1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **hometownbanc.com** using a Basic scan methodology. The analysis commenced on **March 19th** at **00:00** and concluded in **12 minutes and 36 seconds**. The scope of the work included a comprehensive evaluation of web applications and infrastructure, focusing on identifying High and Medium-risk vulnerabilities.

1.2 Short Summary of Main Issues

The security assessment identified a total of **23 issues**, categorized as **1 High-risk**, **1 Medium-risk**, **3 Low-risk**, and **18 informational**. The most critical finding is the High-risk exposure of **21 leaked email addresses and passwords** on the deep web, posing significant threats such as phishing attacks and unauthorized access, which could severely impact business operations and reputation. Additionally, a Medium-risk issue was detected with open HTTP ports lacking encryption, necessitating immediate review. The assessment also revealed that all services are running on standard ports, and no high-density services or brute-force vulnerabilities were found. It is crucial to address the High-risk exposure promptly and implement stronger security measures to mitigate these vulnerabilities.

1.3 Key Security Issues

Title	Risk
Email Addresses and/or Passwords Leaked on the Deep Web	High
Nmap Port Scan Results Analysis	Medium
Shared Hosting Environment Analysis	Low
SSL/TLS Protocols Security Assessment	Low
Login Form Detection Analysis	Low

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

Description:
A total of **21 leaked credentials** were identified on the deep web, involving email addresses and passwords from multiple databases such as AntiPublic and BreachCompilation. This exposure poses a serious security vulnerability due to potential phishing attacks, unauthorized access, social engineering, business disruptions, and reputational damage.

Affected Assets:
- Email addresses and passwords of employees from the organization.

Recommendations:
Immediate action is required to mitigate this risk. It is recommended to perform a password reset for all affected accounts, implement multi-factor authentication (MFA), and conduct security awareness training for employees to recognize phishing attempts. Regular monitoring of deep web sources for new leaks should also be established.

1.3.2 Nmap Port Scan Results Analysis

Description:
The scan identified **two open ports**, specifically port **80 (HTTP)** and port **443 (SSL/HTTPS)**. Port 80 is potentially insecure due to the lack of encryption, which could expose sensitive data to interception.

Affected Assets:

- IP Address: **107.162.166.85** - Open Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:

Ensure that HTTP traffic is redirected to HTTPS and consider enabling HTTP Strict Transport Security (HSTS) to enforce secure connections. Regularly update SSL/TLS configurations to adhere to best practices.

1.4 General Recommendations

To enhance overall security posture, it is advised to implement a comprehensive security strategy that includes regular vulnerability assessments, patch management, network segmentation, and continuous monitoring. Additionally, fostering a culture of security awareness among employees will help mitigate risks associated with human factors.