1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **oceanbank-uat.hepsiian.com**. The analysis was initiated on **March 26th** at **02:00** and completed in **00h:08m:02s**. The assessment was performed using a basic scan methodology. The scope of the work included evaluating the security posture of the web application and its infrastructure, focusing on identifying High and Medium-risk issues.

1.2 Short Summary

The security assessment identified a total of **19** issues, categorized as **0** High-risk, **2** Medium-risk, **1** Low-risk, and **16** informational. The most critical findings include the absence of Web Application Firewall (WAF) protection on **100%** of analyzed hosts, significantly increasing the risk of cyber-attacks, particularly injection-based attacks. Additionally, a Medium-risk issue was found in subdomain naming, which could expose sensitive endpoints like development environments to potential threats. The SSL/TLS protocol assessment revealed that while TLS 1.2 is in use, there is no support for the more secure TLS 1.3. Actionable insights include implementing WAF protection to mitigate attack risks and reviewing subdomain security to prevent unauthorized access.

1.3 Key Security Issues

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

1.3.1 Absence of WAF

Description The analysis revealed that there is no Web Application Firewall (WAF) protection implemented on the domain **oceanbank-uat.hepsiian.com**. This absence results in a **100%** vulnerability rate, significantly elevating the risk of successful cyber-attacks, particularly those based on injection techniques. Without a WAF, the application is susceptible to unauthorized data access, data breaches, and potential system compromise.

Affected Assets

- Host: **oceanbank-uat.hepsiian.com**

Recommendations It is recommended to implement a robust Web Application Firewall (WAF) to provide an additional layer of security against common web-based attacks. This will help in mitigating risks associated with injection attacks and unauthorized access attempts.

1.3.2 Subdomain Naming Security Assessment

Description The assessment identified a sensitive subdomain, **oceanbank-uat.hepsiian.com**, categorized under “Development/Staging” with a Medium risk level. This subdomain may indicate the presence of administrative interfaces, internal systems, or development environments that could contain unpatched vulnerabilities or debug information. There is a potential risk of exposing critical systems and sensitive data through these endpoints.

Affected Assets

- Subdomain: **oceanbank-uat.hepsiian.com**

Recommendations Review and secure all subdomains to ensure they do not expose sensitive information or systems. Consider implementing access controls and monitoring for development and staging environments to prevent unauthorized access.

1.3.3 SSL/TLS Protocols Security Assessment

Description The SSL/TLS protocol assessment showed that while TLS 1.2 is in use, there is no support for the more secure TLS 1.3. Although TLS 1.2 is currently acceptable, TLS 1.3 offers improved security and performance benefits.

Affected Assets

- Endpoint using TLS 1.2: **oceanbank-uat.hepsiian.com**

Recommendations Upgrade to TLS 1.3 to enhance security and performance. Ensure that all cryptographic protocols are up-to-date and configured according to best practices to protect against known vulnerabilities.

1.4 General Recommendation

To enhance the overall security posture, it is crucial to implement a comprehensive security strategy that includes deploying a Web Application Firewall (WAF), securing subdomains, and upgrading cryptographic protocols to the latest standards. Regular security assessments should be conducted to identify and mitigate emerging threats promptly.