1 Executive-Level Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **api.cbreproperties.cz**. The analysis commenced on **July 31st at 17:45** and concluded in **00h:20m:07s**. The assessment was identified with tracking ID **0afcb203c0c4** and was performed using a Basic scan type. The primary objective was to evaluate the security posture of the web application and its infrastructure, focusing on identifying High and Medium-risk vulnerabilities.

1.2 Summary of Key Findings

The security assessment identified **1 High-risk**, **5 Medium-risk**, **5 Low-risk**, and **9 informational issues**. The most critical finding is the presence of unencrypted HTTP traffic across **3 URLs**, posing significant risks of data interception and man-in-the-middle attacks. Additionally, the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts increases vulnerability to injection-based attacks. Medium-risk issues include insecure open ports and high service density, with **100%** of hosts having more than **4 services**, expanding the attack surface. The SSL certificate for one domain is nearing expiration, with only **35 days** remaining, necessitating prompt renewal. Addressing these vulnerabilities is crucial to enhance security posture and protect sensitive data.

1.3 Issues Table

Title	Risk
Unencrypted HTTP Traffic Detected	High
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
Service Density Analysis	Medium
SSL Certificate Expiration Analysis	Medium
Subdomain Naming Security Assessment	Medium

1.4 Detailed Findings

1.4.1 Unencrypted HTTP Traffic Detected

Description

The analysis identified that **3 URLs** are utilizing unencrypted HTTP protocol, which exposes data to interception and eavesdropping. This lack of encryption allows for potential man-in-the-middle attacks, compromising sensitive information and failing to meet security compliance requirements.

Affected Assets:

- URLs: - `http://185.115.1.68/../` - `http://185.115.1.68/./` - `http://185.115.1.68:80`

Recommendations:

Implement HTTPS for all web traffic to ensure data encryption in transit. Utilize SSL/TLS certificates to secure communications and prevent unauthorized access or data tampering.

1.4.2 Absence of WAF

Description:

The domain lacks a Web Application Firewall (WAF), resulting in a **100% vulnerability rate** for

the analyzed host. This absence significantly elevates the risk of successful cyber-attacks, particularly injection-based attacks.

Affected Assets:

- Host: api.cbreproperties.cz

Recommendations:

Deploy a robust WAF to filter and monitor HTTP requests, providing an additional layer of defense against common web application attacks such as SQL injection and cross-site scripting (XSS).

1.4.3 Nmap Port Scan Results Analysis

Description:

The scan revealed **10 open ports**, some associated with potentially insecure services or protocols, such as FTP, SMTP, and HTTP, which may pose security risks due to clear text authentication and lack of encryption.

Affected Assets:

- IP Address: 185.115.1.68

Recommendations:

Review and close unnecessary open ports. Implement secure versions of services (e.g., FTPS, SMTPS) and ensure all communications are encrypted.

1.4.4 Service Density Analysis

Description:

The host exhibits high service density with **10 services**, increasing the attack surface and potential entry points for attackers.

Affected Assets:

- Host IP: 185.115.1.68

Recommendations:

Conduct a thorough review of all active services, disabling those that are non-essential or redundant to minimize exposure.

1.4.5 SSL Certificate Expiration Analysis

Description:

The SSL certificate for the domain api.cbreproperties.cz is set to expire in **35 days**, categorized under the "Warning" risk level.

Affected Assets:

- HTTPS-enabled subdomain: api.cbreproperties.cz

Recommendations:

Initiate the renewal process for the SSL certificate to avoid service disruption and maintain secure communications.

1.4.6 Subdomain Naming Security Assessment

Description:

A sensitive subdomain, api.cbreproperties.cz, was identified, which may provide access to critical systems and sensitive data.

Affected Assets:

- Subdomain: api.cbreproperties.cz

Recommendations:

Ensure that subdomains are adequately secured and monitored for unauthorized access or exposure of sensitive information.

1.5 General Recommendations

To enhance the overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, timely patch management, and continuous monitoring of network traffic. Additionally, adopting best practices such as enforcing strong authentication mechanisms, encrypting sensitive data, and educating staff on cybersecurity awareness can significantly mitigate potential risks.