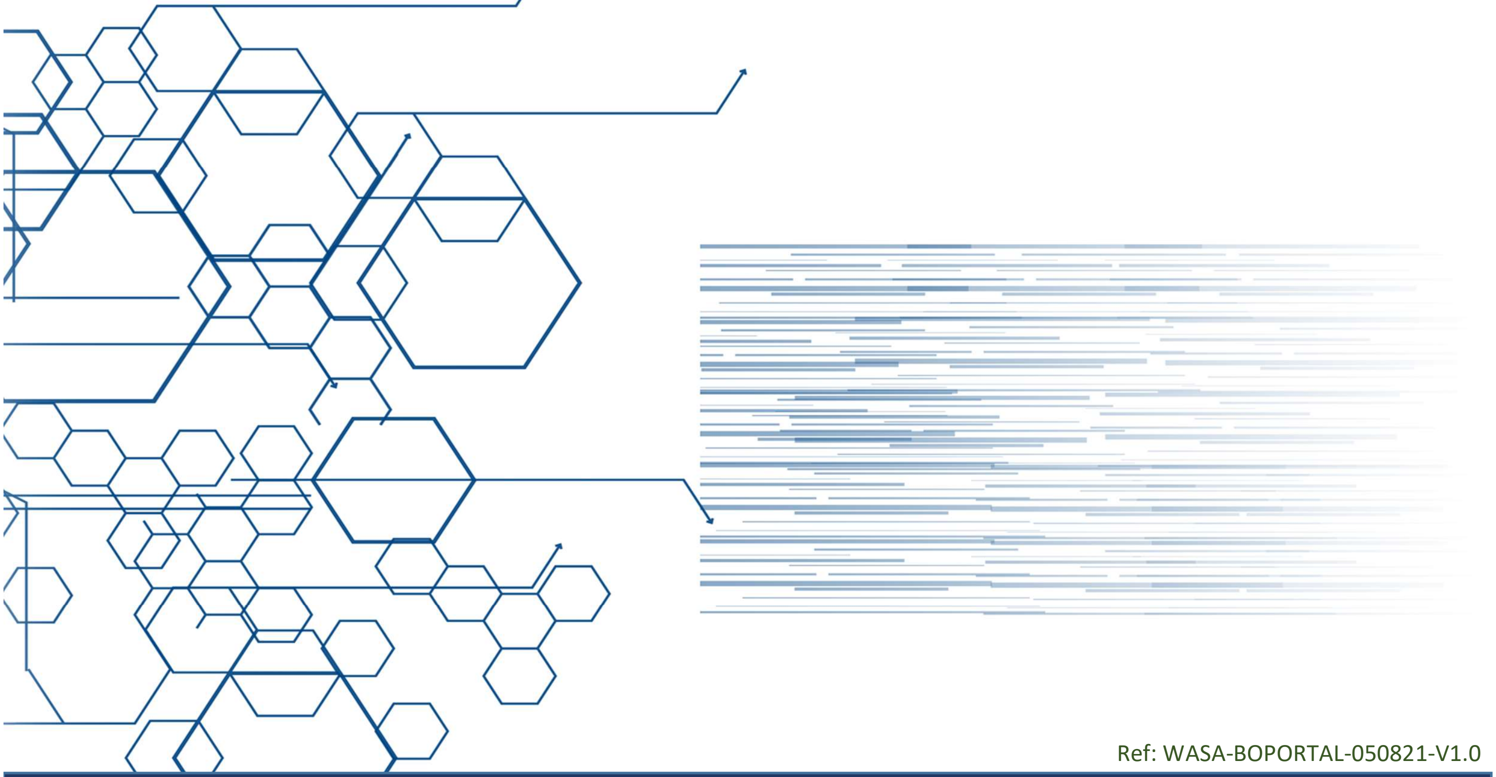


Ref: WASA-BOPORTAL-050821-V1.0

# Web Application Security Assessment Report (BO Portal)

**5 August 2021**

**Prepared by:**

**Muzaffar Mohamed**
IT Security
Information Services Division
Payments Network Malaysia Sdn Bhd (PayNet)
Email: muzaffar.mohamed@paynet.my

## Table of Contents

## Document Properties

| | |
|---|---|
| **Document Title** | Web Application Security Assessment Report |
| **Reference Number** | WASA-BOPORTAL-050821-V1.0 |
| **Target Scope** | BO Portal |
| **Version** | 1.0 |
| **Pentesters** | Muzaffar Mohamed |
| **Authors** | Muzaffar Mohamed |
| **Classification** | Confidential |
| **Document Type** | Private |
| **Reviewed by** | |
| **Approved by** | |
| **Date** | 05 August 2021 |

**Version Control**

| Date | Author | Version | Remarks |
|---|---|---|---|
| 05/08/2021 | Muzaffar Mohamed | 0.1 | Draft Report |
| 05/08/2021 | Muzaffar Mohamed | 1.0 | Final Report |

**Contact**

For more information about this document and its contents please contact the following person.

| | |
|---|---|
| **Name & Position** | **Muzaffar Mohamed**<br>IT Security<br>Information Services Division<br>Payments Network Malaysia Sdn Bhd |
| **Phone** | +603.2264.8600 |
| **Email** | Muzaffar.mohamed@paynet.my |

This document contains information, which is confidential and proprietary to **Payment Network Malaysia Sdn Bhd**. Extreme care should be exercised before distributing copies of this document, or the extracted contents of this document. This document should be marked "CONFIDENTIAL" and therefore we suggest that this document be disseminated on a "need to know" basis.

# 1.0 Project Definition

## 1.1 Definition

In line with PayNet's security enhancement initiative, the **IT Security Engineer (ITSE)** has been tasked to perform a detailed web security posture assessment of Paynet's **BO Portal**. To perform the test, the ITSE was provided access to a UAT system.

It is important to note that this report represents a snapshot of the security of the environment assessed at a point in time. Conditions may have improved, deteriorated, or remained the same since this assessment was completed.

This testing effort took place on **2 August 2021** and concluded on **5 August 2021**. This report is being presented to show the full results of the testing efforts and to make recommendations where appropriate.

## 1.2 Objective

The ITSE performed a Web Application Penetration Test to:

- Identify the surface of the attack of the systems undergoing the Penetration Testing exercise.
- Identify the vulnerabilities of the systems undergoing the Penetration Testing exercise.
- Determine the feasibility of a set of attack vectors.
- Provide evidence of the real status of the systems to the management of the company.

# 2.0 Executive Summary

## 2.1 Background

This report presents the results of the “Grey Box” penetration testing for PayNet’s BO Portal. The recommendations provided in this report are structured to facilitate remediation of the identified security risks.

Evaluation ratings compare information gathered during the engagement to “best in class” criteria for security standards. The IT Security Engineer (ITSE) believes that the statements made in this document provide an accurate assessment of PayNet current security as it relates to infrastructure and network perimeter.

The ITSE highly recommends reviewing the section of the summary of business risks and High-Level Recommendations for a better understanding of risks and discovered security issues.

| Scope | Security Level | Grade |
|---|---|---|
| PAYNET BO Portal | Good | B |

The IT Security Engineer (ITSE) Grading Criteria:

| Grade | Security | Criteria Description |
|---|---|---|
| A | Excellent | The security exceeds “Industry Best Practice” standards. The overall posture was found to be excellent with only a few low-risk findings identified. |
| B | Good | The security meets with accepted standards for “Industry Best Practice”. The overall posture was found to be strong with only a handful of medium and low-risk shortcomings identified. |
| C | Fair | Current solutions protect some areas of the enterprise from security issues. Moderate changes are required to elevate the discussed areas to “Industry Best Practice” standards |
| D | Poor | Significant security deficiencies exist. Immediate attention should be given to the discussed issues to address the exposures identified. Major changes are required to elevate to “Industry Best Practice” standards. |
| F | Inadequate | Serious security deficiencies exist. Shortcomings were identified throughout most or even all of the security controls examined. Improving security will require a major allocation of resources. |

## 2.2 Scope of Security Assessment

The scope of this assessment was limited to a TSP UAT web application portal. This is a BO Portal and the specific instantiation of the portal ITSE was asked to test was for the PayNet Network.

The landing page to the application under review was at the following addresses:

| BO Application | URL |
|---|---|
| External Portal | https://rppportalp2uat.paynet.com.my/common/Login.do |
| Internal Portal | http://172.16.100.71:8080/common/Login.do |

** Internal and External portal was running the same version but different DB

The testing included both unauthenticated as well as authenticated testing. For this testing, the ITSE was provided with 5 unique accounts for the BO Portal. These accounts were used to test the applications of internal and external security controls. These accounts are listed in the table below.

| Account Name | Role | Category |
|---|---|---|
| Paynet Admin | adminmaker1@paynet.my | External Portal |
| Merchant Maker | husna.aqeela2010@gmail.com | Internal Portal |
| Merchant Checker | qaleefhakimi@gmail.com | |
| Bank Maker | mbbbankmaker@mbb.com | |
| Bank Checker | mbbbankchecker@mbb.com | |

## 2.3 Assessment Methodology

The Penetration Testing Methodology is grounded on the following guides and standards:

1. Penetration Testing Execution Standard
2. OWASP Top 10 Application Security Risks - 2017
3. OWASP Testing Guide

The ITSE strongly avoids exploiting the vulnerabilities related to the Denial of Service (DOS) attack, as it may cause service disruption to critical services. Among the checks performed over the Web Application, the following checks related to the most common vulnerabilities (OWASP Top 10) were included:

| | |
|---|---|
| **A1 - Injection** | • Injection flaws, such as SQL, NoSQL, OS, and LDAP injection<br>• Occur when untrusted data is sent to an interpreter as part of a command or query. |
| **A2 - Broken Authentication** | • Application functions related to authentication and session management are often implemented incorrectly. |
| **A3 - Sensitive Data Exposure** | • Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII.<br>• Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. |
| **A4 - XML External Entities (XXE)** | • Many older or poorly configured XML processors evaluate external entity references within XML documents. |
| **A5 - Broken Access Control** | • Restrictions on what authenticated users are allowed to do are often not properly enforced. |
| **A6 - Security Misconfiguration** | • This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. |
| **A7 - Cross-Site Scripting (XSS)** | • XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. |
| **A8 - Insecure Deserialization** | • Insecure deserialization often leads to remote code execution. |
| **A9 - Using Components with Known Vulnerabilities** | • If a vulnerable previleged component is exploited, such an attack can facilitate serious data loss or server takeover. |
| **A10 - Insufficient Logging & Monitoring** | • Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. |

## 2.4 Severity Scoring

The ITSE follows the Common Vulnerability Scoring System Version 3.0 (CVSS v3.0) scoring system to rate vulnerabilities. The CVSS assessment measures three areas of concern:

- Base Metrics for qualities intrinsic to a vulnerability
- Temporal Metrics for characteristics that evolve over the lifetime of vulnerability
- Environmental Metrics for vulnerabilities that depend on an implementation or environment

For more information on what the Base, Temporal, and Environment Metrics in the CVSS scoring system are, please visit:
https://www.first.org/cvss/calculator/3.0

Unless otherwise stated, the findings in the report are scored on the base-metric rating of the vulnerability. The ITSE may consider Environmental and Temporal Metrics depending on the information provided at project initiation and if this is a mandatory reporting requirement.

☣ **Critical ( 9.0 - 10.0 )**
•Immediate threat to key business processes.

☠ **High ( 7.0 - 8.9 )**
•Direct threat to key business processes

⚡ **Medium ( 4.0 - 6.9 )**
•Indirect threat to key business processes or partial threat to business processes

⚠ **Low ( 0.1 - 3.9 )**
• No direct threat exists. Vulnerability may be exploited using other vulnerabilities.

ℹ **None ( 0.0 )**
•This finding does not indicate vulnerability, but states a comment that notifies about design flaws and improper implementation that might cause a problem in the long run

## 2.5 Performed Tests

Application penetration test includes all the items in the OWASP API Security Top 10 and more. The penetration tester remotely tries to compromise the OWASP API Top 10 flaws. The flaws listed by OWASP in its most recent Top 10 and the status of the application against those are depicted in the table below.

| Criteria Label | Status |
|---|---|
| A1 – Injection | ☺ **PASS** |
| A2 - Broken Authentication | ☺ **PASS** |
| A3 - Sensitive Data Exposure | ☺ **PASS** |
| A4 - XML External Entities (XXE) | ☺ **PASS** |
| A5 - Broken Access Control | ☹ **FAIL** |
| A6 - Security Misconfiguration | ☺ **PASS** |
| A7 - Cross-Site Scripting (XSS) | ☺ **PASS** |
| A8 - Insecure Deserialization | ☺ **PASS** |
| A9 - Using Components with Known Vulnerabilities | ☹ **FAIL** |
| A10 - Insufficient Logging & Monitoring | ☺ **PASS** |

**** OWASP for Web Application does not specifically include rate-limiting vulnerability in the Top 10 chart.

## 2.6 Overall Findings

Throughout the assessment, the ITSE discovered **1 Medium,** and **2 Low** Severity security findings. The brief descriptions of each covered all possible tests, initiated from the automated tools, and finished with manual testing and exploitation attempts. The overall assessment summary is as below:

| **Domain** | Critical | High | Medium | Low |
|---|---|---|---|---|
| Internal Portal | - | - | 1 | 2 |
| External Portal | - | - | - | - |
| **Total Vulnerability** | - | - | 1 | 2 |

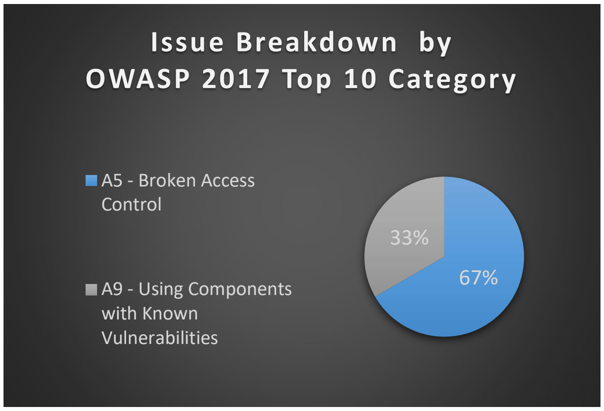
## 2.7 Overall Vulnerability Distribution

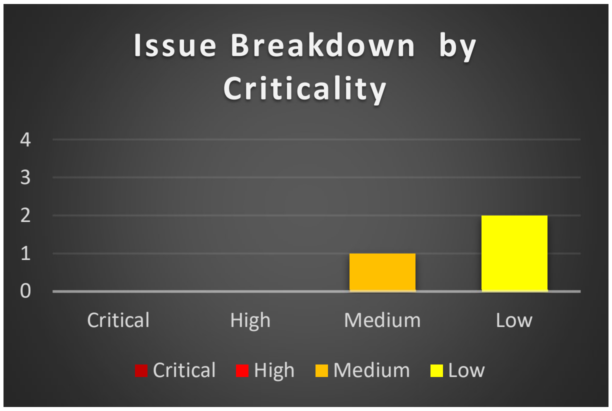
The following table shows the overall risk assessment result summary.

Internal User Portal

| Chapter | Findings | Severity | Page | Current Status |
|---|---|---|---|---|
| 3.1.1 | Authenticated IDOR: Merchant User Maintenance | Medium | 13 | OPEN |
| 3.1.2 | Authenticated IDOR: Merchant Audit Trail | Low | 15 | OPEN |
| 3.1.3 | Usage of Vulnerable Components | Low | 17 | OPEN |

The following charts group discovered vulnerabilities by OWASP vulnerability type, and by overall estimated severity.





# 3.0 Web Application Penetration Test Findings

## 3.1 Internal User Portal

### 3.1.1 Authenticated IDOR: Merchant User Maintenance

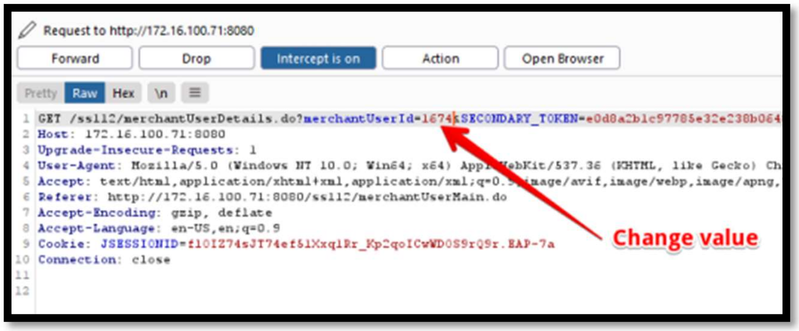
| OWASP Category | A5-Broken Access Control | Severity Score | ⚠ Medium (4.4) |
|---|---|---|---|
| CVSS V3 Vector String | CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:L | | |
| Affected URL | • http://172.16.100.71:8080/ss112/merchantUserDeleteConfirm.do?merchantUserId=1454&SECONDARY_TOKEN={random token}<br>• http://172.16.100.71:8080/ss112/merchantUserDetails.do?merchantUserId=1454&SECONDARY_TOKEN={random token}<br>• http://172.16.100.71:8080/ss112/merchantUserDetailsEdit.do?merchantUserId=1454&SECONDARY_TOKEN={random token} | | |
| **Description**<br>An insecure direct object reference occurs when an attacker gains direct access by using user-supplied input to an object that has no authorization to access. Attackers can bypass the authorization mechanism to access resources in the system directly by exploiting this vulnerability.<br>The ITSE discovered that the tested application was vulnerable to this vulnerability and the detail of it were discussed in the PoC section. | | | |
| **Proof of Concept (POC)** | | | |

**Credential**

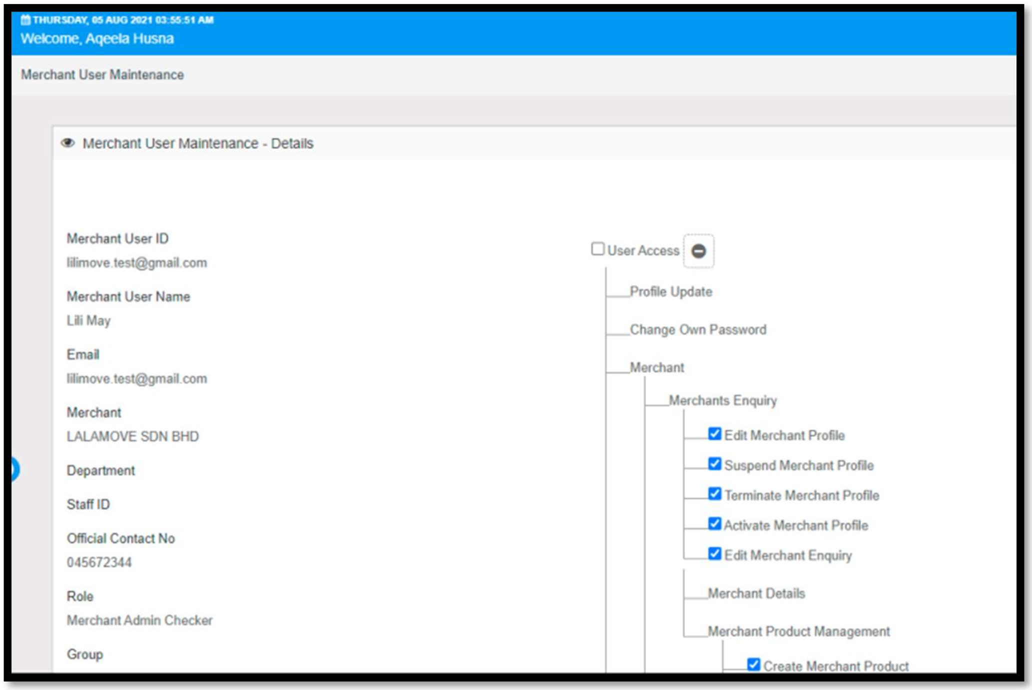
**Merchant:** Aressa Education || **User:** Aqila Husna || **Role:** Merchant Maker

**View another user information**

1. Go to the **Merchant User Maintenance** module and Click Search.
2. On Result output, choose 👁 icon and intercept the request.
3. Change the **merchantUserId** value to any other valid number and we now can view any user from any company information. This number can be guessed or brute-forced.



```
GET /ss112/merchantUserDetails.do?merchantUserId=1674&SECONDARY_TOKEN=e0d8a2b1c97785e32e238b064
Host: 172.16.100.71:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
Referer: http://172.16.100.71:8080/ss112/merchantUserMain.do
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=f10I274sJT74ef51Xxq1Rr_Kp2qoICwWD0S9rQ9r.EAP-7a
Connection: close
```



Merchant User Maintenance - Details

Merchant User ID
lilimove.test@gmail.com

Merchant User Name
Lili May

Email
lilimove.test@gmail.com

Merchant
LALAMOVE SDN BHD

Department

Staff ID

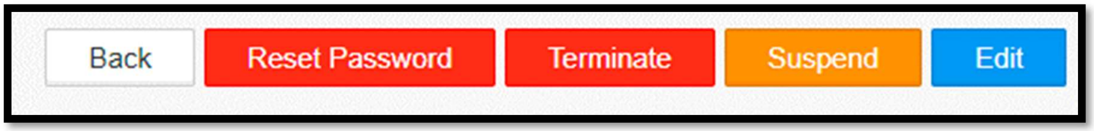
Official Contact No
045672344

Role
Merchant Admin Checker

Group

- □ User Access
  - Profile Update
  - Change Own Password
  - Merchant
    - Merchants Enquiry
      - ☑ Edit Merchant Profile
      - ☑ Suspend Merchant Profile
      - ☑ Terminate Merchant Profile
      - ☑ Activate Merchant Profile
      - ☑ Edit Merchant Enquiry
    - Merchant Details
    - Merchant Product Management
      - ☑ Create Merchant Product

Successfully view users from other company personal information and their role details



This vulnerability when chained enables us to Reset Passwords, Terminate, Suspend, and even Edit the data for the target user. However, checker approval was mandatory to realize these changes.

| | |
|---|---|
| Recommendation | Perform user authorization properly and consistently. The user should not have access to the data to which they were not supposed to have access. In addition, the developer also can hash (with salt) the value to make it harder to guess. |

| | |
|---|---|
| Review by | Name:<br>Position: |
| Status | OPEN |

### 3.1.2 Authenticated IDOR: Merchant Audit Trail

| | | | |
|---|---|---|---|
| OWASP Category | A5-Broken Access Control | Severity Score | ⚠ Low (2.6) |
| CVSS V3 Vector String | CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N | | |
| Affected URL | • http://172.16.100.71:8080/ss129/rppMerchantAuditLogDetail.do?viewActivityId=4197&SECONDARY_TOKEN={random _roken} | | |

**Description**

An insecure direct object reference occurs when an attacker gains direct access by using user-supplied input to an object that has no authorization to access. Attackers can bypass the authorization mechanism to access resources in the system directly by exploiting this vulnerability.

The ITSE discovered that the tested application was vulnerable to this vulnerability and the detail of it were discussed in the PoC section.

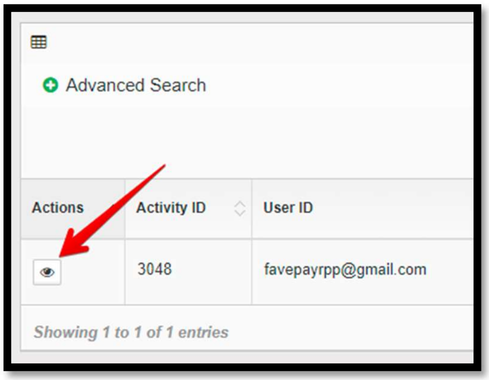
**Proof of Concept (POC)**

**Credential**

**Merchant:** Aressa Education || **User:** Aqila Husna || **Role:** Merchant Maker

**View another user information**

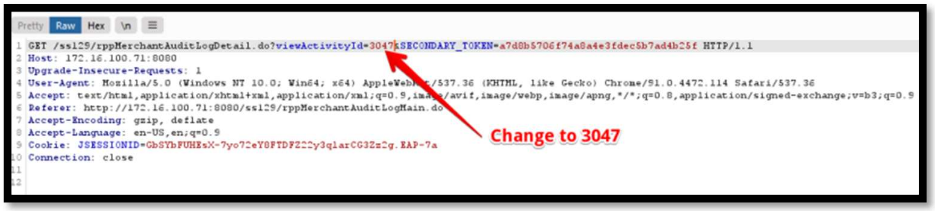
1. Go to the **Merchant Audit Trail** module and Click Search.
2. On any result, choose 👁 icon and intercept the request.
3. Change the **viewActivityID** value to any other valid number and we now can view any Audit Trail information. This number can be guessed, or brute-forced.



Advanced Search

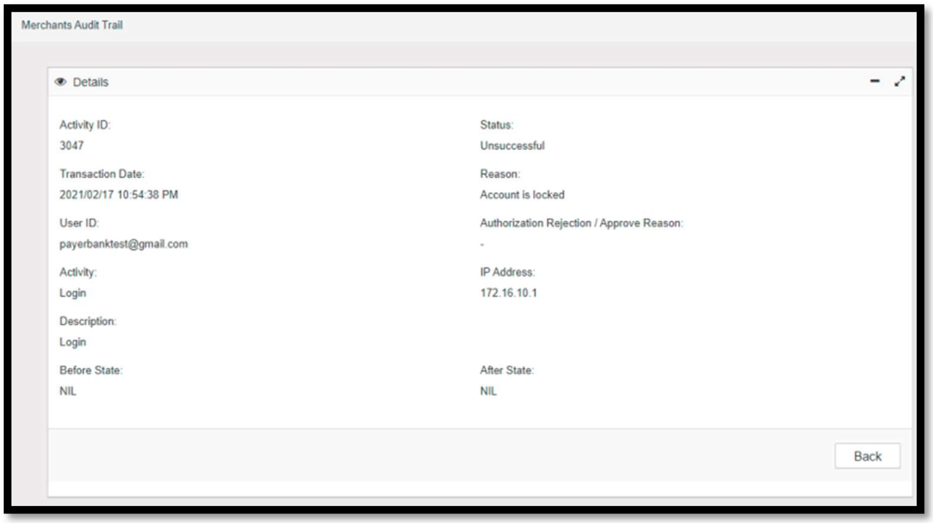
| Actions | Activity ID | User ID |
|---|---|---|
| 👁 | 3048 | favepayrpp@gmail.com |

*Showing 1 to 1 of 1 entries*



```
GET /ss129/rppMerchantAuditLogDetail.do?viewActivityId=3047&SECONDARY_TOKEN=a7d8b5706f74a8a4e3fdec5b7ad4b25f HTTP/1.1
Host: 172.16.100.71:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 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=0.9
Referer: http://172.16.100.71:8080/ss129/rppMerchantAuditLogMain.do
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=GbSYbFUHEsX-7yo72eY0FTDFZ22y3qlarCG3Zz2g.EAP-7a
Connection: close
```

Change to 3047



Merchants Audit Trail

Details

| | |
|---|---|
| Activity ID:<br>3047 | Status:<br>Unsuccessful |
| Transaction Date:<br>2021/02/17 10:54:38 PM | Reason:<br>Account is locked |
| User ID:<br>payerbanktest@gmail.com | Authorization Rejection / Approve Reason:<br>- |
| Activity:<br>Login | IP Address:<br>172.16.10.1 |
| Description:<br>Login | |
| Before State:<br>NIL | After State:<br>NIL |

Successfully view the Audit Trail

| | |
|---|---|
| Recommendation | Perform user authorization properly and consistently. The user should not have access to the data to which they were not supposed to have access. In addition, the developer also can hash (with salt) the value to make it harder to guess. |
| Review by | Name:<br>Position: |
| Status | **OPEN** |

### 3.1.3 Usage of Vulnerable Components

| | | | |
|---|---|---|---|
| OWASP Category | A9 - Using Components with Known Vulnerabilities | Severity Score | N/A |
| CVSS V3 Vector String | N/A | | |
| Affected URL | - http://172.16.100.71:8080/js/bootstrap/bootstrap.min.js<br>- http://172.16.100.71:8080/js/libs/jquery-2.1.1.min.js | | |

**<u>Description</u>**

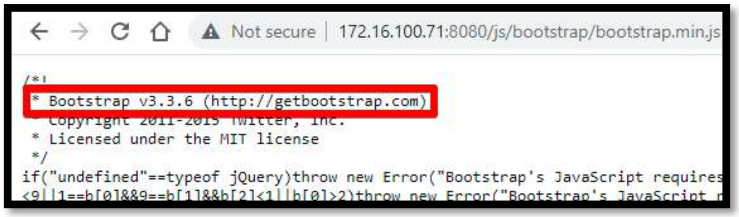
**<u>Description</u>**

Based on the enumeration activity, the ITSE discovered that the web application was using the following technology:

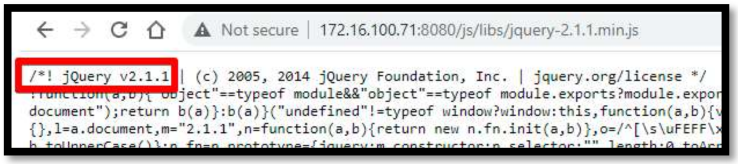
| Component | Version | Known CVE |
|---|---|---|
| Bootstrap | 3.3.6 | CVE-2019-8331, CVE-2018-14041, CVE-2018-14040 and CVE-2018-14042 |
| JQuery | 2.1.1 | CVE-2015-9251, CVE-2015-9251, CVE-2019-11358, CVE-2020-11022 and CVE-2020-11023 |

A cross-check with a vulnerability database discovered that both components running the said version were vulnerable to Cross-Site Scripting (XSS).

**Proof of Concept (POC)**



```
/*!
 * Bootstrap v3.3.6 (http://getbootstrap.com)
 * Copyright 2011-2015 Twitter, Inc.
 * Licensed under the MIT license
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires
<9||1==b[0]&&9==b[1]&&b[2]<1||b[0]>2)throw new Error("Bootstrap's JavaScript r
```



```
/*! jQuery v2.1.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.expor
document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){v
{},l=a.document,m="2.1.1",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\x
b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArr
```

| | |
|---|---|
| Recommendation | • For Bootstrap, it is advisable to upgrade the library to version 3.4.1.<br>• For jQuery, it is advisable to upgrade the library to version 3.5.0. |
| Review by | Name:<br>Position: |
| Status | **OPEN** |

## 4.0 Conclusion

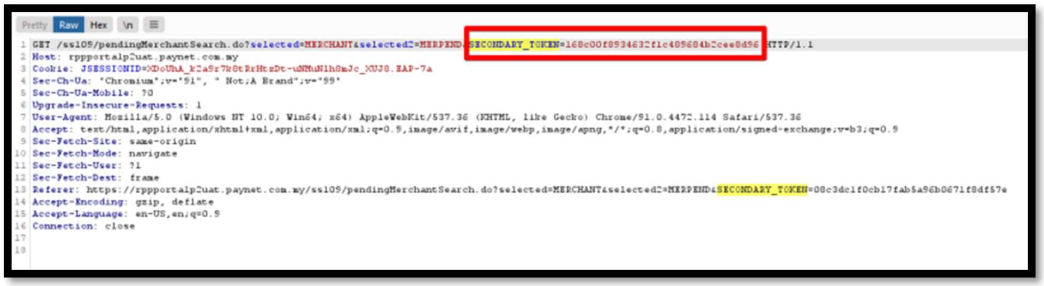
The assessment concluded with **1 Medium,** and **2 Low** severity security finding while we found the application to be built around a solid security model. The IDOR vulnerability is a major common vulnerability discovered which in the future requires a developer to focus on. Therefore, the overall web application security posture of the BO Portal is considered **Good**.

# 5.0 Appendix

The application has been tested using various common web application testing techniques. Web crawling and directory/file brute force failed to discover any juicy information which may lead to vulnerability discovery. Some of the test screen captures were as follows:

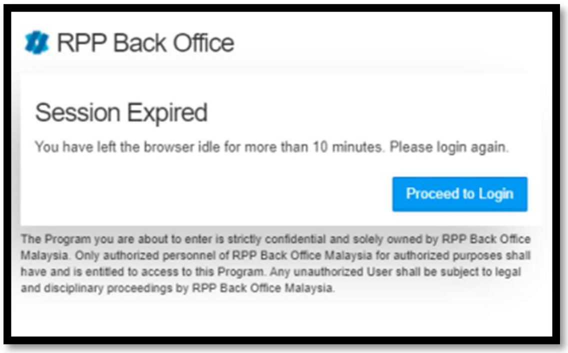
## 5.1 Screen Captures

### 5.1.1 Cloudflare DDoS Protection



```
GET /ss109/pendingMerchantSearch.do?selected=MERCHANT&selected2=MERPEND&SECONDARY_TOKEN=168c00f8934632f1c489684b2cee8d96 HTTP/1.1
Host: rppportalp2uat.paynet.com.my
Cookie: JSESSIONID=XDoUhA_k2a9r7k8tRrHtzDt-uNMuNlh8mJc_XUJ8.EAP-7a
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: frame
Referer: https://rppportalp2uat.paynet.com.my/ss109/pendingMerchantSearch.do?selected=MERCHANT&selected2=MERPEND&SECONDARY_TOKEN=08c3dc1f0cb17fab5a96b0671f8df57e
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Each request was protected by a one-time random token, thus reducing the capability of a fuzzing attack



RPP Back Office

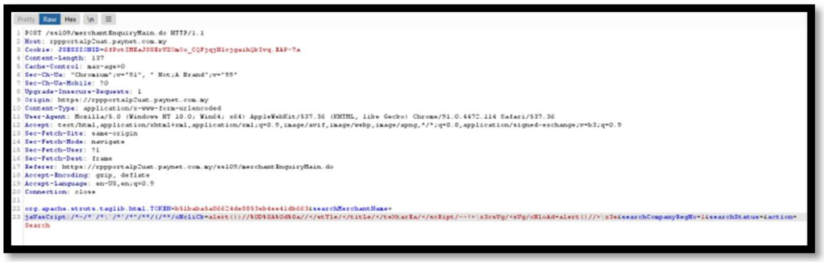
Session Expired

You have left the browser idle for more than 10 minutes. Please login again.

The Program you are about to enter is strictly confidential and solely owned by RPP Back Office Malaysia. Only authorized personnel of RPP Back Office Malaysia for authorized purposes shall have and is entitled to access to this Program. Any unauthorized User shall be subject to legal and disciplinary proceedings by RPP Back Office Malaysia.

The user was automatically logout if the system traces the usage of the same token

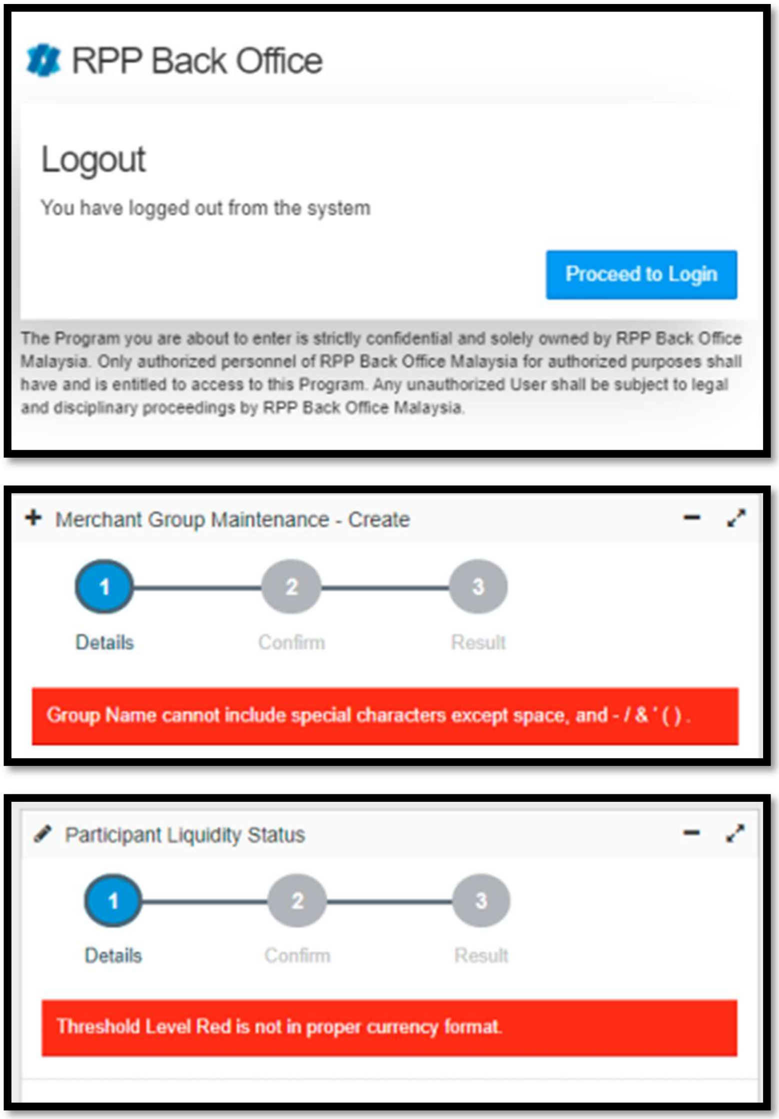
### 5.1.2 Failed Injection Test



```
POST /ss109/merchantEnquiryMain.do HTTP/1.1
Host: rppportalp2uat.paynet.com.my
Cookie: JSESSIONID=dfPotIMKaJS8KrVZOm0o_CQFjqjNlcjgaihQkIvq.EAP-7a
Content-Length: 137
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: https://rppportalp2uat.paynet.com.my
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/91.0.4472.114 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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: frame
Referer: https://rppportalp2uat.paynet.com.my/ss109/merchantEnquiryMain.do
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

org.apache.struts.taglib.html.TOKEN=b51baba5a86624de8853eb4ee41db663&searchMerchantName=
jaVasCript:/*-/*`/*\`/*'/*"/**/(/**/oNcliCk=alert())//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert()//>\x3e&searchCompanyRegNo=1&searchStatus=&action=
Search
```

Common injection payload failed to be executed indicating a strong filter mechanism in place.



Logout

You have logged out from the system

The Program you are about to enter is strictly confidential and solely owned by RPP Back Office Malaysia. Only authorized personnel of RPP Back Office Malaysia for authorized purposes shall have and is entitled to access to this Program. Any unauthorized User shall be subject to legal and disciplinary proceedings by RPP Back Office Malaysia.

Group Name cannot include special characters except space, and - / & ' ( ) .

Threshold Level Red is not in proper currency format.

Usage of illegal character will lead to forced lockout or warning.