



[APM0002772]
HK.APP.LDA.HKG.Flight
Information
Security Test Report

Version 1.0

Restricted

Table of Contents

1	Introduction	3
1.1	Scope of Work.....	3
1.2	Test Environment.....	4
1.3	Disclaimer.....	4
2	Executive Summary	5
2.1	General Impression	5
3	Detailed Technical Findings	6
3.1	Detailed Penetration Test Findings	6
3.1.1	Weak Cipher Suite Supported [BitSight Related]	6
3.1.2	Missing Referrer-Policy Headers [BitSight Related]	8
3.1.3	Cookies Missing 'SameSite' Attributes [BitSight Related].....	9
4	Appendix : Web application Test Cases	10

Version Control

Version number	Date	Prepared by	Reviewed by
1.0	23/05/2025	Hariprasanth.R	Rajesh Kumar Munimadugu

1 Introduction

1.1 Scope of Work

Information Security Services was engaged to perform a Web application assessment based on OWASP Top 10 Web standards and Testing Guide Checklist for DHL Express on HK.APP.LDA.HKG.Flight Information 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- A06 Vulnerable and Outdated Components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	APM0002772
Application Name	HK.APP.LDA.HKG.Flight Information
Application Interfacing	External
Test Scope	Web
Production URL	https://apps.dhl.com.hk/eng_fi

Test Duration	Application Environment	Target	Test Authentication	Note
20 May 2025 - 23 May 2025	UAT	https://mykullstc000536.apis.dhl.com/eng_fi/	User accounts: Not Required	Initial test done by Hariprasanth.R

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.

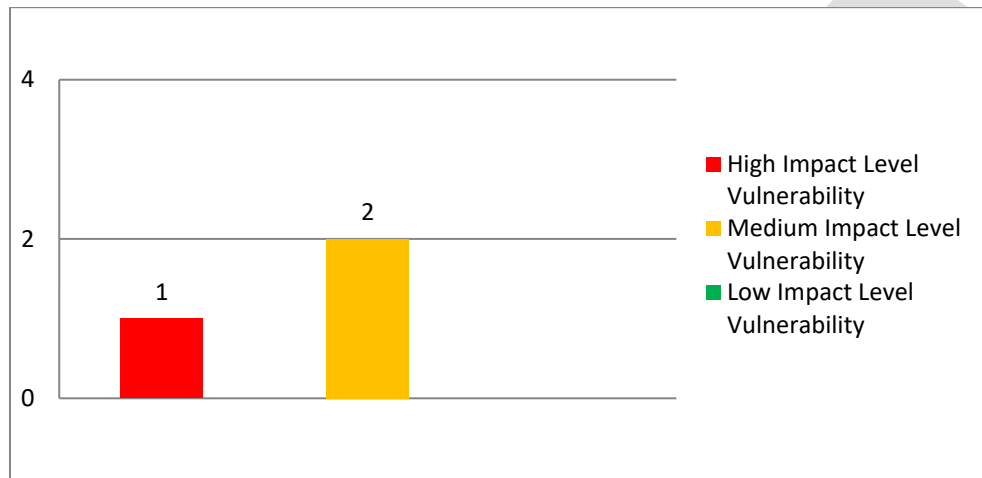
BitSight score is an independent security rating of companies which is closely monitored by DHL customers, investors, vendors. BitSight related vulnerabilities can have significant impact on DHL security posture and reputation, affecting the business and potentially leading to breaches or compromised 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 impact level and two (2) 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	Weak Cipher Suite Supported	High	7.6	Open
2	Missing Referrer-Policy Headers	Medium	5.4	Open
3	Cookies Missing 'SameSite' Attributes	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 Weak Cipher Suite Supported [[BitSight Related](#)]

Finding	Weak Cipher Suite Supported [BitSight Related]	Open
OWASP Category	A02:2021 – Cryptographic Failures	
Relative Risk	HIGH	
Description	<p>Observed that weak Cipher {'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA', 'TLS_RSA_WITH_AES_128_CBC_SHA', 'TLS_DHE_RSA_WITH_AES_128_CBC_SHA', 'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA', 'TLS_RSA_WITH_AES_256_GCM_SHA384', 'TLS_RSA_WITH_AES_256_CBC_SHA', 'TLS_DHE_RSA_WITH_AES_128_CBC_SHA256', 'TLS_DHE_RSA_WITH_AES_256_CBC_SHA'} are supported, but should be rejected. Depending on the configuration of the server and any intervening caching devices, it may also be possible to use this for cache poisoning attacks.</p> <div> Affected Assets: https://apps.dhl.com.hk/eng_fi </div>	
Impact	<p>The use of weak cipher suites exposes the application to significant security risks. Exploitation of the Lucky 13 vulnerability could lead to unauthorized access to sensitive data transmitted over the insecure connection. Additionally, the susceptibility to man-in-the-middle attacks raises concerns about data integrity and confidentiality.</p>	
Remediation, Recommendations & References	<p>Below are some countermeasures that can be taken to remediate this vulnerability.</p> <ul style="list-style-type: none"> • Disable the Use of above-mentioned ciphers. • Try to update the TLS version to 1.3, to disable all vulnerable CBC ciphers by default. 	
Detailed Evidence / Exploitation Steps	<p>Host: https://apps.dhl.com.hk/eng_fi</p> <p>Steps to Reproduce</p> <ol style="list-style-type: none"> 1. Use Sslyze tool and verify the weak cipher suites. <pre> apps.dhl.com.hk:443: FAILED - Not compliant. * certificate_path_validation: Certificate path validation failed for OU=Zscaler Inc.,O=Zscaler Inc.,CN=apps.dhl.com.hk,L=Bonn,ST=Nordrhein-Westfalen,C=DE. * tls_versions: TLS versions {'TLSv1.1', 'TLSv1'} are supported, but should be rejected. * ciphers: Cipher suites {'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA', 'TLS_RSA_WITH_AES_128_CBC_SHA', 'TLS_DHE_RSA_WITH_AES_128_CBC_SHA', 'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA', 'TLS_RSA_WITH_AES_256_GCM_SHA384', 'TLS_RSA_WITH_AES_256_CBC_SHA', 'TLS_DHE_RSA_WITH_AES_128_CBC_SHA256', 'TLS_DHE_RSA_WITH_AES_256_CBC_SHA', 'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384'} are supported, but should be rejected. * tls_curves: TLS curves {'secp256r1'} are supported, but should be rejected. </pre>	

2. Use ssllscan tool and verify the SSL Protocols.

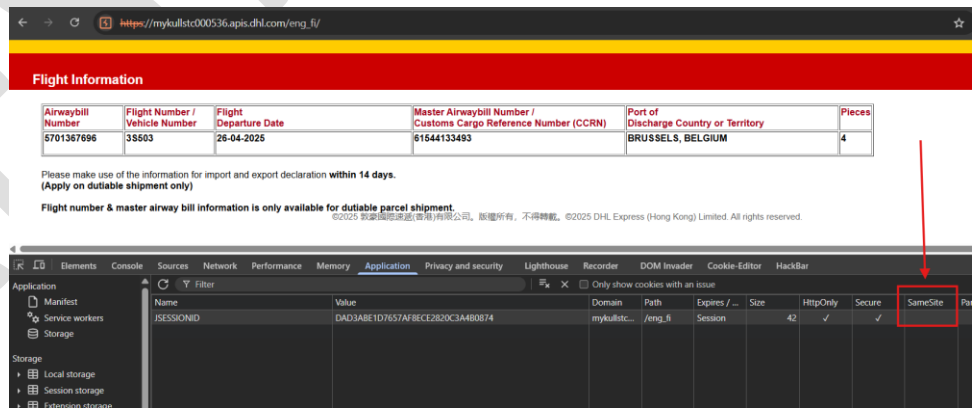
```
Connected to 199.40.254.11
Testing SSL server apps.dhl.com.hk on port 443 using SNI name apps.dhl.com.hk

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    enabled
TLSv1.1    disabled
TLSv1.2    enabled
TLSv1.3    enabled
```

3.1.2 Missing Referrer-Policy Headers [\[BitSight Related\]](#)

Finding	Missing Referrer-Policy Headers [BitSight Related]		Open				
OWASP Category	A05:2021 – Security Misconfiguration						
Relative Risk	MEDIUM						
Description	<p>Referrer-Policy controls how much referrer information is included in requests made by the browser. This can help protect sensitive data by restricting the exposure of referral information.</p> <div>Affected Assets: https://mykullstc000536.apis.dhl.com/eng_fi/</div>						
Impact	<ul style="list-style-type: none">Information Leakage: A missing Referrer-Policy can unintentionally expose sensitive information in the referrer header, such as session data or URLs containing sensitive parameters						
Remediation, Recommendations & References	<p>Following is the recommended value for missing header:</p> <table><tr><td>Header name</td><td>Proposed value</td></tr><tr><td>Referrer-Policy</td><td>no-referrer-when-downgrade</td></tr></table>			Header name	Proposed value	Referrer-Policy	no-referrer-when-downgrade
Header name	Proposed value						
Referrer-Policy	no-referrer-when-downgrade						
Detailed Evidence / Exploitation Steps	<p>Host: https://mykullstc000536.apis.dhl.com/eng_fi/</p> <p>Steps to Reproduce</p> <ol style="list-style-type: none">1. Open the web application in your browser.2. Start a proxy tool like Burp Suite or OWASP ZAP.3. Capture the HTTP requests sent by the browser to the server.4. Inspect the response headers for each request.5. Check the Referrer-Policy headers are missing. <pre>HTTP/1.1 200 Date: Fri, 23 May 2025 04:26:28 GMT Server: Web Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-Security-Policy: default-src 'self' 'unsafe-inline' Cache-Control: no-store Pragma: no-cache Content-Type: text/html; charset=ISO-8859-1 Content-Length: 2813 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive</pre>						

3.1.3 Cookies Missing 'SameSite' Attributes [\[BitSight Related\]](#)

Finding	Cookies Missing 'SameSite' Attributes [BitSight Related]	Open
OWASP Category	A05:2021 – Security Misconfiguration	
Relative Risk	MEDIUM	
Description	<p>Cookies missing the 'SameSite' attributes can lead to security vulnerabilities.</p> <ul style="list-style-type: none"> SameSite restricts the cookie to same-origin requests to protect against Cross-Site Request Forgery (CSRF) attacks. <div> <p>Affected Assets:</p> <p>https://mykullstc000536.apis.dhl.com/eng_fi/</p> </div>	
Impact	<ul style="list-style-type: none"> CSRF Vulnerability: Cookies without the SameSite attribute can be sent with cross-origin requests, making the application susceptible to CSRF attacks. 	
Remediation, Recommendations & References	<ul style="list-style-type: none"> Set 'SameSite' to 'Strict' or 'Lax' to restrict cross-site requests. <p>Reference</p> <p>SameSite cookies explained Articles web.dev</p>	
Detailed Evidence / Exploitation Steps	<p>Host: https://mykullstc000536.apis.dhl.com/eng_fi/</p> <p>Steps to Reproduce</p> <ol style="list-style-type: none"> Use browser developer tools or a tool like Burp Suite to inspect the cookies set by the application. Identify the cookie that is missing the SameSite attribute. 	

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	Passed
Check for old, backup and unreferenced files	Passed
Test file extensions handling	Passed
Test for security HTTP headers (e.g. X-Frame-Options, HSTS, referrer) [BitSight Related]	Failed
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]	Passed
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]	Failed
Testing for CSRF	N/A
Check for Session Token in URL [BitSight Related]	N/A
Testing for Password recovery/reset vulnerabilities	N/A
Testing for Session Timeout	N/A
Testing for Session Fixation	N/A
Testing for CSRF tokens missing [BitSight Related] (Only if CSRF present)	N/A
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]	N/A
Mixed Content [BitSight Related]	N/A
4.0 ERROR HANDLING	
Testing for Improper Error Handling (Internal Server Error, Stack Traces) [BitSight Related]	Passed
4.0 AUTHENTICATION	
Test for user enumeration	N/A
Test for authentication bypass	N/A
Test for default logins	N/A
Test for brute force protection	N/A
Test password quality rules	N/A
CMS Administration Portal Exposed [BitSight Related]	N/A
External Service Interaction (DNS/HTTP/HTTPS)	N/A
User registration related vulnerabilities	N/A
5.0 AUTHORIZATION	
Testing for Horizontal access issue (IDOR)	N/A
Testing for Vertical access issues (privilege escalation)	N/A
Sensitive information disclosure in GET URI	N/A
Test for missing authorization	N/A
Testing for Directory Listing [BitSight Related]	Passed
6.0 CLIENT-SIDE	
Testing for CORS (CORS violation, Overly Permissive CORS) [BitSight Related]	N/A
Testing for HTML injection	Passed
Testing for Reverse Tabnabbing [BitSight Related]	Passed

7.0 DATA VALIDATION	
Testing for injection (SQL, XSS, XSE,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	N/A
Test for trust relationships (access control for user performing certain action)	N/A
Test for integrity of data	N/A