1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **premiercommunity.onlinebank.com**. The analysis was performed using a certified web application and infrastructure penetration testing tool, following OWASP and OSCP methodologies. The assessment was initiated on **July 24th** at **06:45** and completed in **00h:20m:46s**. The analysis type was categorized as “Basic”.

1.2 Summary of Findings

The security assessment identified a total of **19** issues, categorized as **0** High, **3** Medium, **2** Low, and **14** 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, and the SSL certificate nearing expiration with only **58** days remaining, which could impact secure communications. Additionally, a Medium risk was noted due to potentially insecure open ports, such as HTTP on port **80**, which lacks encryption. Immediate actions should focus on implementing WAF protection, renewing SSL certificates, and securing open ports to mitigate these vulnerabilities.

1.3 Key Security Issues

Title	Risk
Absence of WAF	Medium
SSL Certificate Expiration Analysis	Medium
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assessment	Low
Denial of Service (DoS) Vulnerability	Low

1.3.1 Absence of WAF

Description:

The assessment revealed that the domain lacks Web Application Firewall (WAF) protection, resulting in a **100%** vulnerability rate. This absence significantly elevates the risk of successful cyber-attacks, particularly injection-based attacks, unauthorized data access, data breaches, and potential system compromise.

Affected Assets:

- Host: **premiercommunity.onlinebank.com**

Recommendations:

Implement a robust WAF solution to provide an additional layer of security against web-based attacks. Regularly update and configure the WAF to ensure it effectively mitigates emerging threats.

1.3.2 SSL Certificate Expiration Analysis

Description:

The SSL certificate for the domain is set to expire in **58** days, placing it in a warning status. Failure to renew the certificate could lead to disruptions in secure communications and potential trust issues with users.

Affected Assets:
- Domain: **premiercommunity.onlinebank.com**

Recommendations:
Plan for the renewal of the SSL certificate well before its expiration date to maintain secure communications and avoid service disruptions.

1.3.3 Nmap Port Scan Results Analysis

Description:
The scan identified open ports, including HTTP on port **80**, which lacks encryption. This poses a risk unless there is a redirection to HTTPS or if HTTP Strict Transport Security (HSTS) is enabled.

Affected Assets:
- IP Address: **66.6.25.95** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:
Ensure that all HTTP traffic is redirected to HTTPS and consider enabling HSTS to enforce secure connections. Regularly review open ports and services to minimize exposure.

1.3.4 SSL/TLS Protocols Security Assessment

Description:
The domain supports TLS 1.2, which is currently acceptable, however, it lacks support for TLS 1.3, which is considered best practice for enhanced security and performance.

Affected Assets:
- Endpoint using TLS 1.2

Recommendations:
Upgrade to support TLS 1.3 to benefit from improved security features and performance enhancements.

1.3.5 Denial of Service (DoS) Vulnerability Assessment

Description:
A Low-risk DoS vulnerability was identified with a **0.12%** timeout rate. While currently Low risk, it indicates potential performance issues under specific conditions.

Affected Assets:
- Service Ports: **80** (HTTP), **443** (HTTPS)

Recommendations:
Monitor server performance during peak times and optimize server responses to mitigate potential DoS impacts.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, timely patch management, and continuous monitoring of network activities. Additionally, user awareness training should be conducted to mitigate risks associated with social engineering attacks.