model

An invoice will be issued upon completion of deliverables Late payments may delay report release.

---

11. Termination

Either party may terminate the Agreement with written notice.
Upon termination, the Tester must:

- Stop all testing activities immediately
- Return or destroy all Client data
- Provide partial findings if requested

12. Legal Authorization

By signing this Agreement, the Client confirms that they have legal authority over the systems being tested and explicitly authorize the Tester to perform the activities outlined.

13. Signatures

Client Representative
Name: ParoCyber
Date: 4th December, 2025

Penetration Tester
Name: Umoru Martha Nkem (Fumi Nkem)
Date:4th December, 2025

Repository Purpose

This GitHub repository serves as:

- A portfolio demonstration of academic cybersecurity work

- Documentation of course assignments

- A structured template showing professional pentest agreement formatting.

License