1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **autodiscover.cbre.hr**. The analysis commenced on **May 22nd at 19:45** and concluded after a duration of **10 minutes**. The tracking ID for this assessment is **175a4349da16**, and it was performed using a Basic scan type. The scope of the work included evaluating the web application and infrastructure for potential vulnerabilities, focusing on High and Medium-risk issues.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **2 Medium-risk**, **1 Low-risk**, and **15 informational**. The most critical findings include Medium-risk vulnerabilities related to shared hosting environments and potentially insecure open ports (HTTP on port **80** and **8080**) that could expose the organization to web service vulnerabilities. The shared hosting analysis revealed one host with Medium interest due to **39 shared domains**, indicating a need for caution. Additionally, the Nmap port scan detected **four open ports**, emphasizing the importance of reviewing these for potential security risks. While no High-risk issues were found, addressing the Medium-risk vulnerabilities is crucial to mitigate potential threats. The assessment also noted that all services are running on standard ports, and no unusual port assignments were detected, which is a positive indicator of network configuration.

1.3 Table of Issues

Title	Risk
Shared Hosting Environment Analysis	Medium
Nmap Port Scan Results Analysis	Medium
Login Form Detection Analysis	Low

1.4 Detailed Findings

1.4.1 Shared Hosting Environment Analysis

Description

The analysis identified that the domain **autodiscover.cbre.hr** is hosted in a shared environment with **39 shared domains**, categorizing it as Medium interest. Shared hosting can pose security risks as vulnerabilities in one domain may affect others on the same server.

Affected Assets

- Hostname: **autodiscover.cbre.hr**

Recommendations

It is recommended to evaluate the necessity of shared hosting for critical services. Consider migrating to a dedicated hosting environment to minimize exposure to risks associated with shared hosting. Regularly monitor and audit shared domains for any unauthorized changes or vulnerabilities.

1.4.2 Nmap Port Scan Results Analysis

Description

The Nmap scan revealed **four open ports** on IP address **104.18.33.135**. Notably, ports **80/tcp** and **8080/tcp** are associated with HTTP services without encryption, which could lead to web service vulnerabilities if not properly secured.

Affected Assets

- IP Address: **104.18.33.135**
- Ports: **80/tcp, 443/tcp, 8080/tcp, 8443/tcp**

Recommendations

Ensure that HTTP services on ports **80** and **8080** are redirected to HTTPS or have HSTS enabled to enforce encryption. Regularly update and patch web services to protect against known vulnerabilities. Implement firewall rules to restrict access to necessary ports only.

1.5 General Recommendation

To enhance overall security posture, it is crucial to address Medium-risk vulnerabilities promptly. Regular security assessments should be conducted to identify new threats and ensure compliance with best practices. Implementing a robust patch management process and continuous monitoring will help mitigate potential risks effectively.