1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **riskservices.fta.cashedge.com**. The assessment was initiated on **March 27th** at **00:45** and concluded in **00h:11m:16s**. The analysis was performed using a Basic scan type, with tracking ID **038f05bc9ed5**. The scope of the work included a comprehensive evaluation of the web application and infrastructure security posture, following OWASP and OSCP methodologies.

1.2 Summary of Findings

The security assessment identified a total of **18** issues, with **1** low-risk and **17** informational findings. Notably, there were no high or medium-risk issues identified. The primary concern is the use of TLS 1.2 without support for the more secure TLS 1.3, which could impact data protection standards. All analyzed hosts are on dedicated infrastructure, with no shared hosting risks detected. Geographic distribution is normal, with all servers located in the USA, and no services were found vulnerable to brute force attacks. The SSL certificate is valid for **272** days, indicating no immediate renewal concerns. Overall, the assessment suggests a stable security posture with recommendations to enhance TLS protocols for improved security.

1.3 Issues Table

Title	Risk
SSL/TLS Protocols Security Assessment	Low

1.4 Detailed Findings

1.4.1 SSL/TLS Protocols Security Assessment

Description

The assessment of SSL/TLS protocols revealed that the endpoint is using TLS 1.2, which is currently an acceptable minimum standard. However, it lacks support for TLS 1.3, which is considered best practice due to its enhanced security and performance features. No endpoints were found using deprecated or vulnerable protocols such as SSLv3, TLS 1.0, or TLS 1.1.

Affected Assets

- **1** endpoint is using TLS 1.2.

Recommendations

To improve the security posture, it is recommended to enable support for TLS 1.3 across all applicable endpoints. This will ensure compliance with current best practices and enhance both security and performance. Regular reviews of cryptographic protocols should be conducted to stay updated with evolving standards and vulnerabilities.

1.5 General Recommendation

While the current security posture appears stable, it is advisable to implement TLS 1.3 to align with industry best practices and enhance data protection measures. Continuous monitoring and periodic reassessment of security configurations are recommended to maintain robust defenses against emerging threats.