1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **gitlab.com** using a Basic analysis type. The evaluation commenced on **April 30th at 13:00** and concluded in **23 minutes and 26 seconds**. The analysis aimed to identify potential security vulnerabilities within the web application and infrastructure, focusing on high and medium-risk issues.

1.2 Summary of Key Findings

The security assessment identified **4 high-risk** and **4 medium-risk** issues. Critical findings include the exposure of **1,597 leaked credentials** on the deep web, posing significant risks of phishing and unauthorized access, and the presence of unencrypted HTTP traffic, which exposes sensitive data to interception. Additionally, open FTP ports and unusual port assignments increase the attack surface. Immediate actions should focus on securing leaked credentials, enforcing HTTPS, and closing or securing vulnerable ports to mitigate these risks effectively.

1.3 Issues Table

Title	Risk
Email Addresses and/or Passwords Leaked	High
FTP Service	High
Unencrypted HTTP Traffic Detected	High
Login Form Detection Analysis	High
Unusual Port Assignments Detected	Medium
Nmap Port Scan Results Analysis	Medium
Service Density Analysis	Medium
Services Vulnerable to Brute Force Attacks	Medium

1.4 Detailed Findings

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

Description:
A total of **1,597 leaked credentials** were discovered 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's employees.

Recommendations:
Immediate steps should be taken to secure all affected accounts by enforcing password resets and implementing multi-factor authentication (MFA). Regular monitoring of deep web sources for new leaks is advised. Educate employees on recognizing phishing attempts.

1.4.2 FTP Service

Description:
An open FTP port was detected, leading to several risks including unauthorized access to sensitive files, uploading of malicious files, website defacement, denial of service attacks, cleartext

transmission of FTP traffic, exploitation of FTP server vulnerabilities, and FTP brute-force attacks for credential guessing.

Affected Assets:
- IP Address: **172.65.251.78** - Hostname: `www.gitlab.com`

Recommendations:
Close the open FTP port or replace it with a secure alternative such as SFTP or FTPS. Ensure strong password policies are enforced and consider implementing IP whitelisting for access control.

1.4.3 Unencrypted HTTP Traffic Detected

Description:
Two URLs were found using unencrypted HTTP traffic, which exposes data to interception and man-in-the-middle attacks. This lack of encryption compromises sensitive information such as login credentials.

Affected Assets:
- URLs: `http://gitlab.com/cdn-cgi/l/email-protection#`, `http://www.gitlab.com/cdn-cgi/l/email-protection#`

Recommendations:
Enforce HTTPS across all web applications by obtaining valid SSL/TLS certificates. Implement HTTP Strict Transport Security (HSTS) to ensure all traffic is encrypted.

1.4.4 Login Form Detection Analysis

Description:
A total of **8 login forms** were detected across the application, indicating a high-interest area for potential exploitation due to the increased attack surface for credential theft.

Affected Assets:
- Various URLs associated with detected login forms.

Recommendations:
Ensure all login forms are protected with HTTPS to prevent credential interception. Implement rate limiting and account lockout mechanisms to mitigate brute force attacks. Consider using CAPTCHA to deter automated login attempts.

1.4.5 Unusual Port Assignments Detected

Description:
Services were identified running on non-standard ports, which may suggest attempts to evade detection or misconfigured applications. This configuration poses a potential security risk.

Affected Assets:
- Hosts: `gitlab.com` and `www.gitlab.com` with IP **172.65.251.78**.

Recommendations:
Review and standardize port assignments to align with best practices. Implement network segmentation and firewall rules to restrict access to non-standard ports.

1.4.6 Nmap Port Scan Results Analysis

Description:
The scan identified **22 open ports**, with several associated with potentially insecure services or protocols, indicating a need for careful review.

Affected Assets:
- IP Address: **172.65.251.78**

Recommendations:
Conduct a thorough review of open ports and associated services. Close unnecessary ports and ensure secure configurations for essential services.

1.4.7 Service Density Analysis

Description:
A single host was identified with a high service density, running **11 services**, which poses a medium risk level due to the increased attack surface.
Affected Assets:
- Host IP: **172.65.251.78**
Recommendations:
Evaluate the necessity of each service running on the host and disable any that are not required. Implement network segmentation to isolate critical services.

1.4.8 Services Vulnerable to Brute Force Attacks

Description:
Six services were identified as vulnerable to brute force attacks due to lack of proper protection mechanisms like account lockout or rate limiting.
Affected Assets:
- IP Address: **172.65.251.78**
Recommendations:
Implement account lockout policies and rate limiting on all affected services. Enforce strong password policies and consider using MFA for additional security.

1.5 General Recommendations

To enhance overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, continuous monitoring, employee training on cybersecurity best practices, and adherence to industry standards such as OWASP and OSCP guidelines.