[AT-ID-1678]
HK Co-Loader Shipment Track and Trace

Security Test Report

Version 2.0

Restricted

Table of Contents

Version Control

Version number	Date	Prepared by	Reviewed By
1.0	*06/09/2023*	*Rajesh Kumar Munimadugu*	*Akash Agasti*
2.0	*22/09/2023*	*Rajesh Kumar Munimadugu*	*Akash Agasti*

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 Co-Loader Shipment Track and Trace 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- A06 Vulnerable and Outdated Components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 Archer ID	*AT-ID-1678*
Application Name	*HK Co-Loader Shipment Track and Trace*
Application Interfacing	*External*
Scope	*Web*

Test Duration	Test Environment	Target	Test Authentication	Note
4th Sep 2023 – 6th Sep 2023	*Test*	*https://mykullstc000536.apis.dhl.com/eng_st/eng_track_home.html*	No Authentication	*Full test*

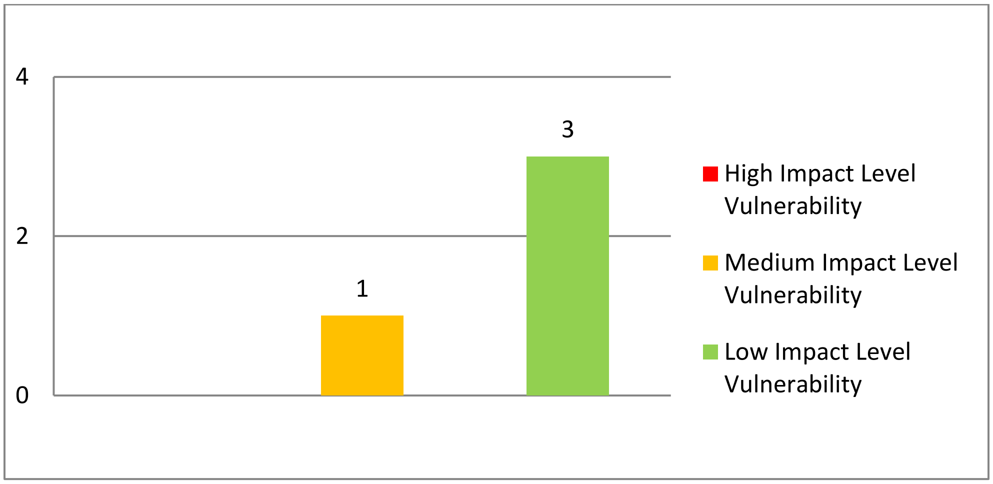
1.3 Disclaimer

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.

2 Executive Summary

2.1 General Impression

The breakdown of web application security vulnerabilities discovered. A total of one (1) Medium & three (3) Low *impact level* vulnerabilities were discovered.



Remaining Open Pentest Findings in Archer (From Previous Pen tests)

Finding ID	**Finding Title**	**URL**	**Risk Rating**
FND-15548	*Missing Security Header*	*https://mykullstc000536.apis.dhl.com/eng_st/eng_track_home.html*	*Low*

New Pentest Findings

No	Findings	Severity	(CVSS) Version 3.1 Score	STATUS
1	*Harvesting of Airwaybill Numbers*	Medium	4.3	*Open*
2	*Test page accessible*	Low	3.5	*Closed*
3	*Default server error page*	Low	3.5	*Closed*

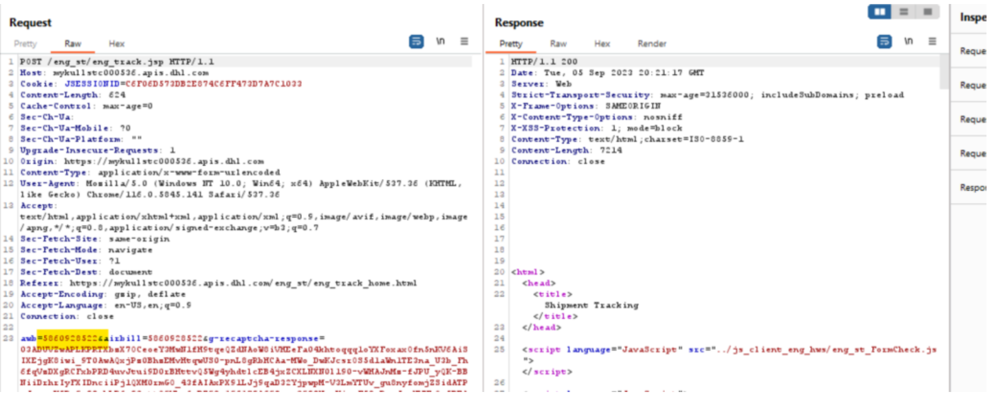
3 Detailed Technical Findings

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 Harvesting of Airwaybill Numbers

Finding	**Harvesting of Airwaybill Numbers**	***Open***
OWASP Category	**A05:2021 - Security Misconfiguration**	
Relative Risk	**Medium**	
Description	The application is allowing to harvest valid Airwaybill numbers using below affected URL. - For valid airway bill numbers, application responds with 200 status code. - For invalid airway bill numbers, application responds with 302 status code. With the above difference in status codes, a malicious user can track all possible valid Airway bill numbers. Affected URL: https://mykullstc000536.apis.dhl.com/eng_st/eng_track.jsp	
Impact	It may lead to harvest valid Airwaybill numbers and subsequently be used against to submit for further investigation for all those valid Airway bills leading to false communications with unknown customers and extra workload on internal teams while looking into these false investigations.	
Remediation, Recommendations & References	Ensure the affected URL can't be used to harvest valid Airway bill numbers via Captcha kind of random token or with email / mobile number being requested to prevent any bots being used to harvest airway bill numbers.	
Detailed Evidence / Exploitation Steps	- *Access the test URL:https://mykullstc000536.apis.dhl.com/eng_st/eng_track_home.html* - Key in valid Airwaybill number "5860928522"and submit. - User will be navigated to the below URL https://mykullstc000536.apis.dhl.com/eng_st/eng_track.jsp - Capture the request in burp. User can try with any numbers in the below POST highlighted request parameter "awb" to know whether its valid or not (or) alternatively can use burp intruder to automate the request with incremental numbers to identify valid numbers.	



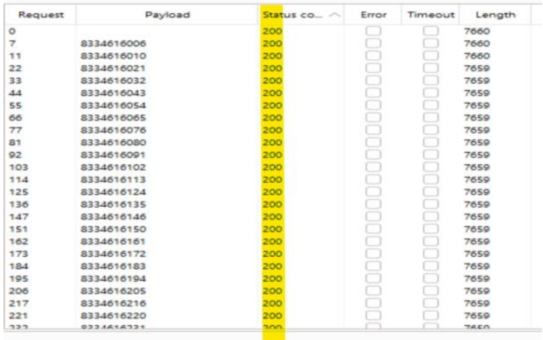
```
POST /eng_st/eng_track.jsp HTTP/1.1
Host: mykullstc000536.apis.dhl.com
Cookie: JSESSIONID=C6F06D573DB2E874C6FF473D7A7C1033
Content-Length: 624
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
Origin: https://mykullstc000536.apis.dhl.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/116.0.5845.141 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://mykullstc000536.apis.dhl.com/eng_st/eng_track_home.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

awb=5860928522&airbill=5860928522&g-recaptcha-response=
03ADUVZwAPLKPRTXbmX70CeoeY3MwN1fM9tqeQZdNAoW8iVMEeFa04khtoqqqloYXFoxax0fn5nKV6AiS
IXEjgK8iwi_9T0AwAQxjPs0BhsEMvHtqwUS0-pnL8gRbHCAa-MWo_DwKJcsr0S5dlaWnlTE3na_U3b_Fh
6fqVsDXgRCFxbPRD4uvJtui9D0rBHttvQ5Wg4yhdtlcEB4jxZCXLNXN01190-vWMAJnMs-fJPU_yQK-BB
NiiDrhrIyFXIDnciiPj1QXM0rmG0_43fAIAxPX91LJj9qaD32YjpwpM-V3LmYTUv_gu8nyfomjZ3idATP
```

```
HTTP/1.1 200
Date: Tue, 05 Sep 2023 20:21:17 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-Type: text/html;charset=ISO-8859-1
Content-Length: 7214
Connection: close










<html>
  <head>
    <title>
      Shipment Tracking
    </title>
  </head>

  <script language="JavaScript" src="../js_client_eng_hws/eng_st_FormCheck.js
  ">
  </script>

```

- For valid airway bill numbers, application responds with 200 status code.
- For invalid airway bill numbers, application responds with 302 status code.

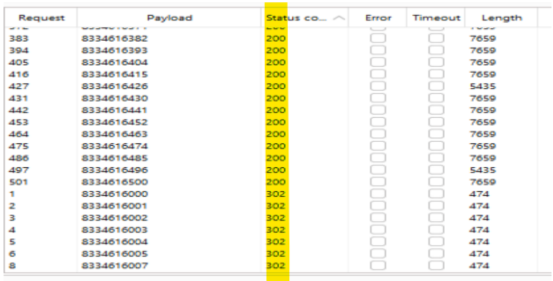
With the difference in status codes, a malicious user can track all possible valid Airway bill numbers.

Valid Airwaybill numbers with 200 status code



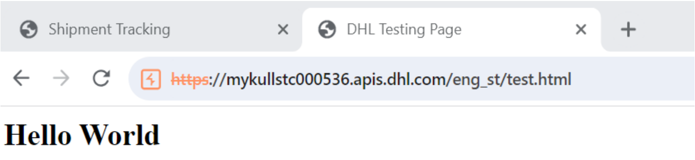
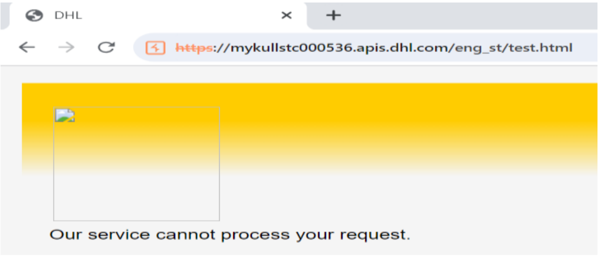
Request	Payload	Status co...	Error	Timeout	Length
0		200	☐	☐	7660
7	8334616006	200	☐	☐	7660
11	8334616010	200	☐	☐	7660
22	8334616021	200	☐	☐	7659
33	8334616032	200	☐	☐	7659
44	8334616043	200	☐	☐	7659
55	8334616054	200	☐	☐	7659
66	8334616065	200	☐	☐	7659
77	8334616076	200	☐	☐	7659
81	8334616080	200	☐	☐	7659
92	8334616091	200	☐	☐	7659
103	8334616102	200	☐	☐	7659
114	8334616113	200	☐	☐	7659
125	8334616124	200	☐	☐	7659
136	8334616135	200	☐	☐	7659
147	8334616146	200	☐	☐	7659
151	8334616150	200	☐	☐	7659
162	8334616161	200	☐	☐	7659
173	8334616172	200	☐	☐	7659
184	8334616183	200	☐	☐	7659
195	8334616194	200	☐	☐	7659
206	8334616205	200	☐	☐	7659
217	8334616216	200	☐	☐	7659
221	8334616220	200	☐	☐	7659

Invalid Airwaybill numbers with 302 status code

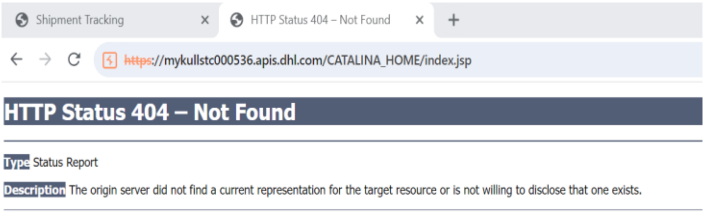


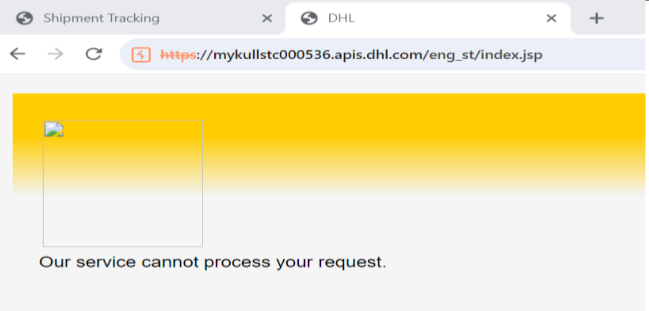
Request	Payload	Status co...	Error	Timeout	Length
383	8334616382	200	☐	☐	7659
394	8334616393	200	☐	☐	7659
405	8334616404	200	☐	☐	7659
416	8334616415	200	☐	☐	7659
427	8334616426	200	☐	☐	5435
431	8334616430	200	☐	☐	7659
442	8334616441	200	☐	☐	7659
453	8334616452	200	☐	☐	7659
464	8334616463	200	☐	☐	7659
475	8334616474	200	☐	☐	7659
486	8334616485	200	☐	☐	7659
497	8334616496	200	☐	☐	5435
501	8334616500	200	☐	☐	7659
1	8334616000	302	☐	☐	474
2	8334616001	302	☐	☐	474
3	8334616002	302	☐	☐	474
4	8334616003	302	☐	☐	474
5	8334616004	302	☐	☐	474
6	8334616005	302	☐	☐	474
8	8334616007	302	☐	☐	474

3.1.2 Test page accessible

Finding	**Test page accessible**	**Closed**
OWASP Category	**A05:2021 - Security Misconfiguration**	
Relative Risk	**Low**	
Description	Test page is accessible via below URL which is hosted in the same server. Affected URL: https://mykullstc000536.apis.dhl.com/eng_st/test.html	
Impact	Even though this test page which got detected has no security risk at moment, it’s highly recommended to remove any test / backup pages inside the application container that are not linked to application functionality to prevent any potential attack. Lot of test files that on UAT usually will be pushed to production systems that developers built while developing applications and are no longer required for production may contain sensitive information or create some kind of backdoor access. Hence it is requested to check for any test / backup files and their usage in application regularly.	
Remediation, Recommendations & References	Ensure no test / back up pages that are not relevant to application exists in the server.	
Detailed Evidence / Exploitation Steps	*Access the below url:* https://mykullstc000536.apis.dhl.com/eng_st/test.html  https://mykullstc000536.apis.dhl.com/eng_st/test.html Hello World **Retest Notes: 9/22/2023**- Affected URL is not accessible. Issue closed.  https://mykullstc000536.apis.dhl.com/eng_st/test.html Our service cannot process your request.	

3.1.3 Default server error page

Finding	**Default server error page**	**Closed**
OWASP Category	**A05:2021 - Security Misconfiguration**	
Relative Risk	**Low**	
Description	Default server error page displayed up on accessing below URL Affected URL: https://mykullstc000536.apis.dhl.com/TOMCAT_HOME/index.jsp https://mykullstc000536.apis.dhl.com/CATALINA_HOME/index.jsp	
Impact	The default error page gives information about the backend server (tomcat) being used. It also conveys that server is not configured securely as the requests are not handled uniformly.	
Remediation, Recommendations & References	Ensure the default application error page gets loaded when application not able to handle the request.	
Detailed Evidence / Exploitation Steps	*Access the below url will redirect user to below default tomcat server error page.* *Note : CATALINA_HOME OR TOMCAT_HOME in the below URL path gives indication that the underlying server is related to Tomcat.* https://mykullstc000536.apis.dhl.com/CATALINA_HOME/index.jsp (or) https://mykullstc000536.apis.dhl.com/TOMCAT_HOME/index.jsp  https://mykullstc000536.apis.dhl.com/CATALINA_HOME/index.jsp HTTP Status 404 – Not Found Type Status Report Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. *Access the below url will redirect user to standard default application error page https://mykullstc000536.apis.dhl.com/eng_st/index.jsp* *The difference in handling of the error pages reveals information about the server being used by the application.*	



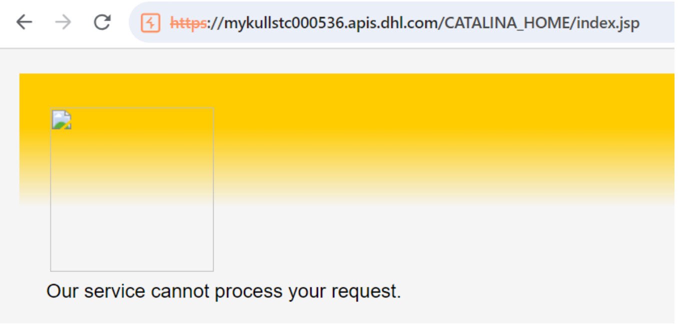
~~https~~://mykullstc000536.apis.dhl.com/eng_st/index.jsp

Our service cannot process your request.

Retest Notes: 9/22/2023-

Affected URLs are not accessible. Issue closed.

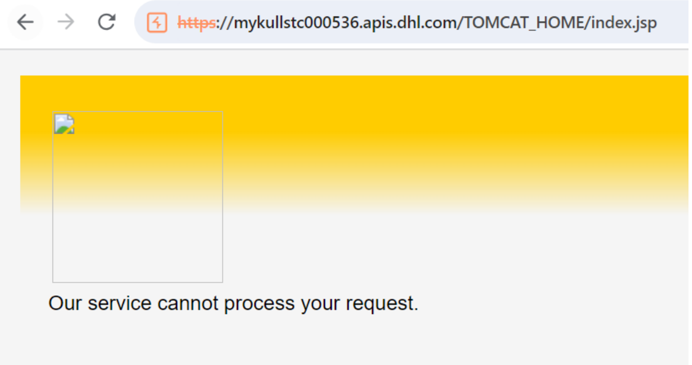
https://mykullstc000536.apis.dhl.com/CATALINA_HOME/index.jsp



~~https~~://mykullstc000536.apis.dhl.com/CATALINA_HOME/index.jsp

Our service cannot process your request.

https://mykullstc000536.apis.dhl.com/TOMCAT_HOME/index.jsp



~~https~~://mykullstc000536.apis.dhl.com/TOMCAT_HOME/index.jsp

Our service cannot process your request.