1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **edocuments.abb.com.cn**. The assessment was initiated on **April 16th at 10:00** and completed in **00h:13m:07s**. The analysis was performed using a basic scan methodology, focusing on identifying High and Medium-risk vulnerabilities within the web application and infrastructure. The tracking ID for this assessment is **10967a1b718b**.

1.2 Summary of Key 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 geographic distribution of servers, with **100%** located in China, posing a potential domain takeover risk. Medium-risk issues include shared hosting environments and insecure HTTP ports, with one host having **12 shared domains** and HTTP services lacking encryption. The Low-risk SSL/TLS assessment shows compliance with modern standards, supporting TLS 1.2 and 1.3. Actionable insights include relocating High-risk servers, securing HTTP services with HTTPS, and monitoring shared hosting configurations to mitigate potential security threats.

1.3 Key Security Issues

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

1.3.1 Geographic Distribution

Description:

The server hosting the domain is located in a High-risk area, specifically Beijing, China. This poses significant risks such as potential domain takeover attempts, unauthorized infrastructure changes, security compromises, and DNS hijacking attempts. The analysis revealed that **100%** of the servers are situated in China, which is considered a High-risk location for hosting critical infrastructure.

Affected Assets:

- Hostname: **edocuments.abb.com.cn** - IP Address: **40.125.200.124**

Recommendations:

It is recommended to relocate the server to a more secure geographic location to mitigate risks associated with domain takeover and unauthorized access. Additionally, implementing robust monitoring and incident response strategies will help in early detection of any malicious activities.

1.3.2 Shared Hosting Environment Analysis

Description:

The domain is hosted in a shared environment with **12 other domains**, categorized as Medium interest due to the number of shared domains. Shared hosting can lead to security risks such as cross-site contamination and increased vulnerability to attacks targeting other domains on the same server.

Affected Assets:
- Hostname: **edocuments.abb.com.cn**

Recommendations:
Consider migrating to a dedicated hosting environment to reduce the risk of cross-site contamination and improve overall security posture. Regularly audit shared hosting configurations to ensure they adhere to best practices.

1.3.3 Nmap Port Scan Results Analysis

Description:
The analysis identified **2 open ports**, including port **80/tcp** which is associated with HTTP service lacking encryption. This exposes data transmitted over this port to potential interception and manipulation.

Affected Assets:
- IP Address: **40.125.200.124** - Open Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:
Ensure that HTTP traffic is redirected to HTTPS by enabling HTTP Strict Transport Security (HSTS). This will enforce encrypted communications and protect data integrity during transmission.

1.3.4 SSL/TLS Protocols Security Assessment

Description:
The SSL/TLS assessment indicates compliance with modern standards, supporting TLS 1.2 and 1.3 protocols. No deprecated protocols such as SSLv3, TLS 1.0, or TLS 1.1 were detected, indicating a strong security posture against known vulnerabilities.

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 timely implementation of any new security protocols to maintain a robust security posture.

1.4 General Recommendations

To enhance the security posture of the domain, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, timely patch management, and continuous monitoring of network activities. Additionally, adopting a defense-in-depth approach by layering security controls will provide better protection against potential threats.