1 Executive Security Assessment Report

1.1 Overview

This report details the findings from a security assessment conducted on the domain **monzo.com**. The assessment was initiated on **July 30th** at **02:00** and concluded in **29 minutes and 15 seconds**. The analysis type was classified as **Basic**. The evaluation focused on identifying High and Medium-risk vulnerabilities using methodologies aligned with OWASP and OSCP standards.

1.2 Summary of Key Issues

The security assessment identified a total of **23 risks**, categorized as **2 High-risk**, **1 Medium-risk**, **1 Low-risk**, and **19 informational**. The most critical issue is the leakage of **1,588 email addresses and/or passwords** on the deep web, posing significant risks of phishing attacks, unauthorized access, and reputational damage. Additionally, **17 login forms** were detected, indicating a high potential for exploitation if not properly secured. A Medium-risk finding includes open HTTP ports without encryption, necessitating verification of HTTPS redirection. While SSL/TLS protocols are up-to-date with TLS 1.3 on **8 endpoints**, continuous monitoring is advised. Immediate action is required to mitigate High-risk vulnerabilities and enhance security measures to protect sensitive information.

1.3 Key Security Issues

Title	Risk
Email Addresses and/or Passwords Leaked	High
Login Form Detection Analysis	High
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assessment	Low

1.3.1 Email Addresses and/or Passwords Leaked

Description:

A total of **1,588** email addresses and passwords were found leaked on the deep web. This exposure poses critical security risks, including unauthorized access, phishing attacks, social engineering, and further data breaches. The breach sources include multiple databases such as AntiPublic and BreachCompilation.

Affected Assets:

- Email addresses and passwords of the organization are affected. Specific examples include: - aafke.leekema@monzo.com - aafke@monzo.com - aaron@monzo.com

Recommendations:

- Implement immediate password resets for all affected accounts. - Enhance email security measures to detect and prevent phishing attacks. - Conduct employee training on recognizing phishing attempts. - Monitor for any unauthorized access attempts or unusual activities.

1.3.2 Login Form Detection Analysis

Description:

A total of **17 login forms** were detected across the application, indicating potential authentication interfaces that require security validation. These forms are potential entry points for unauthorized access if not properly secured.

Affected Assets:
- URLs with detected login forms include: - http://monzo.com/sign-up/ - http://monzo.com/legal/mobile-operating-system-support-policy - http://monzo.com/cookies

Recommendations:
- Conduct a thorough security review of all login forms to ensure they are protected against common web vulnerabilities. - Implement multi-factor authentication (MFA) where possible. - Ensure all login forms are served over HTTPS to protect data in transit.

1.3.3 Nmap Port Scan Results Analysis

Description:
The scan identified **4 open ports**, with port **80** running HTTP without encryption. This poses a risk unless redirected to HTTPS or if HSTS is enabled.

Affected Assets:
- IP addresses: 18.161.156.112 and 99.86.102.15 - Services: HTTP and SSL/HTTP on Amazon CloudFront httpd

Recommendations:
- Ensure all HTTP traffic is redirected to HTTPS. - Enable HSTS to enforce secure connections. - Regularly review open ports and services to minimize exposure.

1.3.4 SSL/TLS Protocols Security Assessment

Description:
The assessment found that all endpoints support TLS 1.3, which is considered best practice for security and performance. No endpoints were found using deprecated protocols such as SSLv3, TLS 1.0, or TLS 1.1.

Affected Assets:
- **8** endpoints using TLS 1.3. - **8** endpoints using TLS 1.2.

Recommendations:
- Continue monitoring for protocol updates and ensure compliance with industry standards. - Regularly test SSL/TLS configurations to maintain optimal security posture.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to implement a comprehensive security awareness program for employees, conduct regular vulnerability assessments, and establish a robust incident response plan. Continuous monitoring and timely updates to security protocols will help mitigate risks and protect sensitive information effectively.