[APM0002754] HK.APP.LDA.HKG.Co-loader track and trace Security Test Report

Version 1.0

Restricted

Table of Contents

Version Control

Version number	Date	Prepared by	Reviewed by
1.0	30-05-2025	Sindam Naresh	Rajesh Munimadugu

1 Introduction

1.1 Scope of Work

Information Security Services was engaged to perform a Mobile assessment based on OWASP Top 10 Mobile standards and Testing Guide Checklist for DHL Express on OPS TMS NEW Application. The tools used during penetration testing include BurpSuite, SSLScan, SQLmap, as well as any other tools identified as necessary by the tester to ensure a thorough security assessment.

Vulnerabilities tests included in the assessment:

OWASP Top 10 - Web (2021)

- A01 Broken Access Control
- A02 Cryptographic Failures
- A03 Injection
- A04 Insecure Design
- A05 Security Misconfiguration
- A06 Vulnerable and Outdated Components
- A07 Identification and Authentication Failures
- A08 Software and Data Integrity Failures
- A09 Security Logging and Monitoring Failures
- A10 Server-Side Request Forgery (SSRF)

1.2 Test Environment

The objectives of the assessment consisted of the following activities defined prior the start of the engagement:

Application ID	APM0002754
Application Name	HK.APP.LDA.HKG.Co-loader track and trace
Application Interfacing	External
Test Scope	Web Manual PenTest
Production URL	https://apps.dhl.com.hk/eng_st/eng_track_home.html

Test Duration	Application Environment	Target	Test Authentication	Note
26 May2025 – 30May2025	Test	Web – UAT https://mykullstc000536.apis.dhl.com/eng_st/eng_track_home.html	User accounts: Not Required	Initial test done by Naresh

1.3 Disclaimer

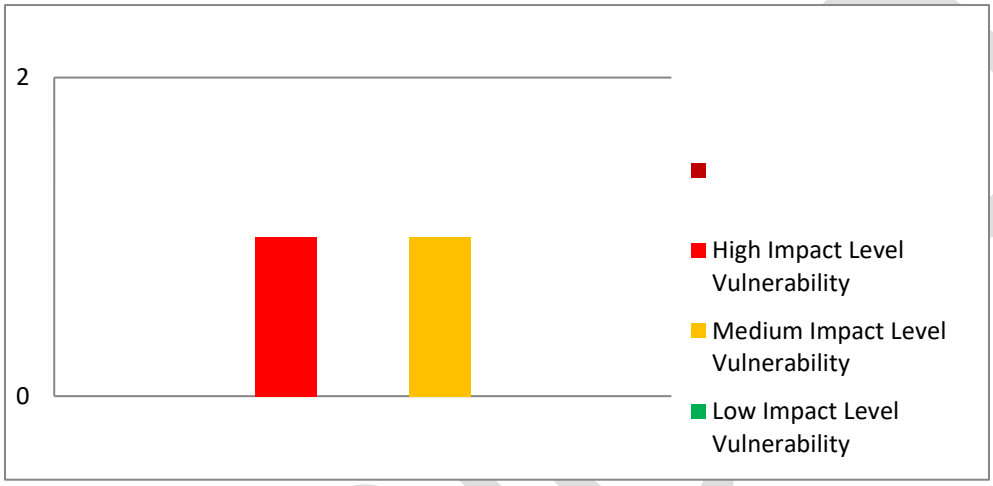
The testing was performed at a "point-in-time" that followed OWASP Top 10 methodologies. The testing is not intended to identify all existing vulnerabilities and security weaknesses, nor does it claim or represent that any applications are free of vulnerabilities or immune to attacks. The security test included Dynamic Application Security Testing (DAST) and was conducted exclusively on the application layer. This report is created solely for the use and benefit of DHL Express and should not be disclosed to any third parties, nor may it be relied upon by any parties other than DHL Express. Any application maintenance, reconfigurations, or changes in general that have occurred following the assessment, may alter the findings and recommendations in this report.

BitSight score is an independent security rating of companies which is closely monitored by DHL customers, investors, vendors. BitSight related vulnerabilities can have significant impact on DHL security posture and reputation, affecting the business and potentially leading to breaches or compromised data.
It is crucial to address all vulnerabilities in timely manner to mitigate the risks. Please consider them equally important in case of internally facing applications. Those are exposed to internal threat and at some point may be also exposed to outside DHL network (planned, deliberate or by accident).

2 Executive Summary

2.1 General Impression

The breakdown of server security vulnerabilities discovered. A total of one (1) high and one (1) medium impact level vulnerabilities were discovered.



Remaining Open Pentest Findings (From Previous Pentests)

Finding ID	Finding Title	Severity

New Pentest Findings

No	Findings	Severity	(CVSS) Version 3.1 Score	STATUS
1	Support for Deprecated TLS Protocols and Weak Cipher Suites	High	8.2	Open
2	Misconfigured CSP	Medium	4.3	Open

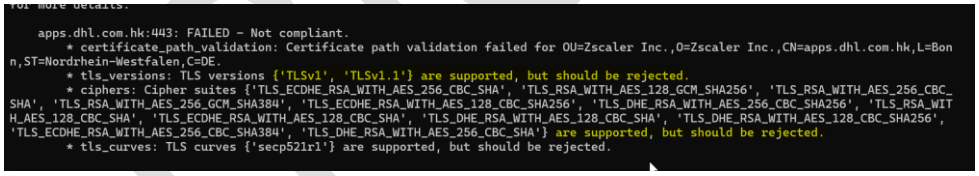
3 Detailed Technical Findings

3.1 Detailed Penetration Test Findings

This section contains details of the security weaknesses, associated risks and recommendations to reduce the exposures identified during the web application penetration testing.

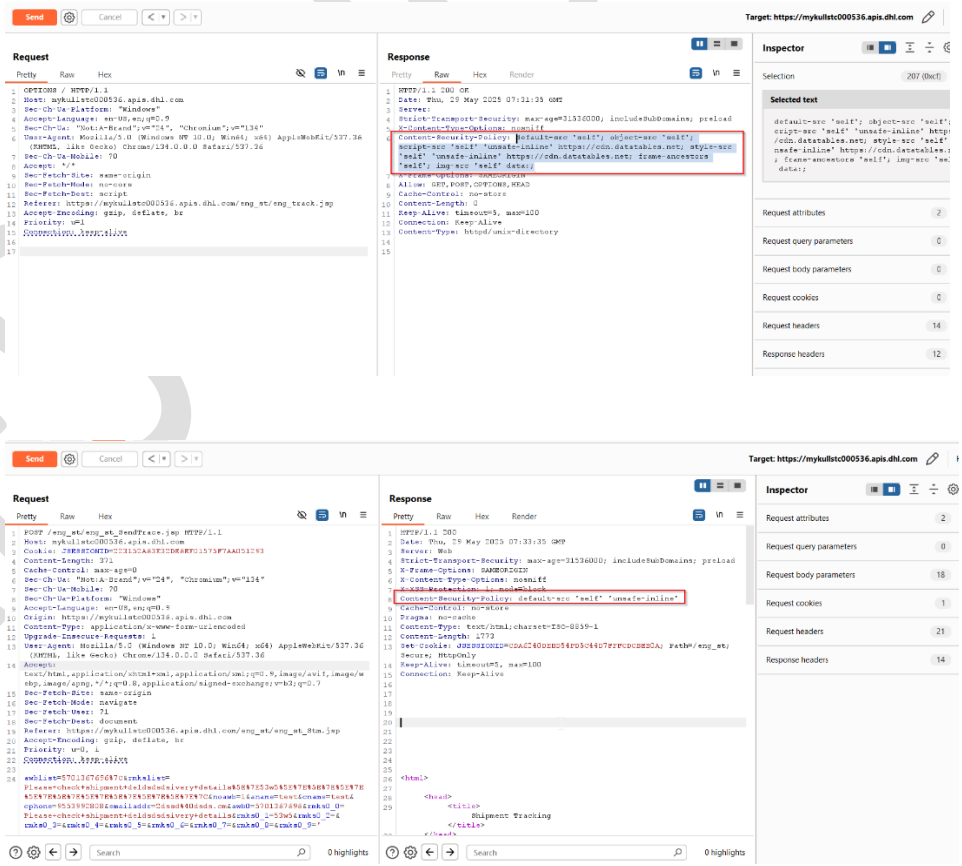
3.1.1 Support for Deprecated TLS Protocols and Weak Cipher Suites

Finding	**Support for Deprecated TLS Protocols and Weak Cipher Suites**	***Open***
OWASP Category	**A02:2021-Cryptographic Failures**	
Relative Risk	**High**	
Description	The server at apps.dhl.com.hk:443 was found to support multiple insecure TLS configurations, including both deprecated protocol versions and weak cipher suites. Deprecated TLS Protocols: TLS 1.0 TLS 1.1 These protocols are formally deprecated (RFC 8996) and no longer receive security updates. While modern browsers and clients may avoid negotiating these versions, their continued availability increases the risk of downgrade attacks and regulatory non-compliance (e.g., PCI DSS, NIST SP 800-52r2). Weak Cipher Suites: The server supports several outdated and weak cipher suites, such as: CBC-mode ciphers (AES_128_CBC_SHA, AES_256_CBC_SHA) RSA-based key exchange (TLS_RSA_*) Diffie-Hellman Ephemeral (DHE) with low security margins These ciphers may be susceptible to known attacks like BEAST, Lucky13, and SWEET32, and lack Forward Secrecy, which is a modern requirement for secure communication. Affected Asset: PROD Domain https://apps.dhl.com.hk/eng_st/eng_track_home.html	
Impact	○ Increases exposure to **downgrade attacks**, where an attacker can coerce a connection into using a weaker protocol or cipher. ○ Non-compliance with modern industry standards such as: PCI DSS v4.0 NIST SP 800-52r2	

	○ OWASP Secure Configuration Guidelines ○ Could result in reputational and legal risk in regulated industries.
Remediation, Recommendations & References	**Server Configuration Hardening:** 1. **Disable deprecated protocols**: Remove TLSv1.0 and TLSv1.1 from the list of accepted protocols. 2. **Enforce minimum TLS 1.2 or higher**: Prefer TLSv1.3 where supported. 3. **Restrict cipher suites** to strong, modern configurations: ○ Enable only AEAD ciphers such as: ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_AES_128_GCM_SHA256 (TLS 1.3) ▪ TLS_CHACHA20_POLY1305_SHA256 ○ Ensure Forward Secrecy via ECDHE 4. **Remove weak elliptic curves**: Retain only X25519 and secp256r1.
Detailed Evidence / Exploitation Steps	**POC:** The following insecure elements were detected when tested on PROD domain using "sslyze". PFB snapshot. 

3.1.2 Misconfigured CSP (BitSight related)

Finding	**Misconfigured CSP**	***Open***
OWASP Category	**A02:2021-Cryptographic Failures**	
Relative Risk	**Medium**	
Description	Content Security Policy (CSP) is a security misconfiguration where a web application does not implement a Content Security Policy header, leaving it vulnerable to attacks such as Cross-Site Scripting (XSS), data injection, and clickjacking. CSP is a browser-based security feature that restricts the sources from which scripts, styles, and other resources can be loaded. Affected Asset: https://mykullstc000536.apis.dhl.com/eng_st/eng_track_home.html	
Impact	1. Increased Risk of XSS Attacks – Without CSP, attackers can inject malicious scripts that execute in users' browsers.	

	2. Clickjacking & UI Redressing – Attackers can frame a site and trick users into interacting with hidden elements.
Remediation, Recommendations & References	Kindly implement additional Security Header to make the application more secure. For more information, refer to: https://owasp.org/www-project-secure-headers/#div-bestpractices Content-Security-Policy: default-src 'self'; script-src 'self' 'nonce-<randomNonce>' 'strict-dynamic'; object-src 'none'; base-uri 'none'; form-action 'self'; frame-ancestors 'none'; upgrade-insecure-requests; block-all-mixed-content;
Detailed Evidence /Exploitation Steps	POC: Capture the request of any of the page to observe the CSP directives in HTTP response as shown below. 

4 Appendix: Web application Test Cases

1.0 INFORMATION GATHERING	
Manually explore the site (test user roles, application logic)	Passed
Crawl site for missed or hidden content	Passed
Identify application entry points	Passed
Perform Web Application Fingerprinting	Passed
Identify technologies used	Passed
2.0 CONFIGURATION MANAGEMENT	
Check for commonly used application and administrative URLs	NA
Check for old, backup and unreferenced files	NA
Test file extensions handling	Passed
Test for security HTTP headers (e.g. X-Frame-Options, HSTS, referrer) [BitSight Related]	passed
Test for HTTP Methods	Passed
Test for Cross-Domain Sub resource Integrity Check [BitSight Related]	Passed
Test for Cross-Domain Sub resource Integrity Failure [BitSight Related]	Passed
Test for Content Security Policy Configurations [BitSight Related]	Passed
Test for Content Security Policy Violations [BitSight Related]	Failed
Test for JavaScript Libraries with Known Vulnerabilities [BitSight Related]	passed
Test for Software with Known Vulnerabilities	Passed
3.0 SESSION MANAGEMENT	
Testing for Cookie Attributes (Secure, samesite flag) [BitSight Related]	Passed
Testing for CSRF	Passed
Check for Session Token in URL [BitSight Related]	Passed
Testing for Password recovery/reset vulnerabilities	Passed
Testing for Session Timeout	Passed
Testing for Session Fixation	Passed
Testing for CSRF tokens missing[BitSight Related](Only if CSRF present)	passed
3.0 SECURE TRANSMISSION	
Check SSL Version and Weak Ciphers [BitSight Related]	Failed
Check for Digital Certificate Validity (Duration, Signature and CN)	passed
Authentication on Insecure Channel [BitSight Related]	passed
Mixed Content [BitSight Related]	passed
4.0 ERROR HANDLING	
Testing for Improper Error Handling (Internal Server Error, Stack Traces) [BitSight Related]	passed
4.0 AUTHENTICATION	
Test for user enumeration	passed
Test for authentication bypass	passed
Test for default logins	passed
Test for brute force protection	passed
Test password quality rules	passed
CMS Administration Portal Exposed [BitSight Related]	passed
External Service Interaction (DNS/HTTP/HTTPS)	passed
User registration related vulnerabilities	passed
5.0 AUTHORIZATION	
Testing for Horizontal access issue (IDOR)	passed
Testing for Vertical access issues (privilege escalation)	passed
Sensitive information disclosure in GET URI	passed
Test for missing authorization	passed
Testing for Directory Listing [BitSight Related]	passed
6.0 CLIENT-SIDE	
Testing for CORS (CORS violation, Overly Permissive CORS) [BitSight Related]	passed

Testing for HTML injection	passed
Testing for Reverse Tabnabbing [BitSight Related]	passed

7.0 DATA VALIDATION	
Testing for injection (SQL, XSS, XXE,SSRF etc)	**Passed**
Testing for command injection	**Passed**
Testing for Open Redirection	**Passed**
Testing on File Upload	**Passed**
Testing for Local File Inclusion	**Passed**
Testing for HTTP Request Smuggling	**Passed**
8.0 BUSINESS LOGIC	
Test for feature misuse	**Passed**
Test for trust relationships (access control for user performing certain action)	**Passed**
Test for integrity of data	**Passed**