1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **base-camp.rivian.com**. The analysis was performed using a Basic scan type, initiated on **August 4th at 07:00** and completed in **00h:07m:37s**. The evaluation focused on identifying vulnerabilities within the web application and infrastructure, adhering to OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18** issues, categorized as **0** High-risk, **1** Medium-risk, **1** Low-risk, and **16** informational. The most significant finding is a Medium-risk issue related to open port **80**, which lacks encryption and could expose data if not redirected to HTTPS or secured with HSTS. This vulnerability could lead to data interception, impacting confidentiality. Additionally, the SSL/TLS protocols are secure, with all endpoints supporting TLS **1.2** and **1.3**, ensuring robust encryption. No shared hosting environments or high-density services were detected, indicating a well-segmented infrastructure. The assessment recommends addressing the open port issue to mitigate potential security risks.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assessment	Low

1.3.1 Nmap Port Scan Results Analysis

Description:

The assessment revealed that port **80/tcp** is open and associated with the HTTP service on IP **99.86.102.39**. This port is flagged as potentially insecure due to the lack of encryption, which could lead to data interception if not properly managed. It is crucial to verify whether there is a redirection to HTTPS or if HTTP Strict Transport Security (HSTS) is enabled to protect data integrity and confidentiality.

Affected Assets:

- IP: **99.86.102.39** - Ports: **80/tcp**, **443/tcp**

Recommendations:

- Implement a redirection from HTTP to HTTPS for all incoming traffic. - Enable HSTS to ensure that browsers only interact with the server over a secure connection. - Regularly monitor and audit open ports to ensure they are necessary and secured.

1.3.2 SSL/TLS Protocols Security Assessment

Description:

The analysis confirmed that all endpoints support TLS **1.2** and TLS **1.3**, which are considered secure and align with current best practices for encryption protocols. No endpoints were found using deprecated or vulnerable protocols such as SSLv3, TLS **1.0**, or TLS **1.1**, indicating a strong security posture in terms of encryption.

Affected Assets:

- **4** endpoints support TLS **1.3** - **4** endpoints use TLS **1.2**

Recommendations:

- Continue to enforce the use of TLS **1.2** and TLS **1.3** across all systems. - Regularly review

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING

and update cryptographic configurations to align with industry standards. - Ensure that all new deployments adhere to these encryption standards.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to address the Medium-risk issue by securing open ports and ensuring all communications are encrypted. Regular security audits should be conducted to identify and mitigate potential vulnerabilities promptly. Additionally, maintaining up-to-date security configurations and adhering to best practices will help safeguard against emerging threats.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING