NetSPI™

Sample Security Audit Report

Mobile Application Penetration Test

Project: ScootShop

ACME Inc. | April 18, 2024

NetSPI™

Contents

Chapter 1 | Engagement Summary

NetSPI performed an analysis of ACME Inc.'s Scoot Shop application 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 Scoot Shop application, 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 Scoot Shop application.

NetSPI completed the following objectives to accomplish this goal:

- Identifying application-based threats to and vulnerabilities in the application
- 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 April 08, 2024 and April 12, 2024. The scope of this project was limited to the Scoot Shop application and the specific infrastructure on which the application resides.

The following table(s) provides details of the application binaries that were in scope for testing:

Description	Value
Application Name	ScootShop
Operating System	**Android**
Application Package Name	com.ns.dev.scoot.a1
Version Name	1
Version Code	1.0.0
SHA256	d8769bcde054de8342c5487a97670daa5fd39bda60601da1080f3fda0fa68ee6

TABLE 1: ANDROID APPLICATION DETAILS

Description	Value
Application Name	ScootShop
Operating System	**iOS**
Application Package Name	com.ns.dev.scoot.a1
Version Name	1
Version Code	1.0.0
SHA256	896950e98b22bdcabdda244a6f06ecac44a38658c1ba9451ad2a2e0068840a68

TABLE 2: iOS APPLICATION DETAILS

The following systems were in scope for testing:

IP ADDRESS	ASSET / URL
34.123.201.87	https://api.ns.scootshop.com

In addition to unauthenticated testing, authenticated application testing was performed using the following credentials:

USERNAME	ROLE
admin@ns.scootshop.com	Administrator
mapen@netspi.com	Standard User
mapentest@netspi.com	Standard User
securitytesting@netspi.com	Standard User
Securitytesting+unregistered@netspi.com	Standard User

NetSPI conducted the tests using a non-production version of Scoot Shop. 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 Scoot Shop application revealed the following vulnerabilities:

- 5 high severity vulnerabilities
- 2 medium severity vulnerabilities
- 1 low severity vulnerability

VULNERABILITY NAME	SEVERITY	OWASP MOBILE	OWASP WEB
Authorization Bypass - Weak Password Reset	High	M6-Insecure Authorization	A1-Broken Access Control
Hard-coded Credentials - Mobile Application Binary	High	M2-Insecure Data Storage	A2-Cryptographic Failures
SQL Injection	High	M8-Code Tampering	A3-Injection
Weak Configuration - SSL/TLS - Lack of Certificate Validation	High	M3-Insecure Communication	A2-Cryptographic Failures
Weak Multi-Factor Authentication - Partial Authentication Bypass	High	M4-Insecure Authentication	A7-Identification and Authentication Failures
Account Policy - Weak Password Policy	Medium	M4-Insecure Authentication	A7-Identification and Authentication Failures
Sensitive Information Disclosure - Mobile Application Storage	Medium	M2-Insecure Data Storage	A5-Security Misconfiguration
Authentication Bypass - Biometric	Low	M4-Insecure Authentication	A7-Identification and Authentication Failures

TABLE 1: FINDINGS 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 Mobile Application Penetration Testing engagement and see how our team can help you secure your mobile 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!