1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a comprehensive security assessment conducted on the domain **bankline.com.br**. The analysis was initiated on **08-10** at **21:45** and concluded after **00h:21m:07s**. The assessment was performed using a Basic scan type, with tracking ID **07cd59a7cf78**. The evaluation focused on identifying High and Medium-risk vulnerabilities within the web application and infrastructure, utilizing methodologies aligned with OWASP and OSCP standards.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **2 High-risk**, **1 Medium-risk**, **2 Low-risk**, and **13 informational**. Critical findings include vulnerabilities in SSL/TLS protocols, with deprecated TLS 1.0 and 1.1 detected, posing significant risks to data integrity and confidentiality. Additionally, a High-risk Denial of Service (DoS) vulnerability was observed on port **80**, with a **91.71%** timeout rate, necessitating immediate mitigation to prevent service disruptions. The Medium-risk issue involves insecure HTTP port exposure, requiring verification of HTTPS redirection. Actionable insights include upgrading to TLS 1.2 or higher, implementing DoS protection, and ensuring secure port configurations to enhance overall security posture.

1.3 Key Security Issues

Title	Risk
SSL/TLS Protocols Security Assessment	High
Denial of Service (DoS) Vulnerability	High
Nmap Port Scan Results Analysis	Medium

1.3.1 SSL/TLS Protocols Security Assessment

Description:

The assessment identified the use of deprecated SSL/TLS protocols, specifically TLS 1.0 and TLS 1.1, across **2 endpoints** each. These protocols are vulnerable to known attacks such as BEAST and lack modern cryptographic algorithms, compromising data integrity and confidentiality.

Affected Assets:

- **Endpoints with TLS 1.0: 2**
- **Endpoints with TLS 1.1: 2**
- **Endpoints with TLS 1.2: 2**
- **Endpoints with TLS 1.3: 2**

Recommendations:

Immediate action is required to disable TLS 1.0 and TLS 1.1 across all endpoints. It is recommended to upgrade to TLS 1.2 or higher, ideally TLS 1.3, to ensure robust encryption standards are maintained.

1.3.2 Denial of Service (DoS) Vulnerability Assessment

Description:

A High-risk DoS vulnerability was detected on HTTP port **80**, characterized by a significant timeout rate of **91.71%** during the analysis period. This indicates a potential for service disruption due to resource exhaustion.

Affected Assets:
- **Endpoint:** bankline.com.br:80

Recommendations:
Implement specific DoS protection measures for the affected endpoint. Consider deploying rate limiting, connection throttling, and firewall rules to mitigate the risk of service disruption. Continuous monitoring of server performance is advised to detect and respond to potential DoS attacks promptly.

1.3.3 Nmap Port Scan Results Analysis

Description:
The scan revealed an open HTTP port (**80**) without encryption, posing a Medium risk due to the potential exposure of sensitive data in transit. Verification of HTTPS redirection or HSTS implementation is necessary to secure data transmission.

Affected Assets:
- **IP: 23.220.161.11**
- **Ports: 80/tcp, 443/tcp**

Recommendations:
Ensure that all HTTP traffic is redirected to HTTPS by implementing strict transport security policies such as HSTS. Regularly review and update security configurations to maintain compliance with best practices for secure communications.

1.4 General Recommendation

To enhance the overall security posture of the domain **bankline.com.br**, it is crucial to address the identified High and Medium-risk vulnerabilities promptly. Implementing robust encryption standards, securing open ports, and deploying effective DoS protection mechanisms will significantly reduce the risk of data breaches and service disruptions. Regular security assessments should be conducted to ensure ongoing compliance with industry standards and best practices.