We Test Pens Incorporated

COMP90074 - Web Security Assignment 2

Xiande Wen

905003

**PENETRATION TEST REPORT FOR**

**Bank of UniMelb Pty. Ltd. - WEB APPLICATION**

**Report delivered: 04/06/2021**

# Executive Summary

We Test Pens Incorporated has carried out an exhaustive penetration test of web application <http://assignment-zeus.unimelb.life/> at the request of Bank of UniMelb Pty. Ltd.

At the conclusion of the test, five vulnerabilities (and their associated risks) have been uncovered:

1. Sensitive testing / development files / directories disclosure;
2. Bypassing client-side authentication;
3. Privilege escalation;
4. Weak authentication; and
5. Insecure direct object references.

Their risks are considered to have high severity, with the most concern falling on the sensitive testing / development files / directories disclosure vulnerability in the Apache directory listing (Finding 1). This vulnerability exposes the entire system to the attacker and might lead to many other uncovered vulnerabilities and reveal system and database credentials, which will result in users’ personal information leakage and potentially direct financial losses.

Another high-risk vulnerability is bypassing the client-side authentication in the web application’s developer login functionality (Finding 2). This vulnerability allows the attacker authenticates into the system as the developer and acquire the developer privilege. The attacker could alter the code for his/her own benefit, which might lead to credentials and personal information leakage, financial losses and denial of services.

The third high-risk vulnerability is the privilege escalation in the admin panel (Finding 3). It allows the attacker to promote him/herself to an admin and perform higher privileged actions, which might lead to the system takeover and unauthorised closure of users’ accounts for denial of services. The fourth high-risk vulnerability is the weak authentication in the password change functionality (Finding 4). It allows the attacker to take over other users’ accounts to steal their personal information and perform unauthorised actions. The attacker could even take over the branch manger’s accounts to perform higher-privileged actions. The last high-risk vulnerability is the insecure object references vulnerability in the user profile page (Finding 5) and it could leak out every user’s personal information.

All these vulnerabilities are high-risk to a bank company since users’ trusts are the key for the company to survive in the industrial and such trusts can be easily destroyed and hardily to be earned back if one of the vulnerabilities ever happens. The slightest possibility of personal data leakage and direct financial losses should never be allowed.

Based on these findings, the website is not secure enough for production release. The high-risk vulnerabilities can cause severe data breach, financial losses and serious damage to the business reputation and they have to be mitigated before release.

Table of Contents

[Executive Summary 2](#_Toc73828715)

[Summary of Findings 5](#_Toc73828716)

[Detailed Findings 6](#_Toc73828717)

[Finding 1 - Sensitive testing / development files / directories disclosure vulnerability presents in the Apache directory listing 6](#_Toc73828718)

[**Description** 6](#_Toc73828719)

[**Proof of Concept** 6](#_Toc73828720)

[**Impact** 6](#_Toc73828721)

[**Likelihood** 6](#_Toc73828722)

[**Risk Rating** 6](#_Toc73828723)

[**References** 6](#_Toc73828724)

[**Recommendation** 6](#_Toc73828725)

[Finding 2 - Client-side authentication bypassing vulnerability presents in the developer login functionality 7](#_Toc73828726)

[**Description** 7](#_Toc73828727)

[**Proof of Concept** 7](#_Toc73828728)

[**Impact** 7](#_Toc73828729)

[**Likelihood** 7](#_Toc73828730)

[**Risk Rating** 7](#_Toc73828731)

[**References** 7](#_Toc73828732)

[**Recommendation** 7](#_Toc73828733)

[Finding 3 - Privilege escalation vulnerability presents in the admin panel 8](#_Toc73828734)

[**Description** 8](#_Toc73828735)

[**Proof of Concept** 8](#_Toc73828736)

[**Impact** 8](#_Toc73828737)

[**Likelihood** 8](#_Toc73828738)

[**Risk Rating** 8](#_Toc73828739)

[**References** 8](#_Toc73828740)

[**Recommendation** 8](#_Toc73828741)

[Finding 4 - Weak authentication vulnerability presents in the password change functionality 9](#_Toc73828742)

[**Description** 9](#_Toc73828743)

[**Proof of Concept** 9](#_Toc73828744)

[**Impact** 9](#_Toc73828745)

[**Likelihood** 9](#_Toc73828746)

[**Risk Rating** 9](#_Toc73828747)

[**References** 9](#_Toc73828748)

[**Recommendation** 9](#_Toc73828749)

[Finding 5 - Insecure direct object references vulnerability presents in the user profile page 10](#_Toc73828750)

[**Description** 10](#_Toc73828751)

[**Proof of Concept** 10](#_Toc73828752)

[**Impact** 10](#_Toc73828753)

[**Likelihood** 10](#_Toc73828754)

[**Risk Rating** 10](#_Toc73828755)

[**References** 10](#_Toc73828756)

[**Recommendation** 10](#_Toc73828757)

[Appendix I - Risk Matrix 11](#_Toc73828758)

[Appendix 2 - Additional Information 12](#_Toc73828759)

# Summary of Findings

A brief summary of all findings appears in the table below, sorted by Risk rating.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Reference** | **Vulnerability** |
| High | Finding 1 | Sensitive testing / development files / directories disclosure vulnerability presents in the Apache directory listing |
| High | Finding 2 | Client-side authentication bypassing vulnerability presents in the developer login functionality |
| High | Finding 3 | Privilege escalation vulnerability presents in the admin panel |
| High | Finding 4 | Weak authentication vulnerability presents in the password change functionality |
| High | Finding 5 | Insecure direct object references vulnerability presents in the user profile page |

# Detailed Findings

## Finding 1 - Sensitive testing / development files / directories disclosure vulnerability presents in the Apache directory listing

|  |  |
| --- | --- |
| **Description** | The **sensitive testing / development files / directories disclosure** vulnerabilitypresents in the Apache directory listing, which reveals the system code and expose everything to the attacker. The attacker could discover other vulnerabilities and exploit them further by inspecting the code. System and database credentials might be leaked as well, which would result in severe personal data breach and might lead to users’ direct financial losses.  The exploitation requires no authentication so the likelihood that it happens significantly increases. |
| **Proof of Concept** | <https://github.com/danielmiessler/SecLists/blob/4a2ab64/Discovery/Web-Content/common.txt> |
| **Impact** | **Negligible/Minor/Moderate/Major/Catastrophic: An attacker could do xyz with this vulnerability** |
| **Likelihood** | **Rare/Unlikely/Possible/Likely/Almost Certain: The possibility of the vulnerability being exploited** |
| **Risk Rating** | **Informational / Low / Medium / High / Extreme**  This is the reasoning behind my rating |
| **References** | **http://example.com** |
| **Recommendation** | The fix goes here |

## Finding 2 - Client-side authentication bypassing vulnerability presents in the developer login functionality

|  |  |
| --- | --- |
| **Description** | The **client-side authentication bypassing** vulnerability presents in the **developer login** functionality. |
| **Proof of Concept** |  |
| **Impact** | **Negligible/Minor/Moderate/Major/Catastrophic: An attacker could do xyz with this vulnerability** |
| **Likelihood** | **Rare/Unlikely/Possible/Likely/Almost Certain: The possibility of the vulnerability being exploited** |
| **Risk Rating** | **Informational / Low / Medium / High / Extreme**  This is the reasoning behind my rating |
| **References** | **http://example.com** |
| **Recommendation** | The fix goes here |

## Finding 3 - Privilege escalation vulnerability presents in the admin panel

|  |  |
| --- | --- |
| **Description** | Detailed description of the vulnerability, including a risk statement. |
| **Proof of Concept** | <https://github.com/danielmiessler/SecLists/blob/25d4ac4/Discovery/Web-Content/burp-parameter-names.txt> |
| **Impact** | **Negligible/Minor/Moderate/Major/Catastrophic: An attacker could do xyz with this vulnerability** |
| **Likelihood** | **Rare/Unlikely/Possible/Likely/Almost Certain: The possibility of the vulnerability being exploited** |
| **Risk Rating** | **Informational / Low / Medium / High / Extreme**  This is the reasoning behind my rating |
| **References** | **http://example.com** |
| **Recommendation** | The fix goes here |

## Finding 4 - Weak authentication vulnerability presents in the password change functionality

|  |  |
| --- | --- |
| **Description** | Detailed description of the vulnerability, including a risk statement. |
| **Proof of Concept** | <https://github.com/danielmiessler/SecLists/blob/25d4ac4/Discovery/Web-Content/burp-parameter-names.txt> |
| **Impact** | **Negligible/Minor/Moderate/Major/Catastrophic: An attacker could do xyz with this vulnerability** |
| **Likelihood** | **Rare/Unlikely/Possible/Likely/Almost Certain: The possibility of the vulnerability being exploited** |
| **Risk Rating** | **Informational / Low / Medium / High / Extreme**  This is the reasoning behind my rating |
| **References** | **http://example.com** |
| **Recommendation** | The fix goes here |

## Finding 5 - Insecure direct object references vulnerability presents in the user profile page

|  |  |
| --- | --- |
| **Description** | Detailed description of the vulnerability, including a risk statement. |
| **Proof of Concept** | <https://github.com/danielmiessler/SecLists/blob/25d4ac4/Discovery/Web-Content/burp-parameter-names.txt> |
| **Impact** | **Negligible/Minor/Moderate/Major/Catastrophic: An attacker could do xyz with this vulnerability** |
| **Likelihood** | **Rare/Unlikely/Possible/Likely/Almost Certain: The possibility of the vulnerability being exploited** |
| **Risk Rating** | **Informational / Low / Medium / High / Extreme**  This is the reasoning behind my rating |
| **References** | **http://example.com** |
| **Recommendation** | The fix goes here |

# Appendix I - Risk Matrix

All risks assessed in this report are in line with the ISO31000 Risk Matrix detailed below:



# Appendix 2 - Additional Information