1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **stage-developer.firstdata.com**. The analysis commenced on **06-08** at **06:00** and concluded in **00h:13m:58s**. The assessment employed a Basic scan type, focusing on identifying High and Medium-risk vulnerabilities within the web application and infrastructure, utilizing methodologies aligned with OWASP and OSCP standards.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18** issues, categorized as **0** High-risk, **2** Medium-risk, **1** Low-risk, and **15** informational. The most significant findings include Medium-risk vulnerabilities related to open HTTP ports, which lack encryption and could expose sensitive data, and potentially sensitive subdomains that may provide access to critical systems. These issues necessitate immediate review and remediation to prevent unauthorised access and data breaches. Additionally, the SSL/TLS assessment revealed that while TLS 1.2 is in use, there is no support for the more secure TLS 1.3, suggesting an opportunity for protocol enhancement. The analysis also confirmed no shared hosting environments or brute-force vulnerable services, indicating a generally secure infrastructure. Prioritizing the resolution of Medium-risk issues will significantly enhance the organization's security posture.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL/TLS Protocols Security Assessment	Low

1.3.1 Nmap Port Scan Results Analysis

Description:

The Nmap port scan identified **2** open ports on the IP address **107.162.144.155**. Port **80/tcp** is associated with HTTP services that lack encryption, posing a risk of data exposure. It is crucial to verify if there is a redirection to HTTPS or if HTTP Strict Transport Security (HSTS) is enabled to mitigate this risk.

Affected Assets:

- IP: **107.162.144.155** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:

Implement HTTPS redirection for all HTTP requests. - Enable HTTP Strict Transport Security (HSTS) to enforce secure connections. - Regularly monitor and update SSL/TLS configurations to adhere to best practices.

1.3.2 Subdomain Naming Security Assessment

Description:

The assessment identified a potentially sensitive subdomain, **stage-developer.firstdata.com**, categorized under development/staging environments. Such environments may contain unpatched vulnerabilities or debug information that could be exploited by malicious actors to gain unauthorized access to critical systems.

Affected Assets:
- Subdomain: **stage-developer.firstdata.com**

Recommendations:
- Restrict access to development and staging environments using IP whitelisting or VPN. - Regularly audit and patch vulnerabilities in non-production environments. - Ensure sensitive data is not exposed in development or staging environments.

1.3.3 SSL/TLS Protocols Security Assessment

Description:
The SSL/TLS assessment revealed that the endpoint supports TLS 1.2 but lacks support for TLS 1.3, which is considered the current best practice for enhanced security and performance.

Affected Assets:
- Endpoint using TLS 1.2

Recommendations:
- Upgrade to support TLS 1.3 to improve security and performance. - Regularly review and update cryptographic protocols to align with industry standards.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to prioritize the remediation of Medium-risk issues identified in this assessment. Implementing HTTPS with HSTS, securing development environments, and upgrading to TLS 1.3 are critical steps in mitigating potential risks. Continuous monitoring and regular updates of security configurations will further safeguard against emerging threats.