1 Executive Security Assessment Report

1.1 Introduction

This security assessment was conducted on the domain **webapps-accpt.portofantwerp.com**. The analysis was initiated on **December 5th** at **06:45** and concluded in **11 minutes and 39 seconds**. The assessment utilized a basic scanning methodology, focusing on identifying High and Medium-risk vulnerabilities within the web application infrastructure, following OWASP and OSCP methodologies.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **1 Medium-risk**, **2 Low-risk**, and **15 informational**. The most significant finding is the Medium-risk issue related to open port **80**, which lacks encryption and could expose sensitive data if not redirected to HTTPS. This poses a potential risk for data interception and should be prioritized for remediation. Additionally, the SSL/TLS analysis revealed that all endpoints support modern protocols, with **1 endpoint** using TLS 1.3, ensuring robust encryption standards. The SSL certificate for the domain is set to expire in **145 days**, requiring monitoring to avoid service disruption. Overall, the assessment indicates a well-maintained infrastructure with minor areas for improvement, particularly in securing HTTP traffic and monitoring SSL certificate expiration.

1.3 Issues Table

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assessment	Low
SSL Certificate Expiration Analysis	Low

1.4 Detailed Findings

1.4.1 Nmap Port Scan Results Analysis

Description:
The scan identified **2 open ports** on the IP address **94.107.237.234**. Port **80/tcp** is associated with HTTP service, which lacks encryption, posing a risk of data interception if not properly redirected to HTTPS or if HSTS is not enabled.

Affected Assets:
- IP: **94.107.237.234** - Ports: **80/tcp (http)**, **443/tcp (ssl/https?)**

Recommendations:
Implement HTTPS redirection for all HTTP traffic on port **80** and consider enabling HSTS to ensure secure communication. Regularly review open ports and services to minimize exposure to potential threats.

1.4.2 SSL/TLS Protocols Security Assessment

Description:
The analysis confirmed that all endpoints support modern encryption protocols, with **1 endpoint** utilizing TLS 1.3 and another using TLS 1.2. No deprecated protocols such as SSLv3, TLS 1.0, or TLS 1.1 were detected, indicating adherence to current security standards.

Affected Assets:
- **1 endpoint** with TLS 1.3 support - **1 endpoint** using TLS 1.2

Recommendations:
Continue monitoring protocol configurations to ensure compliance with evolving security standards. Consider phasing out TLS 1.2 in favor of TLS 1.3 where possible to enhance security and performance.

1.4.3 SSL Certificate Expiration Analysis

Description:
The SSL certificate for the domain is set to expire in **145 days**, placing it in the “Monitor” category. No certificates are currently in the “Critical” or “Warning” categories.
Affected Assets:
- HTTPS-enabled subdomains of **webapps-accpt.portofantwerp.com**
Recommendations:
Establish a process for regular monitoring of SSL certificate expiration dates to prevent service disruptions. Plan for timely renewal of certificates well before expiration.

1.5 General Recommendations

To enhance the security posture of the domain, it is recommended to prioritize the implementation of HTTPS redirection for all HTTP traffic and maintain vigilance over SSL/TLS configurations and certificate expirations. Regular security assessments should be conducted to identify and mitigate emerging threats promptly.