SECURITY ANALYSIS REPORT

Security Analysis Report

Provider:

Client: {'name': 'Client Name', 'address': '456 Client Avenue, Suite 789, App City, 12345'}

Scan ID: 9b1361ea-20f0-46ac-baaf-1fe5907249f0

Date: 2026-02-05 05:39:30

Version: 1.0.0

CONFIDENTIAL

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The security assessment of the provided repository identified several potential security vulnerabilities across various severity levels. This report outlines the findings, their potential impact, and provides recommendations for mitigation to enhance the overall security posture of the application.

Identified Vulnerabilities

ID	Title	CVSS	Page
C1	Unsafe Hugging Face Hub Download	9.0	5
C2	Potential Sensitive Data Exposure in Errors	8.5	10

METHODOLOGY

Introduction

This report details the results of a security assessment conducted on the specified repository. The analysis involved a multi-layered approach, combining automated static analysis tools with advanced, AI-driven verification and enrichment to identify potential security vulnerabilities.

Objective

The primary objective of this assessment was to identify security weaknesses, assess their potential impact, and provide actionable recommendations for remediation to improve the overall security posture of the application.

Scope

The assessment was performed on the source code of the repository cloned at the time of the scan. The analysis focused on common web application vulnerabilities, insecure coding practices, and dependency risks.

Systems in Scope

No systems explicitly defined.

User Accounts

As this was a static source code analysis, no user accounts were provisioned or tested.

FINDINGS

C1 – Unsafe Hugging Face Hub Download

Severity:	Critical
CVSS Score:	9.0
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Target:	Hugging Face model downloads

Overview

The application uses Hugging Face models without specifying a revision, making it vulnerable to potential security issues in updated models.

Details

The `AutoTokenizer.from_pretrained` and `AutoModelForCausalLM.from_pretrained` calls do not specify a revision, which can lead to unintended model updates.

Evidence

- **Vulnerable Code:** analysis_engine/analyzers/llm_analyzer.py:60-61

References

- https://huggingface.co/docs/hub/security

Recommendation

- Specify a model revision when downloading from the Hugging Face Hub. - Implement regular model updates and security reviews. - Use a pinned version of the Hugging Face library to control updates.

M1 – Insecure Tempfile Usage

Severity:	Medium
CVSS Score:	6.5
CVSS Vector:	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
Target:	Temporary file handling

Overview

The application uses temporary files insecurely, which could lead to information disclosure or tampering.

Details

The regex pattern for insecure tempfile usage has been identified, indicating potential issues with temporary file handling.

Evidence

- **Vulnerable Code:** analysis_engine/analyzers/regex_analyzer.py:212

References

- https://docs.python.org/3/library/tempfile.html

Recommendation

- Use secure tempfile handling practices. - Implement proper error handling for tempfile operations. - Regularly review and update tempfile-related code for security.

L1 – Sensitive Data Exposure in Errors

Severity:	Low
CVSS Score:	3.5
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Target:	Error handling and logging

Overview

The application may expose sensitive data through error messages, potentially leaking internal implementation details or user data.

Details

Error messages contain detailed information about internal errors, which could be exploited to gather sensitive information.

Evidence

- **Vulnerable Code:** app/routes/main.py:75, app/routes/main.py:166, app/routes/main.py:195, app/routes/main.py:259, app/services/flaskFastApi_info_service.py:347

References

- https://owasp.org/www-community/attacks/Information_disclosure

Recommendation

- Implement custom error handlers to provide generic error messages. - Log detailed error information securely for diagnostic purposes. - Train developers on secure error handling practices.

ENDPOINT SECURITY ANALYSIS

This section provides a detailed security-oriented analysis of the identified API endpoints, including authentication mechanisms, data handling characteristics, potential security risks, and regulatory compliance considerations.

Endpoint Path	/api/auth/google/login
HTTP Methods	GET
Source Location	: 23
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
GDPR	No	low	Endpoint appears to be for authentication initiation and does not directly process personal data for non-auth purposes.
CCPA/CPRA	No	low	Endpoint appears to be for authentication initiation and does not directly process personal data for non-auth purposes.
LGPD	No	low	Endpoint appears to be for authentication initiation and does not directly process personal data for non-auth purposes.
PIPEDA	No	low	Endpoint appears to be for authentication initiation and does not directly process personal data for non-auth purposes.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path	/api/auth/google/callback
HTTP Methods	GET
Source Location	: 46
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
GDPR	No	low	Endpoint appears to be for authentication callback and does not directly process personal data for non-auth purposes.
CCPA/CPRA	No	low	Endpoint appears to be for authentication callback and does not directly process personal data for non-auth purposes.
LGPD	No	low	Endpoint appears to be for authentication callback and does not directly process personal data for non-auth purposes.
PIPEDA	No	low	Endpoint appears to be for authentication callback and does not directly process personal data for non-auth purposes.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path	/api/auth/google/session
HTTP Methods	GET
Source Location	: 82
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
GDPR	No	low	Endpoint appears to retrieve session information and does not directly process personal data for non-auth purposes.
CCPA/CPRA	No	low	Endpoint appears to retrieve session information and does not directly process personal data for non-auth purposes.
LGPD	No	low	Endpoint appears to retrieve session information and does not directly process personal data for non-auth purposes.
PIPEDA	No	low	Endpoint appears to retrieve session information and does not directly process personal data for non-auth purposes.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path	/api/change-plan
HTTP Methods	POST
Source Location	: 55
Authentication Required	Yes (unknown)
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: .

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is required for this endpoint but not detected.

  Potential Attack Scenario:

  An unauthenticated user could change their plan, potentially leading to unauthorized access or billing issues.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
GDPR	Yes	medium	Endpoint modifies user's plan which may involve personal data. Lack of authentication increases risk of unauthorized data modification.
CCPA/CPRA	Yes	medium	Endpoint modifies user's plan which may involve personal data. Lack of authentication increases risk of unauthorized data modification.
LGPD	Yes	medium	Endpoint modifies user's plan which may involve personal data. Lack of authentication increases risk of unauthorized data modification.
PIPEDA	Yes	medium	Endpoint modifies user's plan which may involve personal data. Lack of authentication increases risk of unauthorized data modification.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path	/api/auth/logout
HTTP Methods	POST
Source Location	: 79
Authentication Required	Yes (unknown)
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: .

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is required for this endpoint but not detected.

  Potential Attack Scenario:

  An unauthenticated user could attempt to log out, which might expose session-related information or cause denial-of-service if improperly handled.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
GDPR	No	low	Logout endpoint typically does not process personal data directly, but proper authentication is crucial for session security.
CCPA/CPRA	No	low	Logout endpoint typically does not process personal data directly, but proper authentication is crucial for session security.
LGPD	No	low	Logout endpoint typically does not process personal data directly, but proper authentication is crucial for session security.
PIPEDA	No	low	Logout endpoint typically does not process personal data directly, but proper authentication is crucial for session security.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path	/api/get-plan
HTTP Methods	GET
Source Location	: 87
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (medium): Authentication is recommended for this endpoint but not detected.

  Potential Attack Scenario:

  Unauthorized users could access plan details, potentially revealing sensitive subscription information.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
GDPR	Yes	medium	Endpoint may expose plan details which could be linked to a user, thus falling under personal data if not properly secured.
CCPA/CPRA	Yes	medium	Endpoint may expose plan details which could be linked to a user, thus falling under personal data if not properly secured.
LGPD	Yes	medium	Endpoint may expose plan details which could be linked to a user, thus falling under personal data if not properly secured.
PIPEDA	Yes	medium	Endpoint may expose plan details which could be linked to a user, thus falling under personal data if not properly secured.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path	/api/analyze
HTTP Methods	POST
Source Location	: 98
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is required for this endpoint but not detected.

  Potential Attack Scenario:

  Unauthorized users could trigger repository analysis, potentially consuming excessive resources or gaining insights into internal structures.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
GDPR	Yes	medium	Repository analysis might indirectly involve personal data if the repository contains PII. Unauthorized access could lead to data breaches.
CCPA/CPRA	Yes	medium	Repository analysis might indirectly involve personal data if the repository contains PII. Unauthorized access could lead to data breaches.
LGPD	Yes	medium	Repository analysis might indirectly involve personal data if the repository contains PII. Unauthorized access could lead to data breaches.
PIPEDA	Yes	medium	Repository analysis might indirectly involve personal data if the repository contains PII. Unauthorized access could lead to data breaches.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path	/api/generate-report
HTTP Methods	POST
Source Location	: 176
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is required for this endpoint but not detected.

  Potential Attack Scenario:

  Unauthorized users could generate reports, potentially leading to resource exhaustion or the creation of misleading/unwanted reports.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
GDPR	Yes	medium	Report generation might involve or create summaries of personal data. Lack of authentication allows unauthorized access/creation.
CCPA/CPRA	Yes	medium	Report generation might involve or create summaries of personal data. Lack of authentication allows unauthorized access/creation.
LGPD	Yes	medium	Report generation might involve or create summaries of personal data. Lack of authentication allows unauthorized access/creation.
PIPEDA	Yes	medium	Report generation might involve or create summaries of personal data. Lack of authentication allows unauthorized access/creation.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path	/api/auth/me
HTTP Methods	GET
Source Location	: 200
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is required for this endpoint but not detected.

  Potential Attack Scenario:

  An unauthenticated user could view the profile information of any user, leading to a severe data breach.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
GDPR	Yes	high	Endpoint retrieves user profile, which is sensitive personal data. Lack of authentication poses a high risk of unauthorized data access.
CCPA/CPRA	Yes	high	Endpoint retrieves user profile, which is sensitive personal data. Lack of authentication poses a high risk of unauthorized data access.
LGPD	Yes	high	Endpoint retrieves user profile, which is sensitive personal data. Lack of authentication poses a high risk of unauthorized data access.
PIPEDA	Yes	high	Endpoint retrieves user profile, which is sensitive personal data. Lack of authentication poses a high risk of unauthorized data access.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path	/healthz
HTTP Methods	GET
Source Location	: 264
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
GDPR	No	low	Health check endpoint typically does not process personal data.
CCPA/CPRA	No	low	Health check endpoint typically does not process personal data.
LGPD	No	low	Health check endpoint typically does not process personal data.
PIPEDA	No	low	Health check endpoint typically does not process personal data.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path	/api/models
HTTP Methods	GET
Source Location	: 271
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
GDPR	No	low	Endpoint lists available models, which does not appear to directly involve personal data.
CCPA/CPRA	No	low	Endpoint lists available models, which does not appear to directly involve personal data.
LGPD	No	low	Endpoint lists available models, which does not appear to directly involve personal data.
PIPEDA	No	low	Endpoint lists available models, which does not appear to directly involve personal data.

Security Assessment Notes

CVSS Vector: N/A

References

METRICS SUMMARY

Total Findings: 2

Severity	Count
CRITICAL	**2**
HIGH	**0**
MEDIUM	**4**
LOW	**5**

DISCLAIMER

This report is generated by an automated security analysis tool.

BUSINESS RISK ADVICE

Based on a comprehensive security analysis, here are the prioritized recommendations to enhance the security posture and mitigate identified risks.

No specific business risk advice was generated for this report.