SPARTA Security Framework

Technical Assessment Report

Version 2.1 - January 2026

CONFIDENTIAL

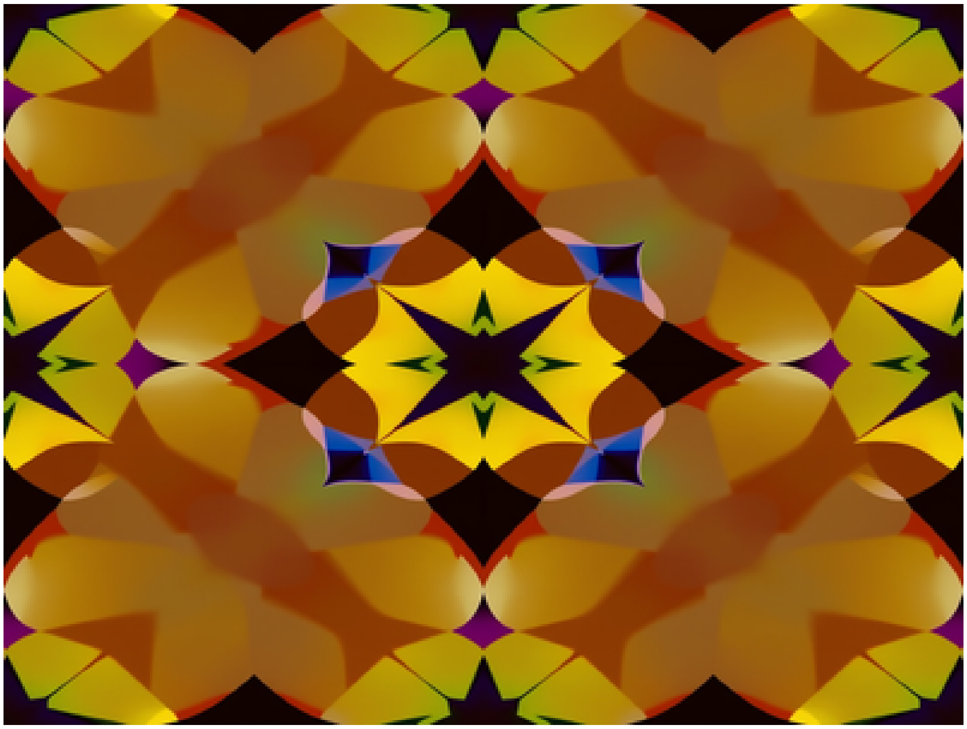

Figure 0: Cover illustration (decorative)

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

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 with both automated scanning and manual penetration testing.

2. System Architecture

The target infrastructure consists of a multi-tier architecture
with segregated network zones. The following diagram illustrates the high-level topology:

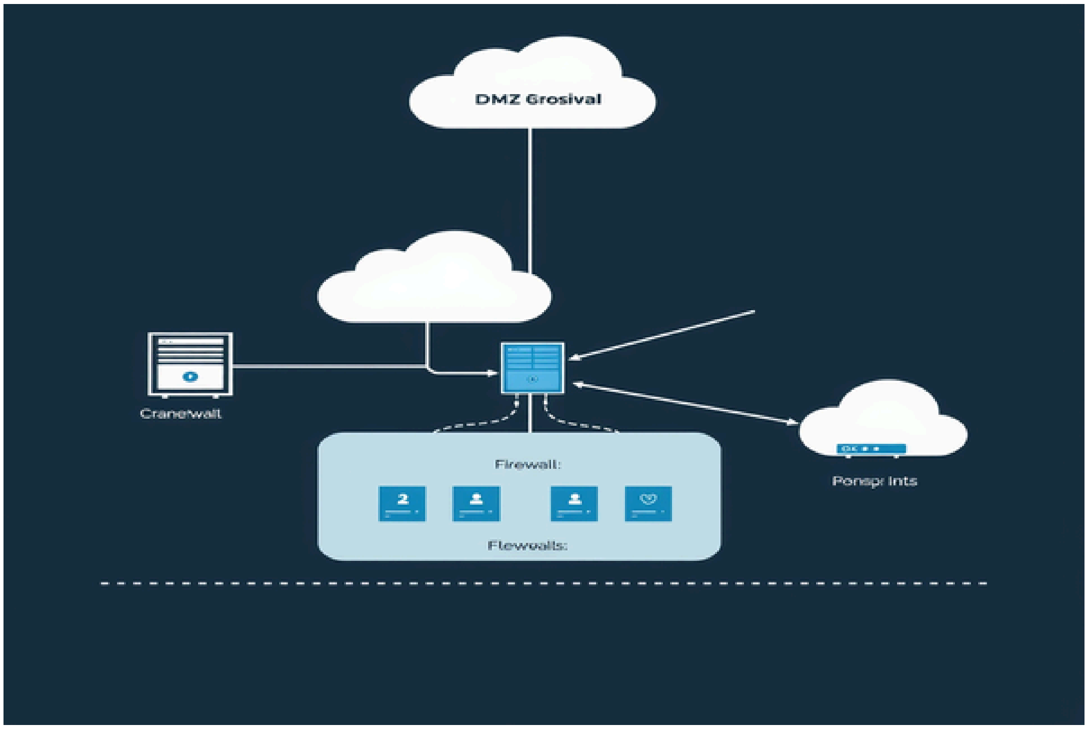

Figure 1: Network Architecture Overview

2.1 Network Segmentation

The network is divided into three primary zones: DMZ, Internal,
and Management. Each zone is protected by dedicated firewall rules and IDS sensors.

3. Vulnerability Assessment Results

The following table summarizes identified vulnerabilities by severity:

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V-005	Outdated SSL/TLS version	High	Remediated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 vulnerability remediation workflow implemented during this assessment:

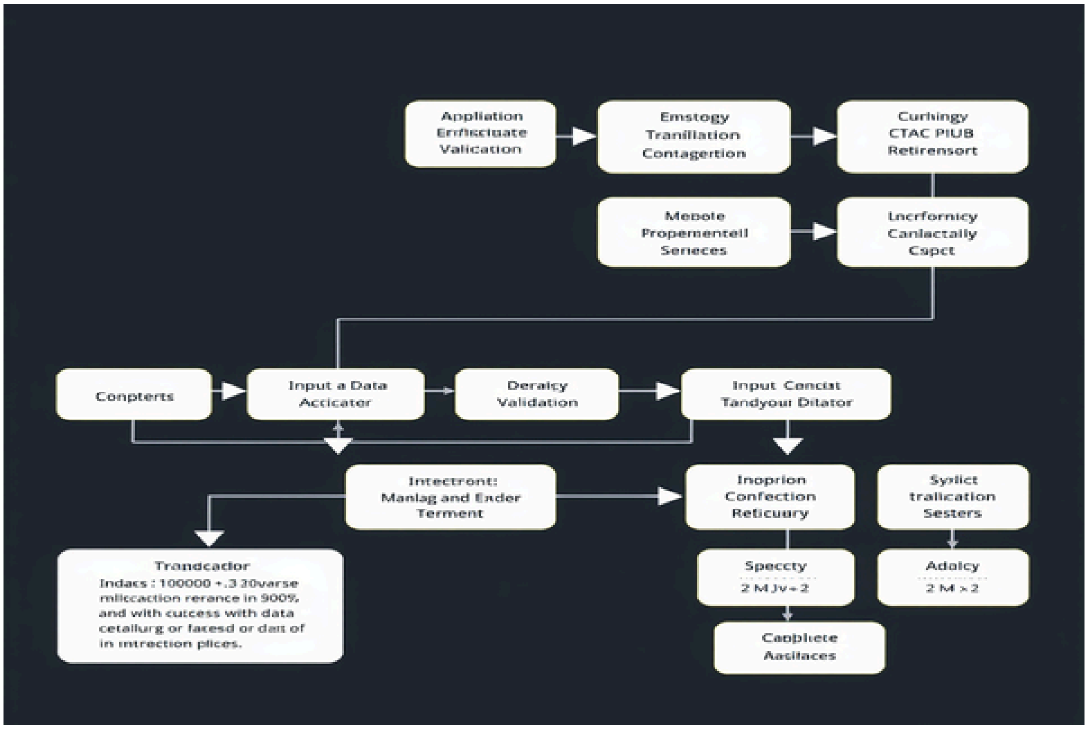
Appliation Erfiscistate Valication
Emstogy Tranillation Contagertion
Curhingy CTAC PIUB Retirensort
Mebote Propementell Seneces
Lncrfornicy Canlactally Capct
Conpterts
Input a Data Acticater
Deraicy Validation
Input Cancist Tandyour Ditator
Intectront: Manlag and Exder Terment
Inoprion Confection Reticuury
Sylict tralication Sesters
Trandcacior
Indacs : 100000 +.3 30varse milccaction rerance in 900%, and with cutcess with data cetallurg or facesd or dait of in intraction plices.
Specctу
2 M Jv+2
Adalcy
2 M >2
Canpliete Aasilaces

Figure 2: Remediation Workflow

5. Access Control Assessment

Access controls were evaluated across all system components. Role-based access control (RBAC) is implemented but requires refinement.

5.1 Authentication Mechanisms

Multi-factor authentication is deployed for administrative access. User authentication relies on Active Directory integration.

5.2 Authorization Controls

Privilege escalation paths were identified in the CI/CD pipeline. Service accounts have excessive permissions.

6. Cryptographic Controls

Encryption standards vary across the infrastructure. Data at rest uses AES-256, but key management practices need improvement.

6.1 Key Management

HSMs are used for production keys. Development environments use software vaults.

6.2 Certificate Management

SSL certificates are managed via Let's Encrypt with auto-renewal.

7. Logging and Monitoring

Centralized logging is implemented using ELK stack. SIEM rules require tuning to reduce false positives.

7.1 Log Retention

Logs are retained for 90 days in hot storage, 1 year in cold storage.

7.2 Alerting Configuration

Critical alerts route to PagerDuty. Medium alerts create Jira tickets.

8. Incident Response

IR playbooks exist for common scenarios. Tabletop exercises conducted quarterly.

8.1 Detection Capabilities

Mean time to detect (MTTD) is approximately 4 hours for critical events.

8.2 Response Procedures

Documented procedures for containment, eradication, and recovery phases.

9. Compliance Status

The organization maintains SOC 2 Type II and ISO 27001 certifications.

9.1 Gap Analysis

Minor gaps identified in asset inventory and change management processes.

9.2 Remediation Timeline

All compliance gaps targeted for remediation within Q2 2026.

10. Recommendations

Priority recommendations focus on access control hardening and key management.

10.1 Short-term Actions

Implement least privilege for service accounts within 30 days.

10.2 Long-term Roadmap

Zero-trust architecture adoption planned for 18-month horizon.

Appendix A: Testing Tools

The following tools were used during this assessment:

- Nmap 7.94 for network scanning
- Burp Suite Professional for web application testing
- Metasploit Framework for exploitation verification
- Nessus for vulnerability scanning
- Custom Python scripts for automation

Appendix B: Glossary

DMZ - Demilitarized Zone

IDS - Intrusion Detection System

RBAC - Role-Based Access Control

MTTD - Mean Time to Detect

SIEM - Security Information and Event Management