SPARTA Security Framework

Technical Assessment Report

Version 1.0 - Test Fixture

CONFIDENTIAL

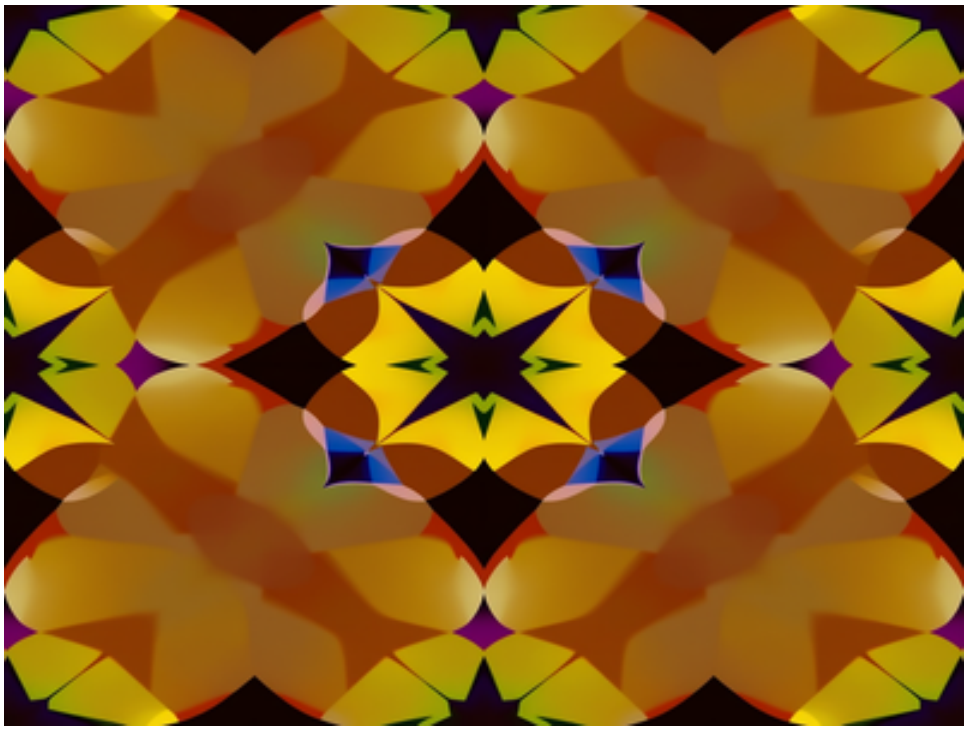

Figure 0: Cover illustration (decorative)

1. Executive Summary // This section gives a brief overview of the technical

This document presents findings.

1.1 Scope

1.2 Methodology

The assessment followed NIST SP 800-53 guidelines and incorporated threat modeling using STRIDE methodology. Testing was conducted over a 4-week period.

2. System Architecture

The target infrastructure consists of a multi-tier architecture with segregated network zones.

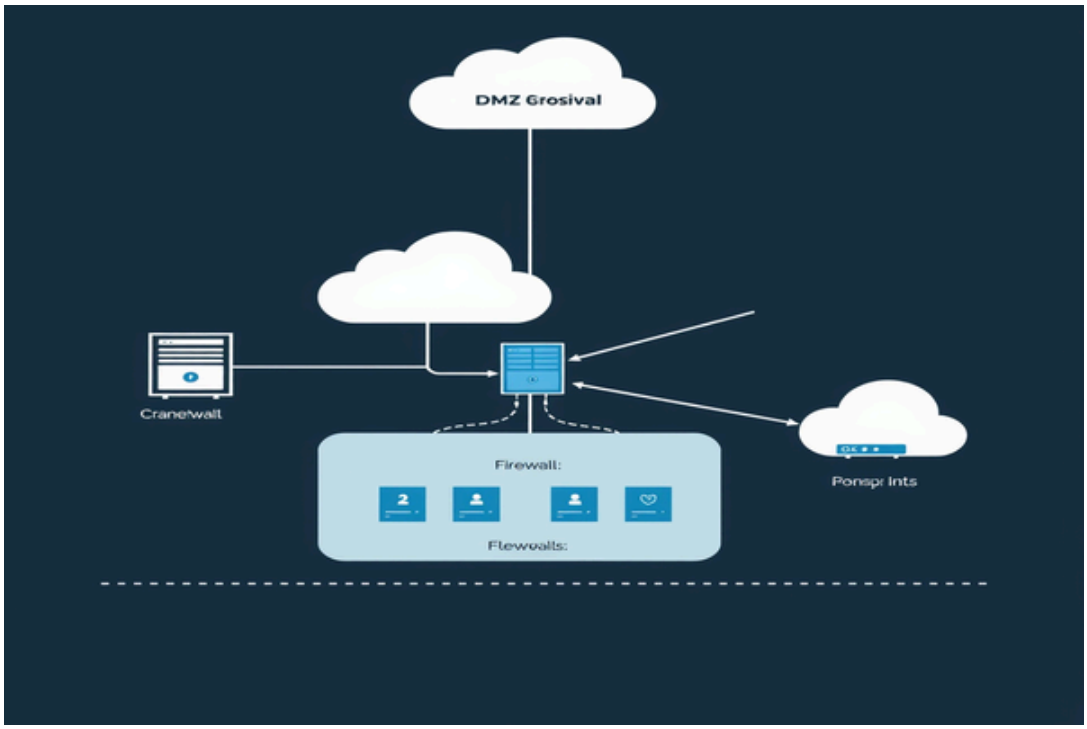

Figure 1: Network Architecture Overview

3. Vulnerability Assessment Results

The following table summarizes identified vulnerabilities:

ID	Vulnerability	Severity	Status
V-001	SQL Injection in login form	Critical	Remediated
V-002	XSS in search function	High	In Progress
V-003	Missing CSRF tokens	Medium	Open
V-004	Weak password policy	Medium	Open
V-005	Outdated SSL/TLS version	High	Remediated
V-006	Information disclosure in errors	Low	Open

Table 1: Vulnerability Summary

4. Remediation Process

The following flowchart outlines the remediation workflow:

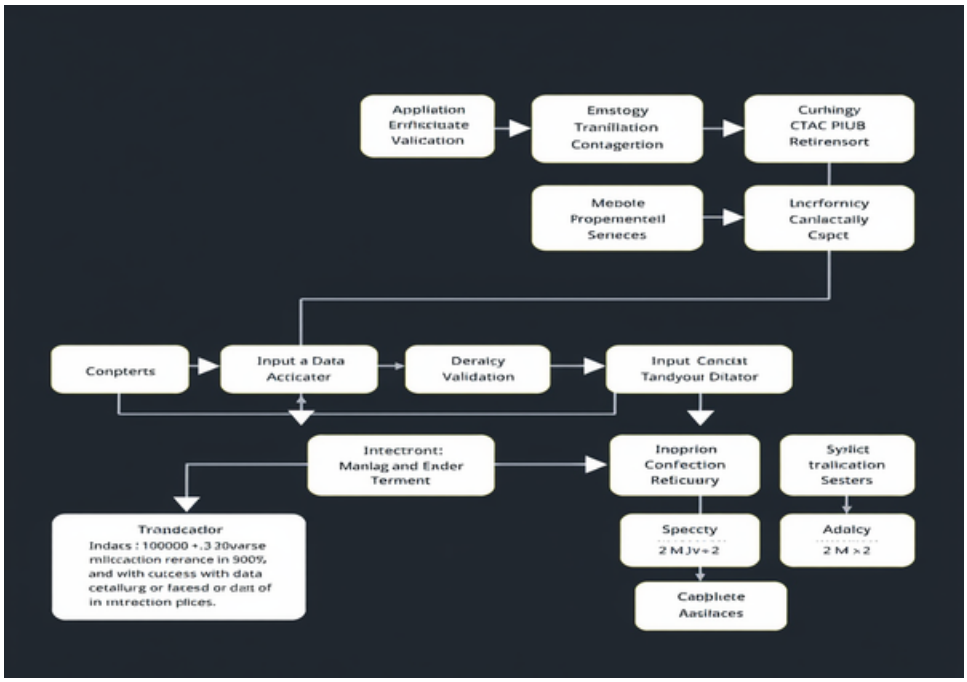

Figure 2: Remediation Workflow

5. Access Control Assessment

Access controls were evaluated across all system components.

5.1 Authentication Mechanisms

Multi-factor authentication is deployed for administrative access.

5.2 Authorization Controls

Privilege escalation paths were identified in the CI/CD pipeline.

6. Cryptographic Controls

Encryption standards vary across the infrastructure.

6.1 Key Management

HSMs are used for production keys.

6.2 Certificate Management

SSL certificates are managed via Let's Encrypt.

7. Logging and Monitoring

Centralized logging is implemented using ELK stack.

7.1 Log Retention

Logs are retained for 90 days in hot storage.

7.2 Alerting Configuration

Critical alerts route to PagerDuty.

8. Incident Response

IR playbooks exist for common scenarios.

8.1 Detection Capabilities

Mean time to detect is approximately 4 hours.

8.2 Response Procedures

Documented procedures for containment phases.

9. Compliance Status

The organization maintains SOC 2 Type II certification.

9.1 Gap Analysis

Minor gaps identified in asset inventory.

9.2 Remediation Timeline

All gaps targeted for Q2 2026.

10. Recommendations

Priority recommendations focus on access control.

10.1 Short-term Actions

Implement least privilege within 30 days.

10.2 Long-term Roadmap

Zero-trust architecture planned for 18-month horizon.

Appendix A: Testing Tools

The following tools were used: Nmap 7.94 for network scanning, Burp Suite Professional for web application testing, Metasploit Framework for exploitation verification, Nessus for vulnerability scanning.