



[www.getastra.com](http://www.getastra.com)

# Vulnerability Assessment & Penetration Test Report

Automated Full Scan + Manual Pentest

## Demo

2 targets

Report Generated On **September 30, 2026**

## About Astra

Astra is a leading Penetration Testing as a Service (PTaaS) platform which combines continuous automated vulnerability scanning with on-demand manual pentests by security experts. Astra follows the highest standards for security testing, vulnerability scanning and is an active contributor to industry leading Open source security standards and tools (OWASP WSTG, ZAP). Astra is CREST certified & CERT-In empanelled.

The assessment was performed within the predefined scope of this engagement, and its findings and recommendations have been shared with the customer. A penetration test is considered a snapshot in time. The findings and recommendations solely reflect the information gathered during the assessment period and do not account for any subsequent changes or modifications.

**Astra IT Inc.**

[help@getastra.com](mailto:help@getastra.com)

2093 Philadelphia Pike 4080,  
Claymont, Delaware, 19703,  
United States



**Report Generated On:** 30th September 2026

Astra was engaged by Demo to perform a Vulnerability Assessment and Penetration Test of **2** targets during the period **1st July 2025** to **16th September 2026**. Manual pentest was performed on **1** target, and Automated vulnerability scanning was performed on **1** target.

The testing was performed from a remote attacker's perspective with the following goals:

- To identify security loopholes, business logic errors, and evaluate the effectiveness of existing security controls through expert manual testing and automated vulnerability scanning.
- Recommend technical security best practices to improve security posture of the target applications audited.
- Explain the potential impact of the identified vulnerabilities, such as the extent of data exposure, potential financial losses, or reputational damage that could occur if they were exploited by malicious actors.
- Provide clear and actionable recommendations for addressing the identified vulnerabilities.

A total of **14 vulnerabilities/recommendations** were reported. Out of a score of 10, the highest risk score assigned to a vulnerability was **9**, the lowest was **2.8**, and the average score was **5.8**.

The total potential loss due to these vulnerabilities is estimated to be **\$9,280.00**.

## Vulnerability Statistics

| Severity    | Solved | Unsolved | Help Wanted | Under Review | Accepted Risk | Grand Total |
|-------------|--------|----------|-------------|--------------|---------------|-------------|
| Critical    | 0      | 3        | 0           | 0            | 0             | 3           |
| High        | 0      | 2        | 0           | 0            | 0             | 2           |
| Medium      | 0      | 5        | 0           | 0            | 0             | 5           |
| Low         | 0      | 2        | 0           | 0            | 0             | 2           |
| Info        | 0      | 2        | 0           | 0            | 0             | 2           |
| Grand Total | 0      | 14       | 0           | 0            | 0             | 14          |

Overall vulnerability statistics

# Scope of Testing

Security assessment includes testing for security loopholes in the scope defined below. Apart from the following, no other information was provided. Nothing was assumed at the start of the security assessment. The following assets were covered under the assessment:

| Astra Target Name             | Asset Kind | Scope URI                         | Start Grade | Closure Grade |
|-------------------------------|------------|-----------------------------------|-------------|---------------|
| API Scanner Demo API Target 2 | API        | https://hypetest.getastra.dev     | B           | B             |
| Demo API                      | API        | http://hypejabbedv2.getastra.dev/ | D           | D             |

# Assessment Duration and Dates

| Scan Mode             | Target Name                   | Authentication | Started       | Reporting Completed On |
|-----------------------|-------------------------------|----------------|---------------|------------------------|
| Automated (Full)      | API Scanner Demo API Target 2 | 1 user         | 16th Sep 2026 | 16th Sep 2026          |
| Manual Pentest (VAPT) | Demo API                      | 0 users        | 01st Jul 2025 | 01st Jul 2025          |

# Vulnerabilities Overview Table

| No. | Vulnerability ID | Target   | Reported by      | Title                                                                                                 | Severity | Risk Score | Status   |
|-----|------------------|----------|------------------|-------------------------------------------------------------------------------------------------------|----------|------------|----------|
| 1   | 32bd             | Demo API | Security Analyst | [CRITICAL] Unauthorized Access To API Endpoints                                                       | Critical | 9          | Unsolved |
| 2   | c89c             | Demo API | Security Analyst | [CRITICAL] Weak JWT Token Implementation - No Signature Validation                                    | Critical | 8.7        | Unsolved |
| 3   | 29a7             | Demo API | Security Analyst | [CRITICAL] Broken Access Control (Sensitive Information Disclosure from Unauthenticated API Requests) | Critical | 8.3        | Unsolved |
| 4   | de67             | Demo API | Security Analyst | Old version of API [v1] is Used" Along with [v3]                                                      | High     | 6.6        | Unsolved |
| 5   | c2ec             | Demo API | Security Analyst | Sensitive Information Disclosure via Publicly Accessible WordPress REST API                           | High     | 6.3        | Unsolved |
| 6   | 0793             | Demo API | Security Analyst | Lack of Input Validation                                                                              | Medium   | 5.2        | Unsolved |

| No. | Vulnera              | Target                        | Reported by      | Title                                                                                | Severity | RiskScore | Status   |
|-----|----------------------|-------------------------------|------------------|--------------------------------------------------------------------------------------|----------|-----------|----------|
| 7   | <a href="#">e782</a> | Demo API                      | Security Analyst | <a href="#">Missing API Security Headers</a>                                         | Medium   | 4.8       | Unsolved |
| 8   | <a href="#">b998</a> | Demo API                      | Security Analyst | <a href="#">No rate limiting on API key generation</a>                               | Medium   | 4.6       | Unsolved |
| 9   | <a href="#">c274</a> | Demo API                      | Security Analyst | <a href="#">API Endpoints Without Authentication</a>                                 | Medium   | 4.5       | Unsolved |
| 10  | <a href="#">b76d</a> | Demo API                      | Security Analyst | <a href="#">Open Redirection Via Referer &amp; X-Forwarded-Host Header Poisoning</a> | Medium   | 4.5       | Unsolved |
| 11  | <a href="#">c1ff</a> | Demo API                      | Security Analyst | <a href="#">Slowloris DOS Vulnerable</a>                                             | Low      | 3.4       | Unsolved |
| 12  | <a href="#">bb7d</a> | API Scanner Demo API Target 2 | Astronaut bot    | <a href="#">DNSSEC Not Found in DNS Records</a>                                      | Low      | 2.8       | Unsolved |
| 13  | <a href="#">0c5c</a> | API Scanner Demo API Target 2 | Astronaut bot    | <a href="#">[Recommendation] Implement Idempotency Header</a>                        | Info     | n/a       | Unsolved |
| 14  | <a href="#">a948</a> | API Scanner Demo API Target 2 | Astronaut bot    | <a href="#">Strict-Transport-Security (HSTS) Header Not Set (script)</a>             | Info     | n/a       | Unsolved |

## Assessment Methodology

An **in-depth vulnerability assessment and penetration testing** was conducted by Astra's experienced security professionals, along with an automated full vulnerability scan consisting of **10,000+ tests**. Please refer to the 'Scan Mode' column in the table below to understand the extent of testing performed.

The assessment follows **industry standards** such as OWASP Web Security Testing Guide (WSTG), OWASP Top 10, OWASP Application Security Verification Standard (ASVS), NIST 800-115 etc.

Using the **same techniques as sophisticated real-world attackers**, the applications have been tested thoroughly for business logic, chained & application functionality specific vulnerabilities. This hands-on approach with manual checks goes beyond traditional scanning tools, allowing to uncover critical issues that may not be detected by automated scanners.

All false positives have been removed from the manual pentest report, and once the vulnerabilities have been resolved the fixes are verified on a case to case basis.

## Types of Tests Performed

Gray-box & black-box testing was performed to identify vulnerabilities, public exposure, misconfiguration errors, best practices and any other potential security loopholes which might impact security of the targets