1 Executive Summary

1.1 Security Assessment Overview

A comprehensive security assessment was conducted on the domain **itjobs.cbre.com**. The scan, identified with tracking ID **0c85f6eb4161**, was initiated on **March 13th at 09:42** and concluded in **00h:05m:32s**. This evaluation employed a Basic analysis type, adhering to OWASP and OSCP methodologies, to assess the web application and infrastructure security posture of the specified domain.

1.2 Key Findings Summary

The security assessment for **itjobs.cbre.com** revealed a Low-risk profile with no High or Medium-risk issues identified. One Low-risk issue was noted, alongside two informational findings. The perimeter security is robust, with all scanned ports filtered, indicating effective firewall and anti-scanning measures. A low-interest shared hosting environment was detected, with one host sharing its IP with **3-10** domains, suggesting minimal exposure. All servers are located in the USA, reducing the risk of domain takeover from high-risk locations.

1.3 Issues Table

Title	Risk
Shared Hosting Environment Analysis	Low

1.4 Detailed Findings

1.4.1 Shared Hosting Environment Analysis

Description

An analysis of the shared hosting environment revealed that **itjobs.cbre.com** shares its IP address with a small number of domains, classified as low interest due to only **4 shared domains**. This indicates minimal exposure and reduced risk of cross-site contamination or resource competition issues often associated with shared hosting environments.

Affected Assets

- Hostname: **itjobs.cbre.com**

Recommendations

While the current shared hosting environment poses a Low risk, it is recommended to continuously monitor the hosting environment for changes in shared domain counts. Consideration should be given to migrating to a dedicated hosting environment if the number of shared domains increases significantly, which could enhance security and performance.

1.5 General Recommendations

Given the findings of this assessment, it is advisable to maintain regular security audits and continuous monitoring to sustain the current security posture. As no High or Medium-risk issues were detected, focus should be on maintaining perimeter security and monitoring shared hosting environments to ensure they remain Low-risk. Additionally, implementing regular updates and patches will help mitigate potential vulnerabilities in the future.