PENETRATION TESTING AGREEMENT

Between ParoCyber (Client) and Shola (Independent Pentester)

Date: 02/12/2025

1. Parties Involved

Client: ParoCyber

Pentester: Shola

Both parties agree to the terms and conditions outlined in this Penetration Testing Agreement ("Agreement").

2. Purpose of This Agreement

The purpose of this Agreement is to define the scope, responsibilities, methodologies, legal permissions, deliverables, timelines, and liabilities related to the penetration testing services to be performed by the Pentester for ParoCyber.

The goal of the penetration test is to:

- Identify vulnerabilities in ParoCyber's systems
- Assess security posture against realistic threats
- Provide remediation guidance
- Improve ParoCyber's overall cyber resilience
- The assessment will be conducted ethically and in accordance with industry standards (OSSTMM, NIST SP 800-115, PTES, ISO/IEC 27001)

3.Scope of Work

The objective of the penetration testing is to identify security vulnerabilities, misconfiguration and weakness within the client's systems, networks, infrastructure and applications

The following systems are authorized for testing:

- Web Application: app.parocyber.com
- Corporate Network Segment: 10.20.30.0/24
- Cloud Environment (AWS): EC2 Instances – Production Staging

- User Authentication System
- API Endpoints provided by ParoCyber

3.1 Out-of-Scope Assets

The following are strictly off-limits unless otherwise approved:

- DDoS attacks
- Physical security breaches
- Attacks on third-party systems
- Social engineering against executives (unless written consent)

4.Authorization

ParoCyber formally authorizes the Pentester to perform security against the approved target. This Agreement serves as a legal “Get out of jail free” authorization protecting the Pentester from accusations of unlawful activity, provided all options remain within the agreed scope.

5.Rules of Engagement

- All testing activities must be performed within the agreed timeframe.
- Testing must not cause system outages or loss of data.
- No exploitation beyond proof-of-concept without permission.
- The Pentester will immediately notify ParoCyber of:
  -Critical vulnerabilities
  -Accidental data exposure
  -Any discovered indicators of compromise

6.Deliverables

The Pentester will provide the following:

- A comprehensive written report including:

  -Executive Summary (non-technical)

- Scope & Objectives

- Methodology
- Detailed Findings
- Risk ratings (CVSS v3.1)
- Evidence and screenshots
- Affected assets

6.1 Presentation / Debrief

A virtual or in-person session covering:

- Key findings
- Attack chain walk-through
- Risk prioritisation

7.Legal & Ethical Responsibility

7.1 Confidentiality

All information obtained during the engagement will be kept strictly confidential and not shared with third party.

7.2 Data Protection

The pentester will comply with applicable laws and cybersecurity standards including :

- ISO 27001 Principles
- GDPR
- OWASP Testing Guides

7.3 No unauthorized Disclosure

The Pentester will not disclose vulnerabilities publicly without written permission from ParoCyber.

8. Payment & Terms

ParoCyber agrees to compensate the Pentester based on the agreed rate or contract value

Payment terms include

- 50% due at project start, 50% upon final report delivery

- Payments must be completed within 15 days of invoice

9. Timeline

- Engagement Start: 02/12/2025
- Testing Window: 5 days
- Reporting Delivery: Within 7 business days after testing
- Final Debrief Session: Within 14 days after report submission

Signatures

By signing below, both parties acknowledge and agree to all terms of this Penetration Testing Agreement.

For ParoCyber (Client):

Name: ParoCyber

Signature: PC

Date: 04/12/2025

Pentester (Independent Contractor):

Name: Shola

Signature: SA

Date: 04/12/2025