1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **atlanticusfeds.hepsiian.com**. The analysis commenced on **March 31st at 11:45** and concluded in **00h:08m:34s**. This evaluation was categorized as a “Basic” type scan. The assessment aimed to identify potential vulnerabilities within the web application infrastructure, focusing on High and Medium-risk issues.

1.2 Short Summary of Main Issues

The security assessment identified a total of **19 issues**, categorized as **0 High-risk**, **1 Medium-risk**, **1 Low-risk**, and **17 informational**. The most critical finding is the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts, significantly increasing the risk of cyber-attacks, particularly injection-based attacks, which could lead to unauthorized data access and potential system compromise. Additionally, the SSL/TLS protocol analysis revealed that while TLS 1.2 is in use, there is no support for the more secure TLS 1.3. It is recommended to implement a WAF and consider upgrading to TLS 1.3 to enhance security posture.

1.3 Key Security Issues

Title	Risk
Absence of WAF	Medium
SSL/TLS Protocols Security	Low

1.3.1 Absence of WAF

Description

The analysis revealed that there is no Web Application Firewall (WAF) implemented on the host, resulting in a **100% vulnerability rate**. This absence significantly increases the risk of successful cyber-attacks, particularly injection-based attacks, which could lead to unauthorized data access, data breaches, and potential system compromise.

Affected Assets

- **Domain:** atlanticusfeds.hepsiian.com
- **Total Hosts Analyzed: 1**
- **Hosts without WAF: 1**

Recommendations

It is strongly recommended to implement a Web Application Firewall (WAF) to provide an additional layer of security by filtering and monitoring HTTP traffic between a web application and the Internet. This will help mitigate risks associated with injection-based attacks and unauthorized data access.

1.3.2 SSL/TLS Protocols Security Assessment

Description

The SSL/TLS protocol analysis indicated that TLS 1.2 is currently in use, which is considered acceptable as a minimum standard. However, there is no support for TLS 1.3, which is the current best practice for security and performance. No deprecated or vulnerable protocols such as SSLv3, TLS 1.0, or TLS 1.1 were detected.

Affected Assets

- **Endpoints using TLS 1.2: 1**
- **Endpoints with TLS 1.3 support: 0**

Recommendations

To enhance security and performance, it is recommended to upgrade to TLS 1.3. This protocol offers improved security features and better performance compared to its predecessors.

1.4 General Recommendation

To improve the overall security posture of the domain **atlanticusfeds.hepsiian.com**, it is advised to implement a comprehensive security strategy that includes deploying a Web Application Firewall (WAF) and upgrading to TLS 1.3. These measures will help protect against potential cyber threats and ensure compliance with current security standards. Regular security assessments should be conducted to identify and mitigate emerging vulnerabilities promptly.