

# PENETRATION TESTING REPORT

**Target System:** temanpramuka.id

**Scan ID:** 3

**Report Date:** January 30, 2026

**Report Time:** 20:38:11

## **CONFIDENTIAL**

This report contains sensitive security information.  
Handle with appropriate care and restrict distribution.

**Prepared by:** AutoPentestX Team

**Tool:** AutoPentestX v1.0

**Framework:** Automated Penetration Testing Toolkit

## EXECUTIVE SUMMARY

This penetration testing report presents the findings of an automated security assessment conducted on the target system **temanpramuka.id**. The assessment was performed on January 30, 2026 using the AutoPentestX automated penetration testing toolkit.

**Overall Risk Level:** MINIMAL

**Total Vulnerabilities Identified:** 0

**Critical/High Risk Items:** 0

**Web Vulnerabilities:** 0

**SQL Injection Points:** 0

## SCAN DETAILS

**Target:** temanpramuka.id

**Operating System:** Unknown (TTL > 128)

**Scan Duration:** 30.42 seconds

**Total Open Ports:** 0

**Scan Method:** Automated comprehensive scan using Nmap, Nikto, and SQLMap

## OPEN PORTS AND SERVICES

No open ports detected.

## VULNERABILITIES IDENTIFIED

No vulnerabilities detected.

## RISK ASSESSMENT

Based on the comprehensive analysis of identified vulnerabilities, their severity levels, exploitability, and potential impact, the overall risk assessment for the target system is:

**Overall Risk Level:** MINIMAL

**Total Risk Score:** 0.00

**Average Risk per Port:** 0.00

## EXPLOITATION ASSESSMENT

No exploitation attempts were made.

# SECURITY RECOMMENDATIONS

Based on the identified vulnerabilities and risk assessment, the following remediation actions are recommended to improve the security posture of the target system:

## **MEDIUM Priority:**

- **Enable Firewall**

Configure firewall to restrict access to necessary ports only.

- **Update All Services**

Ensure all services are running latest stable versions.

## **LOW Priority:**

- **Implement Monitoring**

Set up intrusion detection and continuous monitoring.

- **Security Hardening**

Apply security hardening guidelines for the operating system.

# CONCLUSION

This automated penetration testing assessment has identified various security vulnerabilities and potential risks in the target system. The findings should be carefully reviewed and prioritized based on the risk levels assigned.

It is strongly recommended to address all CRITICAL and HIGH severity findings immediately, followed by MEDIUM and LOW severity items according to available resources and priorities.

Regular security assessments should be conducted to maintain a strong security posture and protect against emerging threats.

## **Important Notes:**

- This assessment was conducted using automated tools and may not identify all vulnerabilities
- Manual verification and testing is recommended for critical systems
- Results should be validated before taking remediation actions
- This report is confidential and should be handled securely

**DISCLAIMER:** This penetration testing report is provided for educational and authorized security assessment purposes only. The tools and techniques used are intended for legitimate security testing in controlled environments with proper authorization. Unauthorized use of these tools against systems you do not own or have explicit permission to test is illegal and unethical. The developers and users of AutoPentestX assume no liability for misuse or damage caused by this tool.