1 Executive Security Assessment Report

1.1 Introduction

This report details the findings from a security assessment conducted on the domain **web-srv.wm.cashedge.com**. The analysis was initiated on **April 1st** at **01:00** and completed in **00h:10m:44s**. The assessment was performed using a Basic scan type, identified by tracking ID **11cc3d657d3c**. The scope of the work included a comprehensive evaluation of the SSL/TLS protocols in use, focusing on identifying potential vulnerabilities and assessing the overall security posture of the domain.

1.2 Short Summary of Main Issues

The security assessment reveals a predominantly low-risk profile with **0** high-risk, **0** medium-risk, **1** low-risk, and **17** informational issues identified. The primary concern is the SSL/TLS Protocols Security Assessment, which indicates the absence of TLS 1.3, a best practice for enhanced security. All other findings, such as shared hosting, geographic distribution, and unusual port assignments, show no immediate threats, with **100%** of servers located in low-risk areas and all services running on standard ports. The analysis highlights the need for upgrading to TLS 1.3 to mitigate potential vulnerabilities and enhance security posture. Continuous monitoring and regular updates are recommended to maintain robust security defenses.

1.3 Key Security Issues

Title	Risk
SSL/TLS Protocols Security Assessment	Low

1.3.1 SSL/TLS Protocols Security Assessment

Description The assessment of SSL/TLS protocols revealed that the domain is currently utilizing TLS 1.2, which is considered an acceptable minimum standard. However, there is no support for TLS 1.3, which is the current best practice for enhanced security and performance. The absence of TLS 1.3 may expose the domain to potential vulnerabilities that could be mitigated with its implementation. While deprecated protocols such as SSLv3, TLS 1.0, and TLS 1.1 were not detected, it is crucial to adopt the latest standards to ensure robust security.

Affected Assets

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

Recommendations It is recommended to upgrade to TLS 1.3 to leverage its improved security features and performance benefits. This upgrade will help mitigate potential vulnerabilities associated with older protocols and align with industry best practices. Regularly review and update cryptographic protocols to maintain a strong security posture.

1.4 General Recommendation

To enhance the overall security posture, it is advised to implement continuous monitoring and regular updates of all systems and protocols. Adopting TLS 1.3 across all endpoints will significantly improve security resilience against emerging threats. Additionally, maintaining awareness of industry standards and best practices will ensure that security measures remain effective and up-to-date.