Nitpicksy

Security Assessment Findings Report

Business Confidential

Date: February 07th, 2021
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Nitpicksy. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of Nitpicksy.

Nitpicksy may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Nitpicksy recommends conducting vulnerability assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

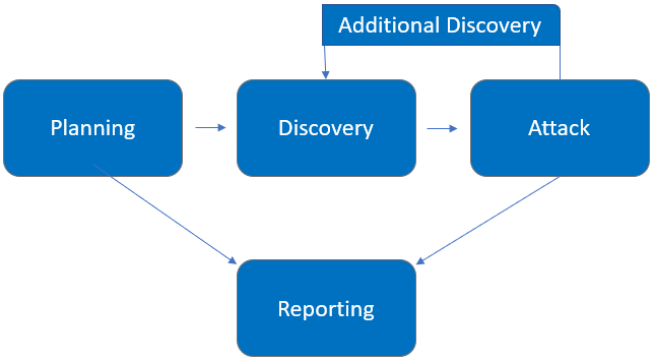
Name	Title	Contact Information
Project - Nitpicksy		
Jelena Popov	Developer	Email: popov.jelena@uns.ac.rs
Nikola Brodić	Developer	Email: nbrodic@uns.ac.rs
Dušan Nikolić	Developer	Email: nikolic.dusan@uns.ac.rs

Assessment Overview

From February 01st, 2021 to February 07th, 2021, Nitpicksy was engaged to evaluate the security posture of its infrastructure that included an internal penetration test. All testing performed is based on *OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker attempting to detect inner vulnerabilities of the internal network with internal resources and inside knowledge. A Nitpicksy developer attempts to gather sensitive information through open-source code, including authentication information, JWT tokens and more. The developer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
Internal Penetration Test	127.0.0.1, 192.168.0.0/24

- Full scope information provided in "*-report.html"

Scope Exclusions

Nitpicksy did not perform any Denial of Service attacks during testing.

Client Allowances

User authentication credentials and JWT tokens were provided to assist the testing.

Executive Summary

Nitpicksy evaluated it's external security posture through an internal network penetration test from February 01th, 2021 to February 07th, 2021. By leveraging a series of attacks, Nitpicksy did not find any critical level vulnerabilities that would allow application disruption. Therefore, at the given moment no immediate remediation is required.

Attack Summary

The following table describes what Nitpicksy has attempted to perform and evaluate:

	Action	Result and recommendations
1	Port scanning and reconnaissance.	*Nmap* from *Metasploit Framework* discovered the following ports: 8080, 8090, 8761. Payment Gateway was left undiscovered.
2	Passive inbound and outbound HTTPS traffic scans for faulty headers.	*X-Powered-By* header exposed and *Unix* timestamps. It is recommended to hide any technology stack from the end-user, as it can be used as means in further deliberate attacks.
3	Authenticated – '*happy path*' active scan. Attempted find vulnerabilities in the system as a privileged merchant.	Application permitted authenticated with valid credentials. However, *Best practices* recommend to implement Multi-Factor Authentication (MFA) on all external services. Application did not permit unlimited login attempts. Application recommends an improved password policy of: 1) *Best practice length* characters or longer 2) Use different passwords for each account accessed.
4	Attempted to authenticate via SQL Injection techniques, provided by *sqlmap* and *Zed Attack Proxy*. Form based and direct approach.	OWASP *Zed Attack Proxy* evaluates false positives. *sqlmap* breach attempt was evaluated as unsuccessful (HTTP 400 on each technique).

Security Strengths

Restricted Login Attempts

During the assessment, *Zed Attack Proxy* and *sqlmap* performed multiple brute-force attacks against login forms found on the localhost network. Limited attempts exist for all logins, which block the incoming IP address if the attempt threshold was exceeded.

Strong Password Policy

Zed Attack Proxy unsuccessfully performed password guessing attacks against login forms. Standard dictionary attacks are rendered difficult as the password length, special characters and numbers restrictions are in place.

Security Weaknesses

SIEM alerts of vulnerability scans

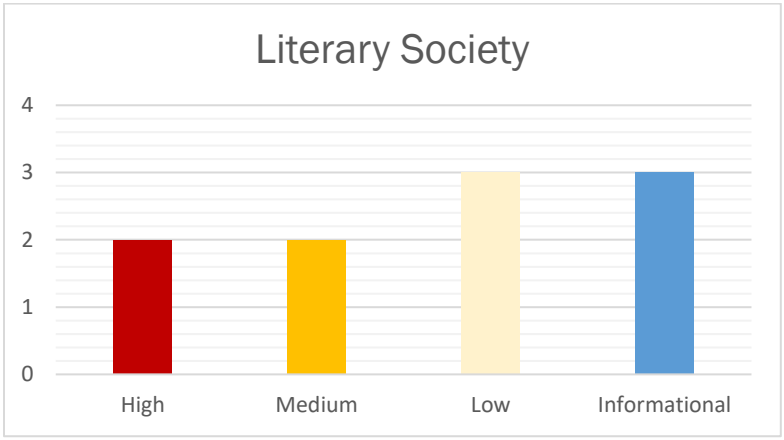
No SIEM tool was implemented to monitor the system, thus the applications failed to alert Nitpicksy developers of detected vulnerability scanning against their systems. The application was uncapable of blacklisting the attacker from further scanning actions.

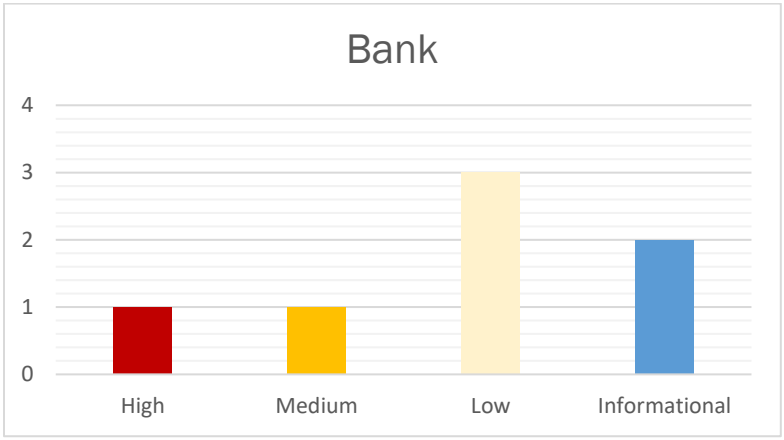
Missing Multi-Factor Authentication

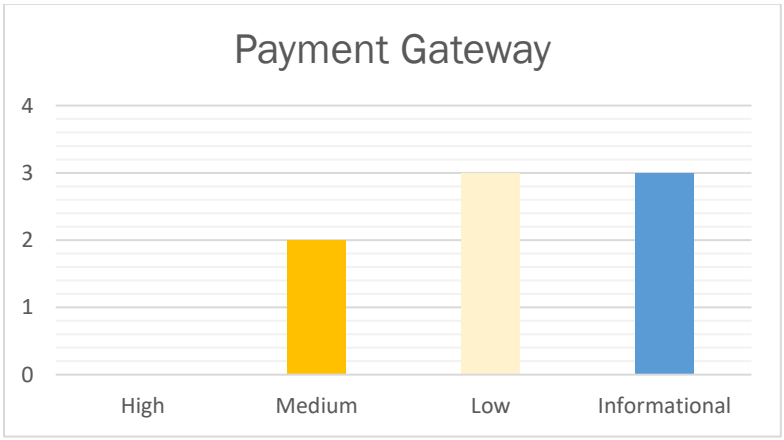
Penetration tester leveraged multiple attacks using valid credentials harvested through open-source intelligence. The use of multi-factor authentication would have prevented full access and required the penetration tester to utilize additional attack methods to gain internal network access.

Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:







Appendix – Scanning and Reconnaissance Findings

Nmap – Port Scanning Results (Informational)

Description:	*Nmap* provides scanning and reconnaissance of the given microservice architecture. Results of the scan are given below.
Impact:	Informational
System:	127.0.0.1, ports: 8090,8080,8761,8672,8100,42342.

Scanning results

Nitpicksy *pentest* gathered ports and additional underlying OS information. Given the *Metasploit Framework*, *nmap* was configured to scan and discover the top 1000 ports in the given system (*DNS*).

```
msf6 > nmap -v -sV localhost
[*] exec: nmap -v -sV localhost
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-01 14:34 CET
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 14:34
Scanning localhost (127.0.0.1) [2 ports]
Completed Ping Scan at 14:34, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 14:34
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 8080/tcp on 127.0.0.1
Discovered open port 8090/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Completed Connect Scan at 14:34, 0.03s elapsed (1000 total ports)
Initiating Service scan at 14:34
Scanning 4 services on localhost (127.0.0.1)
Completed Service scan at 14:34, 26.23s elapsed (4 services on 1 host)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 14:34
Completed NSE at 14:34, 0.34s elapsed
Initiating NSE at 14:34
Completed NSE at 14:34, 0.15s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s latency).
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
631/tcp open ipp CUPS 2.3
3306/tcp open mysql MySQL 8.0.22-0ubuntu0.20.10.2
8080/tcp open ssl/http-proxy
8090/tcp open ssl/opsmessaging?
Nmap done: 1 IP address (1 host up) scanned in 27.34 seconds
```

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set ports 10000-65000
ports => 10000-65000
msf6 auxiliary(scanner/portscan/tcp) > set threads 50
threads => 50
msf6 auxiliary(scanner/portscan/tcp) > run
[+] 127.0.0.1: - 127.0.0.1:30666 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:33060 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:35673 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:36027 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:36381 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:36925 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:37685 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:37705 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:37985 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:39271 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:39719 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:41141 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:41393 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:45112 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:63342 - TCP OPEN
[*] 127.0.0.1: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > set ports 1-10000
ports => 1-10000
msf6 auxiliary(scanner/portscan/tcp) > run
[+] 127.0.0.1: - 127.0.0.1:631 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:3306 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:5433 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:5443 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:6942 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:8080 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:8090 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:8762 - TCP OPEN
[+] 127.0.0.1: - 127.0.0.1:8761 - TCP OPEN
[*] 127.0.0.1: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Additional Reports and Scans (Informational)

Nitpicksy provides all report information gathered during testing. This includes vulnerability scans in html format and dependency report. For more information, please see the following documents:

- literary-society-report.html
- bank-report.html
- gateway-report.html
- .*dependency-check-report.html