SECURITY ANALYSIS REPORT

Generated By

Backstage Rookie

Provider: Backstage Rookie

contact - swarajdarekar9@gmail.com

Client: swaraj darekar

swarajdarekar9@gmail.com

Scan ID: 3a01643c-9769-4af1-9fde-a8a641455e64

Date: 2026-02-06 19:24:13

Version: 1.0.0

TABLE OF CONTENTS

EXECUTIVE SUMMARY

A comprehensive security assessment was conducted on the provided repository, focusing on identifying potential security vulnerabilities and providing recommendations for remediation. The analysis revealed several critical, high, medium, and low-severity vulnerabilities that could potentially impact the security posture of the application.

Identified Vulnerabilities

ID	Title	CVSS	Page
C1	Unsafe Hugging Face Hub Download	9.0	
C2	Probable Insecure Usage of Temp File	8.5	
H1	Possible Binding to All Interfaces	7.5	
H2	Unsafe Hugging Face Hub Download Without Revision Pinning	7.0	
H3	Probable Insecure Temp File Usage	6.5	
M1	Insecure Temp File	5.0	
M2	Bandit B615	4.5	
L1	DNSSEC Not Enabled	2.0	
L2	Sensitive Data Exposure in Error	1.5	
L3	Sensitive Data Exposure in Error	1.0	
L4	Sensitive Data Exposure in Error	0.5	
L5	Sensitive Data Exposure in Error	0.0	

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: The application's model initialization

Overview

An unsafe Hugging Face Hub download without revision pinning was identified, which could lead to potential security vulnerabilities.

Details

The application uses the Hugging Face Hub to download models without specifying a revision. This could result in the application downloading a malicious or outdated model, potentially leading to security vulnerabilities.

Evidence

- **analysis_engine\analyzers\llm_analyzer.py:60:** The model is downloaded without specifying a revision.

References

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

Recommendation

- Pin the model revision to a specific version. - Use a secure connection to download the model. - Validate the model's integrity after download.

C2 – Probable Insecure Usage of Temp File

Severity: Critical

CVSS Score: 8.5

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Target: The application's temporary file usage

Overview

A probable insecure usage of temporary files was identified, which could lead to potential security vulnerabilities.

Details

The application uses temporary files without proper validation, which could result in temporary file vulnerabilities.

Evidence

- **analysis_engine\analyzers\regex_analyzer.py:212:** The application uses temporary files without validation.

References

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

Recommendation

- Validate temporary file usage. - Use secure temporary file creation mechanisms. - Ensure proper cleanup of temporary files.

H1 – Possible Binding to All Interfaces

Severity: High

CVSS Score: 7.5

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Target: The application's network binding

Overview

A possible binding to all interfaces was identified, which could lead to potential security vulnerabilities.

Details

The application binds to all available network interfaces, which could result in unintended exposure of the application to unauthorized access.

Evidence

- **run.py:10:** The application binds to all available network interfaces.

References

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

Recommendation

- Bind the application to a specific interface. - Use a firewall to restrict access to the application. - Use authentication and authorization mechanisms to control access.

H2 – Unsafe Hugging Face Hub Download Without Revision Pinning

Severity: High

CVSS Score: 7.0

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Target: The application's model initialization

Overview

An unsafe Hugging Face Hub download without revision pinning was identified, which could lead to potential security vulnerabilities.

Details

The application uses the Hugging Face Hub to download models without specifying a revision. This could result in the application downloading a malicious or outdated model, potentially leading to security vulnerabilities.

Evidence

- **analysis_engine\utils\model_manager.py:50:** The model is downloaded without specifying a revision.

References

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

Recommendation

- Pin the model revision to a specific version. - Use a secure connection to download the model. - Validate the model's integrity after download.

H3 – Probable Insecure Temp File Usage

Severity: High

CVSS Score: 6.5

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Target: The application's temporary file usage

Overview

A probable insecure usage of temporary files was identified, which could lead to potential security vulnerabilities.

Details

The application uses temporary files without proper validation, which could result in temporary file vulnerabilities.

Evidence

- **app\routes\main.py:212:** The application uses temporary files without validation.

References

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

Recommendation

- Validate temporary file usage. - Use secure temporary file creation mechanisms. - Ensure proper cleanup of temporary files.

M1 – Insecure Temp File

Severity: Medium

CVSS Score: 5.0

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Target: The application's temporary file usage

Overview

An insecure temp file was identified, which could lead to potential security vulnerabilities.

Details

The application uses temporary files without proper validation, which could result in temporary file vulnerabilities.

Evidence

- **analysis_engine\analyzers\regex_analyzer.py:212:** The application uses temporary files without validation.

References

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

Recommendation

- Validate temporary file usage. - Use secure temporary file creation mechanisms. - Ensure proper cleanup of temporary files.

M2 – Bandit B615

Severity: Medium

CVSS Score: 4.5

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Target: The application's model initialization

Overview

A bandit B615 vulnerability was identified, which could lead to potential security vulnerabilities.

Details

The application uses the Hugging Face Hub to download models without specifying a revision. This could result in the application downloading a malicious or outdated model, potentially leading to security vulnerabilities.

Evidence

- **analysis_engine\analyzers\llm_analyzer.py:61:** The model is downloaded without specifying a revision.

References

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

Recommendation

- Pin the model revision to a specific version. - Use a secure connection to download the model. - Validate the model's integrity after download.

L1 – DNSSEC Not Enabled

Severity: Low

CVSS Score: 2.0

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Target: The application's DNS configuration

Overview

DNSSEC was not enabled, which could lead to potential security vulnerabilities.

Details

The application's DNS configuration does not have DNSSEC enabled, which could result in DNS spoofing vulnerabilities.

Evidence

- **analysis_engine\analyzers\regex_analyzer.py:237:** DNSSEC is not enabled.

References

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

Recommendation

- Enable DNSSEC. - Use a secure connection to download the model. - Validate the model's integrity after download.

L2 – Sensitive Data Exposure in Error

Severity: Low

CVSS Score: 1.5

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Target: The application's error handling

Overview

Sensitive data exposure in error was identified, which could lead to potential security vulnerabilities.

Details

The application exposes sensitive data in error messages, which could result in sensitive data exposure vulnerabilities.

Evidence

- **app\routes\main.py:75:** Sensitive data is exposed in error messages.

References

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

Recommendation

- Implement secure error handling mechanisms. - Use logging mechanisms to track errors. - Ensure sensitive data is not exposed in error messages.

L3 – Sensitive Data Exposure in Error

Severity: Low

CVSS Score: 1.0

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Target: The application's error handling

Overview

Sensitive data exposure in error was identified, which could lead to potential security vulnerabilities.

Details

The application exposes sensitive data in error messages, which could result in sensitive data exposure vulnerabilities.

Evidence

- **app\routes\main.py:166:** Sensitive data is exposed in error messages.

References

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

Recommendation

- Implement secure error handling mechanisms. - Use logging mechanisms to track errors. - Ensure sensitive data is not exposed in error messages.

L4 – Sensitive Data Exposure in Error

Severity: Low

CVSS Score: 0.5

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Target: The application's error handling

Overview

Sensitive data exposure in error was identified, which could lead to potential security vulnerabilities.

Details

The application exposes sensitive data in error messages, which could result in sensitive data exposure vulnerabilities.

Evidence

- **app\routes\main.py:195:** Sensitive data is exposed in error messages.

References

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

Recommendation

- Implement secure error handling mechanisms. - Use logging mechanisms to track errors. - Ensure sensitive data is not exposed in error messages.

L5 – Sensitive Data Exposure in Error

Severity: Low

CVSS Score: 0.0

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Target: The application's error handling

Overview

Sensitive data exposure in error was identified, which could lead to potential security vulnerabilities.

Details

The application exposes sensitive data in error messages, which could result in sensitive data exposure vulnerabilities.

Evidence

- **app\services\flaskFastApi_info_service.py:347:** Sensitive data is exposed in error messages.

References

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

Recommendation

- Implement secure error handling mechanisms. - Use logging mechanisms to track errors. - Ensure sensitive data is not exposed in error messages.

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

Endpoint Path	/api/auth/google/login
HTTP Methods	GET
Source Location	..\routes\GoogleIntegra.py - 23
Authentication Required	No
Risk Severity	Low
CVSS Score	2.5

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
SOC 2	No	low	Authentication endpoint, typically part of a larger user management system. No sensitive data exposure detected.
ISO/IEC 27001	No	low	Authentication endpoint, typically part of a larger user management system. No sensitive data exposure detected.
CSA STAR	No	low	Authentication endpoint, typically part of a larger user management system. No sensitive data exposure detected.

Security Assessment Notes

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

References

- https://nvd.nist.gov/vuln-resources/scores/cvss

Endpoint Path /api/auth/google/callback

Endpoint Path	/api/auth/google/callback
HTTP Methods	GET
Source Location	..\routes\GoogleIntegra.py - 46
Authentication Required	No
Risk Severity	Low
CVSS Score	2.5

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
SOC 2	No	low	Callback endpoint for OAuth. Sensitive data is handled during the authentication process, but no direct exposure from this endpoint is apparent.
ISO/IEC 27001	No	low	Callback endpoint for OAuth. Sensitive data is handled during the authentication process, but no direct exposure from this endpoint is apparent.
CSA STAR	No	low	Callback endpoint for OAuth. Sensitive data is handled during the authentication process, but no direct exposure from this endpoint is apparent.

Security Assessment Notes

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

References

- https://nvd.nist.gov/vuln-resources/scores/cvss

Endpoint Path /api/auth/google/session

Endpoint Path	/api/auth/google/session
HTTP Methods	GET
Source Location	..\routes\GoogleIntegra.py - 82
Authentication Required	No
Risk Severity	Low
CVSS Score	2.5

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
SOC 2	No	low	Endpoint to retrieve Google session information. Without knowing the exact content, it's assumed to be non-sensitive user session tokens.
ISO/IEC 27001	No	low	Endpoint to retrieve Google session information. Without knowing the exact content, it's assumed to be non-sensitive user session tokens.
CSA STAR	No	low	Endpoint to retrieve Google session information. Without knowing the exact content, it's assumed to be non-sensitive user session tokens.

Security Assessment Notes

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

References

- https://nvd.nist.gov/vuln-resources/scores/cvss

Endpoint Path /api/change-plan

Endpoint Path	/api/change-plan
HTTP Methods	POST
Source Location	..\routes\main.py - 55
Authentication Required	Yes (unknown)
Risk Severity	Critical
CVSS Score	9.8

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 POST endpoint, but no authentication mechanism is detected.

  Potential Attack Scenario:
  An attacker could change the plan of any user without authentication.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Missing authentication on a write operation (POST) could lead to unauthorized changes, violating access control principles (CC6.1).
ISO/IEC 27001	Yes	high	Lack of authentication on a change-plan endpoint could lead to unauthorized access and modification of service plans, impacting confidentiality and integrity (A.9.1.2, A.9.2.1).
CSA STAR	Yes	high	Unauthenticated plan changes can lead to unauthorized access and modification of critical service configurations.

Security Assessment Notes

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References

- https://nvd.nist.gov/vuln-resources/scores/cvss

Endpoint Path /api/auth/logout

Endpoint Path	/api/auth/logout
HTTP Methods	POST
Source Location	..\routes\main.py - 79
Authentication Required	Yes (unknown)
Risk Severity	Medium
CVSS Score	6.5

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** (medium): Authentication is required for this POST endpoint, but no authentication mechanism is detected.

  Potential Attack Scenario:
  An attacker could potentially trigger logout for any user, disrupting service.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Missing authentication on a logout endpoint could be abused, though the impact is typically lower than unauthorized access. It affects session management (CC7.1).
ISO/IEC 27001	Yes	medium	Lack of authentication on logout could allow attackers to disrupt user sessions, affecting availability and potentially integrity if not handled carefully (A.9.1.2, A.9.2.1).

Regulation	Applicable	Risk Level	Reason
CSA STAR	Yes	medium	Unauthenticated logout attempts could be used for denial-of-service against users.

Security Assessment Notes

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References

- https://nvd.nist.gov/vuln-resources/scores/cvss

Endpoint Path /api/get-plan

Endpoint Path	/api/get-plan
HTTP Methods	GET
Source Location	..\routes\main.py - 87
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	2.5

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 86, 87, 86.

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
SOC 2	No	low	Read-only endpoint for plan details. Authentication is present, suggesting access control is intended.

Regulation	Applicable	Risk Level	Reason
ISO/IEC 27001	No	low	Read-only endpoint for plan details. Authentication is present, suggesting access control is intended.
CSA STAR	No	low	Read-only endpoint for plan details. Authentication is present, suggesting access control is intended.

Security Assessment Notes

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

References

- https://nvd.nist.gov/vuln-resources/scores/cvss

Endpoint Path /api/analyze

Endpoint Path	/api/analyze
HTTP Methods	POST
Source Location	..\routes\main.py - 98
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	2.5

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 97, 98, 97.

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
SOC 2	No	low	Authenticated endpoint for repository analysis. The nature of the input and output is not specified, but the authenticated access is a positive security control.
ISO/IEC 27001	No	low	Authenticated endpoint for repository analysis. The nature of the input and output is not specified, but the authenticated access is a positive security control.
CSA STAR	No	low	Authenticated endpoint for repository analysis. The nature of the input and output is not specified, but the authenticated access is a positive security control.

Security Assessment Notes

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

References

- https://nvd.nist.gov/vuln-resources/scores/cvss

Endpoint Path /api/generate-report

Endpoint Path	/api/generate-report
HTTP Methods	POST
Source Location	..\routes\main.py - 176
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	2.5

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 175, 176, 175.

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
SOC 2	No	low	Authenticated endpoint for report generation. Access control is in place.
ISO/IEC 27001	No	low	Authenticated endpoint for report generation. Access control is in place.
CSA STAR	No	low	Authenticated endpoint for report generation. Access control is in place.

Security Assessment Notes

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

References

- https://nvd.nist.gov/vuln-resources/scores/cvss

Endpoint Path /api/auth/me

Endpoint Path	/api/auth/me
HTTP Methods	GET
Source Location	..\routes\main.py - 200
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	2.5

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 199, 200, 200, 207, 199, 208, 208, 208.

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
SOC 2	No	low	Endpoint for retrieving user profile information. Authentication is required, which is appropriate for accessing personal data.
ISO/IEC 27001	No	low	Endpoint for retrieving user profile information. Authentication is required, which is appropriate for accessing personal data.
CSA STAR	No	low	Endpoint for retrieving user profile information. Authentication is required, which is appropriate for accessing personal data.

Security Assessment Notes

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

References

- https://nvd.nist.gov/vuln-resources/scores/cvss

Endpoint Path /healthz

Endpoint Path	/healthz
HTTP Methods	GET
Source Location	..\routes\main.py - 264
Authentication Required	No
Risk Severity	Low
CVSS Score	2.5

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
SOC 2	No	low	Health check endpoint. Typically does not require authentication and should not expose sensitive information.
ISO/IEC 27001	No	low	Health check endpoint. Typically does not require authentication and should not expose sensitive information.
CSA STAR	No	low	Health check endpoint. Typically does not require authentication and should not expose sensitive information.

Security Assessment Notes

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

References

- https://nvd.nist.gov/vuln-resources/scores/cvss

Endpoint Path /api/models

Endpoint Path	/api/models
HTTP Methods	GET
Source Location	..\routes\main.py - 271
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	2.5

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 270, 271, 270.

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
SOC 2	No	low	Authenticated endpoint for listing models. Access control is applied, which is appropriate for internal resource listing.
ISO/IEC 27001	No	low	Authenticated endpoint for listing models. Access control is applied, which is appropriate for internal resource listing.
CSA STAR	No	low	Authenticated endpoint for listing models. Access control is applied, which is appropriate for internal resource listing.

Security Assessment Notes

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

References

- https://nvd.nist.gov/vuln-resources/scores/cvss

METRICS SUMMARY

Total Findings: 5

Severity	Count
CRITICAL	2
HIGH	3
MEDIUM	2
LOW	5

BUSINESS RISK ADVICE

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

Enforce Authentication and Authorization on `/api/change-plan` Endpoint (Priority: Immediate)

Description: The `/api/change-plan` (POST) endpoint is reported as lacking sufficient authentication, allowing any unauthenticated user to potentially modify service plans (CVSS 9.8).

Why it Matters: This is a critical access control vulnerability directly violating SOC 2 (CC6.1), ISO 27001 (A.9.1.2), and CSA STAR principles. Unauthorized modification of service plans can lead to significant financial loss, operational disruption, and data integrity compromise.

Recommended Actions:

- Apply a robust authentication and authorization decorator (e.g., `login_required` combined with role-based access control) to the `/api/change-plan` POST endpoint in `app\routes\main.py:55`.
- Implement server-side validation to ensure the authenticated user is explicitly authorized to perform the requested plan change.
- Conduct a comprehensive review of all write-operations (POST, PUT, DELETE) endpoints to confirm proper authentication and fine-grained authorization controls are in place.

Expected Outcome: Prevents unauthorized modification of user service plans, ensuring data integrity, compliance with access control policies, and preventing business logic abuse.

Pin Hugging Face Model Revisions for Secure Downloads (Priority: Immediate)

Description: Multiple instances of Hugging Face model downloads (C1, H2, M2) are performed without specifying an immutable revision, introducing a critical supply chain risk (CVSS 9.0, 7.0, 4.5).

Why it Matters: Relying on mutable 'latest' versions can lead to the application downloading malicious or compromised models, potentially resulting in remote code execution, sensitive data exfiltration, or denial-of-service. This is a critical supply chain vulnerability.

Recommended Actions:

- Update all Hugging Face model download calls (e.g., in `analysis_engine\analyzers\llm_analyzer.py:60`, `analysis_engine\utils\model_manager.py:50`, `analysis_engine\analyzers\llm_analyzer.py:61`) to explicitly use an immutable Git commit hash or a cryptographically verified version tag.
- Implement checksum validation for all downloaded external dependencies to verify their integrity against a known good value.
- Establish and enforce a policy requiring revision pinning and integrity checks for all third-party and open-source dependencies.

Expected Outcome: Ensures the integrity and authenticity of downloaded models, significantly mitigating supply chain attack vectors and ensuring deterministic application behavior.

Secure Temporary File Creation and Handling (Priority: Immediate)

Description: The application exhibits probable insecure usage of temporary files (C2, H3, M1), lacking proper validation and secure creation mechanisms (CVSS 8.5, 6.5, 5.0).

Why it Matters: Insecure temporary file handling can lead to critical vulnerabilities such as information disclosure, arbitrary file writes, privilege escalation, or denial-of-service, compromising system integrity and confidentiality.

Recommended Actions:

- Replace insecure temporary file creation methods (e.g., `analysis_engine\analyzers\regex_analyzer.py:212`, `app\routes\main.py:212`) with Python's built-in `tempfile` module functions (e.g., `tempfile.NamedTemporaryFile`, `tempfile.mkstemp`).
- Ensure `tempfile` functions are used with appropriate permissions (e.g., `mode=0o600`) and that files are securely and promptly deleted after use.
- Validate the content, origin, and expected format of any data written to or read from temporary files to prevent injection or manipulation.

Expected Outcome: Prevents temporary file vulnerabilities, safeguarding sensitive data, preserving system resources, and preventing unauthorized code execution.

Restrict Application Network Binding to Specific Interfaces (Priority: Immediate)

Description: The application is configured to bind to all available network interfaces (H1), potentially exposing it to unintended network segments and increasing its attack surface (CVSS 7.5).

Why it Matters: Binding to '0.0.0.0' or similar significantly expands the application's exposure. This can lead to unauthorized access from internal, management, or even external networks if not properly firewalled, violating the principle of least privilege.

Recommended Actions:

- Modify the application's configuration (`run.py:10`) to explicitly bind to specific, necessary IP addresses (e.g., `127.0.0.1` for local-only access, or a specific internal IP) instead of all interfaces.
- Strengthen network segmentation and firewall rules to restrict inbound connections to only trusted hosts and ports, irrespective of the application's binding configuration.

Expected Outcome: Minimizes the application's network attack surface, reducing the risk of unauthorized access and enhancing network security posture.

Implement Authentication for Logout Endpoint and Standardize Secure Error Handling (Priority: Short-Term)

Description: The `/api/auth/logout` (POST) endpoint (`app\routes\main.py:79`) lacks explicit authentication (CVSS 6.5). Additionally, sensitive data is exposed in error messages (L2-L5) across multiple files (CVSS 1.5-0.0), and DNSSEC is not enabled (L1) (CVSS 2.0).

Why it Matters: An unauthenticated logout endpoint can be exploited for denial-of-service attacks, impacting user availability and session integrity (SOC 2 CC7.1, ISO 27001 A.9.1.2, CSA STAR). Exposing sensitive data in errors provides valuable reconnaissance to attackers. Lack of DNSSEC makes the application vulnerable to DNS spoofing, potentially redirecting users to malicious sites.

Recommended Actions:

- Apply `login_required` or an equivalent authentication middleware/decorator to the `/api/auth/logout` endpoint in `app\routes\main.py:79` to ensure only authenticated users can trigger their own logout.
- Implement a centralized error handling mechanism to catch all exceptions and return generic, non-informative error messages to clients. Log detailed error information internally for debugging, ensuring no sensitive data leaves the application.
- Review and refactor code at identified locations (e.g., `app\routes\main.py:75, 166, 195`, `app\services\flaskFastApi_info_service.py:347`) to prevent sensitive data exposure in client-facing error responses.
- Enable DNSSEC for all public-facing domains associated with the application to protect against DNS spoofing (`analysis_engine\analyzers\regex_analyzer.py:237`).

Expected Outcome: Prevents unauthorized session terminations, reduces information leakage through errors, and enhances protection against DNS-based attacks, improving overall application resilience and user experience.

Integrate Automated Static Application Security Testing (SAST) (Priority: Mid-Term)

Description: The presence of recurring vulnerabilities (e.g., insecure temporary file usage, unpinned dependencies) indicates a need for proactive and automated code-level security checks within the development lifecycle.

Why it Matters: Integrating SAST into the SDLC allows for early detection of security vulnerabilities directly within the source code, reducing remediation costs and preventing insecure patterns from reaching production environments. This aligns with SOC 2 (CC7.1) and ISO 27001 (A.14.2.5) requirements for secure system engineering.

Recommended Actions:

- Select and integrate a SAST tool (e.g., Bandit for Python, Semgrep) into the CI/CD pipeline.
- Configure SAST scans to run automatically on every code commit, pull request, or at least nightly, providing immediate feedback to developers.
- Establish gating criteria within the CI/CD pipeline to block builds or merges that introduce new critical or high-severity SAST findings.

Expected Outcome: Significantly reduces the number of new vulnerabilities introduced during development, improves code quality, and fosters a secure coding culture.

Enhance Security Monitoring, Alerting, and Incident Response Capability (Priority: Long-Term)

Description: The scan highlights several critical and high-risk areas which, combined with the general application behavior, necessitate a more robust security observation strategy to detect and respond to potential threats.

Why it Matters: Comprehensive logging, monitoring, and alerting are fundamental for detecting, responding to, and recovering from security incidents (SOC 2 CC7.2, ISO 27001 A.12.4). Without these capabilities, exploitations may go unnoticed for extended periods, increasing impact.

Recommended Actions:

- Implement centralized logging for all application, system, and network events into a Security Information and Event Management (SIEM) system with appropriate retention policies.
- Define and configure specific alerts for suspicious activities, failed authentication attempts, authorization failures, unusual system resource usage, and critical application errors.
- Establish and regularly test a formal incident response plan (IRP) to ensure timely and effective handling of security breaches, including clear roles, responsibilities, and communication protocols.

Expected Outcome: Improved visibility into security events, enabling proactive threat detection, faster incident response times, and enhanced compliance with security control requirements.