1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain **microsoftedge.microsoft.com**. The evaluation commenced on **May 26th at 20:45** and concluded after a duration of **19 minutes and 24 seconds**. The assessment was performed using a **Basic** scan type. The primary objective was to identify and evaluate potential security vulnerabilities within the web application and its infrastructure, focusing on High and Medium-risk issues.

1.2 Short Summary of Main Issues

The security assessment identified a total of **21 issues**, categorized as **0 High-risk**, **3 Medium-risk**, **4 Low-risk**, 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 unusual port assignments that may indicate misconfigurations or attempts to evade detection. Medium-risk issues also include potential vulnerabilities from services running on non-standard ports and insecure port configurations detected by Nmap. Immediate actions should focus on implementing WAF protection and reviewing port configurations to mitigate these risks.

1.3 Key Security Issues

Title	Risk
Absence of WAF	Medium
Unusual Port Assignments Detected	Medium
Nmap Port Scan Results Analysis	Medium
Usage of PHP Technology Detected	Low
Usage of ASP Technology Detected	Low
SSL/TLS Protocols Security Assess...	Low
Login Form Detection Analysis	Low

1.3.1 Absence of WAF

Description:
The analysis revealed that the domain lacks Web Application Firewall (WAF) protection, exposing it to a wide range of cyber threats, particularly injection-based attacks. The absence of WAF results in a **100%** vulnerability rate, leaving the application susceptible to unauthorized data access, data breaches, and potential system compromise.

Affected Assets:
Host: **microsoftedge.microsoft.com**

Recommendations:
Implement a robust Web Application Firewall to provide an additional layer of security against common web-based attacks. Regularly update and configure the WAF to adapt to emerging threats and ensure comprehensive protection.

1.3.2 Unusual Port Assignments Detected

Description:
The assessment identified unusual port assignments on the host, which may suggest miscon-

figurations or attempts to evade detection. Specifically, port **80** is running unexpected services such as `upnp` instead of standard HTTP services.

Affected Assets:

- Host: **microsoftedge.microsoft.com (13.107.9.203)**

Recommendations:

Review and standardize port configurations to align with best practices. Ensure that services are running on expected ports to prevent potential exploitation or misuse.

1.3.3 Nmap Port Scan Results Analysis

Description:

The Nmap scan detected open ports, including port **80**, which is running `upnp` on Microsoft IIS httpd without encryption. This configuration poses a risk due to the lack of HTTPS redirection or HSTS implementation.

Affected Assets:

- IP Address: **13.107.9.203**

Recommendations:

Ensure that all HTTP traffic is redirected to HTTPS and implement HSTS to enforce secure connections. Regularly audit open ports and services to maintain secure configurations.

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 adherence to security best practices. Prioritize the deployment of a Web Application Firewall and review network configurations to mitigate identified risks effectively. Additionally, conduct continuous monitoring and incident response planning to swiftly address any potential threats.