Penetration Testing Agreement

This Agreement is made on December 2nd, 2025

BETWEEN:

Owoyemi Olaoluwa (Pentester)
owoyemisamuel73@gmail.com
An independent cybersecurity professional.

AND

ParoCyber ("Client")
Paro Cyber
Parocyber@gmail.com
A cybersecurity firm.

1.0 Objectives

This Agreement governs the provision of authorized penetration testing services by the Owoyemi Olaoluwa for the ParoCyber.
The primary objective is to identify, safely exploit, and document security vulnerabilities within the defined scope to improve the ParoCyber's overall security posture. All activities will be conducted ethically, professionally, and in accordance with this Agreement and applicable laws.

2.0 Scope of Work (SOW)

The specific targets, systems, applications, and testing methods are detailed in the Appendix A: Statement of Work (SOW), which is incorporated herein by reference. The SOW includes:

· Defined Targets: Specific IP addresses, URLs, application names, or network ranges.
· In-Scope Testing Methodologies: (e.g., External Network, Web Application, Internal Network, Social Engineering).
· Explicitly Out-of-Scope Items: Any system, service, or activity not listed in Appendix A is strictly prohibited.
· Testing Windows: Agreed-upon dates and times (e.g., "Weekdays between 18:00 - 06:00 UTC").
Owoyemi Olaoluwa shall not deviate from the SOW without prior written authorization from the ParoCyber's designated point of contact.

3.0 Rules of Engagement

1. Authorization: Testing is limited to in-scope assets. Owoyemi Olaoluwa will immediately cease testing on any system found to be out-of-scope and notify the ParoCyber.
2. Avoidance of Harm: Owoyemi Olaoluwa will use best efforts to avoid actions that could cause system instability, data corruption, or denial of service. Techniques considered "high-risk" (e.g., DoS testing, physical testing) require separate, explicit written approval.
3. Privacy & Data Handling: Owoyemi Olaoluwa will not intentionally access, copy, transfer, or store the ParoCyber's proprietary data beyond what is necessary to demonstrate a vulnerability. Any sensitive data encountered will be treated as confidential and handled securely.
4. Communication: A primary point of contact (POC) for each Party will be established for urgent issues (e.g., discovery of a critical, actively exploitable vulnerability).

4.0 Term & Deliverables

· Term: This engagement shall commence on [Start Date] and conclude on [End Date], unless terminated earlier per Section 9.
· Key Deliverables:
  1. Draft Report: A comprehensive report detailing findings, risk ratings, evidence, and remediation recommendations will be provided within 10 business days after the testing window concludes.
  2. Executive Briefing: A presentation or meeting summarizing key findings for management.
  3. Final Report: An updated report incorporating Client feedback will be delivered within 5 business days of receiving comments on the draft.
· Format: All reports will be delivered in password-protected PDF format via a secure method agreed upon by both Parties.

5.0 Fees & Payment Terms

· Total Fee: The total fixed fee for services outlined in the SOW is [Amount].
· Payment Schedule:
  · 50% due upon signing this Agreement.
  · 50% due upon delivery and acceptance of the Final Report.
· Expenses: Any pre-approved expenses (e.g., specialized tools, travel) will be invoiced separately with receipts.
· Invoicing: Invoices are payable within 30 days of receipt.

6.0 Confidentiality

Both Parties agree to hold in strict confidence all non-public information exchanged during this engagement ("Confidential Information"). This includes, but is not limited to, findings, reports, system information, and business processes. This obligation survives the termination of this Agreement for a period of three (3) years.

7.0 Intellectual Property

· Client IP: All pre-existing Client materials and the contents of the Final Report are the property of the Client.
· Pentester IP: The Pentester retains ownership of their proprietary methodologies, tools, and techniques used in the engagement.

8.0 Liability & Indemnification

· No Warranties: Services are provided "as is." The Pentester does not guarantee the discovery of all vulnerabilities or that remediated systems will be impenetrable.
· Limitation of Liability: The Pentester's total liability shall not exceed the total fees paid under this Agreement. Neither Party shall be liable for any indirect, special, or consequential damages.
· Indemnification: The Pentester agrees to indemnify the Client against any claims resulting from the Pentester's gross negligence or willful misconduct in performing the services. The Client agrees to indemnify the Pentester against any claims arising from testing performed within the authorized scope of this Agreement.

9.0 Termination

Either Party may terminate this Agreement with 7 days' written notice. Upon termination, the Client will pay the Pentester for all services rendered and expenses incurred up to the termination date. Upon payment, the Pentester will deliver any completed work product.

10.0 Legal Compliance & Independent Contractor Status

The Pentester warrants that all activities will comply with relevant laws (e.g., Computer Fraud and Abuse Act, GDPR, etc.). The Pentester is an independent contractor, not an employee of ParoCyber. The Pentester is solely responsible for their own taxes, insurance, and benefits.

11.0 Entire Agreement

This document, including its Appendices, constitutes the entire agreement between the Parties and supersedes all prior discussions. Amendments must be in writing and signed by both Parties.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date first written above.

For the Pentester:

Owoyemi Olaoluwa
Date: _____

For the Client (ParoCyber):

Authorized Signatory, ParoCyber
Name: _____
Title: _____
Date: _____

APPENDIX A: Statement of Work (SOW)

SOW Reference: PC-PEN-001
Valid Dates: [Start Date] to [End Date]

1. Primary Objectives:

· Assess the external attack surface of ParoCyber's client-facing web applications.
· Identify vulnerabilities that could lead to data breach or system compromise.

2. Defined In-Scope Targets:

· Web Application: https://portal.parocyber.com
· API Endpoint: https://api.parocyber.com/v1/*
· IP Range: 203.0.113.10 - 203.0.113.30 (Production DMZ)

3. Approved Testing Methods:

· Automated vulnerability scanning (using tools like Burp Suite, Nessus).
· Manual web application testing (OWASP Top 10 focus).
· Authentication and session management testing.
· API security testing.

4. Explicitly Out-of-Scope (Prohibited):

· Denial-of-Service (DoS/DDoS) attacks.
· Physical security or social engineering attacks.
· Testing against third-party services not hosted by ParoCyber.
· Any system or domain not explicitly listed in "In-Scope Targets."

· The internal corporate network (10.0.0.0/8).

5. Testing Schedule:

· Planned Start: [Date], 22:00 UTC
· Planned End: [Date], 06:00 UTC
· Note: All testing must occur within these pre-approved windows.

Client POC for Urgent Issues:
Name: [Name]
Title: [Title]
Phone: [After-Hours Phone]
Email: [Email]

Pentester POC:
Name: Owoyemi Olaoluwa
Phone: [Phone]
Email: [Email]

APPENDIX B: Testing Schedule & Status Updates

(To be maintained and updated throughout the engagement)

Date/Time (UTC)	Activity/Phase	Status	Notes
[Date] 22:00	Engagement Start / Reconnaissance	Planned	
Date] 23:00	Automated Scanning	Planned	
Date+1] 02:00	Manual Exploitation & Validation	Planned	
[Date+1] 06:00	Testing Window Concludes	Planned	
[Date+1]	Analysis & Report Drafting	Planned	