1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain `display.cbresi.com.au` using a Basic scan type. The analysis commenced on June 3rd at 14:45 and concluded in a duration of **00h:10m:54s**. The evaluation focused on identifying High and Medium-risk vulnerabilities within the web application and infrastructure, adhering to OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **1 High-risk**, **2 Medium-risk**, **1 Low-risk**, and **14 informational**. The most critical finding is the High-risk shared hosting environment, with one host sharing its IP with over **100 domains**, potentially increasing exposure to cross-domain vulnerabilities. Medium-risk issues include insecure open ports, notably HTTP on port **80**, which lacks encryption, and an SSL certificate nearing expiration in **85 days**, requiring prompt renewal to maintain secure communications. The Low-risk finding involves the use of TLS **1.2**, which is acceptable but lacks the enhanced security of TLS **1.3**. Immediate actions should focus on mitigating the High-risk shared hosting and addressing Medium-risk vulnerabilities to enhance the organization's security posture.

1.3 Key Security Issues

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

1.3.1 Shared Hosting Environment Analysis

Description:

The domain `display.cbresi.com.au` is hosted in a shared environment where its IP address is shared with over **598 domains**. This configuration poses a High risk due to potential cross-domain vulnerabilities that could be exploited by attackers.

Affected Assets:

- Hostname: `display.cbresi.com.au`

Recommendations:

It is recommended to migrate to a dedicated hosting environment to minimize exposure to cross-domain vulnerabilities. Additionally, implement strict access controls and monitoring to detect any unauthorized activities.

1.3.2 Nmap Port Scan Results Analysis

Description:

The scan identified open ports, including HTTP on port **80**, which lacks encryption. This poses a Medium risk as unencrypted HTTP traffic can be intercepted, leading to potential data breaches.

Affected Assets:

- IP: `221.121.159.204` - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:
Implement HTTPS with a valid SSL certificate for all web traffic. Ensure HTTP traffic is redirected to HTTPS and consider enabling HTTP Strict Transport Security (HSTS) to enforce secure connections.

1.3.3 SSL Certificate Expiration Analysis

Description:
The SSL/TLS certificate for `display.cbresi.com.au` is set to expire in **85 days**, categorized under the "Warning" risk level. Failure to renew the certificate could lead to service disruptions and loss of secure communications.

Affected Assets:
- HTTPS-enabled subdomain: `display.cbresi.com.au`

Recommendations:
Initiate the renewal process for the SSL/TLS certificate well before the expiration date to ensure continuous secure communications. Implement automated reminders for certificate renewals to prevent future lapses.

1.4 General Recommendations

To enhance the overall security posture, it is crucial to address the identified High and Medium-risk issues promptly. Transitioning to a dedicated hosting environment, securing open ports with encryption, and ensuring timely renewal of SSL certificates are essential steps. Regular security assessments should be conducted to identify and mitigate emerging threats, ensuring robust protection against potential vulnerabilities.