

PENETRATION TESTING AGREEMENT

WebApplication Pentest Agreement

DEBORAH N BINYANYA

binyanyadebby@gmail.com

PENETRATION TESTING AGREEMENT

1. Parties to the Agreement

Client

Name: **Paro Cyber**

Address: McCarthy Hill, Accra, Ghana

Email: parocyber@gmail.com

Phone: +233 50 981 1131 / +233 54 312 9758

Penetration Tester

Name: **Binyanya Deborah Nyatichi**

Address: Nairobi, Kenya

Email: binyanyadebby@gmail.com

Phone: +254 742 222 670

2. Purpose of Engagement

The purpose of this engagement is to conduct a controlled and authorized **Web Application Penetration Test** on Paro Cyber's web application to identify potential vulnerabilities, security weaknesses, and risks. The test aims to provide actionable recommendations to improve the security posture of the application.

3. Scope of Testing

3.1 In-Scope Assets

- **Web Application:** <https://parocyber.com>
- **Environment:** Production
- **Application Type:** Customer-facing cybersecurity services platform
- **Technologies:** HTML, JavaScript, PHP, MySQL
- **User Roles Provided:** Admin, Standard User

3.2 Testing Activities Included

- OWASP Top 10 vulnerability testing
- Authentication & session management assessment
- API endpoint testing (exposed and hidden)
- Authorization & privilege escalation testing
- Input validation & injection testing
- Server-side configuration and control review
- File upload security testing
- Business logic and workflow abuse testing

- Sensitive data exposure testing

3.3 Out-of-Scope Items

The following activities are **explicitly excluded**:

- Denial-of-Service (DoS/DDoS) attacks
- Physical security assessments
- Social engineering (phishing, vishing, impersonation, tailgating)
- Network infrastructure testing
- Employee device assessments
- Third-party systems not owned by Paro Cyber

4. Rules of Engagement (ROE)

- **Testing Window:** 6 December 2025 – 20 December 2025
- Testing will be performed in a safe, controlled, and non-destructive manner
- No client data will be intentionally altered, deleted, or corrupted
- High-risk findings (e.g., data exposure) will be reported immediately
- Only client-provided credentials will be used
- All testing activities will be logged and documented

5. Testing Methodology

The penetration test will follow recognized industry standards, including:

- OWASP Web Security Testing Guide (WSTG)
- OWASP Top 10, 2025 Edition
- NIST SP 800-115 Technical Guide to Information Security Testing

Testing Approach: Grey-box (credentials provided)

6. Client Responsibilities

Paro Cyber agrees to:

- Ensure all system backups are up to date before testing begins
- Provide valid credentials for all required user roles
- Notify their hosting provider of approved penetration testing activities
- Maintain application availability during the testing period
- Inform the Tester of any planned system changes or downtime

7. Authorization to Test

Paro Cyber grants **Deborah Nyatichi Binyanya** full authorization to:

- Conduct penetration testing on <https://parocyber.com>
- Perform controlled exploitation to validate vulnerabilities
- Capture and store proof-of-concept evidence
- Scan, enumerate, and probe within the defined scope

This authorization protects the Tester from any legal claims arising from approved testing activities conducted during the engagement period.

8. Confidentiality & Data Protection

Both parties agree to the following:

- All findings and sensitive data will remain confidential
- No information will be disclosed to third parties without written consent
- Testing evidence will be securely deleted within **15 days** after report delivery
- Reports will be securely transferred and encrypted upon request
- The Tester will avoid unnecessary access to personal or sensitive data

9. Reporting

Upon completion of the engagement, the Tester will provide:

1. Executive Summary
2. Detailed Technical Vulnerability Report
3. Risk Ratings (OWASP risk methodology)
4. Remediation Recommendations
5. **One free retest within 30 days** (upon request)

Report Delivery Date: 15 December 2025

10. Liability

The Tester is **not liable** for:

- Service interruptions beyond the Tester's control
- Pre-existing vulnerabilities or misconfigurations
- Loss of revenue, reputation, or downtime

Total liability is limited to the **total fee paid** for this engagement.

11. Payment Terms

- **Total Engagement Fee:** KES 200,000
- **Payment Structure:**
 - 50% upfront: **KES 100,000**
 - 50% upon delivery of the final report: **KES 100,000**
- Payments are due within **14 days** of invoice submission

12. Termination

Either party may terminate this agreement with written notice.

Paro Cyber remains responsible for payment for work completed prior to termination.

13. Signatures

For Paro Cyber

Name: Paro Cyber

Signature:

Date: **6 December 2025**

For the Tester

Name: **Deborah Nyatichi Binyanya**

Position: Penetration Tester

Signature:

Date: **6 December 2025**