NetSPI™

Sample Security Audit Report

API Penetration Test

Engagement: NetSPA

ACME Inc. | June 11, 2024

NetSPI™

Contents

Chapter 1 | Engagement Summary

NetSPI performed an analysis of ACME Inc.'s NetSPA APIs to identify vulnerabilities, determine the level of risk they present to ACME Inc., and provide actionable recommendations to reduce this risk. NetSPI compiled this report to provide ACME Inc. with detailed information on each vulnerability discovered within the NetSPA APIs, including potential business impacts and specific remediation instructions.

1.1 Engagement Objectives

NetSPI's primary goal within this engagement was to provide ACME Inc. with an understanding of the current level of security in the NetSPA APIs and its infrastructure components.

NetSPI completed the following objectives to accomplish this goal:

- Identifying API-based threats to and vulnerabilities in the APIs
- Comparing ACME Inc.'s current security measures with industry best practices
- Providing recommendations that ACME Inc. can implement to mitigate threats and vulnerabilities and meet industry best practices

1.2 Scope & Timeframe

Testing and verification was performed between June 3rd, 2024 and June 7th, 2024. The scope of this engagement was limited to the NetSPA APIs and the specific infrastructure on which the APIs reside.

The following systems and/or endpoints were in scope for testing:

IP ADDRESS	ASSET / URL
35.92.206.84	example.api.netspa.vuln.netspi-u.com
35.92.63.156	app.netspa.vuln.netspi-u.com
35.92.63.129	api.netspa.vuln.netspi-u.com

Authenticated API testing was performed using the following credentials:

USERNAME	ROLE
test@netspi.com	Test Service Account
test3@netspi.com	Test Standard Account

NetSPI conducted the tests using a non-production version of NetSPA APIs. All other applications and servers were out of scope. All testing and verification was conducted from outside of ACME Inc.'s offices.

1.3 Summary of Findings

NetSPI's assessment of the NetSPA APIs revealed the following vulnerabilities:

- 1 critical severity vulnerability
- 1 high severity vulnerability
- 1 medium severity vulnerability
- 1 low severity vulnerability

VULNERABILITY NAME	SEVERITY	OWASP API
NoSQL Injection	Critical	API2-Broken Authentication

VULNERABILITY NAME	SEVERITY	OWASP API
Authorization Bypass - Missing Function Level Access Controls	High	API5-Broken Function Level Authorization
Information Disclosure - Password in Server Response	Medium	API3-Broken Object Property Level Authorization
User Enumeration - Error Messages	Low	API8-Security Misconfiguration

TABLE 1: FINDINGS SUMMARY

The following table lists the OWASP API Top 10 vulnerabilities and indicates which issues were identified in the NetSPA APIs.

CATEGORY	FOUND
API1-Broken Object Level Authorization	No
API2-Broken Authentication	Yes
API3-Broken Object Property Level Authorization	Yes
API4-Unrestricted Resource Consumption	No
API5-Broken Functional Level Authorization	Yes
API6-Unrestricted Access to Sensitive Business Flaws	Yes
API7-Server-Side Request Forgery (SSRF)	No
API8-Security Misconfiguration	No
API9-Improper Inventory Management	No
API10-Unsafe Consumption of APIs	No

TABLE 2: OWASP SUMMARY

NetSPI™

Want to see the full Sample security audit report?

Every engagement with NetSPI will provide you with a PDF report of findings, as well as access to The NetSPI Platform, delivering streamlined vulnerability management, team communication, and real-time updates. In this sample report, gain insights into vulnerabilities and misconfigurations that we might find during a API Penetration Testing engagement and see how our team can help you secure your applications.

- Project overview: objectives, scope & timeframe, and findings summary
- Technical detail: critical, high, medium, and low severity findings
- Testing methodology
- Risk management approach

Show Me The Sample Security Audit Report!