1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a comprehensive security assessment conducted on the domain **i18n.api.just-eat.io**. The assessment was initiated on **April 30th at 10:00** and completed in **12 minutes and 2 seconds**. The analysis was performed using a **Basic** scan methodology. The primary focus was to identify High and Medium-risk issues that could potentially impact the security posture of the domain.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **4 Medium-risk**, **2 Low-risk**, and **12 informational**. Key Medium-risk findings include the presence of potentially insecure open ports (HTTP on port **80** and **8080**) and a subdomain naming issue that could expose sensitive endpoints. Additionally, an SSL certificate is nearing expiration in **88 days**, requiring prompt renewal to maintain secure communications. The shared hosting environment and subdomain resolution indicate a need for enhanced infrastructure security. While no High-risk vulnerabilities were found, addressing these Medium-risk issues is crucial to mitigate potential threats and ensure a robust security posture.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL Certificate Expiration Analysis	Medium
Shared Hosting Environment Analysis	Medium
SSL/TLS Protocols Security Assessment	Low
Login Form Detection Analysis	Low

1.3.1 Nmap Port Scan Results Analysis

Description:
The scan identified **4 open ports** on the IP address **172.64.153.241**, with ports **80** and **8080** flagged as potentially insecure due to the lack of encryption. These ports are associated with HTTP services that do not provide secure communication, increasing the risk of data interception and unauthorized access.

Affected Assets:
- IP Address: **172.64.153.241** - Ports: **80/tcp, 443/tcp, 8080/tcp, 8443/tcp**

Recommendations:
- Implement HTTPS for all web services to ensure encrypted communication. - Configure HTTP to redirect to HTTPS or enable HTTP Strict Transport Security (HSTS). - Regularly update and patch web services to mitigate vulnerabilities.

1.3.2 Subdomain Naming Security Assessment

Description:
The subdomain **i18n.api.just-eat.io** was identified as potentially sensitive, as it may provide access to critical systems and sensitive data. Such subdomains can expose development or staging environments that might contain unpatched vulnerabilities or debug information.

Affected Assets:
- Subdomain: **i18n.api.just-eat.io**

Recommendations:
- Review and secure access controls for sensitive subdomains. - Ensure that development and staging environments are not publicly accessible. - Regularly audit subdomains for exposure of sensitive information.

1.3.3 SSL Certificate Expiration Analysis

Description:
The SSL certificate for the domain **i18n.api.just-eat.io** is set to expire in **88 days**, placing it in the warning category. Timely renewal is essential to maintain secure communications and prevent service disruptions.

Affected Assets:
- Domain: **i18n.api.just-eat.io**

Recommendations:
- Plan for the renewal of the SSL certificate well before expiration. - Implement automated reminders or monitoring tools to track certificate expiration dates. - Consider using a certificate management solution to streamline renewals.

1.3.4 Shared Hosting Environment Analysis

Description:
The domain **i18n.api.just-eat.io** is hosted in a shared environment with **19 other domains**, categorized as medium interest. Shared hosting can lead to resource contention and potential security risks if other hosted domains are compromised.

Affected Assets:
- Hostname: **i18n.api.just-eat.io**

Recommendations:
- Evaluate the feasibility of moving to a dedicated hosting environment. - Implement robust isolation mechanisms to prevent cross-domain attacks. - Regularly monitor shared hosting environments for unusual activity.

1.4 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 access controls, encrypting sensitive data, and conducting security awareness training for staff will further mitigate risks and protect critical assets.