1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **stgproptrack.nonprodtops.cbre.com.au**. The analysis was initiated on **April 17th at 18:00** and completed in **15 minutes and 43 seconds**. The assessment was identified with tracking ID **1b12172568b4** and categorized as a **Basic** type analysis. The scope of the work included evaluating the security posture of the web application and infrastructure, focusing on identifying High and Medium-risk vulnerabilities.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 risks**, categorized as **0 High-risk**, **4 Medium-risk**, **4 Low-risk**, and **10 informational issues**. Key Medium-risk findings include unusual port assignments and high service density on a single host, which increase the attack surface and potential for exploitation. Notably, **100%** of the analyzed host has a high service density, with **9 open ports**, indicating a need for immediate security hardening. Additionally, shared hosting environments and services vulnerable to brute force attacks were detected, necessitating enhanced monitoring and access controls. While SSL/TLS protocols are generally secure, with **5 endpoints supporting TLS 1.3**, ongoing vigilance is required to maintain robust security postures.

1.3 Key Security Issues

Title	Risk
Shared Hosting Environment Analysis	Medium
Unusual Port Assignments Detected	Medium
Nmap Port Scan Results Analysis	Medium
Service Density Analysis	Medium
SSL/TLS Protocols Security Assessment	Low
Services Vulnerable to Brute Force Attacks	Low
SSL Certificate Expiration Analysis	Low
Login Form Detection Analysis	Low

1.4 Shared Hosting Environment Analysis

Description:

The analysis identified a shared hosting environment on the host **stgproptrack.nonprodtops.cbre.com.au**, which is categorized under Medium interest due to **71 shared domains**. Shared hosting can lead to increased risk exposure as vulnerabilities in one domain may affect others sharing the same server.

Affected Assets:

- Hostname: **stgproptrack.nonprodtops.cbre.com.au**

Recommendations:

Implement isolation measures for hosted applications to minimize cross-domain vulnerabilities. Regularly monitor and update all hosted applications to mitigate potential risks from shared environments.

1.5 Unusual Port Assignments Detected

Description:

Unusual port assignments were detected on the host **45.223.100.7**, with services running on

non-standard ports such as **21, 25, 80, 110, and 3306**. This may indicate attempts to evade detection or misconfigured applications, increasing the risk of unauthorized access.

Affected Assets:

- Host: **stgproptrack.nonprodtops.cbre.com.au (45.223.100.7)**

Recommendations:

Review and standardize port assignments to align with best practices. Implement network segmentation and access controls to restrict unauthorized access to critical services.

1.6 Nmap Port Scan Results Analysis

Description:

The Nmap scan revealed **9 open ports** on IP address **45.223.100.7**, associated with potentially insecure services such as FTP, SMTP, HTTP, POP3, and MySQL. These services may allow clear text authentication or expose sensitive interfaces.

Affected Assets:

- IP Address: **45.223.100.7**

Recommendations:

Conduct a thorough review of open ports and associated services. Disable unnecessary services and enforce encryption protocols where applicable to protect data in transit.

1.7 Service Density Analysis

Description:

A high service density was observed on the host **45.223.100.7**, with **9 services** running concurrently. This increases the attack surface and poses a Medium risk level due to potential vulnerabilities in multiple services.

Affected Assets:

- Host: **45.223.100.7**

Recommendations:

Optimize service configurations to reduce density where possible. Implement robust monitoring and logging to detect and respond to potential threats promptly.

1.8 General Recommendations

To enhance the overall security posture, it is recommended to implement comprehensive monitoring solutions, enforce strict access controls, and regularly update all systems and applications. Conduct periodic security assessments to identify new vulnerabilities and ensure compliance with industry standards and best practices.