



[APM0002782]

HK.APP.HomepageWaybillPrinting

Security Test Report

Version 2.0

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 Ciphers.....	6
3.1.2	Improper Implementation of Content-Security-Policy Header [BitSight Related]	10
3.1.3	Improper Session Management.....	13
3.1.4	Improper Cookies Attributes [BitSight Related]	18

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- A06 Vulnerable and Outdated Components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

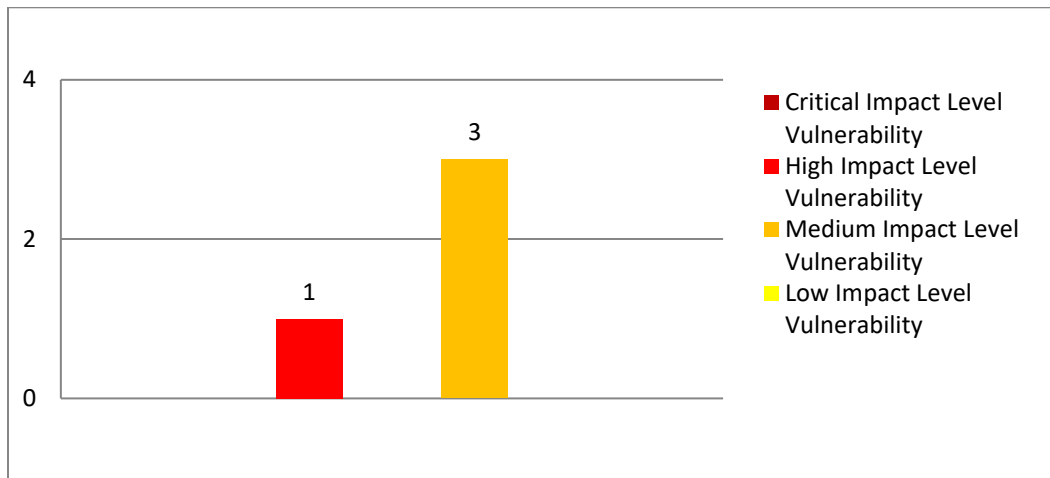
The testing was performed at a “point-in-time” that followed OWASP Top 10 methodologies. The testing is not intended to identify all existing vulnerabilities and security weaknesses, nor does it claim or represent that any applications are free of vulnerabilities or immune to attacks. This report is 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

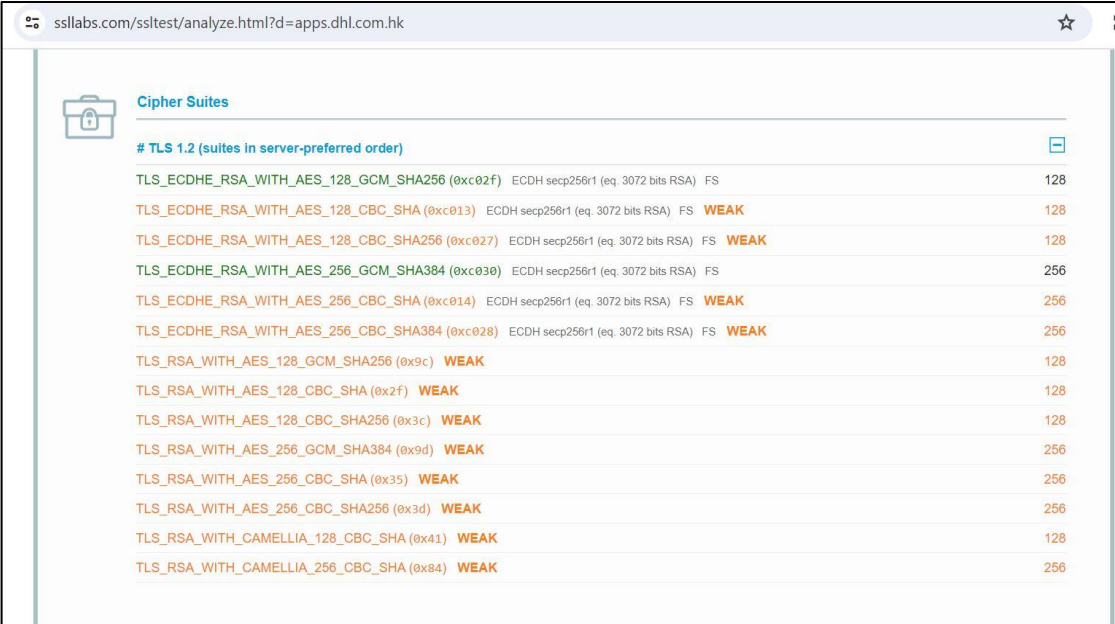
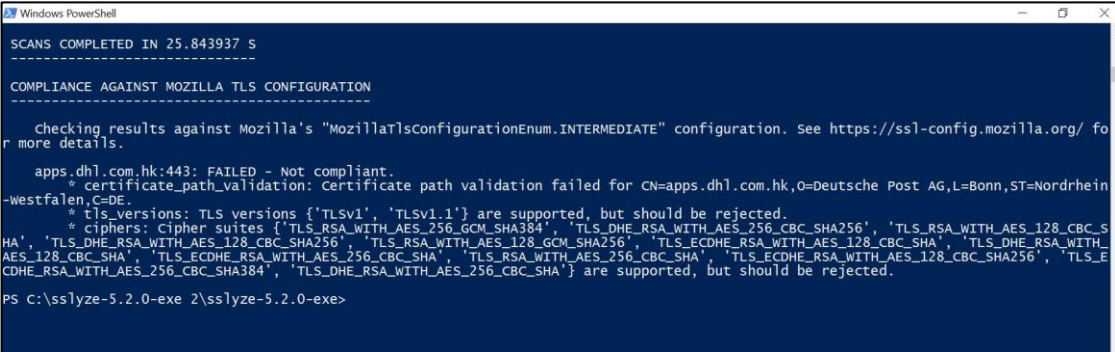
3 Detailed Technical Findings

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	<p>The server accepts the following weak cipher suites:</p> <pre> 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 </pre> <p>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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Affected Assets:</p> <p>PROD: https://apps.dhl.com.hk/print_waybill</p> <p>UAT: https://mykullstc000536.apis.dhl.com/print_waybill</p> </div>	
Impact	<p>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.</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>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.</p>  <p>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.</p> 

```

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/ for 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
```

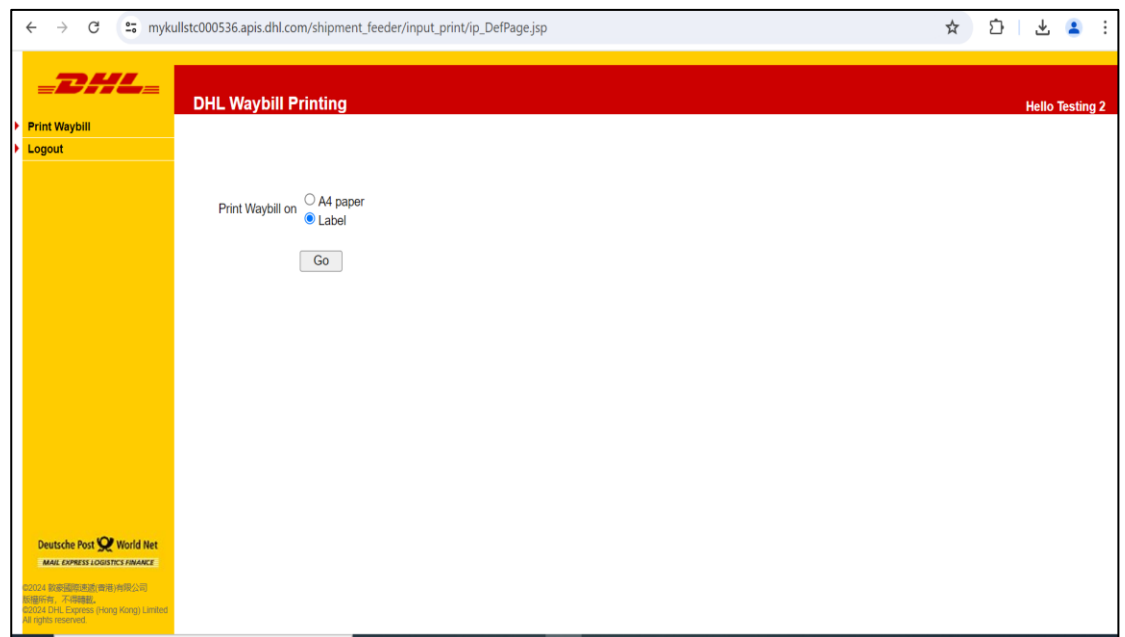
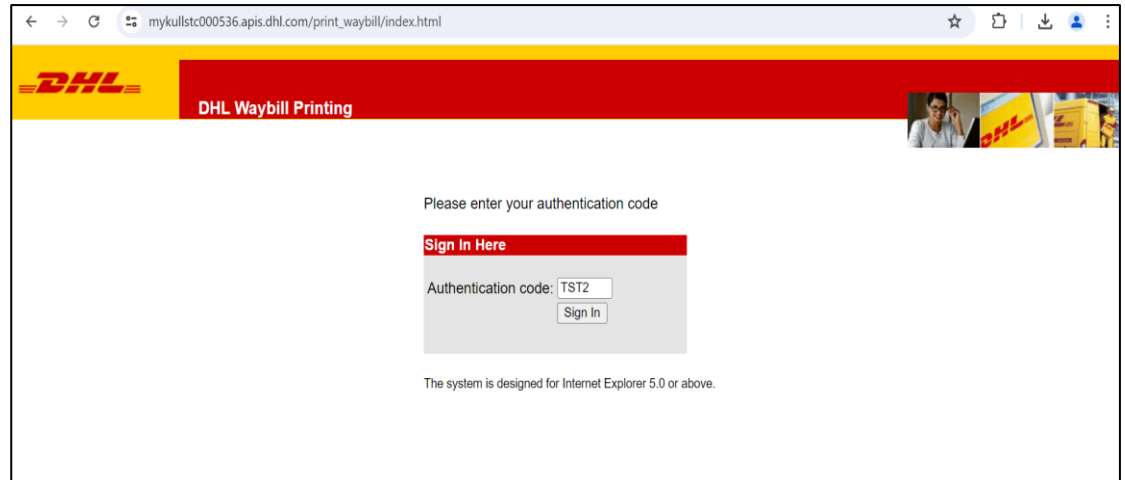
3.1.2 Improper Implementation of Content-Security-Policy Header [\[BitSight Related\]](#)

Finding	Improper Implementation of Content-Security-Policy Header [BitSight Related]		Open				
OWASP Category	A05:2021 – Security Misconfiguration						
Relative Risk	Medium						
Description	<p>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.</p> <p>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.</p> <p>While assessment, it was found that Improper Implementation of Content-Security-Policy from the response headers.</p> <ul style="list-style-type: none">Content-Security-Policy (CSP) <div><p>Affected Assets:</p><p>https://mykullstc000536.apis.dhl.com/print_waybill</p></div>						
Impact	<p>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.</p> <p>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.</p>						
Remediation, Recommendations & References	<p>To remediate the issue of Improper Implementation of Content-Security-Policy header in web application responses, the following steps can be taken:</p> <p>Kindly implement the below recommended CSP values in the response headers:</p> <table><tr><th>Header name</th><th>Proposed value</th></tr><tr><td>Content-Security-Policy</td><td>default-src 'self'; object-src 'none'; frame-ancestors 'none'; upgrade-insecure-requests; block-all-mixed-content</td></tr></table>			Header name	Proposed value	Content-Security-Policy	default-src 'self'; object-src 'none'; frame-ancestors 'none'; upgrade-insecure-requests; block-all-mixed-content
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

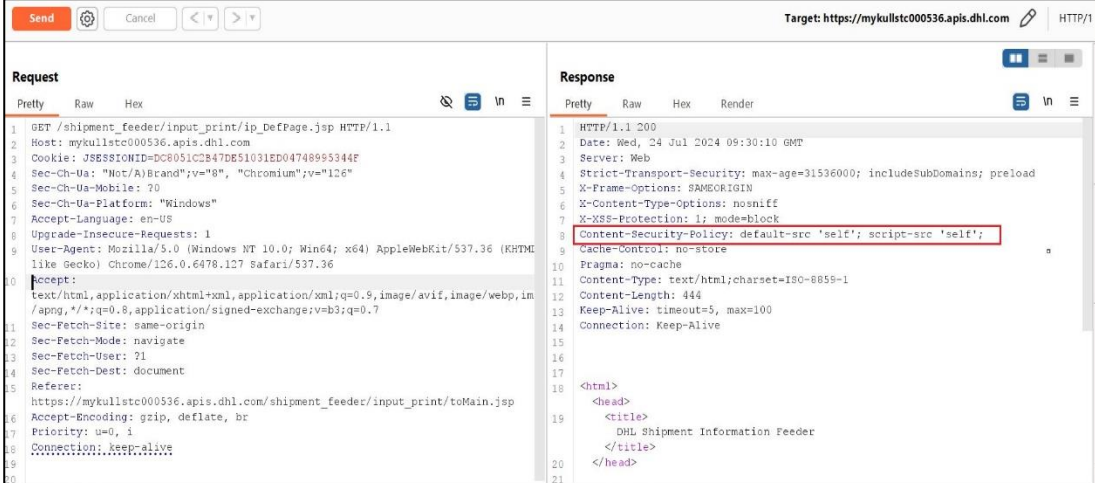
Kindly check the evidence for Burp Response.

Login into an app: https://mykullstc000536.apis.dhl.com/print_waybill/index.html



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



Request

```

1 GET /shipment_feeder/input_print/ip_DefPage.jsp HTTP/1.1
2 Host: mykullstc000536.apis.dhl.com
3 Cookie: JSESSIONID=DC8051C2B47DE51031ED04748995344F
4 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
10 like Gecko) Chrome/126.0.6478.127 Safari/537.36
11 Accept:
12 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
13 /png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer:
19 https://mykullstc000536.apis.dhl.com/shipment_feeder/input_print/toMain.jsp
20 Accept-Encoding: gzip, deflate, br
21 Connection: keep-alive

```

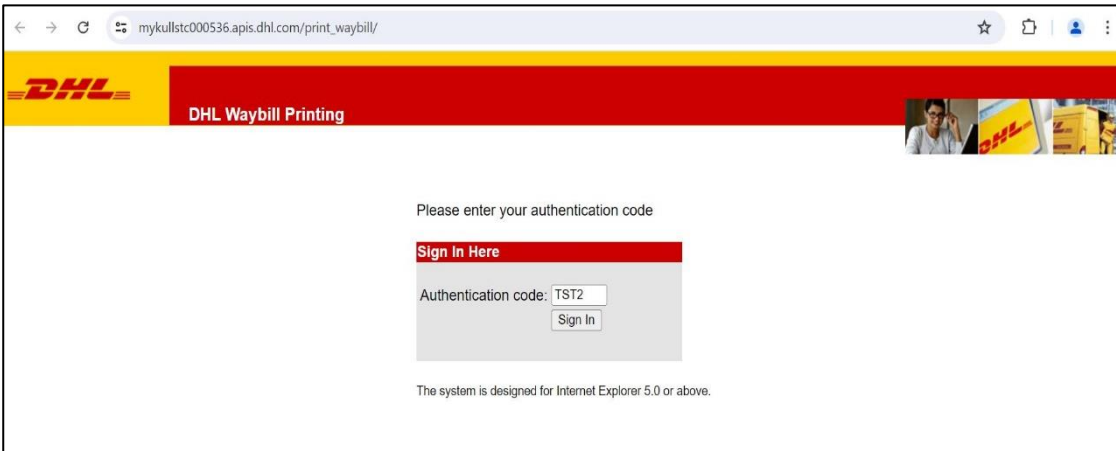
Response

```

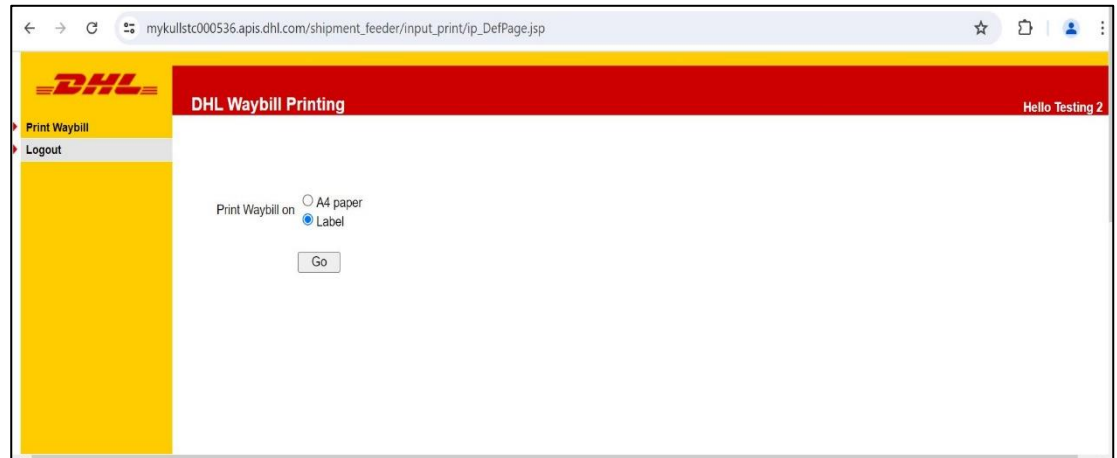
1 HTTP/1.1 200
2 Date: Wed, 24 Jul 2024 09:30:10 GMT
3 Server: Web
4 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
5 X-Frame-Options: SAMEORIGIN
6 X-Content-Type-Options: nosniff
7 X-XSS-Protection: 1; mode=block
8 Content-Security-Policy: default-src 'self'; script-src 'self';
9 Cache-Control: no-store
10 Pragma: no-cache
11 Content-Type: text/html; charset=ISO-8859-1
12 Content-Length: 444
13 Keep-Alive: timeout=5, max=100
14 Connection: Keep-Alive
15
16
17
18 <html>
19 <head>
20 <title>
21 DHL Shipment Information Feeder
22 </title>
23 </head>

```

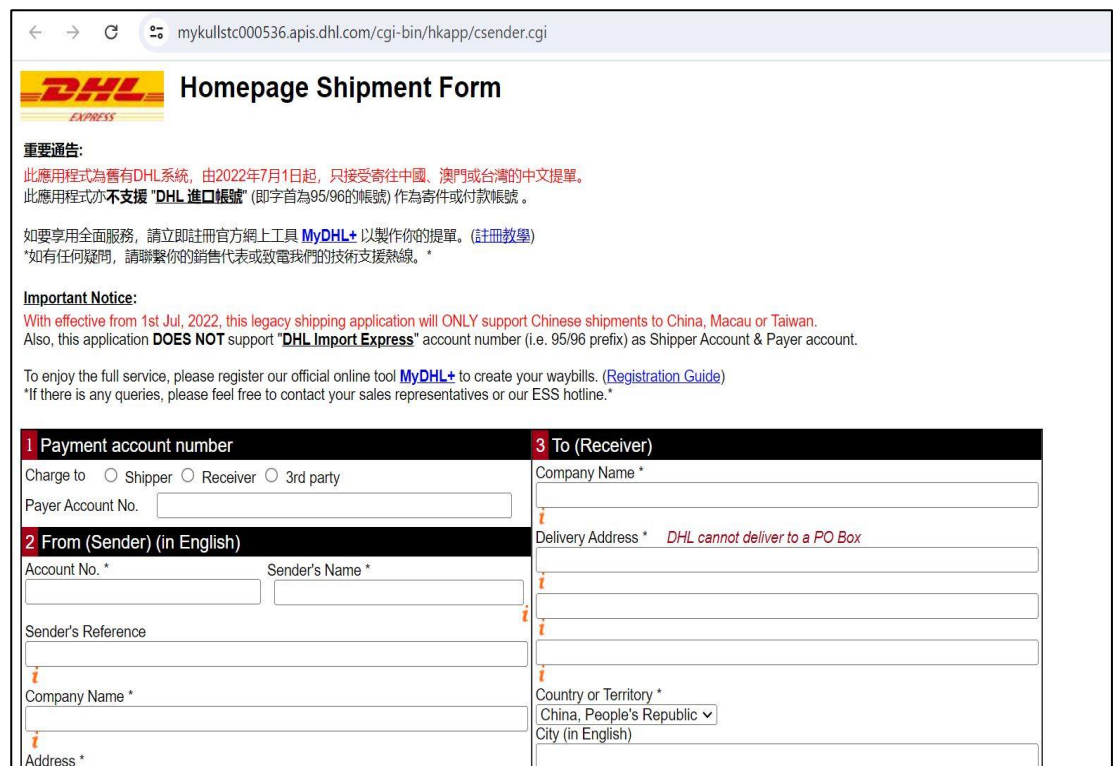
3.1.3 Improper Session Management

Finding	Improper Session Management	Open
OWASP Category	A02:2021-Cryptographic Failures	
Relative Risk	Medium	
Description	<p>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.</p> <div> <p>Affected Assets:</p> <p>https://mykullstc000536.apis.dhl.com/print_waybill</p> </div>	
Impact	<p>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.</p>	
Remediation, Recommendations & References	<ul style="list-style-type: none"> • 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	<p>In Login Page, Enter the Authentication code and Click Sign In.</p> 	

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.



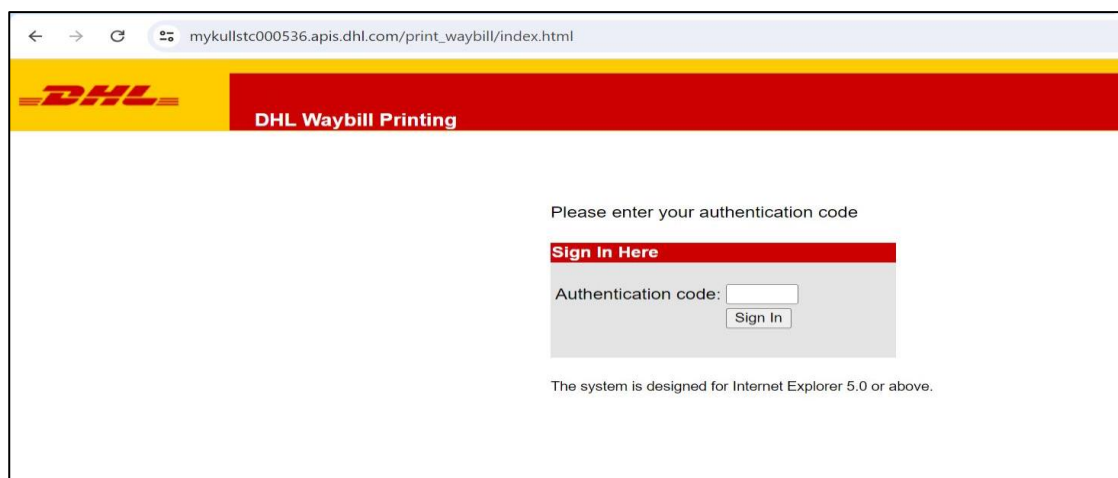
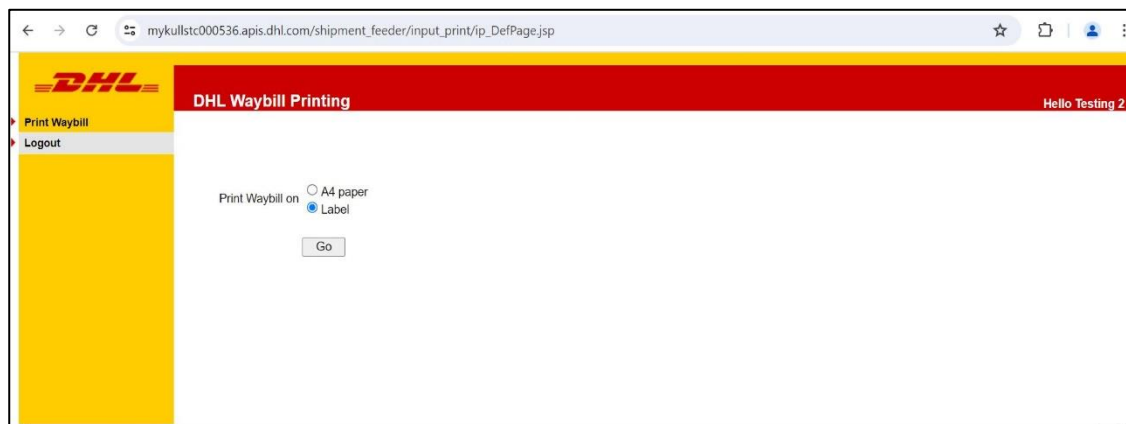
重要通告:
此應用程式為舊有DHL系統，由2022年7月1日起，只接受寄往中國、澳門或台灣的中文提單。
此應用程式亦不支援 "DHL 進口帳號" (即字首為95/96的帳號) 作為寄件或付款帳號。

如要享用全面服務，請立即註冊官方網上工具 [MyDHL+](#) 以製作你的提單。(註冊教學)
如有任何疑問，請聯繫你的銷售代表或致電我們的技術支援熱線。

Important Notice:
With effective from 1st Jul, 2022, this legacy shipping application will ONLY support Chinese shipments to China, Macau or Taiwan.
Also, this application **DOES NOT** support "DHL Import Express" account number (i.e. 95/96 prefix) as Shipper Account & Payer account.
To enjoy the full service, please register our official online tool [MyDHL+](#) to create your waybills. ([Registration Guide](#))
If there is any queries, please feel free to contact your sales representatives or our ESS hotline.

1 Payment account number	3 To (Receiver)
Charge to <input type="radio"/> Shipper <input type="radio"/> Receiver <input type="radio"/> 3rd party	Company Name *
Payer Account No. <input type="text"/>	<input type="text"/>
2 From (Sender) (in English)	Delivery Address * <i>DHL cannot deliver to a PO Box</i>
Account No. * <input type="text"/>	<input type="text"/>
Sender's Name * <input type="text"/>	<input type="text"/>
Sender's Reference <input type="text"/>	<input type="text"/>
Company Name * <input type="text"/>	Country or Territory *
Address * <input type="text"/>	China, People's Republic ▾
	City (in English) <input type="text"/>

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.

← → ↻ mykullstc000536.apis.dhl.com/cgi-bin/hkapp/csender.cgi

To enjoy the full service, please register our official online tool [myDHL+](#) to create your waybills. ([Registration Guide](#))
 If there is any queries, please feel free to contact your sales representatives or our ESS hotline.

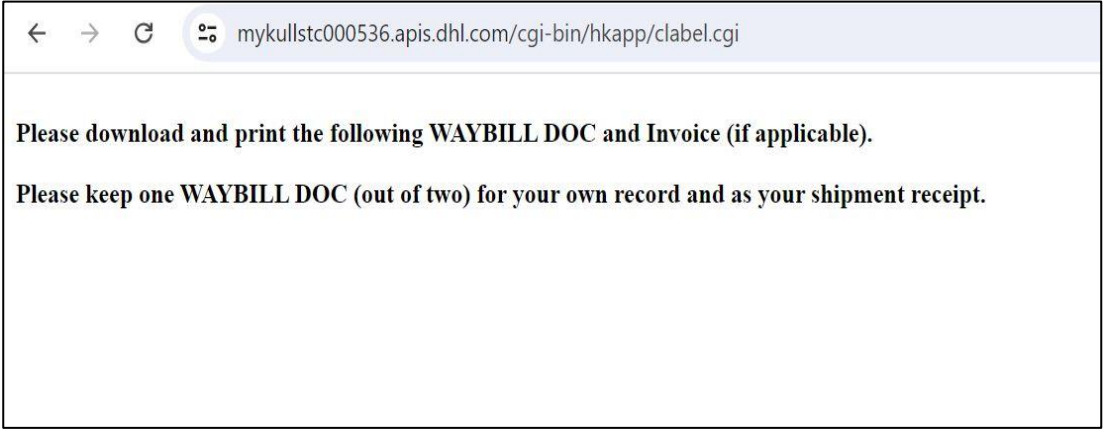
1 Payment account number Charge to <input checked="" type="radio"/> Shipper <input type="radio"/> Receiver <input type="radio"/> 3rd party Payer Account No. <input type="text"/> 2 From (Sender) (in English) Account No. * <input type="text"/> Sender's Name * <input type="text"/> 631144757 test5 Sender's Reference <input type="text"/> Company Name * <input type="text"/> pentest Address * <input type="text"/> st Hong Kong <input checked="" type="radio"/> Phone <input type="radio"/> Fax <input type="radio"/> Email * 123 <small>(country code + phone number e.g. +852 XXXX XXXXX)</small>	3 To (Receiver) Company Name * <input type="text"/> test3 Delivery Address * <small>DHL cannot deliver to a PO Box</small> test3 street Country or Territory * <input type="text"/> Macau City (in English) <input type="text"/> MACAU Postcode (in English) <input type="text"/> Contact Person * <input type="text"/> Mobile (preferred) / Landline * <input type="text"/> ssa +853 3456 Email <input type="text"/> NEXT
---	---

← → ↻ mykullstc000536.apis.dhl.com/cgi-bin/hkapp/cservice.cgi

 **Homepage Shipment Form**

4 Shipment details (Not all payment and service options are available in all countries) <input checked="" type="radio"/> International Document <input type="radio"/> International Non-Document Services (For details about DHL Express Services, please click HERE) Express Worldwide # Availability of the guaranteed services is subject to destination postcode, area name and shipment details. Please call Customer Service Hotline at 2400-3388 to check for availability of service for your shipment. <input type="checkbox"/> Check this box to select Extended Liability (for Document only): In the rare event of physical loss or damage of your documents, DHL will compensate for the cost of recovery with a fixed lump sum of HKD3,500.00. Surcharge is applied with this service. Full description of contents * Certificate 5 Non-Document shipment only (Customs Requirements)	6 Size and weight Total no. of Packages * <input type="text"/> Total Weight * <input type="text"/> kg 5 60 Each package must not over 300kg in weight and 300cm in Length/Width/Height. Shipment not compliant to this will not be accepted. <input checked="" type="checkbox"/> I have read and accept the Terms and Conditions , and Personal Information Collection Statement . *
--	---

Waybill was downloaded successfully without login into an application.



← → ↻ 📄 mykullstc000536.apis.dhl.com/cgi-bin/hkapp/clabel.cgi

Please download and print the following WAYBILL DOC and Invoice (if applicable).

Please keep one WAYBILL DOC (out of two) for your own record and as your shipment receipt.

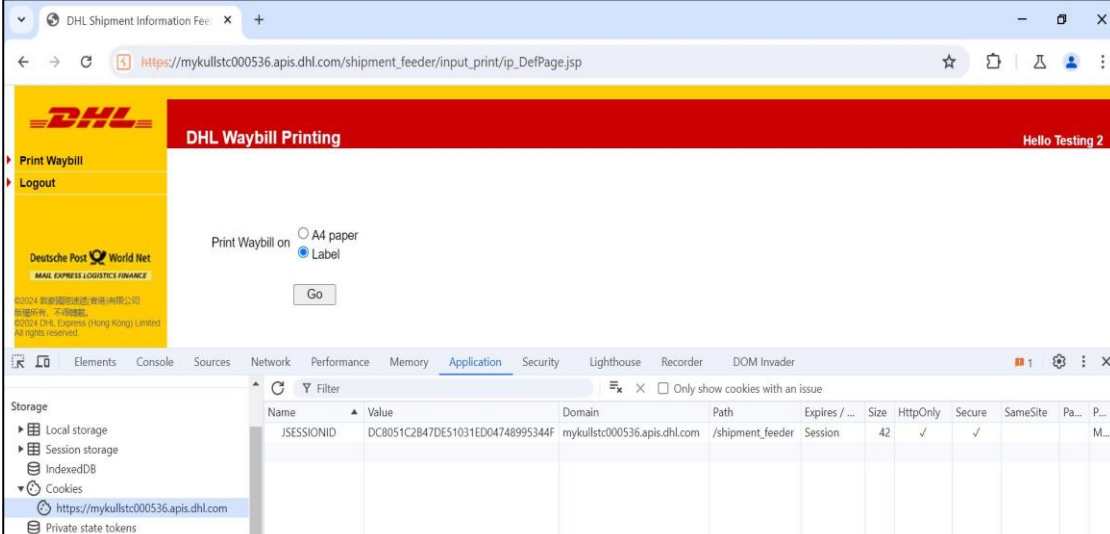
3.1.4 Improper Cookies Attributes [\[BitSight Related\]](#)

Finding	Improper Cookies Attributes [BitSight Related]	Open
OWASP Category	A05:2021 – Security Misconfiguration	
Relative Risk	MEDIUM	
Description	<p>During the PenTest Execution, it was observed that the application uses session cookies (SameSite attribute) were not set properly.</p> <p>SameSite Attribute</p> <p>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:</p> <ul style="list-style-type: none"> - Strict - Lax - None <p>Strict Value:</p> <p>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.</p> <p>Lax Value:</p> <p>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.</p> <p>None Value:</p> <p>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).</p> <div> <p>Affected Assets:</p> <p>https://mykullstc000536.apis.dhl.com/print_waybill</p> </div>	
Impact	<p>SameSite attribute:</p> <p>Attacks can extend to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).</p>	
Remediation, Recommendations & References	<p>It is recommended to set SameSite attribute flag for all cookie values as followings:</p> <ul style="list-style-type: none"> • 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



Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Pa...	P...
JSESSIONID	DC8051C2B47DE51031ED04748995344F	mykullstc000536.apis.dhl.com	/shipment_feeder	Session	42	✓	✓			M...