1 Security Assessment Report

1.1 Scan Details

- **Domain:** support.malwarebytes.com
- **Tracking ID:** 0114ae11fc8d
- **Type of Analysis:** Basic
- **Initiation Date and Time:** March 17, 17:00
- **Duration:** **14** minutes and **26** seconds

1.2 Short Summary of Main Issues

The security assessment revealed a total of **18 issues**, with **1 high-risk** and **3 medium-risk** findings. The most critical issue is the high-risk shared hosting environment, where a single host supports over **238,576 shared domains**, significantly increasing exposure to potential attacks. Medium-risk issues include insecure open ports (HTTP on ports **80** and **8080**) and an SSL certificate nearing expiration with only **35 days** remaining. These vulnerabilities require immediate attention to prevent data breaches and service disruptions.

1.3 Executive Summary

Title	Risk
Shared Hosting Environment Analysis	High
Nmap Port Scan Results Analysis	Medium
SSL Certificate Expiration Analysis	Medium
Login Form Detection Analysis	Medium

1.3.1 Shared Hosting Environment Analysis

Description:
The analysis identified a high-risk shared hosting environment on the domain support.malwarebytes.com, where a single host supports over **238,576 shared domains**. This configuration poses a significant security risk as it increases the potential attack surface and the likelihood of cross-domain vulnerabilities.

Affected Assets:
- Hostname: support.malwarebytes.com

Recommendations:
It is recommended to evaluate the necessity of such a large number of shared domains on a single host. Consider implementing isolation measures or migrating critical services to dedicated hosting environments to reduce exposure.

1.3.2 Nmap Port Scan Results Analysis

Description:
The scan detected **4 open ports**, with ports **80** and **8080** identified as potentially insecure due to the lack of encryption. These ports are associated with HTTP services that may not redirect to HTTPS, posing risks of data interception and web service vulnerabilities.

Affected Assets:
- IP Address: **216.198.53.1** - Ports: **80/tcp, 443/tcp, 8080/tcp, 8443/tcp**

Recommendations:

Ensure that HTTP services on ports **80** and **8080** are configured to redirect to HTTPS. Implement HSTS (HTTP Strict Transport Security) to enforce secure connections and mitigate risks associated with unencrypted traffic.

1.3.3 SSL Certificate Expiration Analysis

Description:

The SSL certificate for support.malwarebytes.com is set to expire in **35 days**, placing it in the warning category. Failure to renew the certificate could lead to service disruptions and loss of trust from users.

Affected Assets:

- Domain: support.malwarebytes.com

Recommendations:

Initiate the renewal process for the SSL certificate immediately to avoid expiration. Implement automated alerts for certificate expiration to ensure timely renewals in the future.

1.3.4 Login Form Detection Analysis

Description:

Three login forms were detected across the application, indicating potential authentication interfaces that require security validation. The presence of multiple login forms increases the risk of unauthorized access if not properly secured.

Affected Assets:

- URLs: - `https://support.malwarebytes.com/credentials_api3` - `http://support.malwarebytes.com/tymeshift-frontend/az.fc04f015869d0e046b0eda38972e22c7.json` - `http://support.malwarebytes.com:8080/wfm/v2` - `http://216.198.53.1:8080` - `http://216.198.53.1:80`

Recommendations:

Conduct a thorough security review of all login forms to ensure they are protected against common vulnerabilities such as SQL injection and cross-site scripting (XSS). Implement multi-factor authentication (MFA) to enhance security.

1.4 General Recommendation

To improve the overall security posture, it is crucial to address high and medium-risk vulnerabilities promptly. Regularly update security configurations, conduct periodic security assessments, and implement robust monitoring solutions to detect and respond to potential threats effectively.