Afiq Nasrudin

afiqnas@gmail.com

Abstract

This report presents a consolidated view of security findings derived from recent API security testing and infrastructure-level vulnerability assessments (VA). The analysis identifies key weaknesses across authentication, data protection, and system configuration domains. Through quantitative summaries and visual insights, this report enables targeted remediation planning and informs strategic decisions to enhance the organization's security posture.

Technical Escalation Report

Vulnerability Assessment Scan Findings API Security Findings

**Version Control**

| **Version** | **Date** | **Page** | **Description** | **Approved By** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Contents

[1. Executive Summary 3](#_Toc199493989)

[2. Assessment Scope 3](#_Toc199493990)

[3. Summary Metrics 3](#_Toc199493991)

[4. API Security Findings 4](#_Toc199493992)

[4.1 API Vulnerability Findings 4](#_Toc199493993)

[4.2 Visual Insights 5](#_Toc199493994)

[5. Infrastructure / VA Findings 6](#_Toc199493995)

[5.1 VA Vulnerability Findings 6](#_Toc199493996)

[5.2 Visual Insights 9](#_Toc199493997)

[6. Key Observations 11](#_Toc199493998)

[7. Recommendations 11](#_Toc199493999)

# 1. Executive Summary

This report consolidates findings from both the API Security Assessment and the Infrastructure/Application-Level Vulnerability Assessment (VA). The goal is to highlight key technical risks, categorize the most prevalent vulnerabilities, and provide data-driven recommendations to inform remediation and security hardening efforts.

# 2. Assessment Scope

|  |  |
| --- | --- |
| **Category** | **Description** |
| **API Security** | Focused on vulnerabilities identified across multiple application APIs, including authentication, authorization, data leakage, and rate limiting weaknesses. |
| **Vulnerability Assessment (VA)** | Focused on host and application layer vulnerabilities, including misconfigurations, outdated components, and critical CVEs exploitable over the network. |

# 3. Summary Metrics

|  |  |  |
| --- | --- | --- |
| **Metric** | **API Assessment** | **VA Assessment** |
| Total Findings Identified | 100 | 17694 |
| Unique Applications / Hosts Assessed | 20 | 164 |
| High / Critical Risk Issues | N/A | High: 20  Critical: 35 |

# 4. API Security Findings

## 4.1 API Vulnerability Findings

The following are the API vulnerabilities identified:

|  |  |
| --- | --- |
| **Finding Name** | **Count** |
| Insecure Login Endpoint Allowing Credential Stuffing | 10 |
| Improper Session Termination on Logout | 8 |
| Mass Assignment on User Role Field | 8 |
| Token Refresh Endpoint Missing Session Validation | 8 |
| No Rate Limiting on Feedback Submission Endpoint | 7 |
| Sensitive User Data Returned in API Response | 7 |
| Overexposed Admin Reports with Unfiltered Data | 6 |
| SQL Injection via Unsanitized Search Parameter | 6 |
| Missing Authorization Check on User Settings Access | 6 |
| Hardcoded API Keys Found in Response | 5 |
| Exposed Internal Debug Endpoint | 4 |
| Improper CORS Configuration Allowing Wildcard Origins | 4 |
| Brute-Forceable 2FA Verification Endpoint | 4 |
| Improper Error Handling Revealing Stack Trace | 3 |
| SQL Injection in Product Filtering Endpoint | 3 |
| Insufficient Logging and Monitoring | 3 |
| Direct Object Reference to Other Users' Invoices | 2 |
| Unrestricted File Upload in Profile Update | 2 |
| Improper Asset Management of Deprecated Endpoints | 2 |
| Lack of Access Control on Admin Functions | 2 |

## 4.2 Visual Insights

**Figure 1: Top 10 API Vulnerabilities**

A graph of data with blue and white bars

AI-generated content may be incorrect.

This chart shows the most frequently recurring vulnerability types across tested APIs.

**Figure 2: Vulnerability Heatmap by Application Version**

A table with numbers and text

AI-generated content may be incorrect.

The heatmap highlights the spread and intensity of vulnerabilities across different application versions, enabling targeted remediation planning.

# 5. Infrastructure / VA Findings

## 5.1 VA Vulnerability Findings

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding Name** | **Count** | **Severity** | **CVSS Score** |
| Service Detection | 1615 | Informational | 0 |
| HyperText Transfer Protocol (HTTP) Information | 1456 | Informational | 0 |
| HTTP Server Type and Version | 1451 | Informational | 0 |
| Web Server No 404 Error Code Check | 786 | Informational | 0 |
| SSL Cipher Suites Supported | 718 | Informational | 0 |
| SSL / TLS Versions Supported | 718 | Informational | 0 |
| TLS ALPN Supported Protocol Enumeration | 705 | Informational | 0 |
| SSL Certificate Information | 694 | Informational | 0 |
| SSL Perfect Forward Secrecy Cipher Suites Supported | 693 | Informational | 0 |
| SSL Root Certification Authority Certificate Information | 693 | Informational | 0 |
| TLS Version 1.2 Protocol Detection | 693 | Informational | 0 |
| TLS Version 1.3 Protocol Detection | 692 | Informational | 0 |
| SSL/TLS Recommended Cipher Suites | 684 | Informational | 0 |
| SSL Cipher Block Chaining Cipher Suites Supported | 684 | Informational | 0 |
| TLS Next Protocols Supported | 636 | Informational | 0 |
| HSTS Missing From HTTPS Server | 599 | Informational | 0 |
| SSL Certificate Signed Using Weak Hashing Algorithm (Known CA) | 451 | Informational | 0 |
| HSTS Missing From HTTPS Server (RFC 6797) | 438 | Medium | 5.8 |
| TLS Version 1.1 Deprecated Protocol | 335 | Medium | 6.1 |
| TLS Version 1.1 Protocol Detection | 335 | Informational | 0 |
| TLS Version 1.0 Protocol Detection | 316 | Medium | 6.1 |
| Nessus SYN scanner | 255 | Informational | 0 |
| Nessus Scan Information | 255 | Informational | 0 |
| Common Platform Enumeration (CPE) | 251 | Informational | 0 |
| OS Identification | 250 | Informational | 0 |
| Device Type | 250 | Informational | 0 |
| TCP/IP Timestamps Supported | 204 | Informational | 0 |
| Host Fully Qualified Domain Name (FQDN) Resolution | 146 | Informational | 0 |
| Additional DNS Hostnames | 90 | Informational | 0 |
| SSL Medium Strength Cipher Suites Supported (SWEET32) | 80 | Medium | 5 |
| SSL Certificate Chain Contains Certificates Expiring Soon | 74 | Informational | 0 |
| SSL Certificate Expiry - Future Expiry | 74 | Informational | 0 |
| Inconsistent Hostname and IP Address | 67 | Informational | 0 |
| TLS NPN Supported Protocol Enumeration | 54 | Informational | 0 |
| Web Server robots.txt Information Disclosure | 32 | Informational | 0 |
| nginx HTTP Server Detection | 29 | Informational | 0 |
| Apache 2.4.x < 2.4.60 Multiple Vulnerabilities | 16 | Critical | 10 |
| QUIC Service Detection | 15 | Informational | 0 |
| Web Server Crafted Request Vendor/Version Information Disclosure | 12 | Informational | 0 |
| Web Application Cookies Are Expired | 10 | Informational | 0 |
| SSL Certificate 'commonName' Mismatch | 9 | Informational | 0 |
| Apache 2.4.x < 2.4.47 Multiple Vulnerabilities | 7 | High | 7.5 |
| HTTP Methods Allowed (per directory) | 6 | Informational | 0 |
| Apache 2.4.x < 2.4.59 Multiple Vulnerabilities | 6 | High | 7.8 |
| Open Port Re-check | 5 | Informational | 0 |
| Non-compliant Strict Transport Security (STS) | 5 | Informational | 0 |
| Strict Transport Security (STS) Detection | 5 | Informational | 0 |
| OS Identification Failed | 5 | Informational | 0 |
| OpenSSL 1.1.1 < 1.1.1t Multiple Vulnerabilities | 4 | High | 7.1 |
| OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities | 4 | Medium | 5 |
| Apache 2.4.x < 2.4.53 Multiple Vulnerabilities | 4 | High | 7.5 |
| Apache < 2.4.49 Multiple Vulnerabilities | 3 | Medium | 6.8 |
| Apache 2.4.x < 2.4.54 Multiple Vulnerabilities | 3 | Medium | 6.4 |
| HTTP/2 Cleartext Detection | 3 | Informational | 0 |
| Apache 2.4.x < 2.4.55 Multiple Vulnerabilities | 3 | High | 7.6 |
| SSH Algorithms and Languages Supported | 2 | Informational | 0 |
| Patch Report | 2 | Informational | 0 |
| Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod\_lua) | 2 | Medium | 5 |
| OpenSSL 1.1.1 < 1.1.1l Multiple Vulnerabilities | 2 | High | 7.5 |
| Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF | 2 | High | 7.5 |
| OpenSSL 1.1.1 < 1.1.1k Multiple Vulnerabilities | 2 | Medium | 5.8 |
| SSH Server Type and Version Information | 2 | Informational | 0 |
| Apache 2.4.x < 2.4.56 Multiple Vulnerabilities | 2 | Critical | 10 |
| OpenSSL 1.1.1 < 1.1.1j Multiple Vulnerabilities | 2 | Medium | 5 |
| SSL Certificate with Wrong Hostname | 2 | Medium | 5 |
| Apache HTTP Server Version | 2 | Informational | 0 |
| Apache 2.4.x < 2.4.58 Multiple Vulnerabilities | 2 | High | 7.8 |
| OpenSSL 1.1.1 < 1.1.1v Multiple Vulnerabilities | 2 | Medium | 5 |
| Wireless Access Point Detection | 2 | Informational | 0 |
| OpenSSL 1.1.1 < 1.1.1x Multiple Vulnerabilities | 2 | Medium | 5 |
| OpenSSL 1.1.1 < 1.1.1y Multiple Vulnerabilities | 2 | Medium | 5.4 |
| Web Server Reverse Proxy Detection | 1 | Medium | 5 |
| SSH Password Authentication Accepted | 1 | Informational | 0 |
| OpenSSL 1.1.1 < 1.1.1i Vulnerability | 1 | Medium | 4.3 |
| OpenSSL 1.1.1 < 1.1.1p Vulnerability | 1 | Critical | 10 |
| OpenSSL 1.1.1 < 1.1.1m Vulnerability | 1 | Medium | 4.3 |
| OpenSSL 1.1.1 < 1.1.1q Vulnerability | 1 | Medium | 5 |
| OpenSSL 1.1.1 < 1.1.1o Vulnerability | 1 | Critical | 10 |
| Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability | 1 | Medium | 5 |
| Backported Security Patch Detection (SSH) | 1 | Informational | 0 |
| Grafana Labs Web Detection | 1 | Informational | 0 |
| Unknown Service Detection: Banner Retrieval | 1 | Informational | 0 |
| Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122) | 1 | High | 7.8 |
| Web Server HTTP Header Internal IP Disclosure | 1 | Low | 2.6 |
| OpenSSL 1.1.1 < 1.1.1w Vulnerability | 1 | Medium | 6.8 |
| SSL Certificate Cannot Be Trusted | 1 | Medium | 6.4 |
| Apache >= 2.4.17 < 2.4.49 mod\_http2 | 1 | Medium | 5 |
| OS Security Patch Assessment Not Available | 1 | Informational | 0 |
| Apache 2.4.x < 2.4.52 mod\_lua Buffer Overflow | 1 | High | 7.5 |
| Apache >= 2.4.30 < 2.4.49 mod\_proxy\_uwsgi | 1 | Medium | 5 |
| OpenSSL 1.1.1 < 1.1.1za Vulnerability | 1 | Medium | 4.3 |
| Apache 2.4.x < 2.4.54 Authentication Bypass | 1 | High | 7.5 |
| OpenSSL 1.1.1 < 1.1.1zb Vulnerability | 1 | Medium | 6.8 |
| SSH Protocol Versions Supported | 1 | Informational | 0 |
| SSL Self-Signed Certificate | 1 | Medium | 6.4 |
| UPnP Client Detection | 1 | Informational | 0 |
| SSL Session Resume Supported | 1 | Informational | 0 |
| SSH SHA-1 HMAC Algorithms Enabled | 1 | Informational | 0 |
| OpenSSL Detection | 1 | Informational | 0 |
| SSH Weak Key Exchange Algorithms Enabled | 1 | Low | 2.6 |
| OpenSSL Version Detection | 1 | Informational | 0 |
| OpenSSL 1.1.1 < 1.1.1n Vulnerability | 1 | Medium | 5 |
| Target Credential Status by Authentication Protocol - No Credentials Provided | 1 | Informational | 0 |
| Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330) | 1 | Medium | 5 |
| OpenSSH Detection | 1 | Informational | 0 |

## 5.2 Visual Insights

**Figure 1: CVSS Score Distribution**

A graph of a person with a number of lines

AI-generated content may be incorrect.

*This distribution illustrates the relative spread of severity scores. A notable volume of vulnerabilities fall within the 7.0–8.9 range, indicating a prevalence of high-risk issues.*

**Figure 2: Combined VA Risk Distribution**

A graph of a number of blue squares

AI-generated content may be incorrect.

*The risk distribution chart segments vulnerabilities by their severity level (Critical, High, Medium, Low), supporting prioritization for patching and remediation.*

# 6. Key Observations

* **Authentication & Authorization Gaps** are widespread in APIs, increasing the risk of access control bypass and data leakage.
* **Patch Management Deficiencies** are evident, with multiple high-severity CVEs present on live systems.
* **Configuration Weaknesses** in both APIs and infrastructure expose sensitive data and increase attack surface.
* **Inconsistent Security Hygiene** across environments suggests the need for centralized hardening and DevSecOps enforcement.

# 7. Recommendations

|  |  |
| --- | --- |
| **Area** | **Recommendation** |
| API Security | Implement input validation, enforce proper authentication and RBAC, adopt OAuth2 standards |
| Patch Management | Automate and enforce patch cycles for OS, middleware, and libraries |
| Secure Configuration | Harden TLS, disable default accounts, enforce secure headers, rate limiting |
| CI/CD Integration | Incorporate security scans into build pipelines (SAST, DAST, dependency checks) |
| Continuous Monitoring | Enable API logging, use WAF/API Gateway, and implement SIEM integration |