1 Executive Security Assessment Report

1.1 Introduction

The following security assessment was conducted on the domain **masterlifecrm.com**. The analysis was initiated on **07-11** at **09:45** and completed in **00h:24m:49s**. The assessment type was classified as “Basic”. The evaluation focused on identifying High and Medium-risk vulnerabilities using OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **21** risks, including **2** High-risk and **4** Medium-risk issues. Critical findings include the exposure of email addresses and passwords on the deep web, which poses significant risks such as phishing attacks and unauthorized access. Additionally, unencrypted HTTP traffic was detected across **4** URLs, increasing the risk of data interception. Medium-risk issues involve shared hosting environments and CMS installations requiring regular updates.

1.3 Key Security Issues

Title	Risk
Email Addresses and/or Passwords Leaked	High
Unencrypted HTTP Traffic Detected	High
Shared Hosting Environment Analysis	Medium
Nmap Port Scan Results Analysis	Medium
SSL Certificate Expiration Analysis	Medium
CMS Detection Analysis	Medium

1.3.1 Email Addresses and/or Passwords Leaked on the Deep Web

Description:
A total of **2** leaked credentials were discovered on the deep web, including email addresses associated with the domain. This exposure poses a significant security vulnerability, leading to potential unauthorized access, phishing attacks, and reputational damage.

Affected Assets:
- Email Address: viacheslav@masterlifecrm.com

Recommendations:
Immediate action is required to secure the leaked credentials. Implement multi-factor authentication, conduct a password reset for affected accounts, and monitor for any unauthorized access attempts. Educate employees on recognizing phishing attempts.

1.3.2 Unencrypted HTTP Traffic Detected

Description:
Unencrypted HTTP traffic was detected across **4** URLs, exposing data to interception and man-in-the-middle attacks. This lack of encryption compromises data integrity and authenticity.

Affected Assets:
- URLs: - http://www.masterlifecrm.com/cdn-cgi/l/email-protection# - http://masterlifecrm.com/cdn-cgi/l/email-protection# - http://masterlifecrm.com:8080/cdn-cgi/l/email-protection# - http://www.masterlifecrm.com:8080/cdn-cgi/l/email-protection#

Recommendations:
Enforce HTTPS across all web applications by obtaining and installing SSL/TLS certificates. Implement HTTP Strict Transport Security (HSTS) to ensure secure connections.

1.3.3 Shared Hosting Environment Analysis

Description:
The domain is hosted in a shared environment with **medium interest**, where multiple domains share the same IP address. This configuration can lead to security risks if one of the shared domains is compromised.

Affected Assets:
- Hostnames: masterlifecrm.com, www.masterlifecrm.com

Recommendations:
Consider migrating to a dedicated hosting environment to isolate resources and reduce security risks. Regularly monitor shared hosting configurations for unauthorized changes.

1.3.4 Nmap Port Scan Results Analysis

Description:
A total of **8** open ports were detected, with ports **80** and **8080** flagged for potential security risks due to lack of encryption and possible web service vulnerabilities.

Affected Assets:
- IP Address: **104.18.29.180** - Services running on ports: **80**, **443**, **8080**, **8443**

Recommendations:
Ensure that all services are running over encrypted channels. Redirect HTTP traffic to HTTPS and verify that HSTS is enabled. Regularly update web services to mitigate vulnerabilities.

1.3.5 SSL Certificate Expiration Analysis

Description:
SSL certificates for two domains are set to expire in **45** days, categorized under “Warning” status, indicating a need for timely renewal to maintain secure communications.

Affected Assets:
- Domains: masterlifecrm.com, www.masterlifecrm.com

Recommendations:
Plan for SSL certificate renewal before expiration to avoid service disruptions. Consider implementing automated certificate management solutions for timely renewals.

1.3.6 Content Management System (CMS) Detection Analysis

Description:
Two WordPress installations were detected, requiring regular security maintenance including updates, plugin management, and access control to prevent potential security risks.

Affected Assets:
- Affected URL: `https://masterlifecrm.com/`

Recommendations:
Regularly update WordPress core, themes, and plugins to their latest versions. Implement security plugins to enhance protection and conduct periodic security audits.

1.4 General Recommendations

To enhance overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, employee training on cybersecurity

best practices, and continuous monitoring of network activities. Establishing incident response protocols will also help in mitigating potential threats effectively.