[APM0002782] HK.APP.HomepageWaybillPrinting Security Test Report

Version 2.0

Restricted

Table of Contents

Version Control

Version number	Date	Prepared by	Reviewed by
1.0	01/08/2024	Mohan Ram Moola Vidya Sagar	Rajesh Kumar Munimadugu
2.0	03/09/2024	Mohan Ram Moola Vidya Sagar	Rajesh Kumar Munimadugu

1 Introduction

1.1 Scope of Work

Information Security Services was engaged to perform a WEB security assessment based on OWASP Top 10 WEB standards and Testing Guide Checklist for DHL Express on HK.APP.HomepageWaybillPrinting Application.

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- A06 Vulnerable and Outdated Components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 APM Number	APM0002782
Application Name	HK.APP.HomepageWaybillPrinting
Application Interfacing	Internal
Test Scope	WEB

Test Duration	Application Environment	Target	Test Authentication	Note
24 July 2024 – 01 Aug 2024	Test	UAT: https://mykullstc000536.apis.dhl.com/print_waybill PROD: https://apps.dhl.com.hk/print_waybill	Test Credentials	Full Test
03 Sep 2024 – 03 Sep 2024	Test	UAT: https://mykullstc000536.apis.dhl.com/print_waybill PROD: https://apps.dhl.com.hk/print_waybill	Test Credentials	Retest – High Finding

1.3 Disclaimer

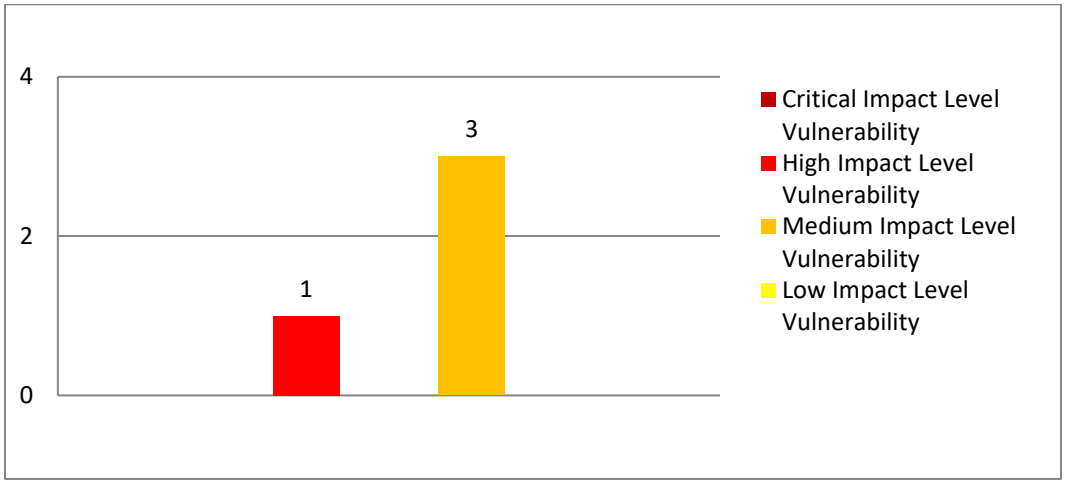
The testing was performed at a "point-in-time" that followed OWASP Top 10 methodologies. The testing is not intended to identify all existing vulnerabilities and security weaknesses, nor does it claim or represent that any applications are free of vulnerabilities or immune to attacks. This report is 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 three (3) medium impact level vulnerabilities were discovered.



Remaining Open Pentest Findings in GSN (From Previous Pentests)

Finding ID	Finding Title	Risk Rating

New Pentest Findings

No	Findings	Severity	(CVSS) Version 3.1 Score	STATUS
1	Weak Ciphers	High	7.1	Closed
2	Improper Implementation of Content-Security-Policy Header [BitSight Related]	Medium	6.5	Open
3	Improper Session Management	Medium	5.4	Open
4	Improper Cookies Attributes - [BitSight Related]	Medium	4.3	Open

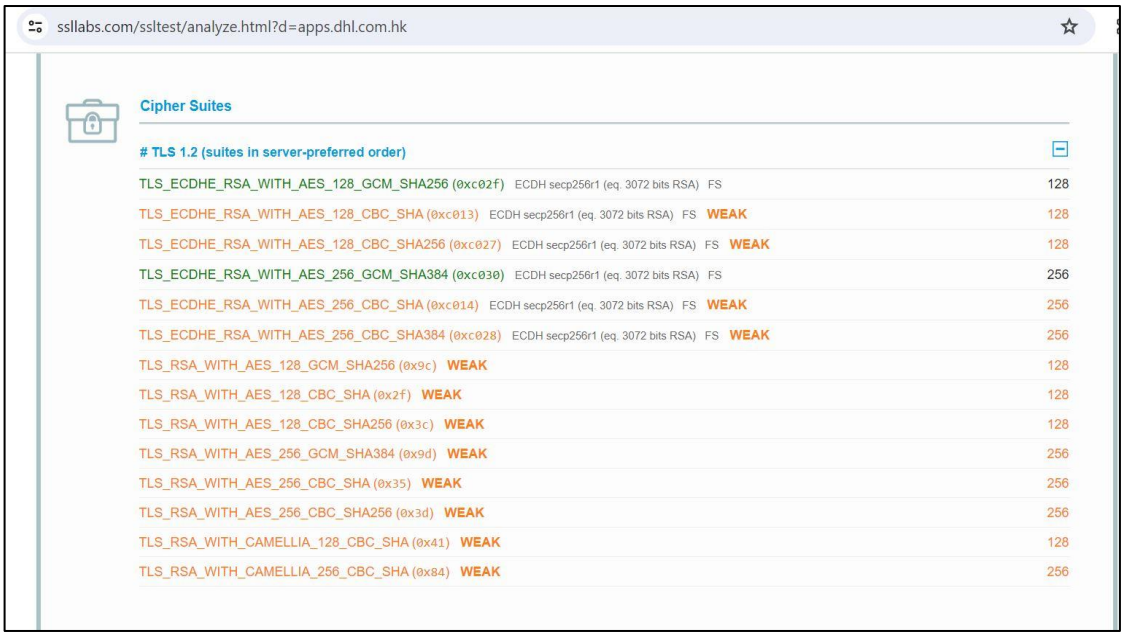
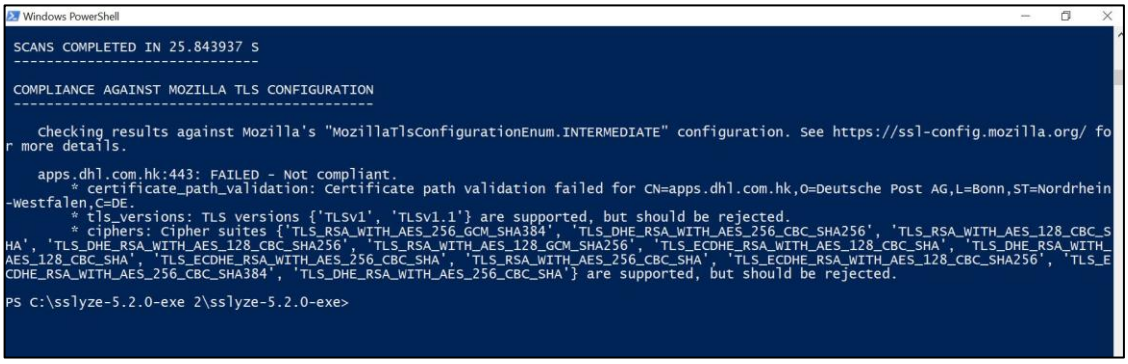
3 Detailed Technical Findings

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 Ciphers

Finding	**Weak Ciphers**	**Closed**
OWASP Category	**A05:2021 – Security Misconfiguration**	
Relative Risk	**HIGH**	
Description	The server accepts the following weak cipher suites: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA These cipher suites are deemed weak due to their use of vulnerable encryption methods or modes. For example, some use the CBC (Cipher Block Chaining) mode, which is susceptible to Padding Oracle Attack and LUCKY13 Attack. Affected Assets: PROD: https://apps.dhl.com.hk/print_waybill UAT: https://mykullstc000536.apis.dhl.com/print_waybill	
Impact	The impact of this vulnerability is severe, posing a high risk of compromising the confidentiality and integrity of data exchanged between the server and the client. An attacker intercepting network traffic could exploit these weaknesses to decrypt ciphertexts, potentially gaining unauthorized access to sensitive information like user details, etc.	

Remediation, Recommendations & References	Below are some countermeasures that can be taken to remediate this vulnerability. • 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	Scan the host in SSL Labs: https://apps.dhl.com.hk/ and observe that the tool has flagged that the server is supporting the highlighted weak cipher suites with flagging potential LUCKY 13 vulnerabilities.  Scan the host in sslyze: https://apps.dhl.com.hk/ and observe that the tool has flagged that the server is supporting the highlighted weak cipher suites with flagging potential LUCKY 13 vulnerabilities. 

ssllabs.com/ssltest/analyze.html?d=apps.dhl.com.hk

Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	WEAK	256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	WEAK	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	WEAK	256

Windows PowerShell

```
 SCANS COMPLETED IN 25.843937 S
 ------------------------------

 COMPLIANCE AGAINST MOZILLA TLS CONFIGURATION
 --------------------------------------------

    Checking results against Mozilla's "MozillaTlsConfigurationEnum.INTERMEDIATE" configuration. See https://ssl-config.mozilla.org/ fo
r more details.

    apps.dhl.com.hk:443: FAILED - Not compliant.
        * certificate_path_validation: Certificate path validation failed for CN=apps.dhl.com.hk,O=Deutsche Post AG,L=Bonn,ST=Nordrhein
-Westfalen,C=DE.
        * tls_versions: TLS versions {'TLSv1', 'TLSv1.1'} are supported, but should be rejected.
        * ciphers: Cipher suites {'TLS_RSA_WITH_AES_256_GCM_SHA384', 'TLS_DHE_RSA_WITH_AES_256_CBC_SHA256', 'TLS_RSA_WITH_AES_128_CBC_S
HA', 'TLS_DHE_RSA_WITH_AES_128_CBC_SHA256', 'TLS_RSA_WITH_AES_128_GCM_SHA256', 'TLS_ECDHE_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_CBC_SHA', 'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256', 'TLS_E
CDHE_RSA_WITH_AES_256_CBC_SHA384', 'TLS_DHE_RSA_WITH_AES_256_CBC_SHA'} are supported, but should be rejected.

PS C:\sslyze-5.2.0-exe 2\sslyze-5.2.0-exe>
```

```
Windows PowerShell
* TLS 1.2 Cipher Suites:
    Attempted to connect using 156 cipher suites.

    The server accepted the following 16 cipher suites:
       TLS_RSA_WITH_AES_256_GCM_SHA384                 256
       TLS_RSA_WITH_AES_256_CBC_SHA                    256
       TLS_RSA_WITH_AES_128_GCM_SHA256                 128
       TLS_RSA_WITH_AES_128_CBC_SHA                    128
       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384           256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384           256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA              256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256           128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256           128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA              128       ECDH: prime256v1 (256 bits)
       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384             256       DH (2048 bits)
       TLS_DHE_RSA_WITH_AES_256_CBC_SHA256             256       DH (2048 bits)
       TLS_DHE_RSA_WITH_AES_256_CBC_SHA                256       DH (2048 bits)
       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256             128       DH (2048 bits)
       TLS_DHE_RSA_WITH_AES_128_CBC_SHA256             128       DH (2048 bits)
       TLS_DHE_RSA_WITH_AES_128_CBC_SHA                128       DH (2048 bits)

    The group of cipher suites supported by the server has the following properties:
      Forward Secrecy                    OK - Supported
      Legacy RC4 Algorithm               OK - Not Supported
```

Retest Notes – 03.09.2024: Closed

Now there are no weak ciphers in web application.

Scan the host in SSL Labs: https://apps.dhl.com.hk/ and observed that there are no weak ciphers.

```
ssllabs.com/ssltest/analyze.html?d=apps.dhl.com.hk&hideResults=on

Cipher Suites

# TLS 1.2 (suites in server-preferred order)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)  ECDH secp256r1 (eq. 3072 bits RSA)  FS   128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)  ECDH secp256r1 (eq. 3072 bits RSA)  FS   256
```

Scan the host in sslyze: https://apps.dhl.com.hk/ and observed that there are no weak ciphers.

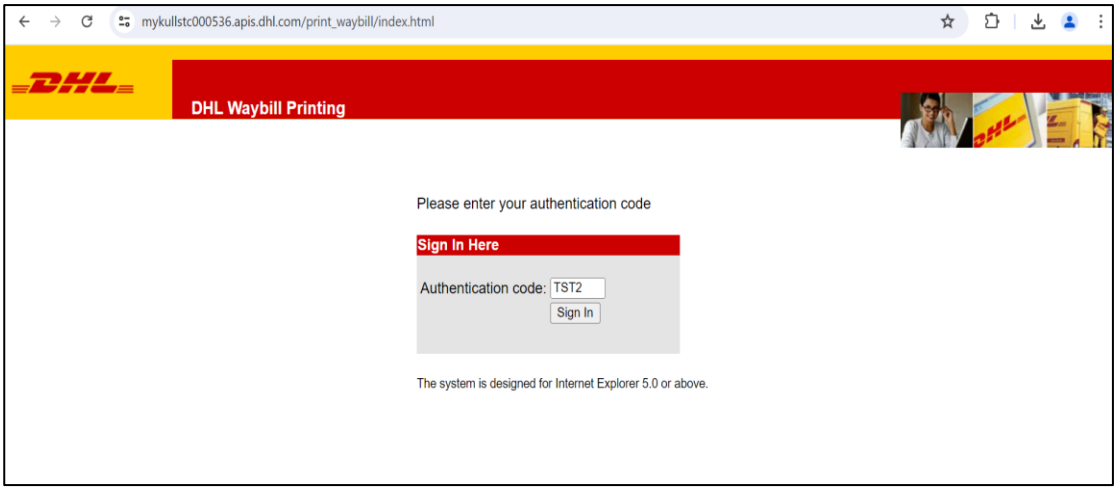
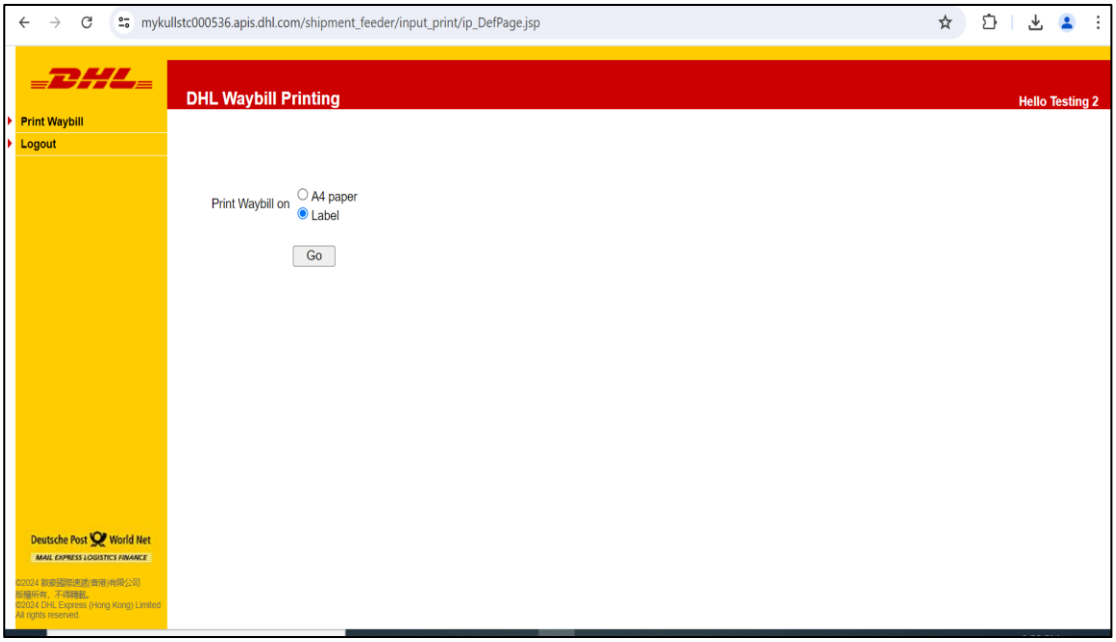
```
Windows PowerShell
 SCANS COMPLETED IN 58.329734 S
 -------------------------------

 COMPLIANCE AGAINST MOZILLA TLS CONFIGURATION
 ---------------------------------------------

    checking results against Mozilla's "MozillaTlsConfigurationEnum.INTERMEDIATE" configuration. See https://ssl-config.mozilla.org/ fo
r more details.

    apps.dhl.com.hk:443: OK - Compliant.

PS C:\sslyze-5.2.0-exe 2\sslyze-5.2.0-exe>
```

```
Windows PowerShell

* TLS 1.2 Cipher Suites:
    Attempted to connect using 156 cipher suites.

    The server accepted the following 2 cipher suites:
       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384            256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256            128       ECDH: prime256v1 (256 bits)

    The group of cipher suites supported by the server has the following properties:
      Forward Secrecy                    OK - Supported
      Legacy RC4 Algorithm               OK - Not Supported
```

3.1.2 Improper Implementation of Content-Security-Policy Header [BitSight Related]

Finding	**Improper Implementation of Content-Security-Policy Header** [BitSight Related]	**Open**
OWASP Category	**A05:2021 – Security Misconfiguration**	
Relative Risk	**Medium**	
Description	Security headers play a vital role in enhancing web communication protection against online threats. These code snippets in HTTP responses guide web browsers in their interactions with a website. In Web security, implementing proper security headers is crucial for safeguarding sensitive data and ensuring communication integrity between clients and servers. These headers act as directives that bolster the security of web applications, addressing vulnerabilities like XSS, CORS, etc. They specify how browsers should handle aspects of the web page response. The absence of these security headers makes Web more vulnerable to malicious activities and potential exploitation. While assessment, it was found that Improper Implementation of Content-Security-Policy from the response headers. • Content-Security-Policy (CSP) Affected Assets: https://mykullstc000536.apis.dhl.com/print_waybill	
Impact	The absence of crucial security headers in a web app response poses a significant risk to its security. Without these protective directives, the app becomes more vulnerable to various cyber threats, Cross Site Scripting (XSS) attack, potentially leading to unauthorized access, data breaches and other malicious activities. Security headers play a pivotal role in fortifying the defense mechanisms and their absence increases the likelihood of exploitation and compromises the overall security posture of the system.	
Remediation, Recommendations & References	To remediate the issue of Improper Implementation of Content-Security-Policy header in web application responses, the following steps can be taken: Kindly implement the below recommended CSP values in the response headers:	

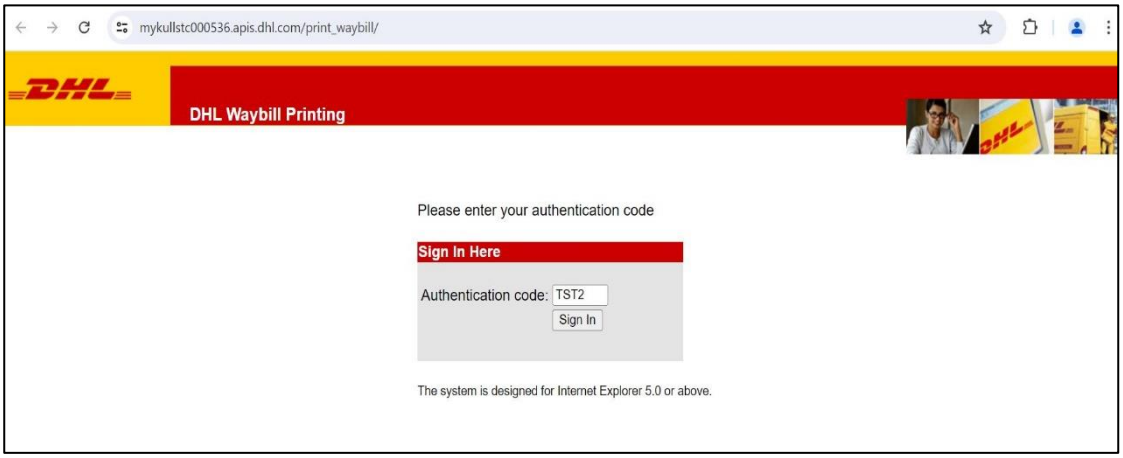
Header name	Proposed value
Content-Security-Policy	default-src 'self'; object-src 'none'; frame-ancestors 'none'; upgrade-insecure-requests; block-all-mixed-content

Detailed Evidence / Exploitation Steps	Kindly check the evidence for Burp Response. Login into an app: https://mykullstc000536.apis.dhl.com/print_waybill  

Captured the below request in Burp and observed that CSP Security headers are not properly implemented in the response headers.

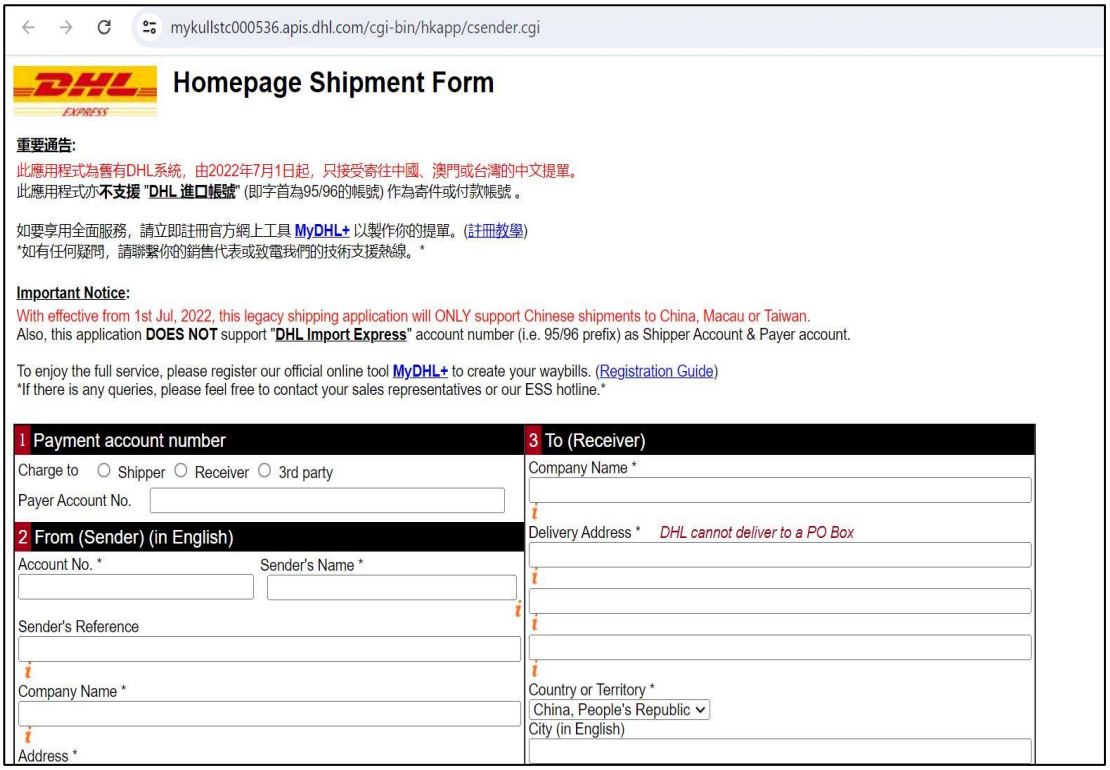
https://mykullstc000536.apis.dhl.com/shipment_feeder/input_print/ip_DefPage.jsp

3.1.3 Improper Session Management

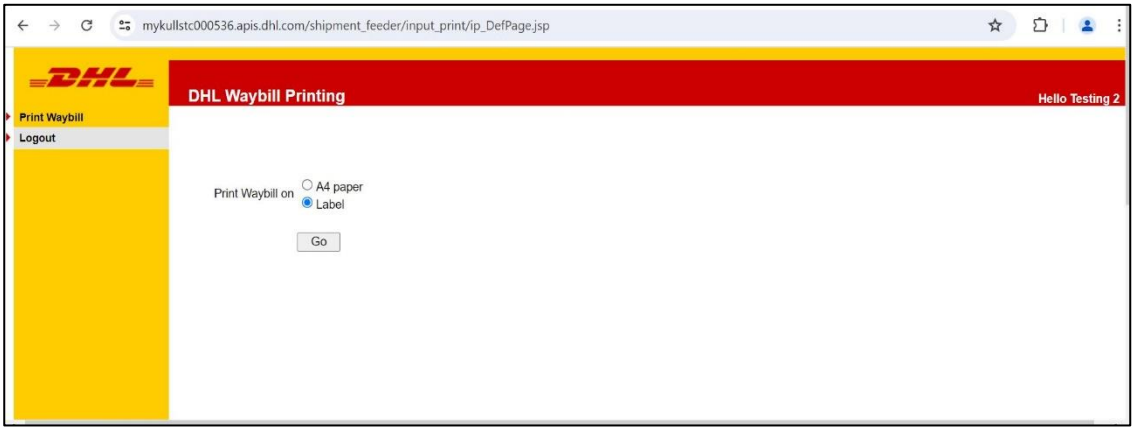
Finding	**Improper Session Management**	**Open**
OWASP Category	**A02:2021-Cryptographic Failures**	
Relative Risk	**Medium**	
Description	During the PenTest Execution, Application session not timed out properly even after the logout still it's accessible when click on the browser back button. Able to access all the application resources in the web app. It was found that the application doesn't invalidates the session id post logout. Affected Assets: https://mykullstc000536.apis.dhl.com/print_waybill	
Impact	A malicious user can easily steal the sensitive information and gain unauthorized access to systems or accounts. This can lead to misuse of the associated resources.	
Remediation, Recommendations & References	• Implement proper application session timed out. • Session should expire immediately after logout. • User should be redirected into the login page only when trying to click on the browser back/forward button after logout. • Should not reveals any sensitive information at any place. • Should not allow to access any resources. • All the corresponding opened tab resources should be logged out automatically after logout and not allowing us to fill any details in shipment form. It should be redirected into Login page when trying to access.	
Detailed Evidence / Exploitation Steps	In Login Page, Enter the Authentication code and Click Sign In.  	

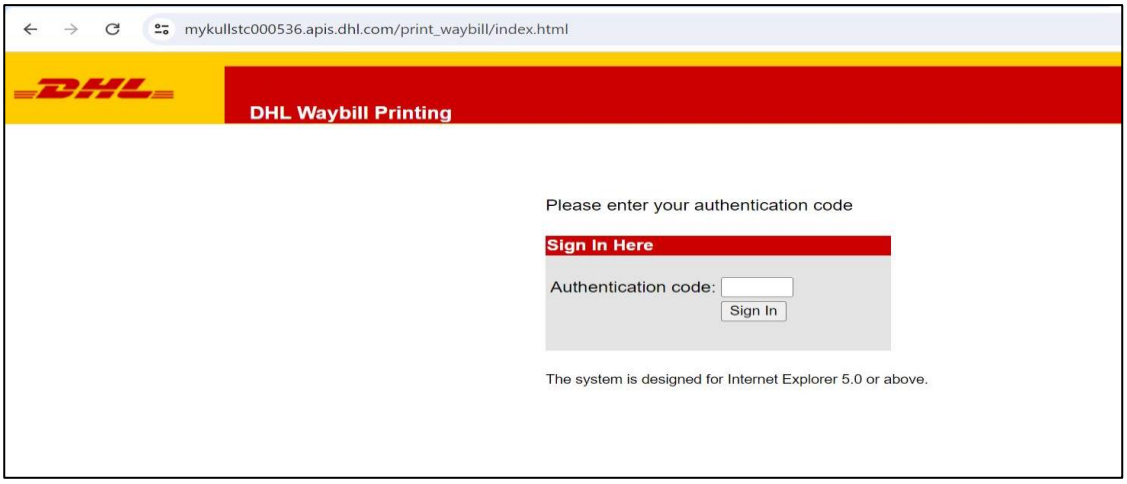
Select Print Waybill on Label/A4 Paper and Click Go

After Click Go button, HomePage Shipment Form page is opened in a new tab from browser.

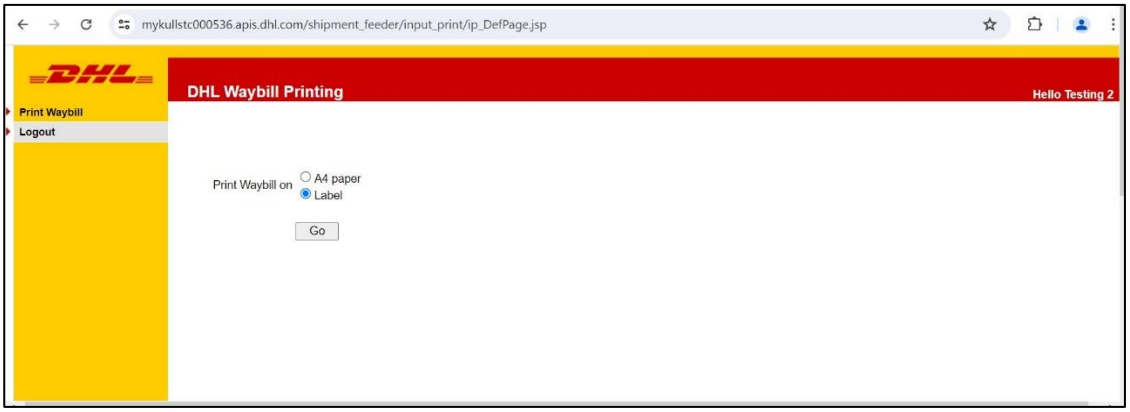


Click Logout button now.

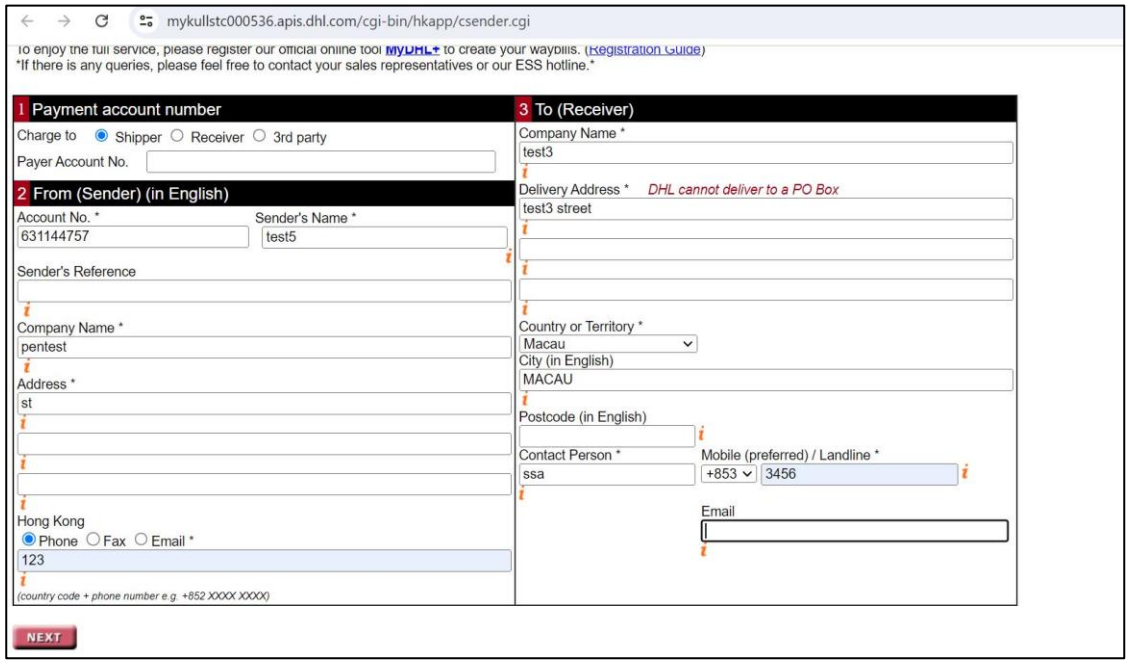


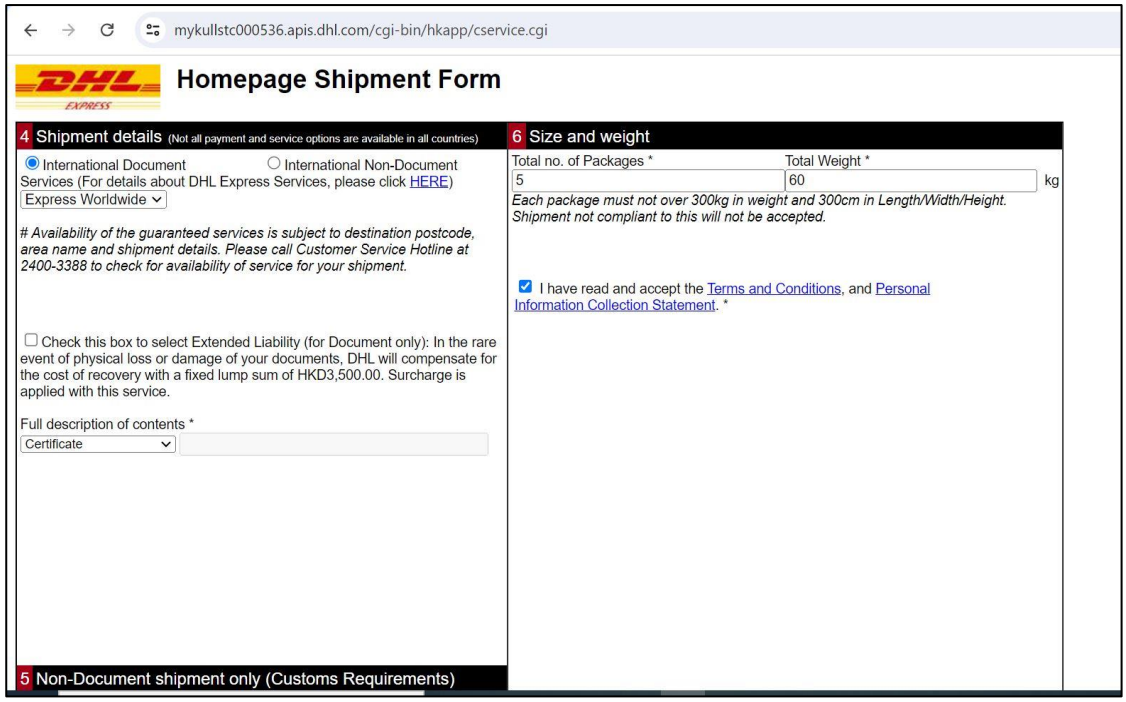


Click on Browser back button, it's observed that Print Waybill page and HomePage Shipment Form page are still accessible even after logout.

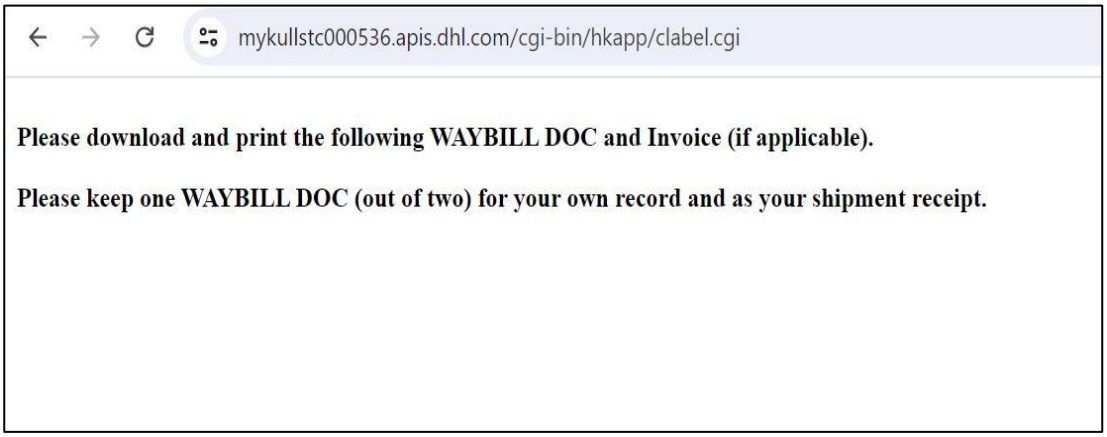


It will be allowing us to fill all the details and able to submit the form.





Waybill was downloaded successfully without login into an application.



3.1.4 Improper Cookies Attributes [BitSight Related]

Finding	**Improper Cookies Attributes [BitSight Related]**	**Open**
OWASP Category	**A05:2021 – Security Misconfiguration**	
Relative Risk	**MEDIUM**	
Description	During the PenTest Execution, it was observed that the application uses session cookies (SameSite attribute) were not set properly. **SameSite Attribute** The SameSite attribute can be used to assert whether a cookie should be sent along with cross-site requests. This feature allows the server to mitigate the risk of cross-origin information leakage. In some cases, it is used too as a risk reduction (or defense in depth mechanism) strategy to prevent cross-site request forgery attacks. This attribute can be configured in three different modes: - Strict - Lax - None **Strict Value:** The Strict value is the most restrictive usage of SameSite, allowing the browser to send the cookie only to first-party context without top-level navigation. **Lax Value:** The Lax value is less restrictive than Strict. The cookie will be sent if the URL equals the cookie's domain (first-party) even if the link is coming from a third-party domain. **None Value:** The None value specifies that the browser will send the cookie in all contexts, including cross-site requests (the normal behavior before the implementation of SameSite). Affected Assets: https://mykullstc000536.apis.dhl.com/print_waybill	
Impact	**SameSite attribute:** Attacks can extend to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).	
Remediation, Recommendations & References	It is recommended to set SameSite attribute flag for all cookie values as followings: • Restrict Cookies to a first-party or same-site context. Verify and set the SameSite attribute of the cookie to Strict, to ensure that the cookie will only be sent in a first-party context. Alternatively, if developer want to relax the restrictions of first-party context, then verify and set the SameSite attribute of the cookie to Lax with Secure Flag enabled and transferred over HTTPS.	

Detailed Evidence / Exploitation Steps	Launch the web app url and observed the below cookie's values: https://mykullstc000536.apis.dhl.com/shipment_feeder/input_print/ip_DefPage.jsp