SECURITY ANALYSIS REPORT

Generated By

Backstage Rookie

Provider: Backstage Rookie

contact - swarajdarekar9@gmail.com

Client: Chandrakant Darekar

darekar138@gmail.com

Scan ID: 50fcb68b-ff89-49df-9973-695ce16cef86

Date: 2026-02-10 16:36:06

Version: 1.0.0

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This security assessment report summarizes the findings from a static analysis of the application's source code. Key vulnerabilities identified include a critical hardcoded secret, a dangerous debug mode configuration in production, and a known vulnerable dependency. Additionally, several instances of missing network call timeouts and verbose error messages exposing internal details were found. Addressing these findings is crucial for enhancing the application's security posture and protecting against potential exploitation, denial-of-service attacks, and information leakage.

Identified Vulnerabilities

ID	Title	CVSS	Page
C1	Hardcoded Sensitive Token	9.8	
H1	Flask Debug Mode Enabled in Production	9.8	
H2	Vulnerable Dependency: aiohttp (Request Smuggling)	7.5	
M1	Missing Request Timeout	5.3	
L1	Verbose Error Messages Exposing Internal Details	3.7	

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

Name	IP

User Accounts

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

FINDINGS

C1 – Hardcoded Sensitive Token

Severity: Critical

CVSS Score: 9.8

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

Target: tasks.py

Overview

A JSON Web Token (JWT) is directly hardcoded within the `tasks.py` file. This token, identified as a Supabase JWT, could grant an attacker unauthorized access to backend resources or user accounts if exposed.

Details

The `tasks.py` script contains a hardcoded JWT string used for verification purposes. Hardcoding sensitive information such as API keys, cryptographic keys, or authentication tokens poses a severe security risk. If this codebase is ever leaked, or if an attacker gains read access to the file system, they could obtain this token. Depending on the token's permissions and expiration, this could lead to unauthorized access to the application's backend, data manipulation, or full account takeover. Even if this specific token is for testing, the practice of hardcoding it sets a dangerous precedent and could lead to similar vulnerabilities with production tokens.

Evidence

- **tasks.py:14:** Hardcoded JWT token assignment: python token = "eyJhbGciOiJIUzI1NiIsImtpZCI6IkRUK3NRQURhd0Uwdm9RbkwiLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodHRwczovL2Frd2VtZWZld2ZtenhlZ2lkZXNsLnN1cGFiYXNlLmNvL2F1dGgvdjEi

References

- https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication
- https://cheatsheetseries.owasp.org/cheatsheets/Hardcoded_secrets_Cheat_Sheet.html

Recommendation

- Store all sensitive credentials, including API keys and authentication tokens, in secure environment variables or a dedicated secrets management service (e.g., HashiCorp Vault, AWS Secrets Manager, Azure Key Vault). - Never commit sensitive data directly into source code repositories. - If the token is for development/testing, ensure it is generated dynamically or loaded from a secure, non-version-controlled configuration file (e.g., `.env`) that is excluded from source control. - Implement a process to regularly rotate all sensitive secrets. - Revoke the currently hardcoded token immediately.

Prompt to Solve the Vulnerability:

In `tasks.py` at line 14, replace the hardcoded JWT token with a reference to an environment variable. First, ensure your `.env` file contains `SUPABASE_AUTH_TOKEN='your_actual_token_here'`. Then, modify the line in `tasks.py` to `token = os.getenv('SUPABASE_AUTH_TOKEN')`. Remember to import `os` and use `load_dotenv()` if you are not already doing so. Additionally, verify that `tasks.py` and other relevant files load these environment variables securely and that your `.env` file is excluded from version control (e.g., via `.gitignore`).

H1 – Flask Debug Mode Enabled in Production

Severity: High

CVSS Score: 9.8

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

Target: app.py

Overview

The Flask application is configured to run with `debug=True` in what appears to be a production-like context, potentially exposing the Werkzeug debugger and allowing arbitrary code execution.

Details

Running a Flask application with `debug=True` in a production environment is highly dangerous. The Werkzeug debugger, which is enabled by default in debug mode, allows an attacker who can access the console to execute arbitrary Python code on the server if they can guess or obtain the debugger PIN. This typically provides full access to the server's filesystem, database, and other sensitive resources. Furthermore, debug mode can lead to excessive error logging that may reveal sensitive information about the application's internal workings, including stack traces, environment variables, and configuration details.

Evidence

- **app.py:1872:** Flask application initiated with debug mode enabled: python 1870: if __name__ == '__main__': 1871: # Start the Flask app with debug mode and auto-reloader 1872: app.run(debug=True, port=5000, use_reloader=True)

References

- https://flask.palletsprojects.com/en/2.3.x/deploying/
- https://owasp.org/www-community/vulnerabilities/Server-side_request_forgery_(SSRF)

Recommendation

- Disable Flask's debug mode in production environments by ensuring `debug=False`. - Use a production-ready WSGI server (e.g., Gunicorn, uWSGI) to serve the Flask application, rather than the built-in development server. - Implement robust error handling to prevent sensitive information leakage through verbose error messages, even in a non-debug environment. - Ensure environment variables or configuration flags control debug settings and are correctly set for different deployment stages (development, staging, production).

Prompt to Solve the Vulnerability:

In `app.py` at line 1872, modify the `app.run` call to disable debug mode. Change `app.run(debug=True, ...)` to `app.run(debug=False, ...)`. For production deployments, it is strongly recommended to use a production-grade WSGI server like Gunicorn or uWSGI instead of `app.run()`. For example, you might remove the `if __name__ == '__main__':` block entirely and run the application via `gunicorn app:app`.

H2 – Vulnerable Dependency: aiohttp (Request Smuggling)

Severity: High

CVSS Score: 7.5

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

Target: aiohttp library

Overview

The application uses `aiohttp` version `3.11.10`, which is identified with CVE-2025-53643, a request smuggling vulnerability that could allow attackers to bypass security controls under specific conditions.

Details

The `aiohttp` library version `3.11.10` is vulnerable to a request smuggling attack due to incorrect parsing of HTTP request trailer sections. If the application is running a pure Python version of `aiohttp` (without its C extensions) or if `AIOHTTP_NO_EXTENSIONS` is enabled, an attacker could exploit this to smuggle requests past firewalls or proxy servers. This can lead to unauthorized access to internal resources, bypassing authentication/authorization mechanisms, or cache poisoning, compromising data confidentiality and integrity.

Evidence

- **dependency_file:** Vulnerable dependency: aiohttp==3.11.10 - CVE-2025-53643: ### Summary The Python parser is vulnerable to a request smuggling vulnerability due to not parsing trailer sections of an HTTP request. ### Impact If a pure Python version of aiohttp is installed (i.e. without the usual C extensions) or AIOHTTP_NO_EXTENSIONS is enabled, then an attacker may be able to execute a request smuggling attack to bypass certain firewalls or proxy protections.

References

- https://nvd.nist.gov/vuln/detail/CVE-2025-53643
- https://github.com/aio-libs/aiohttp/commit/e8d774f635dc6d1cd3174d0e38891da5de0e2b6a

Recommendation

- Upgrade `aiohttp` to a version that addresses CVE-2025-53643. Refer to the official `aiohttp` GitHub repository or security advisories for the patched version. - If immediate upgrade is not possible, ensure that `aiohttp` is compiled with its C extensions and that the `AIOHTTP_NO_EXTENSIONS` environment variable is not set or is set to `False` in production environments. - Regularly audit and update all project dependencies to mitigate known vulnerabilities.

Prompt to Solve the Vulnerability:

To fix the `aiohttp` vulnerability, upgrade the library to a patched version. Check the `aiohttp` changelog or security advisories for the specific version that remediates CVE-2025-53643. Then, update your `requirements.txt` or `pyproject.toml` file to reflect the new version (e.g., `aiohttp>=X.Y.Z`) and run `pip install --upgrade aiohttp` or `poetry update aiohttp`.

M1 – Missing Request Timeout

Severity: Medium

CVSS Score: 5.3

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

Target: External API calls in `routes/payments.py`

Overview

Several HTTP requests made using the `requests` library lack a specified `timeout` parameter, which can lead to indefinite hangs and potential denial-of-service conditions.

Details

The application makes multiple calls to external services (e.g., Cashfree API) using `requests.post()` and `requests.get()` without defining a `timeout`. If the external API becomes unresponsive or slow, these requests will wait indefinitely, consuming server resources (e.g., threads, memory, connections). This can lead to resource exhaustion, effectively causing a denial-of-service (DoS) for legitimate users as the application becomes unresponsive or crashes due to lack of available resources.

Evidence

- **routes\payments.py:90:** Call to requests.post without timeout: python 90: response = requests.post(91: f"{CASHFREE_BASE_URL}/orders", 92: headers=get_cashfree_headers(), 93: json=payload 94:)
- **routes\payments.py:136:** Call to requests.get without timeout: python 136: response = requests.get(137: f"{CASHFREE_BASE_URL}/orders/{order_id}", 138: headers=get_cashfree_headers() 139:)
- **routes\payments.py:663:** Call to requests.post without timeout: python 663: payout_response = requests.post(payout_api_url, json=cashfree_payout_payload, headers=cashfree_headers)

References

- https://bandit.readthedocs.io/en/latest/plugins/b113_request_without_timeout.html
- https://docs.python-requests.org/en/master/user/advanced/#timeouts

Recommendation

- Always specify a `timeout` parameter for all HTTP requests made using the `requests` library. - The timeout value should be chosen based on the expected response time of the external service and the application's tolerance for delays. - Consider implementing retry mechanisms with exponential backoff for transient network issues, but always with a maximum overall timeout.

Prompt to Solve the Vulnerability:

In `routes\payments.py`, add a `timeout` parameter to all `requests.post` and `requests.get` calls. For example, change `requests.post(url, headers=headers, json=payload)` to `requests.post(url, headers=headers, json=payload, timeout=10)`. Choose an appropriate timeout value (in seconds) based on the expected response time of the Cashfree API. Apply this change at lines 90, 136, and 663.

L1 – Verbose Error Messages Exposing Internal Details

Severity: Low

CVSS Score: 3.7

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

Target: API error responses across `app.py` and `routes/payments.py`

Overview

The application frequently includes raw Python exception messages (`str(e)`) in its JSON API responses, which can inadvertently expose sensitive internal system details to attackers.

Details

Throughout the application's API endpoints, `except Exception as e:` blocks catch general exceptions and directly expose the string representation of these exceptions in the HTTP response (e.g., `{'error': str(e)}`). This practice, while helpful for debugging during development, is insecure in production. Attackers can leverage these verbose error messages, which may contain stack traces, database query fragments, file paths, or system configuration information, to gain insights into the application's architecture, technologies used, and potential weaknesses. This information can then be used to craft more targeted and effective attacks.

Evidence

- **app.py:117:** Example of verbose error message: python 117: return jsonify({'msg': 'Registration failed', 'error': str(e)}), 500
- **app.py:187:** Example of verbose error message: python 187: return jsonify({'msg': 'Login failed', 'error': str(e)}), 500
- **routes\payments.py:115:** Example of verbose error message: python 115: return jsonify({'msg': 'Internal server error', 'error': str(e)}), 500
- **app.py (29 more locations), routes\payments.py (20 more locations):** Similar patterns of exposing `str(e)` found across numerous endpoints.

References

- https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html
- https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

Recommendation

- Replace direct exposure of `str(e)` with generic, user-friendly error messages that do not reveal internal implementation details. - Log the full exception details on the server-side for debugging purposes, but never return them to the client. - Implement a centralized error handling mechanism that converts raw exceptions into standardized, non-informative client-facing error messages. - Consider using unique error IDs for internal logging, which can be referenced in client-side messages if support calls are needed.

Prompt to Solve the Vulnerability:

Refactor all `except Exception as e:` blocks that return `str(e)` in `jsonify` responses. Instead of `return jsonify({'msg': '...', 'error': str(e)}), 500`, change it to `return jsonify({'msg': 'An unexpected error occurred. Please try again later.'}), 500`. Ensure that the actual exception details (e.g., `traceback.format_exc()`) are logged server-side for debugging without being sent to the client. Apply this consistently across all identified locations in `app.py` and `routes\payments.py`.

ENDPOINT SECURITY ANALYSIS

Endpoint Path /register

Endpoint Path	/register
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 73
Authentication Required	No
Risk Severity	Critical
CVSS Score	9.0

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 missing for the registration endpoint, allowing any user to register.

  Potential Attack Scenario:

  An attacker could create a large number of fake accounts to overwhelm the system or perform other malicious activities.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of authentication on user registration can lead to unauthorized account creation, violating principles of access control and user management.
ISO/IEC 27001	Yes	high	Inadequate access control mechanisms for user registration can lead to unauthorized access and potential compromise of user data.
CSA STAR	Yes	high	Absence of authentication on registration compromises the security of identity and access management, potentially leading to unauthorized access.

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/detail/cve-2023-XXXX
- https://owasp.org/www-community/vulnerabilities/Authentication_Bypass

Endpoint Path /login

Endpoint Path	/login
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 120
Authentication Required	No
Risk Severity	Critical
CVSS Score	9.0

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 missing for the login endpoint, allowing unauthorized access.

  Potential Attack Scenario:

  An attacker could potentially access user accounts without proper authentication, leading to data breaches or account takeover.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Missing authentication on the login endpoint compromises secure access and user authentication controls.
ISO/IEC 27001	Yes	high	Inadequate authentication mechanisms for login can lead to unauthorized access to the system and its data.
CSA STAR	Yes	high	Lack of authentication for login directly impacts the security of access control and identity management.

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/detail/cve-2023-XXXX
- https://owasp.org/www-project-authentication-cheat-sheet/

Endpoint Path /verify-instagram

Endpoint Path	/verify-instagram
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 192
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 191, 192, 193, 194.

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	Yes	low	The endpoint is authenticated, which aligns with secure access controls.
ISO/IEC 27001	Yes	low	Authentication is in place, contributing to access control.
CSA STAR	Yes	low	Authentication mechanisms support secure identity and access management.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /verify-instagram/

Endpoint Path	/verify-instagram/
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 192

Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 191, 192, 193, 194.

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	Yes	low	The endpoint is authenticated, which aligns with secure access controls.
ISO/IEC 27001	Yes	low	Authentication is in place, contributing to access control.
CSA STAR	Yes	low	Authentication mechanisms support secure identity and access management.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /request-password-reset

Endpoint Path	/request-password-reset
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 224
Authentication Required	No
Risk Severity	Low
CVSS Score	N/A

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 missing for the password reset request endpoint. This could allow unauthenticated users to initiate password resets for other users if not properly rate-limited or otherwise protected.

  Potential Attack Scenario:

  An attacker could flood the system with password reset requests for various users, potentially leading to denial of service or facilitating further attacks if the reset mechanism is weak.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	While password reset is a common function, its security is critical. Lack of authentication can be a risk if not properly managed with rate limiting and other controls.

Regulation	Applicable	Risk Level	Reason
ISO/IEC 27001	Yes	medium	Insecure password reset mechanisms can compromise user accounts and data confidentiality.
CSA STAR	Yes	medium	Inadequate protection of password reset functionality can lead to account compromise.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns

Endpoint Path	/api/brand/campaigns
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 248
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 247, 248, 249, 253.

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	Yes	low	Endpoint is authenticated, supporting access control.
ISO/IEC 27001	Yes	low	Authentication is present, contributing to access control.
CSA STAR	Yes	low	Authentication mechanisms are in place for identity and access management.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns

Endpoint Path	/api/brand/campaigns
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 292
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 291, 292, 293, 297.

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	Yes	low	Endpoint is authenticated, supporting access control.
ISO/IEC 27001	Yes	low	Authentication is present, contributing to access control.
CSA STAR	Yes	low	Authentication mechanisms are in place for identity and access management.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/campaigns

Endpoint Path	/api/campaigns
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 329
Authentication Required	No
Risk Severity	Low
CVSS Score	N/A

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): The endpoint for listing all campaigns is not authenticated. This could lead to unauthorized access to campaign data.

  Potential Attack Scenario:

  An attacker could enumerate all campaigns, potentially discovering sensitive campaign details or using this information for further targeting.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Unauthenticated access to campaign data violates principle of least privilege and can lead to unauthorized disclosure.
ISO/IEC 27001	Yes	medium	Lack of authentication for sensitive data retrieval can lead to unauthorized information disclosure.
CSA STAR	Yes	medium	Exposure of campaign data without authentication can lead to unauthorized access and potential misuse.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/campaigns/

Endpoint Path	/api/campaigns/
HTTP Methods	GET

Source Location	..\Mipoe-Backend\app.py - 388
Authentication Required	No
Risk Severity	Low
CVSS Score	N/A

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): Retrieving a specific campaign by ID is not authenticated. This could lead to unauthorized access to campaign details.

  Potential Attack Scenario:

  An attacker could access details of specific campaigns, potentially revealing sensitive information or business logic.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Unauthenticated access to campaign details violates principles of access control and data confidentiality.
ISO/IEC 27001	Yes	medium	Lack of authentication for accessing specific campaign data can lead to unauthorized disclosure.
CSA STAR	Yes	medium	Exposure of campaign details without authentication can lead to unauthorized access.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/your-campaigns

Endpoint Path	/api/creator/your-campaigns
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 495
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 494, 495, 496, 501.

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	Yes	low	Endpoint is authenticated, aligning with secure access controls.
ISO/IEC 27001	Yes	low	Authentication is in place, contributing to access control.

Regulation	Applicable	Risk Level	Reason
CSA STAR	Yes	low	Authentication mechanisms support secure identity and access management.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/submit-clip

Endpoint Path	/api/creator/submit-clip
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 583
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 582, 583, 584, 590.

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	Yes	low	Endpoint is authenticated, supporting access control.
ISO/IEC 27001	Yes	low	Authentication is present, contributing to access control.
CSA STAR	Yes	low	Authentication mechanisms are in place for identity and access management.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/campaign-clips

Endpoint Path	/api/creator/campaign-clips
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 657
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 656, 657, 658, 662.

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	Yes	low	Endpoint is authenticated, supporting access control.
ISO/IEC 27001	Yes	low	Authentication is present, contributing to access control.
CSA STAR	Yes	low	Authentication mechanisms are in place for identity and access management.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/accepted-clip-details/

Endpoint Path	/api/creator/accepted-clip-details/
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 722
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 721, 722, 723, 727.

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	Yes	low	Endpoint is authenticated, supporting access control.
ISO/IEC 27001	Yes	low	Authentication is present, contributing to access control.
CSA STAR	Yes	low	Authentication mechanisms are in place for identity and access management.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns/

Endpoint Path	/api/brand/campaigns/
HTTP Methods	DELETE
Source Location	..\Mipoe-Backend\app.py - 761
Authentication Required	Yes (token)

Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 761, 765, 766, 770.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can delete campaigns.
ISO/IEC 27001	Yes	low	Authentication is required for deletion, ensuring proper access control.
CSA STAR	Yes	low	Authentication for deletion operations is crucial for integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/clip/

Endpoint Path	/api/creator/clip/
HTTP Methods	DELETE
Source Location	..\Mipoe-Backend\app.py - 833
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 832, 833, 837, 838, 842.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can delete clips.
ISO/IEC 27001	Yes	low	Authentication is required for deletion, ensuring proper access control.
CSA STAR	Yes	low	Authentication for deletion operations is crucial for integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/admin/campaigns

Endpoint Path	/api/admin/campaigns
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 888
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 887, 888, 889.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can access admin campaign data.
ISO/IEC 27001	Yes	low	Authentication is in place for administrative functions, maintaining access control.
CSA STAR	Yes	low	Admin-level access requires authentication to ensure proper authorization.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/admin/clip/

Endpoint Path	/api/admin/clip/
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 935
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 934, 935, 936.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can update clip details.
ISO/IEC 27001	Yes	low	Authentication is required for modification of data, ensuring integrity.
CSA STAR	Yes	low	Authentication for update operations is crucial for maintaining data integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/admin/clip/

Endpoint Path	/api/admin/clip/
HTTP Methods	DELETE
Source Location	..\Mipoe-Backend\app.py - 1026
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1025, 1026, 1031.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can delete clips from admin interface.
ISO/IEC 27001	Yes	low	Authentication is required for deletion, ensuring proper access control.
CSA STAR	Yes	low	Authentication for deletion operations is crucial for integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/profile

Endpoint Path	/api/creator/profile
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 1079
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1078, 1079, 1080, 1084.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can access their profile.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing personal profile data.
CSA STAR	Yes	low	Authentication for profile access protects user identity and data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/profile

Endpoint Path	/api/creator/profile
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1113
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1112, 1113, 1114, 1118.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can update their profile.
ISO/IEC 27001	Yes	low	Authentication is required for modification of profile data, ensuring integrity.
CSA STAR	Yes	low	Authentication for profile updates is crucial for maintaining data integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//image

Endpoint Path	/api/brand/campaigns//image

HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1159
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1158, 1159, 1165, 1166, 1170.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can update campaign images.
ISO/IEC 27001	Yes	low	Authentication is required for modification of campaign assets, ensuring integrity.
CSA STAR	Yes	low	Authentication for image updates is crucial for maintaining data integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//budget

Endpoint Path	/api/brand/campaigns//budget
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1198
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1197, 1198, 1199, 1204.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can update campaign budgets.
ISO/IEC 27001	Yes	low	Authentication is required for modification of financial data, ensuring integrity.
CSA STAR	Yes	low	Authentication for budget updates is crucial for maintaining financial integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//requirements

Endpoint Path	/api/brand/campaigns//requirements
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1230
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1229, 1230, 1231, 1235.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can update campaign requirements.
ISO/IEC 27001	Yes	low	Authentication is required for modification of campaign requirements, ensuring integrity.
CSA STAR	Yes	low	Authentication for requirement updates is crucial for maintaining data integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//status

Endpoint Path	/api/brand/campaigns//status
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1259
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1258, 1259, 1260, 1264.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can update campaign status.
ISO/IEC 27001	Yes	low	Authentication is required for modification of campaign status, ensuring integrity.
CSA STAR	Yes	low	Authentication for status updates is crucial for maintaining data integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//view_threshold

Endpoint Path	/api/brand/campaigns//view_threshold
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1290
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1289, 1290, 1291, 1295.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can update campaign view thresholds.
ISO/IEC 27001	Yes	low	Authentication is required for modification of campaign parameters, ensuring integrity.
CSA STAR	Yes	low	Authentication for threshold updates is crucial for maintaining data integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//deadline

Endpoint Path	/api/brand/campaigns//deadline
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1321
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1320, 1321, 1322, 1326.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can update campaign deadlines.
ISO/IEC 27001	Yes	low	Authentication is required for modification of campaign deadlines, ensuring integrity.
CSA STAR	Yes	low	Authentication for deadline updates is crucial for maintaining data integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//pending-payouts

Endpoint Path	/api/brand/campaigns//pending-payouts
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 1358
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1357, 1358, 1365, 1366, 1371.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can view pending payouts.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing financial payout information.
CSA STAR	Yes	low	Authentication for payout information access is important for financial data security.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/profile

Endpoint Path	/api/brand/profile
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 1455
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1454, 1455, 1456, 1460.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can access brand profile.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing brand profile data.
CSA STAR	Yes	low	Authentication for brand profile access protects company data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/profile

Endpoint Path	/api/brand/profile
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1482
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1481, 1482, 1483, 1487.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can update brand profile.
ISO/IEC 27001	Yes	low	Authentication is required for modification of brand profile data, ensuring integrity.

Regulation	Applicable	Risk Level	Reason
CSA STAR	Yes	low	Authentication for profile updates is crucial for maintaining data integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/admin/clip//view-count

Endpoint Path	/api/admin/clip//view-count
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1514
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1513, 1514, 1528, 1529.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can update clip view counts.
ISO/IEC 27001	Yes	low	Authentication is required for modification of view counts, ensuring integrity.
CSA STAR	Yes	low	Authentication for view count updates is crucial for maintaining data integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/admin/campaign//update-views

Endpoint Path	/api/admin/campaign//update-views
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1580
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1579, 1580, 1591, 1592.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can update campaign view counts.
ISO/IEC 27001	Yes	low	Authentication is required for modification of view counts, ensuring integrity.
CSA STAR	Yes	low	Authentication for view count updates is crucial for maintaining data integrity and access control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/admin/analytics/campaign-performance/

Endpoint Path	/api/admin/analytics/campaign-performance/
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 1635
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1634, 1635, 1640, 1641.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can access campaign performance analytics.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing sensitive analytical data.
CSA STAR	Yes	low	Authentication for analytics access is important for data privacy and integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/auth/google-sync

Endpoint Path	/api/auth/google-sync
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 1738
Authentication Required	Yes (token)

Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1737, 1738, 1739, 1744, 1745, 1748, 1761, 1772, 1778.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for Google synchronization.
ISO/IEC 27001	Yes	low	Authentication is in place for third-party integrations, ensuring controlled access.
CSA STAR	Yes	low	Authentication for external service synchronization is crucial for security and data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /refresh

Endpoint Path	/refresh
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 1816
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1815, 1816, 1821, 1822.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for token refreshing.
ISO/IEC 27001	Yes	low	Authentication is in place for token management, ensuring session security.
CSA STAR	Yes	low	Authentication for token refreshing is essential for maintaining session security.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /logout

Endpoint Path	/logout
HTTP Methods	DELETE
Source Location	..\Mipoe-Backend\app.py - 1832
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1831, 1832, 1836.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for logout.
ISO/IEC 27001	Yes	low	Authentication is in place for session termination, ensuring secure logout.
CSA STAR	Yes	low	Authentication for logout ensures the user is properly identified before terminating their session.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/health

Endpoint Path	/api/health
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 1843
Authentication Required	No
Risk Severity	Low
CVSS Score	N/A

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** (low): Health check endpoint does not require authentication. This is generally acceptable for monitoring purposes but should not expose sensitive information.

  Potential Attack Scenario:

  While not a direct security risk, it's important to ensure the health check does not inadvertently reveal sensitive system status or information.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Health check endpoints are typically public for monitoring. Ensure no sensitive data is exposed.
ISO/IEC 27001	Yes	low	Publicly accessible health checks are common for monitoring. Ensure no sensitive information is disclosed.
CSA STAR	Yes	low	Health checks should not expose sensitive operational data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /create-deposit-order

Endpoint Path	/create-deposit-order
HTTP Methods	POST
Source Location	..\routes\payments.py - 49
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 48, 49, 50, 55.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for creating deposit orders.
ISO/IEC 27001	Yes	low	Authentication is in place for financial transaction initiation.
CSA STAR	Yes	low	Authentication for financial operations is crucial for preventing fraud and unauthorized transactions.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /verify-deposit

Endpoint Path	/verify-deposit
HTTP Methods	POST
Source Location	..\routes\payments.py - 121
Authentication Required	Yes (token)
Risk Severity	Low

CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 120, 121, 122, 127.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for deposit verification.
ISO/IEC 27001	Yes	low	Authentication is in place for verifying financial transactions.
CSA STAR	Yes	low	Authentication for deposit verification is essential for financial integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /virtual-account

Endpoint Path	/virtual-account
HTTP Methods	GET
Source Location	..\routes\payments.py - 192
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 191, 192, 193, 198.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can access virtual account information.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing financial account details.
CSA STAR	Yes	low	Authentication for virtual account access is important for financial data security.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /wallet-balance

Endpoint Path	/wallet-balance
HTTP Methods	GET
Source Location	..\routes\payments.py - 243
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 242, 243, 244, 247.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can view wallet balances.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing financial balance information.
CSA STAR	Yes	low	Authentication for wallet balance access is important for financial data security.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /allocate-budget

Endpoint Path	/allocate-budget
HTTP Methods	POST
Source Location	..\routes\payments.py - 269
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 268, 269, 270, 275.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for budget allocation.
ISO/IEC 27001	Yes	low	Authentication is in place for financial budget management.
CSA STAR	Yes	low	Authentication for budget allocation is crucial for financial integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /reclaim-budget

Endpoint Path	/reclaim-budget
HTTP Methods	POST
Source Location	..\routes\payments.py - 349
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 348, 349, 350, 355.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for budget reclamation.
ISO/IEC 27001	Yes	low	Authentication is in place for financial budget management.
CSA STAR	Yes	low	Authentication for budget reclamation is crucial for financial integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /distribute-to-creator

Endpoint Path	/distribute-to-creator
HTTP Methods	POST
Source Location	..\routes\payments.py - 436
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 435, 436, 455, 460.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for distributing funds to creators.
ISO/IEC 27001	Yes	low	Authentication is in place for financial distribution to creators.
CSA STAR	Yes	low	Authentication for creator payouts is crucial for financial integrity and preventing fraud.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator-withdraw

Endpoint Path	/creator-withdraw
HTTP Methods	POST
Source Location	..\routes\payments.py - 560
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 559, 560, 578, 583.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for creator withdrawals.
ISO/IEC 27001	Yes	low	Authentication is in place for creator withdrawal requests.
CSA STAR	Yes	low	Authentication for creator withdrawals is crucial for financial integrity and preventing fraud.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/payout-details

Endpoint Path	/creator/payout-details

HTTP Methods	POST, PUT
Source Location	..\routes\payments.py - 735
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 734, 735, 750, 755.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can save or update payout details.
ISO/IEC 27001	Yes	low	Authentication is required for managing sensitive financial payout information.
CSA STAR	Yes	low	Authentication for payout details management is crucial for financial data security and integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/payout-details

Endpoint Path	/creator/payout-details
HTTP Methods	GET
Source Location	..\routes\payments.py - 823
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 822, 823, 828, 833.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can retrieve payout details.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing sensitive financial payout information.
CSA STAR	Yes	low	Authentication for payout details retrieval is important for financial data security.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/verify-payout-details

Endpoint Path	/creator/verify-payout-details
HTTP Methods	POST
Source Location	..\routes\payments.py - 873
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 872, 873, 878, 883.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for payout details verification.
ISO/IEC 27001	Yes	low	Authentication is in place for the verification of sensitive financial payout information.
CSA STAR	Yes	low	Authentication for payout details verification is crucial for financial integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/withdrawals

Endpoint Path	/creator/withdrawals
HTTP Methods	GET
Source Location	..\routes\payments.py - 933
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 932, 933, 940, 945.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can view withdrawal history.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing financial withdrawal history.
CSA STAR	Yes	low	Authentication for withdrawal history access is important for financial data security.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/notifications/

Endpoint Path	/creator/notifications/
HTTP Methods	GET
Source Location	..\routes\payments.py - 995
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 994, 995, 999, 1000, 1002.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can access creator notifications.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing user-specific notification data.
CSA STAR	Yes	low	Authentication for notification access is important for data privacy and integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /transactions//

Endpoint Path	/transactions//
HTTP Methods	GET
Source Location	..\routes\payments.py - 1030
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1029, 1030, 1031, 1035, 1038, 1042.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can access transaction history.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing financial transaction data.
CSA STAR	Yes	low	Authentication for transaction history access is important for financial data security and privacy.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /refund-campaign

Endpoint Path	/refund-campaign
HTTP Methods	POST
Source Location	..\routes\payments.py - 1110
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1109, 1110, 1126, 1131.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for refund requests.
ISO/IEC 27001	Yes	low	Authentication is in place for initiating financial refund processes.
CSA STAR	Yes	low	Authentication for refund requests is crucial for financial integrity and preventing abuse.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /campaign-summary/

Endpoint Path	/campaign-summary/
HTTP Methods	GET
Source Location	..\routes\payments.py - 1203
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1202, 1203, 1215, 1217.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can access campaign summaries.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing campaign summary data.
CSA STAR	Yes	low	Authentication for campaign summary access is important for data privacy and integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /calculate-earnings//

Endpoint Path	/calculate-earnings//
HTTP Methods	GET
Source Location	..\routes\payments.py - 1270
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1269, 1270, 1283, 1285.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can calculate earnings.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing and calculating sensitive financial earnings data.
CSA STAR	Yes	low	Authentication for earnings calculation is important for financial data security and integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /bulk-distribute

Endpoint Path	/bulk-distribute
HTTP Methods	POST
Source Location	..\routes\payments.py - 1364
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1363, 1364, 1384, 1389.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for bulk distribution.
ISO/IEC 27001	Yes	low	Authentication is in place for bulk financial distribution operations.
CSA STAR	Yes	low	Authentication for bulk creator payouts is crucial for financial integrity and preventing fraud.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /request-refund

Endpoint Path	/request-refund
HTTP Methods	POST
Source Location	..\routes\payments.py - 1535
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1534, 1535, 1548, 1553.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for refund requests.
ISO/IEC 27001	Yes	low	Authentication is in place for initiating financial refund processes.
CSA STAR	Yes	low	Authentication for refund requests is crucial for financial integrity and preventing abuse.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /refund-requests

Endpoint Path	/refund-requests
HTTP Methods	GET
Source Location	..\routes\payments.py - 1629
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1628, 1629, 1636, 1641.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can view refund requests.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing financial refund request data.
CSA STAR	Yes	low	Authentication for refund request access is important for financial data security and integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /admin/approve-refund

Endpoint Path	/admin/approve-refund

HTTP Methods	POST
Source Location	..\routes\payments.py - 1696
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1695, 1696, 1709, 1714.

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	Yes	low	Endpoint is authenticated and intended for administrative use, ensuring proper authorization for refund approval.
ISO/IEC 27001	Yes	low	Authentication is required for administrative approval of financial refunds.
CSA STAR	Yes	low	Administrative authentication for refund approval is crucial for financial integrity and control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /admin/reject-refund

Endpoint Path	/admin/reject-refund
HTTP Methods	POST
Source Location	..\routes\payments.py - 1810
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1809, 1810, 1821, 1826.

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	Yes	low	Endpoint is authenticated and intended for administrative use, ensuring proper authorization for refund rejection.
ISO/IEC 27001	Yes	low	Authentication is required for administrative rejection of financial refunds.
CSA STAR	Yes	low	Administrative authentication for refund rejection is crucial for financial integrity and control.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /refund-status/

Endpoint Path	/refund-status/
HTTP Methods	GET
Source Location	..\routes\payments.py - 1871
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1870, 1871, 1878, 1880.

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	Yes	low	Endpoint is authenticated, ensuring only authorized users can view refund status.
ISO/IEC 27001	Yes	low	Authentication is in place for accessing refund status information.
CSA STAR	Yes	low	Authentication for refund status access is important for financial data security.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /admin/refund-audit-trail

Endpoint Path	/admin/refund-audit-trail
HTTP Methods	GET
Source Location	..\routes\payments.py - 1940
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1939, 1940, 1947.

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	Yes	low	Endpoint is authenticated and intended for administrative use, ensuring proper authorization for refund audit trail access.
ISO/IEC 27001	Yes	low	Authentication is required for administrative access to audit trails, ensuring integrity.
CSA STAR	Yes	low	Administrative authentication for audit trail access is crucial for security monitoring and compliance.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/revert-withdrawal

Endpoint Path	/creator/revert-withdrawal
HTTP Methods	POST
Source Location	..\routes\payments.py - 2019
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 2018, 2019, 2024, 2029.

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	Yes	low	Endpoint is authenticated, ensuring proper authorization for reverting withdrawals.
ISO/IEC 27001	Yes	low	Authentication is in place for modifying financial transaction status.
CSA STAR	Yes	low	Authentication for withdrawal reversion is crucial for financial integrity and control.

Security Assessment Notes

CVSS Vector:

References

METRICS SUMMARY

Total Findings: 5

Severity	Count
CRITICAL	1
HIGH	2
MEDIUM	1
LOW	1

BUSINESS RISK ADVICE

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

Eliminate Hardcoded Supabase JWT (Priority: Immediate)

Description: A critical Supabase JSON Web Token (JWT) is directly embedded in the `tasks.py` file. This credential can grant an attacker unauthorized access to backend resources.

Why it Matters: Direct exposure of critical authentication credentials leads to severe data breaches, unauthorized access, and potential full system compromise, violating SOC 2, ISO 27001, and CSA STAR access control principles.

Recommended Actions:

- Revoke the currently hardcoded JWT immediately.
- Implement a dedicated secrets management solution (e.g., environment variables, HashiCorp Vault, AWS Secrets Manager) to store sensitive credentials.
- Modify `tasks.py` to retrieve the Supabase JWT securely at runtime from the chosen secrets management solution.
- Enforce policies to prevent any sensitive data, including API keys and tokens, from being committed to source code repositories.

Expected Outcome: Prevents direct exposure of critical authentication tokens, significantly reducing the attack surface for credential compromise and unauthorized access.

Disable Flask Debug Mode in Production (Priority: Immediate)

Description: The Flask application is configured to run with `debug=True` in `app.py`, which enables the Werkzeug debugger and is highly dangerous in a production environment.

Why it Matters: This critical misconfiguration allows an attacker to execute arbitrary Python code on the server if the debugger PIN is compromised, leading to full system compromise and unauthorized data access. Violates secure configuration and operational security controls.

Recommended Actions:

- Change `app.run(debug=True, port=5000, use_reloader=True)` to `app.run(debug=False, port=5000)` in `app.py` at line 1872.
- Deploy the application using a production-ready WSGI server (e.g., Gunicorn, uWSGI) instead of Flask's built-in development server.
- Use environment variables or secure configuration files to manage debug settings, ensuring `debug=False` for all production deployments.

Expected Outcome: Eliminates the arbitrary code execution vulnerability, prevents exposure of sensitive internal application details, and establishes a secure execution environment.

Enforce Authentication for User Registration and Login Endpoints (Priority: Immediate)

Description: The `/register` and `/login` API endpoints (at `app.py:73` and `app.py:120` respectively) are publicly accessible without authentication, making them vulnerable to abuse.

Why it Matters: Absence of authentication on these critical endpoints allows attackers to create numerous fake accounts, perform brute-force attacks, or bypass access controls, leading to denial of service, account takeover, or data breaches. Violates core access control and user management compliance requirements.

Recommended Actions:

- Implement robust rate limiting and CAPTCHA mechanisms on both `/register` and `/login` endpoints to mitigate automated attacks.
- Ensure that password hashing (e.g., bcrypt with appropriate salt and iterations) is used for new registrations and during login validation.
- Review and strengthen existing authentication logic to prevent authentication bypass vulnerabilities.
- Consider implementing multi-factor authentication (MFA) for enhanced login security.

Expected Outcome: Secures the user registration and login processes, preventing account creation abuse, unauthorized access, and improving the overall integrity of user authentication.