1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **mypc-uag-au.gslb.cbre.eu**. The analysis commenced on **April 18th** at **08:45** and concluded in **00h:13m:00s**. The assessment was categorized as a **Basic** type scan. The evaluation focused on identifying potential vulnerabilities within the web application and infrastructure, utilizing methodologies aligned with OWASP and OSCP standards.

1.2 Summary of Findings

The security assessment identified **2** Medium-risk, **2** Low-risk, and **14** informational issues. Notably, Medium-risk findings include unusual port assignments and potentially insecure ports detected via Nmap, which could indicate misconfigurations or attempts to evade detection. These vulnerabilities may expose the organization to unauthorized access or data breaches. The SSL/TLS protocols are generally secure, with support for TLS 1.3 and TLS 1.2, but vigilance is advised to maintain compliance with evolving standards. Additionally, the analysis revealed no High-risk locations or shared hosting environments, indicating a robust infrastructure setup. Immediate attention should focus on addressing Medium-risk issues to enhance security posture.

1.3 Issues Table

Title	Risk
Unusual Port Assignments Detected	Medium
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security	Low
Login Form Detection Analysis	Low

1.4 Detailed Findings

1.4.1 Unusual Port Assignments Detected

Description:
The assessment identified **1** unusual port assignment on the host **mypc-uag-au.gslb.cbre.eu (103.55.52.34)**. Port **80** was found running the **rtsp** service instead of the expected HTTP service. This anomaly may suggest misconfigurations or attempts to evade detection by using non-standard ports for services.

Affected Assets:
- Host: **mypc-uag-au.gslb.cbre.eu (103.55.52.34)** - Port: **80**

Recommendations:
It is recommended to review and standardize port assignments to align with expected services. Ensure that all services are running on their designated ports to prevent unauthorized access and reduce the risk of evasion techniques being employed by malicious actors.

1.4.2 Nmap Port Scan Results Analysis

Description:
The Nmap port scan revealed **3** open ports on IP **103.55.52.34**, including port **80/tcp** running an unencrypted HTTP service. This poses a potential security risk as data transmitted over HTTP is susceptible to interception.

Affected Assets:
- IP Address: **103.55.52.34** - Open Ports: **80/tcp**, **443/tcp**, **8443/tcp**

Recommendations:
Ensure that HTTP traffic is redirected to HTTPS and consider enabling HTTP Strict Transport Security (HSTS) to enforce secure connections. Regularly review open ports and services to ensure they are necessary and appropriately secured.

1.5 General Recommendations

To enhance the overall security posture, it is crucial to address Medium-risk issues promptly. Regularly update and patch systems, conduct periodic security assessments, and implement best practices for network configuration and encryption standards. Continuous monitoring and incident response planning will further strengthen defenses against potential threats.

This report provides a comprehensive overview of the identified vulnerabilities and offers actionable recommendations to mitigate risks effectively.