PENETRATION TESTING AGREEMENT

Between ParoCyber (Client) and Zohaib Ashraf (Pentester)
Version 1.0 — 2025
Repository Purpose: Created solely as an academic assignment for the *ParoCyber Ethical Hacking Program*.

1. Introduction

This Penetration Testing Agreement ("Agreement") is entered into between:

Pentester: *Zohaib Ashraf*
Client: *ParoCyber*

The agreement defines the authorized scope, rules, rights, and responsibilities related to security testing on Client-approved systems.

2. Purpose of Engagement

The engagement aims to identify vulnerabilities, evaluate cyber risks, and strengthen the overall security of the Client's digital assets. All findings remain confidential.

3. Scope of Testing

3.1 In-Scope (Authorized Assets)

- **Web Application:**
  https://portal.parocyber.com
  Goal: Identify exploitable web vulnerabilities.
- **Network Range:**
  192.168.10.50 – 192.168.10.200
  Goal: Detect misconfigurations and exposed services.
- **Mobile App:**
  ParoCyber Android App v3.0
  Goal: Evaluate API security, storage controls, permissions.
- **APIs:**
  /v1/auth, /v1/data
  Goal: Access control, token security, injection prevention.

3.2 Out of Scope (Unless Approved)

- DoS/DDoS
- Physical attacks

- Social engineering
- Malware installation
- Data deletion or manipulation
- Unapproved IP ranges or applications

4. Rules of Engagement (ROE)

- Testing occurs only during approved hours
- Sensitive data must not be copied/stored
- No destructive activities
- No brute-force attacks unless approved
- Pentester must stop testing if system instability is detected
- Client emergency contact must be informed in case of major findings

5. Testing Methodology

- OWASP Web Security Testing Guide
- PTES
- NIST SP 800-115
- MITRE ATT&CK

Tools Used

Nmap, BurpSuite, Nessus/OpenVAS, Wireshark, Gobuster, Maltego, OSINT tools, and custom scripts.

6. Client Responsibilities

- Provide accurate system information
- Give formal written authorization
- Designate an emergency technical contact
- Inform internal teams about the test schedule
- Ensure system backups exist
- Provide access credentials (VPN, test accounts)
- Validate the final scope

- Approve any high-risk activities
- Acknowledge inherent risks of testing

7. Pentester Responsibilities

- Follow scope and ROE strictly
- Use safe, non-destructive methods
- Maintain strict confidentiality
- Stop immediately on critical findings
- Securely destroy sensitive data after completion
- Provide clear and professional reporting
- Use only approved devices and IPs
- Comply with national/international cybersecurity laws

8. Non-Disclosure Agreement (NDA)

All information accessed during this engagement is confidential.

Applicable laws include:

- Pakistan PECA 2016
- GDPR (EU)
- CCPA (California)
- Other relevant international regulations

Unauthorized disclosure may result in legal penalties.

9. Legal & Compliance Liability

- Pentester is protected from liability when testing approved assets.
- Client must ensure written authorization is valid.
- The Pentester is not responsible for existing vulnerabilities or unintentional disruptions unless caused by intentional misuse.

10. Reporting & Deliverables

Final deliverables include:

- Executive Summary
- Detailed Vulnerability Report
- CVSS Severity Ratings
- Proof-of-Concept Evidence
- Remediation Recommendations
- Verification Report (optional)
- Pentest Completion Certificate

11. Engagement Timeline

Start Date: *10 March 2025*
End Date: *25 March 2025*

Final Report Delivery:
Between *28 March – 1 April 2025*
(Within 3–7 working days after test completion)

12. Fees

This assessment is part of the **ParoCyber Ethical Hacking Program**, therefore **no financial cost** applies.

13. Signatures

Pentester

Name: Zohaib Ashraf
Signature: Zohaib

Date: *10 March 2025*

Client (ParoCyber)

Representative Name: ParoCyber Security Team
Signature: ParoCyber Representative

Date: *10 March 2025*