1 Executive Security Assessment Report

1.1 Overview

This report details the findings from a security assessment conducted on the domain **callawaydesigngroup.com**. The assessment was initiated on **April 21st** at **03:00** and completed in **00h:04m:19s**. The analysis was performed using a Basic scan type. The primary focus was to identify High and Medium-risk security issues that could impact the organization's security posture.

1.2 Summary of Findings

The security assessment identified **2 High-risk** issues. The most critical finding is the exposure of **10 email addresses** and/or passwords on the deep web, posing significant risks of phishing attacks, unauthorized access, and potential reputational damage. Additionally, a High-risk shared hosting environment was detected, with one host sharing its IP with over **27,000 domains**, increasing the risk of cross-site vulnerabilities. Immediate actions should focus on mitigating credential exposure and evaluating shared hosting risks.

1.3 Key Security Issues

Title	Risk
Email Addresses and/or Passwords Leaked	High
Shared Hosting Environment Analysis	High

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

Description

A total of **10 credentials** were found leaked on the deep web, involving email addresses associated with the organization. These credentials were extracted from various data breaches, including Adobe, Dropbox, and LinkedIn. The exposure of these credentials poses a serious security vulnerability due to potential phishing attacks and unauthorized access to sensitive information.

Affected Assets

- **Email Addresses:** heather@callawaydesigngroup.com, illy@callawaydesigngroup.com, larry@callawaydesig michelle@callawaydesigngroup.com, ob@callawaydesigngroup.com, scott@callawaydesigngroup.com.

Recommendations

- Implement multi-factor authentication (MFA) for all user accounts to mitigate unauthorized access.
- Conduct a password reset for all affected accounts and ensure strong password policies are enforced.
- Educate employees on recognizing phishing attempts and safe email practices.
- Regularly monitor for any new credential exposures using threat intelligence services.

1.3.2 Shared Hosting Environment Analysis

Description

The domain **callawaydesigngroup.com** is hosted in a shared environment with over **27,297 domains** sharing the same IP address. This configuration significantly increases the risk of cross-site vulnerabilities and potential exploitation through neighboring domains.

Affected Assets

- **Hostname:** callawaydesigngroup.com

Recommendations

- Consider migrating to a dedicated hosting environment to reduce exposure to shared hosting risks.
- Implement strict access controls and isolation measures to protect against potential cross-site vulnerabilities.
- Regularly audit server configurations and apply security patches promptly.

1.4 General Recommendations

To enhance overall security posture, it is recommended to:

- Conduct regular security assessments and penetration tests to identify and remediate vulnerabilities.
- Establish a comprehensive incident response plan to address potential security breaches swiftly.
- Ensure continuous monitoring of network traffic and system logs for suspicious activities.
- Foster a culture of security awareness among employees through regular training sessions.

By addressing these High-risk issues promptly, the organization can significantly reduce its exposure to potential threats and enhance its cybersecurity resilience.