

{{app\_name}}

Penetration Test Report

July 2025

Table of Contents

[Legal disclaimer 2](#_Toc205221451)

[Introduction 3](#_Toc205221452)

[Reading This Report 3](#_Toc205221453)

[Approach and Methodology 4](#_Toc205221454)

[Risk Categorization 5](#_Toc205221455)

[Recommendations and Next Steps 5](#_Toc205221456)

[Executive Summary 6](#_Toc205221457)

[List of Application Tested 6](#_Toc205221458)

[Test Credentials 6](#_Toc205221459)

[Test Team Details 6](#_Toc205221460)

[Summary of Findings 7](#_Toc205221461)

[Limitation (Scope Exclusions) 8](#_Toc205221462)

[Detailed Observations 9](#_Toc205221463)

[List of identified vulnerabilities: 9](#_Toc205221464)

[1. Vulnerability Name 9](#_Toc205221465)

[2. Vulnerability Name 11](#_Toc205221466)

# Legal disclaimer

We performed our services and prepared this report based on the information provided by Client. Accordingly, this report does not constitute an opinion or other form of assurance in accordance with any recognized auditing, review, or assurance standards.

Our work was limited to the specific activities described in this report and was based exclusively on the information made available during our fieldwork period. Accordingly, changes in circumstances or information occurring or coming to our knowledge only after completion of our work have not been reflected in the report and could affect the facts, findings, and conclusions included in this report materially.

This report has been prepared for the sole use and benefit of Client. and its parent organizations and may not be published or otherwise distributed or made accessible to third parties without our prior written consent. We disclaim any responsibility or liability to other parties to whom this report may be shown or into whose possession this report may come.

# Introduction

Client. is a software publisher. It offers an industry platform for property and casualty (P&C) insurance carriers in the U.S. and worldwide. They provide software, services, and partner ecosystem to enable our customers to run, differentiate, and grow their business.There are several add-on modules, as well as an increasing number of value-added online services provided via Client Live. Client has been serving more than 350 companies in 32 countries.

Deloitte Touche Tohmatsu India LLP & Deloitte & Touche LLP (“Deloitte & Touche” or “Deloitte” or “we” or “us” or “our”) was engaged by Client. (“Company” or “Client” or “you” or “your”) to assess selected Large Language Model application and Backend Swagger APIs by performing penetration testing to identify known vulnerabilities that could lead to impact of Confidentiality, Integrity, and Availability of systems/data. This report provides the observations and recommendations from this LLM Application Penetration Test (the “assessment”) conducted on the following LLM application selected by you (the “List of Application Tested”)

## Reading This Report

Client. has engaged Deloitte to assess their Application and Swagger API. This report outlines our observations on LLM Application Security Assessment that was conducted from the period:

|  |  |  |
| --- | --- | --- |
| Start Date | | End Date |
| {{ start\_date }} | {{ end\_date }} | |

This report contains the following sections:

**Section I - Executive Summary:** This section contains the background and brief understandings of the project.

**Section II - Detailed Observation:** This section contains detailed observations of LLM Application Security Assessment activity. To facilitate adequate understanding, each exception identified as part of the review is classified into Description (the details of the exception under consideration), Potential business impact (the impact that may cause on business due to successful exploitation of identified vulnerabilities), and Recommendation (detailed remediation plan for prompt closure of vulnerabilities identified).

## Approach and Methodology

The security assessment was performed according to Deloitte’s security assessment methodology. A high-level summary of the approach is detailed in the sections below: The information acquired during this phase was used to:

* Identify potential attack vectors.
* Understand potential technology-specific security vulnerabilities.

Manual testing was performed to identify additional security vulnerabilities in the design of the application. We leveraged our experience related to manual LLM application security testing and our understanding of weaknesses in common coding practices to identify security weaknesses in the application. For each of the identified potential weaknesses, we attempted to exploit the vulnerability to verify that the application is susceptible to attack and to fully understand the impact of the weaknesses. Additionally, we attempted to understand whether multiple lower-risk or medium-risk vulnerabilities constitute a higher risk-rated vulnerability when exploited together based on management-agreed definitions of risk criteria.

We assessed the LLM susceptibility to a variety of attacks including the Open Web Application Security Project (OWASP) – LLM Top Ten 2023 security flaws:

* Prompt Injection
* Insecure Output Handling
* Training Data Poisoning
* Model Denial of Service
* Supply Chain Vulnerabilities
* Sensitive Information Disclosure
* Insecure Plugin Design
* Excessive Agency
* Overreliance
* Model Theft

We assessed the APIs for susceptibility to a variety of attacks including the Open Web Application Security Project (OWASP) – API Top Ten -2023 security flaws:

* Broken Object Level Authorization
* Broken Authentication
* Broken Object Property Level Authorization
* Broken Function Level Authorization
* Unrestricted Access to Sensitive Business Flows
* Server-Side Request Forgery
* Security Misconfiguration
* Improper Inventory Management
* Unsafe Consumption of APIs

## Risk Categorization

To provide management with an indication as to the significance of risk involved and the priority with which the same needs to be addressed; all risks have been rated in accordance with the classifications given below:

|  |  |  |
| --- | --- | --- |
| **Severity** | **CVSS Score** | **Description** |
| ***Critical*** | 9.0 - 10.0 | Weakness in controls that represent exposure to the organization or Risks that could seriously compromise the control framework, data integrity, and/or operational efficiency. These risks need to be addressed with utmost priority. |
| ***High*** | 7.00 – 8.9 | A potential weakness in controls, which could develop into an exposure. Or Issues that represent areas of concern and may impact controls. They should be addressed reasonably promptly. |
| ***Medium*** | 4.0 – 6.9 | Potential weaknesses in controls, which in combination with other weaknesses can develop into exposure. Suggested improvements not immediately/directly affecting controls. |
| ***Low*** | * 1. – 3.9 | Vulnerabilities in the low range typically have very little impact on an organization's business. The exploitation of such vulnerabilities usually requires local or physical system access. |
| ***Info*** | 0.0 | This category vulnerability severity does not represent a threat on its own, however, it may provide significant information to perform sophisticated attacks by an adversary. |

## Recommendations and Next Steps

Using the recommended remediation actions from this review, we have identified the following key actions that management should take as a matter of priority to improve the security of the application before its release into production:

|  |  |
| --- | --- |
|  | Immediate remediation should focus on issues to prevent unauthorized access, data exposure, and system compromise. Key actions include enforcing prompt validation to prevent LLM prompt injection and access control bypass, securing Swagger UI through input sanitization, and mitigating Client-side command injection. Controls must also restrict LLM model version and DevKey manipulations, resolve HTTP request smuggling through consistent parsing, and address clickjacking using secure headers. Misconfigured CORS and CSP policies should be corrected to prevent cross-origin and browser-based attacks. Strengthening authentication, input validation, and secure configurations will reduce the attack surface and align the application with best practices. |

# Executive Summary

Client. engaged Deloitte India to conduct an LLM Application Security Assessment of its applications. The purpose of the engagement was to utilize active exploitation techniques to evaluate the security of the application against best practice criteria and to validate its security mechanisms and identify application-level vulnerabilities.

LLM Application Security Assessment provides Client. with insight into the resilience of an application to withstand attack from unauthorized users and the potential for valid users to abuse their privileges and access. The assessment evaluates the security of the Applications against best practice criteria to validate security mechanisms and identify application-level vulnerabilities.

The summary below provides a non-technical audience with a summary of the key findings and relates these backs to business impacts.

## List of Application Tested

|  |  |  |  |
| --- | --- | --- | --- |
| S. No. | Application Name | Application Version | URL{% for a in app\_details %} |
| {{ loop.index }} | {{ a.app\_name }} | {{ a.app\_version }} | {{ a.app\_url }} {% endfor %} |

## Test Credentials

|  |  |  |  |
| --- | --- | --- | --- |
| S. No | Username | Role | Email-ID {% for c in test\_credentials %} |
| {{ loop.index }} | {{ c.name }} | {{ c.role }} | {{ c.email }} {% endfor %} |

## Test Team Details

|  |  |  |  |
| --- | --- | --- | --- |
| S. No | Team Member Name | Role | Email-ID |
| 1 | Reviewer 1 | Engagement Director | [r@r.com](mailto:r@r.com) |
| 2 | Reviewer 2 | Quality Assurance | [r@r.com](mailto:r@r.com) |
| 3 | Reviewer 3 | Engagement Manager & Penetration Tester | [r@r.com](mailto:r@r.com)  {% for p in pentesters %} |
| {{ loop.index + 3 }} | {{ p.pentester\_name }} | {{ p.pentester\_role }} | {{ p.pentester\_email }}{% endfor %} |

## Summary of Findings

LLM and API security assessment activity performed on {{ app\_name }} uncovered 1 Medium, 4 Low and 4 Informational severity vulnerabilities representing significant threats to the application.

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerability ID | Vulnerability Title | CVSS Score | Risk Rating {% for v in vulnerabilities %} |
| {{ v.vulnerability\_id }} | {{ v.title }} | {{ v.cvss\_score }} | **{{ v.severity }}**{% endfor %} |

## Limitation (Scope Exclusions)

Given the inherent limitations in any system of control, projection of any evaluation of the controls to future periods is subject to the risk that the control procedures may become inadequate because of changes in systems, conditions, or the degree of compliance with those procedures. The assessment is based on the current body of knowledge and not designed to detect all weaknesses in controls.

The procedures we performed did not constitute an examination or a review in accordance with generally accepted auditing standards or attestation standards. Accordingly, we provide no opinion, attestation, or another form of assurance with respect to our work or the information upon which our work was based. We did not audit or otherwise verify the information supplied to us in connection with the engagement, from whatever source, except as may be specified in this report or our engagement letter. Our work was limited to the specific procedures and analysis described in the report and was based only on the information made available to us during the engagement. Accordingly, changes in circumstances after our review could affect the findings outlined in this report.

# Detailed Observations

## List of identified vulnerabilities:

{% for item in vuln\_details %}

### {{ item.title }}

|  |  |
| --- | --- |
| **Vulnerability ID** | {{ item.vulnerability\_id }} |
| **Redacted Summary** | {{ item.summary }} |
| **Description** | {{ item.description }} |
| **Severity** | **{{ item.severity }}** |
| **CVSS Score** | {{ item.cvss\_score }} |
| **CVSS Vector (v3.1)** | {{ item.cvss\_vector }} |
| **Affected Application/ URL** | {{ item.affected\_url }} |
| **Business Impact** | {{ item.business\_impact }} |
| **Recommendation** | {{ item.recommendation }} |
| **CVE ID/CWE ID** | {{ item.cwe\_id }} |
| **Reference** | {{ item.reference }} |

**Steps To Reproduce:**

{% for step in item.step\_entries %}

Step {{ step.index }}: {{ step.description }}

{% if step.screenshot %}

{{ step.screenshot }}

{% endif %}

{% endfor %}

**{% endfor %}**



**About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to Clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest Clients under the rules and regulations of public accounting. Please see [www.deloitte.com/about](https://www2.deloitte.com/us/en/legal/about-deloitte.html) to learn more about our global network of member firms.

Copyright © 2025 Deloitte Development LLC. All rights reserved.