



1 Executive Security Assessment Report

1.1 Overview

The security assessment was conducted on the domain **markonitor.com.bn**. The analysis was initiated on **March 23rd at 16:45** and concluded in **00h:09m:31s**. The assessment type was classified as "Basic". The evaluation focused on identifying High and Medium-risk vulnerabilities using OWASP and OSCP methodologies.

1.2 Key Findings Summary

The security assessment identified **2** High-risk, **1** Medium-risk, and **15** informational issues. Critical findings include a Denial of Service (DoS) vulnerability on port **443**, with a **94.03%** timeout rate, posing a significant risk to service availability. Additionally, a High-risk shared hosting environment was detected, with over **262,000** domains sharing the same IP, potentially impacting data integrity and privacy. A Medium-risk issue was found with HTTP services running on port **80** without encryption, necessitating verification of HTTPS redirection. Immediate actions include enhancing server resilience against DoS attacks and securing shared hosting configurations to mitigate potential threats.

1.3 Issues Table

Title	Risk
Denial of Service (DoS) Assessment	High
Shared Hosting Environment Analysis	High
Nmap Port Scan Results Analysis	Medium

1.4 Detailed Findings

1.4.1 Denial of Service (DoS) Assessment

Description:

A High-risk DoS vulnerability was identified on port **443**, with a **94.03%** timeout rate out of **134** total responses. This indicates a significant risk to service availability, as the server is unable to handle requests efficiently during peak loads or potential attack scenarios.

Affected Assets:

- Port: **443** (HTTPS)

Recommendations:

- Implement rate limiting and traffic filtering to mitigate DoS attacks. - Optimize server configurations to handle higher loads. - Regularly monitor server performance and conduct stress testing.

1.4.2 Shared Hosting Environment Analysis

Description:

The domain **markonitor.com.bn** is hosted in a High-risk shared environment with over **262,000** domains sharing the same IP address. This configuration poses risks related to data integrity and privacy due to shared infrastructure vulnerabilities.

Affected Assets:

- Hostname: **markonitor.com.bn**

Recommendations:

- Consider migrating to a dedicated hosting environment to enhance security. - Implement strict



access controls and monitoring for shared resources. - Regularly audit shared hosting configurations for potential vulnerabilities.

1.4.3 Nmap Port Scan Results Analysis

Description:

Port **80** was identified as running HTTP without encryption, which is flagged as a Medium-risk issue. The lack of encryption poses a risk if there is no redirection to HTTPS or if HTTP Strict Transport Security (HSTS) is not enabled.

Affected Assets:

- IP: **(3.33.139.32)** - Port: **80/tcp** - Service: http - Version: awselb/2.0

Recommendations:

- Ensure all HTTP traffic is redirected to HTTPS. - Enable HSTS to enforce secure connections.
- Regularly update and patch web server software to mitigate vulnerabilities.

1.5 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 traffic. Additionally, consider adopting advanced threat detection solutions and conducting regular security awareness training for staff to mitigate human-related risks.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING