1 Executive Security Assessment Report

1.1 Introduction

This security assessment was conducted on the domain **connectivity.evcharging.abb.com.cn**. The analysis was initiated on **08-07** at **10:45** and concluded in **00h:22m:27s**. The assessment was identified with the tracking ID **0616515f2fc9** and utilized a Basic scan type. The evaluation focused on identifying High and Medium-risk vulnerabilities within the web application and infrastructure, employing methodologies aligned with OWASP and OSCP standards.

1.2 Short Summary of Main Issues

The security assessment identified a total of **19 issues**, categorized as **2 High-risk**, **2 Medium-risk**, and **15 informational**. The most critical findings include a Denial of Service (DoS) vulnerability with a **96.16% timeout rate** across HTTP and HTTPS services, posing a significant risk of service disruption. Additionally, the geographic distribution analysis revealed a High-risk server location in China, indicating potential domain takeover threats. Medium-risk issues include the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts, increasing susceptibility to injection attacks, and the detection of insecure port **8080**, which may expose web service vulnerabilities. Immediate actions are recommended to address these High-risk vulnerabilities, including implementing DoS protection and enhancing WAF coverage to mitigate potential security breaches.

1.3 Key Security Issues

Title	Risk
Denial of Service (DoS)	High
Geographic Distribution	High
Absence of WAF	Medium
Nmap Port Scan Results	Medium

1.3.1 Denial of Service (DoS)

Description:
A High-severity Denial of Service (DoS) vulnerability was identified, with a **96.16% timeout rate** across HTTP and HTTPS services. This indicates a significant risk of service disruption, potentially affecting availability and performance.

Affected Assets:
- Endpoint: **connectivity.evcharging.abb.com.cn:80** - Ports: **80 (HTTP)**, **443 (HTTPS)**

Recommendations:
- Implement specific DoS protection mechanisms. - Review and optimize current security configurations. - Consider firewall rules to limit excessive connections. - Continuously monitor server performance during peak events.

1.3.2 Geographic Distribution

Description:
The server is located in a High-risk location, specifically Guangzhou, China, which poses potential domain takeover risks. This includes unauthorized infrastructure changes, security compromises, and DNS hijacking attempts.

Affected Assets:
- Hostname: **connectivity.evcharging.abb.com.cn** - IP Address: **124.71.196.113**

Recommendations:
- Evaluate the necessity of hosting critical services in High-risk locations. - Implement robust monitoring and alerting for unauthorized changes. - Consider relocating services to more secure geographic locations if feasible.

1.3.3 Absence of WAF

Description:
The absence of a Web Application Firewall (WAF) was detected on all analyzed hosts, resulting in a **100% vulnerability rate**. This significantly elevates the risk of successful cyber-attacks, particularly injection-based attacks.

Affected Assets:
- Host: **connectivity.evcharging.abb.com.cn**

Recommendations:
- Deploy a Web Application Firewall to protect against common web vulnerabilities. - Regularly update and configure WAF rules to adapt to emerging threats. - Conduct periodic security assessments to ensure WAF effectiveness.

1.3.4 Nmap Port Scan Results Analysis

Description:
An open port **8080/tcp** associated with http-proxy services was detected, which is commonly vulnerable to web service vulnerabilities and proxy-related issues.

Affected Assets:
- IP Address: **124.71.196.113** - Port: **8080/tcp** - Service: **http-proxy**

Recommendations:
- Restrict access to non-essential ports such as **8080**. - Regularly update software running on open ports to mitigate vulnerabilities. - Conduct thorough reviews of exposed services to ensure they are securely configured.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to implement comprehensive monitoring solutions, conduct regular security training for staff, and establish incident response protocols. Additionally, periodic security assessments should be conducted to identify and mitigate emerging threats proactively.