1 Executive Security Assessment Report

1.1 Introduction

This report provides an executive-level summary of the security assessment conducted on the domain **ldrpsweb.cbre.com**. The analysis was performed using a certified and qualified web application and infrastructure penetration testing tool, adhering to OWASP and OSCP methodologies. The assessment took place on **April 4th**, commencing at **14:46** and concluding in **00h:07m:07s**. The tracking ID for this assessment is **04b72554c7be**, and the scope included a basic analysis of the domain's security posture.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **2 Medium-risk**, **2 Low-risk**, and **14 informational**. Key medium-risk findings include the detection of shared hosting environments and potentially insecure open ports, such as HTTP on port **80**, which lacks encryption and requires verification for HTTPS redirection or HSTS implementation. These vulnerabilities could expose sensitive data and impact business operations if exploited. Additionally, the SSL/TLS analysis confirmed the use of modern protocols, with **100%** of endpoints supporting TLS **1.2** or higher, ensuring robust encryption standards. Actionable insights include reviewing shared hosting configurations and securing open ports to mitigate potential risks.

1.3 Issues Table

Title	Risk
Shared Hosting Environment Analysis	Medium
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assessment	Low
Login Form Detection Analysis	Low

1.4 Detailed Findings

1.4.1 Shared Hosting Environment Analysis

Description:
The analysis identified that the domain **ldrpsweb.cbre.com** is hosted in a shared environment with **34 shared domains**, categorized as medium interest. Shared hosting can lead to potential security risks due to resource sharing among multiple domains.

Affected Assets:
- Hostname: **ldrpsweb.cbre.com**

Recommendations:
It is recommended to evaluate the shared hosting configuration to ensure isolation between domains. Consider migrating to a dedicated hosting environment if feasible, to enhance security and control over resources.

1.4.2 Nmap Port Scan Results Analysis

Description:
The scan detected **2 open ports** on IP **208.68.246.52**, including port **80/tcp** running an HTTP proxy service without encryption. This poses a potential security risk if not properly configured with HTTPS or HSTS.

Affected Assets:
- IP: **208.68.246.52** - Ports: **80/tcp**, **443/tcp**

Recommendations:
Ensure that port **80** redirects to HTTPS or has HSTS enabled to secure data in transit. Regularly review firewall rules and close unnecessary ports to reduce exposure.

1.4.3 SSL/TLS Protocols Security Assessment

Description:
The assessment confirmed that all endpoints support modern encryption protocols, with one endpoint using TLS **1.3** and another using TLS **1.2**. No deprecated or vulnerable protocols were detected.

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

Recommendations:
Continue monitoring for updates in cryptographic standards and ensure all endpoints are configured to support the latest protocols for optimal security.

1.4.4 Login Form Detection Analysis

Description:
A single login form was detected across the application, indicating potential authentication interfaces that require security validation.

Affected Assets:
- URLs: - `http://ldrpsweb.cbre.com:80` - `https://ldrpsweb.cbre.com:443`

Recommendations:
Implement secure coding practices for login forms, including input validation and protection against common web vulnerabilities such as SQL injection and cross-site scripting (XSS). Ensure that all login pages are served over HTTPS.

1.5 General Recommendation

Overall, it is advised to prioritize addressing medium-risk issues by securing open ports and reviewing shared hosting configurations. Regularly update security policies and practices to align with industry standards, ensuring robust protection against evolving threats.