1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain **mlife.mo**. The evaluation commenced on **05-06** at **23:00** and concluded in **00h:13m:15s**. The analysis was categorized as a “Basic” type assessment. The scope of the work included a comprehensive review of the domain’s web application and infrastructure, utilizing OWASP and OSCP methodologies to identify potential vulnerabilities.

1.2 Short Summary of Main Issues

The security assessment identified **0 high-risk**, **2 medium-risk**, **1 low-risk**, and **15 informational issues**. Key findings include medium-risk vulnerabilities such as insecure open ports (HTTP on port **80**) and an SSL certificate nearing expiration with **44 days** remaining, which could impact secure communications and compliance. The low-risk issue pertains to the use of TLS **1.2** without TLS **1.3**, indicating a need for protocol updates to enhance security. Despite these concerns, no high-density services or shared hosting risks were detected, and all services are running on standard ports. Immediate actions should focus on securing the HTTP service and planning for SSL certificate renewal to mitigate potential security breaches.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL Certificate Expiration Analysis	Medium
SSL/TLS Protocols Security Assessment	Low

1.3.1 Nmap Port Scan Results Analysis

Description:

The assessment identified that port **80** is open and running an HTTP proxy service on an F5 BIG-IP load balancer without encryption. This poses a potential security risk if not redirected to HTTPS or if HTTP Strict Transport Security (HSTS) is not enabled.

Affected Assets:

- IP: **202.175.1[illegible].179** - Ports: **80/tcp** (http-proxy), **443/tcp** (ssl/https)

Recommendations:

- Implement HTTPS redirection for all HTTP traffic. - Enable HSTS to ensure secure connections. - Regularly monitor open ports and services for unauthorized access.

1.3.2 SSL Certificate Expiration Analysis

Description:

The domain “mlife.mo” has an SSL/TLS certificate that will expire in **44 days**, categorized under the “Warning” risk level. This indicates that renewal planning should occur soon to maintain secure communications and compliance.

Affected Assets:

- Domain: **mlife.mo**

Recommendations:

- Initiate the renewal process for the SSL certificate immediately. - Consider implementing automated reminders for certificate renewals. - Evaluate the use of longer-duration certificates if applicable.

1.3.3 SSL/TLS Protocols Security Assessment

Description:
The analysis revealed that the domain supports TLS **1.2** but lacks support for TLS **1.3**, which is the current best practice for enhanced security and performance.

Affected Assets:
- **1** endpoint is using TLS **1.2**.

Recommendations:
- Upgrade to support TLS **1.3** to improve security posture. - Ensure all endpoints are configured to use modern cryptographic algorithms. - Regularly review and update cryptographic protocols in line with industry standards.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to prioritize the implementation of HTTPS across all services, ensure timely renewal of SSL certificates, and upgrade cryptographic protocols to support TLS **1.3**. Continuous monitoring and regular security assessments should be conducted to identify and mitigate emerging threats promptly.