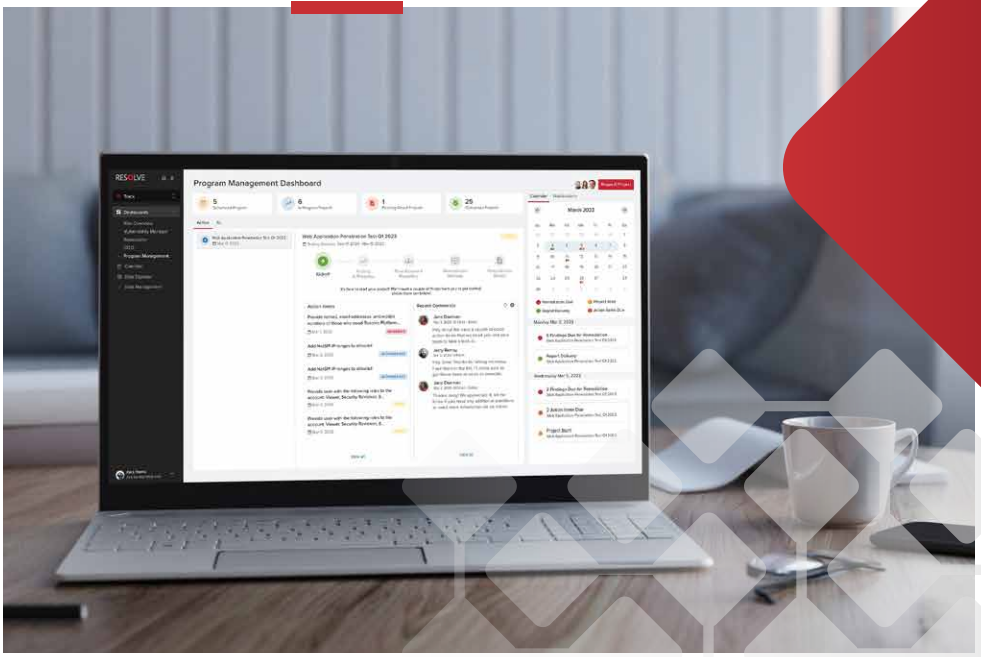
NETSPI®

NetSPI-U | July 11, 2023

Sample Security Audit Report

WEB APPLICATION PENETRATION TESTING

Application Name: NetSPA



NETSPI

Contents

Chapter 1 | Project Summary

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

1.1 Project Objectives

NetSPI's primary goal within this project was to provide NetSPI-U with an understanding of the current level of security in the NetSPA application.

NetSPI completed the following objectives to accomplish this goal:

- Identifying application-based threats to and vulnerabilities in the application
- Comparing NetSPI-U's current security measures with industry best practices
- Providing recommendations that NetSPI-U can implement to mitigate threats and vulnerabilities and meet industry best practices

1.2 Scope & Timeframe

Testing and verification was performed between July 1st, 2023 and July 5th, 2023. The scope of this project was limited to the NetSPA application.

The following systems were in scope for testing:

IP ADDRESS	ASSET / URL
35.92.206.84	Application API Endpoint - https://example.api.netspa.vuln.netspi-u.com
35.92.63.156	Application Frontend - https://example.app.netspa.vuln.netspi-u.com

Authenticated application testing was performed using the following credentials:

USERNAME	ROLE
test@netspi.com	Standard user

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

1.3 Summary of Findings

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

- 1 critical severity vulnerability
- 3 high severity vulnerabilities
- 2 medium severity vulnerabilities
- 2 low severity vulnerabilities

VULNERABILITY NAME	SEVERITY	OWASP
NoSQL Injection	Critical	A3-Injection
Authorization Bypass - Missing Function Level Access Controls	High	A1-Broken Access Control
File Upload - Cross-Site Scripting	High	A3-Injection
Server-Side Request Forgery	High	A10-Server-Side Request Forgery (SSRF)
Information Disclosure - Password in Server Response	Medium	A4-Insecure Design
Insufficient Input Validation - Client-Side Controls	Medium	A3-Injection
Information Disclosure - Verbose Error Message	Low	A5-Security Misconfiguration
User Enumeration - Error Messages	Low	A4-Insecure Design

TABLE 1: FINDINGS SUMMARY

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

CATEGORY	FOUND
A1-Broken Access Control	Yes
A2-Cryptographic Failures	Yes
A3-Injection	Yes
A4-Insecure Design	Yes
A5-Security Misconfiguration	Yes
A6-Vulnerable and Outdated Components	No
A7-Identification and Authentication Failures	Yes
A8-Software and Data Integrity Failures	No
A9-Security Logging and Monitoring Failures	No
A10-Server-Side Request Forgery (SSRF)	Yes

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 NetSPI's Penetration Testing as a Service (PTaaS) 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 Web Application Penetration Testing engagement and see how our team can help you secure your web 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!