1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **loanbuilder.com** using a Basic scan methodology. The analysis commenced on **November 22** at **05:00** and concluded in **33 minutes and 43 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 Summary of Key Issues

The security assessment identified a total of **26 risks**, categorized as **4 High-risk**, **5 Medium-risk**, **7 Low-risk**, and **10 informational issues**. Critical findings include the exposure of email addresses and passwords on the deep web, posing a significant threat of phishing attacks and unauthorized access, and the detection of unusual port assignments, which may indicate attempts to evade security controls. Additionally, the absence of HTTPS across **1420 URLs** exposes the organization to data interception and man-in-the-middle attacks. Notably, **7%** of hosts lack Web Application Firewall (WAF) protection, increasing vulnerability to injection-based attacks. Immediate actions should focus on securing leaked credentials, enforcing HTTPS, and implementing WAF across all hosts to mitigate these risks effectively.

1.3 Key Security Issues

Title	Risk
Email Addresses and/or Passwords Leaked on the Deep Web	High
Unusual Port Assignments Detected	High
Unencrypted HTTP Traffic Detected	High
Denial of Service (DoS) Vulnerability Assessment	High
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL Certificate Expiration Analysis	Medium
Login Form Detection Analysis	Medium

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

Description:

The exposure of email addresses and passwords on the deep web poses critical security risks, including unauthorized access, phishing attacks, social engineering, and further data breaches. A total of **3 leaked credentials** were identified from multiple databases such as AntiPublic and BreachCompilation.

Affected Assets:

- Email addresses: colin.gavigan@loanbuilder.com, justin.oakes@loanbuilder.com

Recommendations:

- Immediately reset passwords for affected accounts. - Implement multi-factor authentication (MFA) across all accounts. - Conduct security awareness training focusing on phishing and social engineering. - Monitor for any unauthorized access attempts or suspicious activities.

1.5 Unusual Port Assignments Detected

Description:

A total of **16 unusual port assignments** were detected, with **8 High-risk assignments**. Services are running on non-standard ports or ports running unexpected services, potentially indicating evasion attempts or misconfigurations.

Affected Assets:

- Hosts under msoid.loanbuilder.com with IPs such as 20.190.157.0, 40.126.29.7, etc.

Recommendations:

- Review and reconfigure port assignments to align with standard practices. - Implement strict firewall rules to restrict access to non-standard ports. - Regularly audit network configurations to detect and rectify anomalies.

1.6 Unencrypted HTTP Traffic Detected

Description:

A total of **1420 URLs** were found using unencrypted HTTP, exposing the organization to data interception, eavesdropping, and man-in-the-middle attacks.

Affected Assets:

- All identified URLs using HTTP protocol without HTTPS alternatives.

Recommendations:

- Enforce HTTPS across all web applications. - Implement HSTS (HTTP Strict Transport Security) to ensure secure connections. - Regularly audit web applications for compliance with security standards.

1.7 Denial of Service (DoS) Vulnerability Assessment

Description:

The analysis indicates a potential DoS vulnerability with a significant timeout rate of **54.68%** on HTTPS services, suggesting susceptibility to DoS attacks.

Affected Assets:

- Port 443 (HTTPS)

Recommendations:

- Implement rate limiting and traffic filtering to mitigate DoS attacks. - Enhance server capacity and redundancy to handle increased loads. - Monitor network traffic for unusual patterns indicative of DoS attempts.

1.8 Absence of WAF

Description:

The absence of a Web Application Firewall (WAF) on **1 host** significantly elevates the risk of successful cyber-attacks, particularly injection-based attacks.

Affected Assets:

- Host: `http://msoid.loanbuilder.com`

Recommendations:

- Deploy a WAF to protect against common web application attacks. - Regularly update WAF rules to address emerging threats. - Conduct periodic security assessments to ensure comprehensive protection.

1.9 General Recommendations

To enhance the overall security posture, it is recommended that the organization implements a robust security framework that includes regular vulnerability assessments, continuous monitoring, and incident response planning. Emphasizing employee training on cybersecurity best practices will further mitigate risks associated with human factors.