SECURITY ANALYSIS REPORT

Generated By

Backstage Rookie

Provider: Backstage Rookie

contact - swarajdarekar9@gmail.com

Client: Chandrakant Darekar

darekar138@gmail.com

Scan ID: 7c5bf698-934a-470f-abd9-b2c68214223a

Date: 2026-02-10 14:53:07

Version: 1.0.0

TABLE OF CONTENTS

/api/creator/profile

/api/creator/profile

/api/brand/campaigns//image

/api/brand/campaigns//budget

/api/brand/campaigns//requirements

/api/brand/campaigns//status

/api/brand/campaigns//view_threshold

/api/brand/campaigns//deadline

/api/brand/campaigns//pending-payouts

/api/brand/profile

/api/brand/profile

/api/admin/clip//view-count

/api/admin/campaign//update-views

/api/admin/analytics/campaign-performance/

/api/auth/google-sync

/refresh

/logout

/api/health

/create-deposit-order

/verify-deposit

/virtual-account

/wallet-balance

/allocate-budget

/reclaim-budget

/distribute-to-creator

/creator-withdraw

/creator/payout-details

/creator/payout-details

/creator/verify-payout-details

/creator/withdrawals

/creator/notifications/

/transactions//

/refund-campaign

/campaign-summary/

/calculate-earnings//

/bulk-distribute

/request-refund

/refund-requests

/admin/approve-refund

EXECUTIVE SUMMARY

This security assessment identified several critical and medium-risk vulnerabilities within the application, alongside a pervasive low-risk issue. The most severe findings include the presence of a hardcoded JWT token, which could lead to unauthorized access, and the configuration of Flask with debug mode enabled, potentially allowing remote code execution. Additionally, a lack of robust error handling results in verbose error messages exposing internal system details, and missing timeouts in external API calls could lead to denial of service. Addressing these issues is paramount to fortifying the application's security posture and protecting against significant compromise.

Identified Vulnerabilities

ID	Title	CVSS	Page
C1	Hardcoded JWT Token	9.8	
C2	Flask Debug Mode Enabled in Production	9.8	
M1	Missing Request Timeouts for External API Calls	5.3	
L1	Verbose Error Messages Exposing Internal Details	3.1	

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 – Hardcoded JWT 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 embedded within the source code, posing a significant security risk. Hardcoding sensitive authentication credentials like JWTs can lead to unauthorized access, impersonation, and a complete compromise of associated user accounts or services if the token is leaked.

Details

The file `tasks.py` contains a variable `token` explicitly assigned a full JWT string. While this might be intended for testing or demonstration, the presence of such a secret in a codebase, especially one that might be committed to version control, represents a critical security oversight. An attacker gaining access to the source code would immediately obtain a valid authentication token, potentially allowing them to bypass authentication mechanisms and access protected resources.

Evidence

- **tasks.py:14:** Hardcoded JWT token assigned to `token` variable.

References

- https://owasp.org/www-project-top-ten/2021/A07_2021-Identification_And_Authentication_Failures

Recommendation

- Remove the hardcoded JWT token from the source code immediately. - Implement secure handling of authentication tokens, such as retrieving them from secure environment variables or a dedicated secret management service. - For testing purposes, use mock tokens or generate tokens dynamically with limited scope and short expiry times, ensuring they are never committed to the repository. - Rotate all affected production JWT tokens, as the hardcoded token might represent a valid, currently active credential.

Prompt to Solve the Vulnerability:

In `tasks.py` at line 14, a JWT token is hardcoded. Refactor this to retrieve the token from a secure environment variable (e.g., `os.getenv('TEST_JWT_TOKEN')`) or a secrets management system. For development, consider using a `.env` file that is excluded from version control, but ensure production deployments use more robust secret handling.

C2 – Flask Debug Mode Enabled in Production

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: app.py

Overview

The Flask application is configured to run with debug mode enabled (`debug=True`), which exposes the Werkzeug debugger. In a production environment, this setting represents a critical vulnerability, allowing attackers to execute arbitrary code on the server.

Details

When `debug=True` is active, Flask applications provide an interactive debugger in the browser for unhandled exceptions. This debugger grants access to a Python shell with the ability to execute code directly on the server. An attacker can trigger an error and then exploit this debugger to achieve Remote Code Execution (RCE), leading to full system compromise, data exfiltration, and service disruption. The presence of `use_reloader=True` further exacerbates the risk by continuously monitoring code changes and reloading the application, potentially leading to instability or additional attack vectors.

Evidence

- **app.py:1872:** Flask app initiated with `debug=True` and `use_reloader=True`.

References

- https://owasp.org/www-community/vulnerabilities/Server-side_Request_Forgery_%28SSRF%29
- https://flask.palletsprojects.com/en/latest/server/

Recommendation

- Ensure `debug=False` for all production deployments. - Use environment variables (e.g., `FLASK_ENV='production'`) or configuration management to control debug settings, preventing hardcoded `debug=True`. - Deploy Flask applications using a production-ready WSGI server (e.g., Gunicorn, uWSGI) in front of an Nginx/Apache proxy, which inherently disables the `app.run()` development server. - Review deployment scripts and CI/CD pipelines to ensure debug mode is never enabled in non-development environments.

Prompt to Solve the Vulnerability:

In `app.py` at line 1872, the Flask application is run with `debug=True`. This must be disabled for production. Modify `app.run(debug=True, ...)` to `app.run(debug=False, ...)` or, preferably, remove `app.run()` entirely and use a production WSGI server like Gunicorn. Ensure this setting is controlled by an environment variable, e.g., `app.run(debug=os.getenv('FLASK_DEBUG') == '1', ...)`.

M1 – Missing Request Timeouts for External API Calls

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: routes\payments.py

Overview

Multiple outbound HTTP requests made using the `requests` library lack a configured timeout, potentially leading to application unresponsiveness or Denial of Service (DoS) if external services become slow or unresponsive.

Details

The application makes calls to external APIs (e.g., Cashfree API) without specifying a `timeout` parameter for the `requests.post` and `requests.get` methods. If these external services experience delays or become unavailable, the application threads making these requests could hang indefinitely, consuming server resources (e.g., network connections, memory, CPU) and preventing other legitimate requests from being processed. This resource exhaustion can lead to a self-inflicted Denial of Service for the application.

Evidence

- **routes\payments.py:90:** `requests.post` call without a timeout parameter.
- **routes\payments.py:136:** `requests.get` call without a timeout parameter.
- **routes\payments.py:663:** `requests.post` call without a timeout parameter.

References

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

Recommendation

- Add a `timeout` parameter to all `requests.post` and `requests.get` calls. - The timeout value should be chosen based on the expected response time of the external API, balancing responsiveness with allowing sufficient time for legitimate requests. - Consider implementing retry mechanisms with exponential backoff for transient network issues, but always combine them with robust timeouts. - Centralize timeout configuration where possible to ensure consistency across the application.

Prompt to Solve the Vulnerability:

In `routes\payments.py` at lines 90, 136, and 663, `requests.post` and `requests.get` calls are missing a `timeout` parameter. Modify these calls to include a reasonable timeout, for example: `requests.post(url, ..., timeout=5)` or `requests.get(url, ..., timeout=(3, 10))` for connect and read timeouts, respectively.

L1 – Verbose Error Messages Exposing Internal Details

Severity: Low

CVSS Score: 3.1

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

Target: Multiple files (e.g., app.py, routes\payments.py)

Overview

The application's API endpoints frequently return raw exception messages (`str(e)`) in error responses to clients, which can expose sensitive internal details about the application's implementation, database schema, or operating environment.

Details

Across numerous endpoints in `app.py` and `routes/payments.py`, `try...except` blocks catch generic `Exception`s and include the string representation of the exception (`str(e)`) directly in the JSON error response. While this is helpful for debugging during development, it is a security risk in production. Attackers can leverage these verbose error messages to gain insights into the backend system, aiding in reconnaissance, identifying potential weaknesses, and crafting more targeted attacks (e.g., understanding database query structures, file paths, or third-party library versions).

Evidence

- **app.py:117:** `return jsonify({'msg': 'Registration failed', 'error': str(e)}), 500`
- **app.py:187:** `return jsonify({'msg': 'Login failed', 'error': str(e)}), 500`
- **app.py:210:** `return jsonify({'msg': 'Failed to update profile', 'error': str(e)}), 500`
- **app.py:243:** `return jsonify({'msg': 'Failed to send reset email', 'error': str(e)}), 500`
- **app.py:288:** `return jsonify({'msg': 'Failed to create campaign', 'error': str(e)}), 500`
- **app.py:326:** `return jsonify({'msg': 'Failed to fetch campaigns', 'error': str(e)}), 500`
- **app.py:385:** `return jsonify({'msg': 'Failed to fetch campaigns', 'error': str(e)}), 500`
- **app.py:491:** `return jsonify({'msg': 'Failed to fetch campaign details', 'error': str(e)}), 500`
- **app.py:579:** `return jsonify({'msg': 'Failed to fetch creator campaigns', 'error': str(e)}), 500`
- **app.py:653:** `return jsonify({'msg': 'Failed to submit clip', 'error': str(e)}), 500`
- **app.py:718:** `return jsonify({'msg': 'Failed to fetch clips', 'error': str(e)}), 500`
- **app.py:754:** `return jsonify({'msg': 'Failed to fetch accepted clip details', 'error': str(e)}), 500`
- **app.py:829:** `return jsonify({'msg': 'Failed to delete campaign', 'error': str(e)}), 500`
- **app.py:884:** `return jsonify({'msg': 'Failed to delete clip', 'error': str(e)}), 500`
- **app.py:931:** `return jsonify({'msg': 'Failed to fetch campaigns', 'error': str(e)}), 500`
- **app.py:1022:** `return jsonify({'msg': 'Failed to update clip', 'error': str(e)}), 500`
- **app.py:1075:** `return jsonify({'msg': 'Failed to delete clip', 'error': str(e)}), 500`
- **app.py:1109:** `return jsonify({'msg': 'Failed to fetch creator profile', 'error': str(e)}), 500`
- **app.py:1155:** `return jsonify({'msg': 'Failed to update creator profile', 'error': str(e)}), 500`
- **app.py:1194:** `return jsonify({'msg': 'Failed to update campaign image', 'error': str(e)}), 500`

- **app.py:1226:** `return jsonify({'msg': 'Failed to update campaign budget', 'error': str(e)}), 500`
- **app.py:1255:** `return jsonify({'msg': 'Failed to update campaign requirements', 'error': str(e)}), 500`
- **app.py:1286:** `return jsonify({'msg': 'Failed to update campaign status', 'error': str(e)}), 500`
- **app.py:1317:** `return jsonify({'msg': 'Failed to update campaign view threshold', 'error': str(e)}), 500`
- **app.py:1354:** `return jsonify({'msg': 'Failed to update campaign deadline', 'error': str(e)}), 500`
- **app.py:1450:** `return jsonify({'msg': 'Failed to retrieve pending payouts', 'error': str(e)}), 500`
- **app.py:1478:** `return jsonify({'msg': 'Failed to fetch brand profile', 'error': str(e)}), 500`
- **app.py:1509:** `return jsonify({'msg': 'Failed to update brand profile', 'error': str(e)}), 500`
- **app.py:1576:** `return jsonify({'msg': 'Failed to update view count', 'error': str(e)}), 500`
- **app.py:1631:** `return jsonify({'msg': 'Failed to update campaign views', 'error': str(e)}), 500`
- **app.py:1729:** `return jsonify({'msg': 'Failed to retrieve analytics', 'error': str(e)}), 500`
- **app.py:1756:** `return jsonify({'msg': 'Failed to sync Google user: could not retrieve user data', 'error': str(e)}), 500`
- **app.py:1808:** `return jsonify({'msg': 'Sync failed due to database error', 'error': str(e)}), 500`
- **app.py:1812:** `return jsonify({'msg': 'Sync failed', 'error': str(e)}), 500`
- **routes\payments.py:115:** `return jsonify({'msg': 'Internal server error', 'error': str(e)}), 500`
- **routes\payments.py:186:** `return jsonify({'msg': 'Verification failed', 'error': str(e)}), 500`
- **routes\payments.py:343:** `return jsonify({'msg': 'Allocation failed', 'error': str(e)}), 500`
- **routes\payments.py:430:** `return jsonify({'msg': 'Reclaim failed', 'error': str(e)}), 500`
- **routes\payments.py:554:** `return jsonify({'msg': 'Distribution failed', 'error': str(e)}), 500`
- **routes\payments.py:729:** `return jsonify({'msg': 'Withdrawal failed', 'error': str(e)}), 500`
- **routes\payments.py:817:** `return jsonify({'msg': 'Failed to save payout details', 'error': str(e)}), 500`
- **routes\payments.py:867:** `return jsonify({'msg': 'Failed to retrieve payout details', 'error': str(e)}), 500`
- **routes\payments.py:927:** `return jsonify({'msg': 'Failed to verify payout details', 'error': str(e)}), 500`
- **routes\payments.py:989:** `return jsonify({'msg': 'Failed to retrieve withdrawal history', 'error': str(e)}), 500`
- **routes\payments.py:1023:** `return jsonify({'msg': 'Failed to retrieve notifications', 'error': str(e)}), 500`
- **routes\payments.py:1105:** `return jsonify({'msg': 'Failed to retrieve transactions', 'error': str(e)}), 500`
- **routes\payments.py:1197:** `return jsonify({'msg': 'Refund failed', 'error': str(e)}), 500`
- **routes\payments.py:1264:** `return jsonify({'msg': 'Failed to retrieve campaign summary', 'error': str(e)}), 500`
- **routes\payments.py:1358:** `return jsonify({'msg': 'Failed to calculate earnings', 'error': str(e)}), 500`
- **routes\payments.py:1529:** `return jsonify({'msg': 'Bulk distribution failed', 'error': str(e)}), 500`
- **routes\payments.py:1623:** `return jsonify({'msg': 'Failed to request refund', 'error': str(e)}), 500`
- **routes\payments.py:1690:** `return jsonify({'msg': 'Failed to retrieve refund requests', 'error': str(e)}), 500`
- **routes\payments.py:1804:** `return jsonify({'msg': 'Failed to approve refund', 'error': str(e)}), 500`
- **routes\payments.py:1865:** `return jsonify({'msg': 'Failed to reject refund', 'error': str(e)}), 500`
- **routes\payments.py:1934:** `return jsonify({'msg': 'Failed to retrieve refund status', 'error': str(e)}), 500`
- **routes\payments.py:2014:** `return jsonify({'msg': 'Failed to retrieve refund audit trail', 'error': str(e)}), 500`
- **routes\payments.py:2088:** `return jsonify({'msg': 'Failed to revert withdrawal', 'error': str(e)}), 500`

References

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

Recommendation

- Replace raw exception messages (`str(e)`) in API responses with generic, user-friendly error messages that do not reveal internal system details. - Log detailed exception information on the server-side (e.g., to a secure log file or monitoring system) for debugging purposes. - Implement a global error handler (e.g., Flask's `app.errorhandler`) to standardize error responses and prevent accidental leakage of sensitive information. - Ensure that only necessary information is returned to the client, such as a unique error reference ID that can be correlated with server-side logs.

Prompt to Solve the Vulnerability:

Numerous endpoints, such as `app.py` line 117 and `routes\payments.py` line 115, expose `str(e)` in error responses. Refactor these error handlers to return a generic message to the client, like `{'msg': 'Internal server error'}`, and log the full exception details on the server-side for debugging without exposing them externally. A global error handler for `Exception`s could also be implemented to ensure consistency.

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 not enforced for this endpoint.

  Potential Attack Scenario:

  Unauthorized users can register new accounts, potentially leading to account abuse or denial of service.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Lack of authentication on registration can lead to unauthorized access and misuse of user data, impacting system integrity and availability.
ISO/IEC 27001	Yes	medium	Absence of authentication controls for user registration violates principles of access control and secure system entry.
CSA STAR	Yes	medium	Inadequate authentication for user registration can compromise data confidentiality and integrity.

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://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

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 not enforced for this endpoint.

  Potential Attack Scenario:

  Without proper authentication mechanisms, attackers could potentially gain unauthorized access to user accounts through brute-force attacks or by exploiting vulnerabilities in the login process.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of enforced authentication on login can lead to unauthorized access and compromise of user accounts and sensitive data.
ISO/IEC 27001	Yes	high	Absence of robust authentication for login processes is a direct violation of access control requirements.

Regulation	Applicable	Risk Level	Reason
CSA STAR	Yes	high	Inadequate authentication on login can lead to unauthorized access and compromise of data confidentiality and integrity.

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://owasp.org/www-community/vulnerabilities/Authentication_and_Authorization

Endpoint Path /verify-instagram

Endpoint Path	/verify-instagram
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 192
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 191, 191, 192, 192, 193, 193, 194, 194, 191, 191, 193, 193, 194, 194, 191, 191, 193, 193, 194, 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	Authentication appears to be implemented, reducing the risk of unauthorized access.

Regulation	Applicable	Risk Level	Reason
ISO/IEC 27001	Yes	low	Presence of authentication controls supports compliance with access management requirements.
CSA STAR	Yes	low	Authentication mechanisms help protect the integrity and confidentiality of operations.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /verify-instagram/

Endpoint Path	/verify-instagram/
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 192
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 191, 191, 192, 192, 193, 193, 194, 194, 191, 191, 193, 193, 194, 194, 191, 191, 193, 193, 194, 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	Authentication appears to be implemented, reducing the risk of unauthorized access.
ISO/IEC 27001	Yes	low	Presence of authentication controls supports compliance with access management requirements.
CSA STAR	Yes	low	Authentication mechanisms help protect the integrity and confidentiality of operations.

Security Assessment Notes

CVSS Vector: None

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	High
CVSS Score	8.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (medium): Authentication is not enforced for this endpoint, allowing anyone to request a password reset.

  Potential Attack Scenario:

An attacker could potentially trigger password reset emails for other users, leading to account takeovers (e.g., via social engineering or if the reset link is compromised).

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Lack of authentication on password reset requests can be exploited for account takeover, impacting data confidentiality and user access.
ISO/IEC 27001	Yes	medium	Weak controls over password reset mechanisms can lead to unauthorized access and compromise of user accounts.
CSA STAR	Yes	medium	Insecure password reset functionality can expose user accounts to compromise.

Security Assessment Notes

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

References

- https://owasp.org/www-community/vulnerabilities/Password_reset_ ataques

Endpoint Path /api/brand/campaigns

Endpoint Path	/api/brand/campaigns
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 248
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 247, 247, 248, 248, 249, 249, 253, 253, 247, 247, 249, 249, 253, 253, 247, 247, 249, 249, 253, 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	Authentication is enforced, ensuring only authorized users can create campaigns.
ISO/IEC 27001	Yes	low	Authentication controls are in place for campaign creation, supporting access management.
CSA STAR	Yes	low	Proper authentication for campaign creation helps maintain data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /api/brand/campaigns

Endpoint Path	/api/brand/campaigns
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 292
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 291, 291, 292, 292, 293, 293, 297, 297, 291, 291, 293, 293, 297, 297, 291, 291, 293, 293, 297, 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	Authentication is enforced, ensuring only authorized users can list campaigns.
ISO/IEC 27001	Yes	low	Authentication controls are in place for viewing campaigns, supporting access management.
CSA STAR	Yes	low	Proper authentication for campaign listing helps maintain data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /api/campaigns

Endpoint Path	/api/campaigns
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 329
Authentication Required	No
Risk Severity	Medium
CVSS Score	5.3

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 not enforced for this endpoint.

  Potential Attack Scenario:

  Sensitive campaign data could be exposed to unauthorized users.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Lack of authentication could lead to unauthorized access to sensitive campaign data.
ISO/IEC 27001	Yes	medium	Missing authentication controls for accessing campaign data can violate access control policies.
CSA STAR	Yes	medium	Unauthorized access to campaign data could compromise confidentiality.

Security Assessment Notes

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

References

- https://owasp.org/www-community/vulnerabilities/Information_Exposure

Endpoint Path /api/campaigns/

Endpoint Path	/api/campaigns/
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 388
Authentication Required	No
Risk Severity	Medium
CVSS Score	5.3

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 not enforced for this endpoint.

  Potential Attack Scenario:

  Unauthorized users could access details of specific campaigns, potentially revealing sensitive information.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Lack of authentication on accessing campaign details may lead to unauthorized disclosure of information.
ISO/IEC 27001	Yes	medium	Missing authentication for accessing specific campaign data can violate access control requirements.
CSA STAR	Yes	medium	Unauthorized access to campaign details can compromise data confidentiality.

Security Assessment Notes

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

References

- https://owasp.org/www-community/vulnerabilities/Information_Exposure

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 494, 494, 495, 495, 496, 496, 501, 501, 494, 494, 496, 496, 501, 501, 494, 494, 496, 496, 501, 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	Authentication is enforced, ensuring creators can only view their own campaigns.
ISO/IEC 27001	Yes	low	Authentication controls protect creator-specific campaign data, aligning with access management.
CSA STAR	Yes	low	Proper authentication for viewing creator campaigns ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 582, 582, 583, 583, 584, 584, 590, 590, 582, 582, 584, 584, 590, 590, 582, 582, 584, 584, 590, 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	Authentication is enforced, ensuring only authorized creators can submit clips.
ISO/IEC 27001	Yes	low	Authentication controls protect the integrity of clip submission processes.
CSA STAR	Yes	low	Proper authentication for submitting clips helps maintain data integrity.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 656, 656, 657, 657, 658, 658, 662, 662, 656, 656, 658, 658, 662, 662, 656, 656, 658, 658, 662, 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	Authentication is enforced, ensuring creators can only view clips for their campaigns.
ISO/IEC 27001	Yes	low	Authentication controls protect creator-specific clip data, aligning with access management.
CSA STAR	Yes	low	Proper authentication for viewing creator clips ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 721, 721, 722, 722, 723, 723, 727, 727, 721, 721, 723, 723, 727, 727, 721, 721, 723, 723, 727, 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	Authentication is enforced, ensuring creators can only view details of their accepted clips.
ISO/IEC 27001	Yes	low	Authentication controls protect creator-specific clip details, aligning with access management.
CSA STAR	Yes	low	Proper authentication for viewing accepted clip details ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /api/brand/campaigns/

Endpoint Path	/api/brand/campaigns/
HTTP Methods	DELETE, OPTIONS
Source Location	..\Mipoe-Backend\app.py - 761
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 761, 761, 765, 765, 766, 766, 770, 770, 765, 765, 766, 766, 770, 770, 765, 765, 766, 766, 770, 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	Authentication and authorization are enforced for campaign deletion.
ISO/IEC 27001	Yes	low	Access controls for campaign deletion are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for deleting campaigns maintain data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /api/creator/clip/

Endpoint Path	/api/creator/clip/
HTTP Methods	DELETE, OPTIONS
Source Location	..\Mipoe-Backend\app.py - 833
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 832, 832, 833, 833, 837, 837, 838, 838, 842, 842, 832, 832, 837, 837, 838, 838, 842, 842, 832, 832, 837, 837, 838, 838, 842, 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	Authentication and authorization are enforced for clip deletion.
ISO/IEC 27001	Yes	low	Access controls for clip deletion are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for deleting clips maintain data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /api/admin/campaigns

Endpoint Path	/api/admin/campaigns
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 888
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 887, 887, 888, 888, 889, 889, 887, 887, 889, 889, 887, 887, 889, 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	Authentication is enforced, ensuring only authorized administrators can access campaign data.
ISO/IEC 27001	Yes	low	Authentication controls for administrator access to campaign data align with access management.
CSA STAR	Yes	low	Proper authentication for administrator access to campaign data ensures confidentiality and integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /api/admin/clip/

Endpoint Path	/api/admin/clip/
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 935
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 934, 934, 935, 935, 936, 936, 934, 934, 936, 936, 934, 934, 936, 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	Authentication and authorization are enforced for updating clip details by administrators.
ISO/IEC 27001	Yes	low	Access controls for administrator clip updates are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for administrator clip updates maintain data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /api/admin/clip/

Endpoint Path	/api/admin/clip/
HTTP Methods	DELETE, OPTIONS
Source Location	..\Mipoe-Backend\app.py - 1026
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1025, 1025, 1026, 1026, 1031, 1031, 1025, 1025, 1031, 1031, 1025, 1025, 1031, 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	Authentication and authorization are enforced for clip deletion by administrators.
ISO/IEC 27001	Yes	low	Access controls for administrator clip deletion are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for administrator clip deletion maintain data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /api/creator/profile

Endpoint Path	/api/creator/profile
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 1079
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1078, 1078, 1079, 1079, 1080, 1080, 1084, 1084, 1078, 1078, 1080, 1080, 1084, 1084, 1078, 1078, 1080, 1080, 1084, 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	Authentication is enforced, ensuring creators can only view their own profiles.
ISO/IEC 27001	Yes	low	Authentication controls protect creator profile data, aligning with access management.
CSA STAR	Yes	low	Proper authentication for viewing creator profiles ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /api/creator/profile

Endpoint Path	/api/creator/profile
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1113
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1112, 1112, 1113, 1113, 1114, 1114, 1118, 1118, 1112, 1112, 1114, 1114, 1118, 1118, 1112, 1112, 1114, 1114, 1118, 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	Authentication and authorization are enforced for updating creator profiles.
ISO/IEC 27001	Yes	low	Access controls for creator profile updates are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for updating creator profiles maintain data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /api/brand/campaigns//image

Endpoint Path	/api/brand/campaigns//image
HTTP Methods	PUT, OPTIONS
Source Location	..\Mipoe-Backend\app.py - 1159
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1158, 1158, 1159, 1159, 1165, 1165, 1166, 1166, 1170, 1170, 1158, 1158, 1165, 1165, 1166, 1166, 1170, 1170, 1158, 1158, 1165, 1165, 1166, 1166, 1170, 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	Authentication and authorization are enforced for updating campaign images by brands.
ISO/IEC 27001	Yes	low	Access controls for brand campaign image updates are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for updating campaign images maintain data integrity.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1197, 1197, 1198, 1198, 1199, 1199, 1204, 1204, 1197, 1197, 1199, 1199, 1204, 1204, 1197, 1197, 1199, 1199, 1204, 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	Authentication and authorization are enforced for updating campaign budgets by brands.
ISO/IEC 27001	Yes	low	Access controls for brand campaign budget updates are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for updating campaign budgets maintain data integrity.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1229, 1229, 1230, 1230, 1231, 1231, 1235, 1235, 1229, 1229, 1231, 1231, 1235, 1235, 1229, 1229, 1231, 1231, 1235, 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	Authentication and authorization are enforced for updating campaign requirements by brands.
ISO/IEC 27001	Yes	low	Access controls for brand campaign requirements updates are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for updating campaign requirements maintain data integrity.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1258, 1258, 1259, 1259, 1260, 1260, 1264, 1264, 1258, 1258, 1260, 1260, 1264, 1264, 1258, 1258, 1260, 1260, 1264, 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	Authentication and authorization are enforced for updating campaign status by brands.
ISO/IEC 27001	Yes	low	Access controls for brand campaign status updates are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for updating campaign status maintain data integrity.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1289, 1289, 1290, 1290, 1291, 1291, 1295, 1295, 1289, 1289, 1291, 1291, 1295, 1295, 1289, 1289, 1291, 1291, 1295, 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	Authentication and authorization are enforced for updating campaign view thresholds by brands.
ISO/IEC 27001	Yes	low	Access controls for brand campaign view threshold updates are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for updating campaign view thresholds maintain data integrity.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1320, 1320, 1321, 1321, 1322, 1322, 1326, 1326, 1320, 1320, 1322, 1322, 1326, 1326, 1320, 1320, 1322, 1322, 1326, 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	Authentication and authorization are enforced for updating campaign deadlines by brands.
ISO/IEC 27001	Yes	low	Access controls for brand campaign deadline updates are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for updating campaign deadlines maintain data integrity.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1357, 1357, 1358, 1358, 1365, 1365, 1366, 1366, 1371, 1371, 1357, 1357, 1365, 1365, 1366, 1366, 1371, 1371, 1357, 1357, 1365, 1365, 1366, 1366, 1371, 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	Authentication is enforced, ensuring brands can only view pending payouts for their campaigns.
ISO/IEC 27001	Yes	low	Authentication controls protect brand-specific payout data, aligning with access management.
CSA STAR	Yes	low	Proper authentication for viewing pending payouts ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /api/brand/profile

Endpoint Path	/api/brand/profile
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 1455
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1454, 1454, 1455, 1455, 1456, 1456, 1460, 1460, 1454, 1454, 1456, 1456, 1460, 1460, 1454, 1454, 1456, 1456, 1460, 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	Authentication is enforced, ensuring brands can only view their own profiles.
ISO/IEC 27001	Yes	low	Authentication controls protect brand profile data, aligning with access management.
CSA STAR	Yes	low	Proper authentication for viewing brand profiles ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /api/brand/profile

Endpoint Path	/api/brand/profile
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1482
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1481, 1481, 1482, 1482, 1483, 1483, 1487, 1487, 1481, 1481, 1483, 1483, 1487, 1487, 1481, 1481, 1483, 1483, 1487, 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	Authentication and authorization are enforced for updating brand profiles.
ISO/IEC 27001	Yes	low	Access controls for brand profile updates are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for updating brand profiles maintain data integrity.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1513, 1513, 1514, 1514, 1528, 1528, 1529, 1529, 1513, 1513, 1528, 1528, 1529, 1529, 1513, 1513, 1528, 1528, 1529, 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	Authentication and authorization are enforced for updating clip view counts by administrators.
ISO/IEC 27001	Yes	low	Access controls for administrator clip view count updates are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for updating clip view counts maintain data integrity.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1579, 1579, 1580, 1580, 1591, 1591, 1592, 1592, 1579, 1579, 1591, 1591, 1592, 1592, 1579, 1579, 1591, 1591, 1592, 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	Authentication and authorization are enforced for updating campaign view counts by administrators.
ISO/IEC 27001	Yes	low	Access controls for administrator campaign view count updates are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for updating campaign view counts maintain data integrity.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1634, 1634, 1635, 1635, 1640, 1640, 1641, 1641, 1634, 1634, 1640, 1640, 1641, 1641, 1634, 1634, 1640, 1640, 1641, 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	Authentication is enforced, ensuring administrators can access campaign performance analytics.
ISO/IEC 27001	Yes	low	Authentication controls protect access to campaign performance analytics, aligning with access management.
CSA STAR	Yes	low	Proper authentication for accessing campaign performance analytics ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1737, 1737, 1738, 1738, 1738, 1739, 1744, 1744, 1745, 1745, 1748, 1748, 1761, 1761, 1761, 1737, 1737, 1739, 1744, 1744, 1745, 1745, 1748, 1748, 1772, 1772, 1778, 1737, 1737, 1744, 1744, 1745, 1745, 1772, 1772, 1778, 1772, 1772, 1782.

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	Authentication is enforced for Google sync operations.
ISO/IEC 27001	Yes	low	Authentication controls protect the integrity of third-party service integrations.
CSA STAR	Yes	low	Proper authentication for Google sync helps maintain data integrity and security.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /refresh

Endpoint Path	/refresh
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 1816
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Regulation	Applicable	Risk Level	Reason
ISO/IEC 27001	Yes	low	Authentication controls protect the session management process.
CSA STAR	Yes	low	Proper authentication for token refresh maintains session security.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /logout

Endpoint Path	/logout
HTTP Methods	DELETE
Source Location	..\Mipoe-Backend\app.py - 1832
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1831, 1831, 1832, 1832, 1836, 1836, 1831, 1831, 1836, 1836, 1831, 1831, 1836, 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	Authentication is enforced for logout operations.
ISO/IEC 27001	Yes	low	Authentication controls protect the session termination process.
CSA STAR	Yes	low	Proper authentication for logout maintains session security.

Security Assessment Notes

CVSS Vector: None

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	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Health check endpoints are typically public and do not pose a security risk if properly implemented.
ISO/IEC 27001	Yes	low	Publicly accessible health checks do not typically impact information security policies.
CSA STAR	Yes	low	Public health checks are generally acceptable and do not pose a direct security risk.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /create-deposit-order

Endpoint Path	/create-deposit-order
HTTP Methods	POST
Source Location	..\routes\payments.py - 49
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 48, 48, 49, 49, 50, 50, 55, 55, 48, 48, 50, 50, 55, 55, 48, 48, 50, 50, 55, 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	Authentication is enforced for creating deposit orders.
ISO/IEC 27001	Yes	low	Authentication controls protect financial transaction integrity.
CSA STAR	Yes	low	Proper authentication for creating deposit orders maintains financial data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /verify-deposit

Endpoint Path	/verify-deposit
HTTP Methods	POST
Source Location	..\routes\payments.py - 121
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 120, 120, 121, 121, 122, 122, 127, 127, 120, 120, 122, 122, 127, 127, 120, 120, 122, 122, 127, 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	Authentication is enforced for verifying deposits.
ISO/IEC 27001	Yes	low	Authentication controls protect financial transaction integrity.
CSA STAR	Yes	low	Proper authentication for verifying deposits maintains financial data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /virtual-account

Endpoint Path	/virtual-account
HTTP Methods	GET
Source Location	..\routes\payments.py - 192

Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 191, 191, 192, 192, 193, 193, 198, 198, 191, 191, 193, 193, 198, 198, 191, 191, 193, 193, 198, 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	Authentication is enforced for retrieving virtual account information.
ISO/IEC 27001	Yes	low	Authentication controls protect access to financial information.
CSA STAR	Yes	low	Proper authentication for virtual account details ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /wallet-balance

Endpoint Path	/wallet-balance
HTTP Methods	GET
Source Location	..\routes\payments.py - 243
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 242, 242, 243, 243, 244, 244, 247, 247, 242, 242, 244, 244, 247, 247, 242, 242, 244, 244, 247, 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	Authentication is enforced for retrieving wallet balance.
ISO/IEC 27001	Yes	low	Authentication controls protect access to financial information.
CSA STAR	Yes	low	Proper authentication for wallet balance ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /allocate-budget

Endpoint Path	/allocate-budget
HTTP Methods	POST
Source Location	..\routes\payments.py - 269
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 268, 268, 269, 269, 270, 270, 275, 275, 268, 268, 270, 270, 275, 275, 268, 268, 270, 270, 275, 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	Authentication is enforced for budget allocation.
ISO/IEC 27001	Yes	low	Authentication controls protect financial transaction integrity.
CSA STAR	Yes	low	Proper authentication for budget allocation maintains financial data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /reclaim-budget

Endpoint Path	/reclaim-budget
HTTP Methods	POST
Source Location	..\routes\payments.py - 349
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 348, 348, 349, 349, 350, 350, 355, 355, 348, 348, 350, 350, 355, 355, 348, 348, 350, 350, 355, 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	Authentication is enforced for budget reclamation.
ISO/IEC 27001	Yes	low	Authentication controls protect financial transaction integrity.
CSA STAR	Yes	low	Proper authentication for budget reclamation maintains financial data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /distribute-to-creator

Endpoint Path	/distribute-to-creator
HTTP Methods	POST
Source Location	..\routes\payments.py - 436
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 435, 435, 436, 436, 455, 455, 460, 460, 435, 435, 455, 455, 460, 460, 435, 435, 455, 455, 460, 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	Authentication is enforced for distributing funds to creators.
ISO/IEC 27001	Yes	low	Authentication controls protect financial transaction integrity.
CSA STAR	Yes	low	Proper authentication for creator distributions maintains financial data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /creator-withdraw

Endpoint Path	/creator-withdraw
HTTP Methods	POST
Source Location	..\routes\payments.py - 560
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 559, 559, 560, 560, 578, 578, 583, 583, 559, 559, 578, 578, 583, 583, 559, 559, 578, 578, 583, 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	Authentication is enforced for creator withdrawals.
ISO/IEC 27001	Yes	low	Authentication controls protect financial transaction integrity.
CSA STAR	Yes	low	Proper authentication for creator withdrawals maintains financial data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /creator/payout-details

Endpoint Path	/creator/payout-details
HTTP Methods	POST, PUT
Source Location	..\routes\payments.py - 735
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 734, 734, 735, 735, 750, 750, 755, 755, 734, 734, 750, 750, 755, 755, 734, 734, 750, 750, 755, 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	Authentication and authorization are enforced for saving creator payout details.
ISO/IEC 27001	Yes	low	Access controls for creator payout details ensure data integrity and confidentiality.
CSA STAR	Yes	low	Proper authentication and authorization for saving payout details maintain data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /creator/payout-details

Endpoint Path	/creator/payout-details
HTTP Methods	GET
Source Location	..\routes\payments.py - 823
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 822, 822, 823, 823, 828, 828, 833, 833, 822, 822, 828, 828, 833, 833, 822, 822, 828, 828, 833, 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	Authentication is enforced, ensuring creators can only view their own payout details.
ISO/IEC 27001	Yes	low	Authentication controls protect creator payout data, aligning with access management.
CSA STAR	Yes	low	Proper authentication for viewing creator payout details ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 872, 872, 873, 873, 878, 878, 883, 883, 872, 872, 878, 878, 883, 883, 872, 872, 878, 878, 883, 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	Authentication is enforced for verifying creator payout details.
ISO/IEC 27001	Yes	low	Authentication controls protect financial transaction integrity.
CSA STAR	Yes	low	Proper authentication for verifying payout details maintains financial data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /creator/withdrawals

Endpoint Path	/creator/withdrawals
HTTP Methods	GET
Source Location	..\routes\payments.py - 933
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 932, 932, 933, 933, 940, 940, 945, 945, 932, 932, 940, 940, 945, 945, 932, 932, 940, 940, 945, 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	Authentication is enforced, ensuring creators can only view their own withdrawal history.
ISO/IEC 27001	Yes	low	Authentication controls protect creator withdrawal history, aligning with access management.
CSA STAR	Yes	low	Proper authentication for viewing creator withdrawals ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /creator/notifications/

Endpoint Path	/creator/notifications/
HTTP Methods	GET
Source Location	..\routes\payments.py - 995
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 994, 994, 995, 995, 999, 999, 1000, 1000, 1002, 1002, 994, 994, 999, 999, 1000, 1000, 1002, 1002, 994, 994, 999, 999, 1000, 1000, 1002, 1002, 1000, 1000, 1002, 1002, 1002, 1002, 1002, 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	Authentication is enforced, ensuring creators can only view their own notifications.
ISO/IEC 27001	Yes	low	Authentication controls protect creator notification data, aligning with access management.
CSA STAR	Yes	low	Proper authentication for viewing creator notifications ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /transactions//

Endpoint Path	/transactions//
HTTP Methods	GET
Source Location	..\routes\payments.py - 1030
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1029, 1029, 1030, 1030, 1030, 1031, 1031, 1035, 1035, 1035, 1038, 1042, 1029, 1029, 1031, 1031, 1035, 1035, 1035, 1038, 1042, 1029, 1029, 1031, 1031, 1035, 1035, 1038, 1042, 1038, 1042, 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	Authentication is enforced, ensuring users can only view their own transaction history.
ISO/IEC 27001	Yes	low	Authentication controls protect user transaction history, aligning with access management.
CSA STAR	Yes	low	Proper authentication for viewing transaction history ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /refund-campaign

Endpoint Path	/refund-campaign
HTTP Methods	POST
Source Location	..\routes\payments.py - 1110
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1109, 1109, 1110, 1110, 1126, 1126, 1131, 1131, 1109, 1109, 1126, 1126, 1131, 1131, 1109, 1109, 1126, 1126, 1131, 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	Authentication is enforced for refund requests.
ISO/IEC 27001	Yes	low	Authentication controls protect financial transaction integrity.
CSA STAR	Yes	low	Proper authentication for refund requests maintains financial data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /campaign-summary/

Endpoint Path	/campaign-summary/
HTTP Methods	GET
Source Location	..\routes\payments.py - 1203
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1202, 1202, 1203, 1203, 1215, 1215, 1217, 1217, 1202, 1202, 1215, 1215, 1217, 1217, 1202, 1202, 1215, 1215, 1217, 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	Authentication is enforced, ensuring authorized users can view campaign summaries.
ISO/IEC 27001	Yes	low	Authentication controls protect campaign summary data, aligning with access management.
CSA STAR	Yes	low	Proper authentication for viewing campaign summaries ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /calculate-earnings//

Endpoint Path	/calculate-earnings//
HTTP Methods	GET
Source Location	..\routes\payments.py - 1270
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1269, 1269, 1270, 1270, 1283, 1283, 1285, 1285, 1269, 1269, 1283, 1283, 1285, 1285, 1269, 1269, 1283, 1283, 1285, 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	Authentication is enforced, ensuring creators can only calculate their own earnings.
ISO/IEC 27001	Yes	low	Authentication controls protect creator earnings data, aligning with access management.
CSA STAR	Yes	low	Proper authentication for calculating creator earnings ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /bulk-distribute

Endpoint Path	/bulk-distribute
HTTP Methods	POST
Source Location	..\routes\payments.py - 1364
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1363, 1363, 1364, 1364, 1384, 1384, 1389, 1389, 1363, 1363, 1384, 1384, 1389, 1389, 1363, 1363, 1384, 1384, 1389, 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	Authentication is enforced for bulk distribution.
ISO/IEC 27001	Yes	low	Authentication controls protect financial transaction integrity.
CSA STAR	Yes	low	Proper authentication for bulk distribution maintains financial data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /request-refund

Endpoint Path	/request-refund
HTTP Methods	POST
Source Location	..\routes\payments.py - 1535
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1534, 1534, 1535, 1535, 1548, 1548, 1553, 1553, 1534, 1534, 1548, 1548, 1553, 1553, 1534, 1534, 1548, 1548, 1553, 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	Authentication is enforced for refund requests.

Regulation	Applicable	Risk Level	Reason
ISO/IEC 27001	Yes	low	Authentication controls protect financial transaction integrity.
CSA STAR	Yes	low	Proper authentication for refund requests maintains financial data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /refund-requests

Endpoint Path	/refund-requests
HTTP Methods	GET
Source Location	..\routes\payments.py - 1629
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1628, 1628, 1629, 1629, 1636, 1636, 1641, 1641, 1628, 1628, 1636, 1636, 1641, 1641, 1628, 1628, 1636, 1636, 1641, 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	Authentication is enforced, ensuring authorized users can view refund requests.
ISO/IEC 27001	Yes	low	Authentication controls protect refund request data, aligning with access management.

Regulation	Applicable	Risk Level	Reason
CSA STAR	Yes	low	Proper authentication for viewing refund requests ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /admin/approve-refund

Endpoint Path	/admin/approve-refund
HTTP Methods	POST
Source Location	..\routes\payments.py - 1696
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1695, 1695, 1696, 1696, 1709, 1709, 1714, 1714, 1695, 1695, 1709, 1709, 1714, 1714, 1695, 1695, 1709, 1709, 1714, 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	Authentication and authorization are enforced for approving refunds by administrators.

Regulation	Applicable	Risk Level	Reason
ISO/IEC 27001	Yes	low	Access controls for administrator refund approval are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for approving refunds maintain financial data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /admin/reject-refund

Endpoint Path	/admin/reject-refund
HTTP Methods	POST
Source Location	..\routes\payments.py - 1810
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1809, 1809, 1810, 1810, 1821, 1821, 1826, 1826, 1809, 1809, 1821, 1821, 1826, 1826, 1809, 1809, 1821, 1821, 1826, 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	Authentication and authorization are enforced for rejecting refunds by administrators.
ISO/IEC 27001	Yes	low	Access controls for administrator refund rejection are in place, ensuring data integrity.
CSA STAR	Yes	low	Proper authentication and authorization for rejecting refunds maintain financial data integrity.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /refund-status/

Endpoint Path	/refund-status/
HTTP Methods	GET
Source Location	..\routes\payments.py - 1871
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1870, 1870, 1871, 1871, 1878, 1878, 1880, 1880, 1870, 1870, 1878, 1878, 1880, 1880, 1870, 1870, 1878, 1878, 1880, 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	Authentication is enforced, ensuring authorized users can view refund status.
ISO/IEC 27001	Yes	low	Authentication controls protect refund status information, aligning with access management.
CSA STAR	Yes	low	Proper authentication for viewing refund status ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

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 (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 1939, 1939, 1940, 1940, 1947, 1947, 1939, 1939, 1947, 1947, 1939, 1939, 1947, 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	Authentication is enforced, ensuring administrators can access the refund audit trail.
ISO/IEC 27001	Yes	low	Authentication controls protect access to audit trail data, aligning with access management.
CSA STAR	Yes	low	Proper authentication for accessing the refund audit trail ensures data confidentiality.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path /creator/revert-withdrawal

Endpoint Path	/creator/revert-withdrawal
HTTP Methods	POST
Source Location	..\routes\payments.py - 2019
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a unknown-based mechanism. Authentication checks were detected at the following code locations: 2018, 2018, 2019, 2019, 2024, 2024, 2029, 2029, 2018, 2018, 2024, 2024, 2029, 2029, 2018, 2018, 2024, 2024, 2029, 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	Authentication is enforced for reverting withdrawals.
ISO/IEC 27001	Yes	low	Authentication controls protect financial transaction integrity.
CSA STAR	Yes	low	Proper authentication for reverting withdrawals maintains financial data integrity.

Security Assessment Notes

CVSS Vector: None

References

METRICS SUMMARY

Total Findings: 4

Severity	Count
CRITICAL	2
HIGH	0
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.

Remediate Critical RCE and Secret Exposure (Priority: Immediate)

Description: Flask debug mode and hardcoded JWT tokens provide a direct path to Remote Code Execution and unauthorized system access.

Why it Matters: Active exploitation of Werkzeug's debugger allows arbitrary code execution; leaked JWTs result in immediate account compromise.

Recommended Actions:

- Set 'debug=False' and remove 'use_reloader=True' in app.py.
- Remove the hardcoded JWT string from tasks.py line 14.
- Shift all secrets (JWT keys, API tokens) to environment variables or a Secret Manager (AWS Secrets Manager, HashiCorp Vault).
- Invalidate and rotate the signing keys for all currently active JWTs.

Expected Outcome: Elimination of the RCE vector and prevention of credential leakage via source code.

Secure Public Authentication Endpoints (Priority: Immediate)

Description: The /register, /login, and /request-password-reset endpoints currently lack rate limiting and secondary validation.

Why it Matters: Open authentication endpoints are highly susceptible to brute-force attacks, credential stuffing, and mass account creation.

Recommended Actions:

- Implement Flask-Limiter to enforce strict rate limits on /login and /register.
- Add CAPTCHA or bot detection to the registration and password reset flows.
- Enforce complex password policies and implement multi-factor authentication (MFA).
- Ensure /request-password-reset uses short-lived, single-use cryptographically secure tokens.

Expected Outcome: Reduction in account takeover (ATO) risk and protection against automated abuse.

Sanitize Global Error Handling (Priority: Short-Term)

Description: API endpoints are returning raw stack traces and exception messages (str(e)) to the client.

Why it Matters: Verbose errors reveal database schemas, file paths, and library versions, aiding attackers in reconnaissance.

Recommended Actions:

- Implement a global @app.errorhandler(Exception) to catch unhandled errors.
- Standardize all error responses to return a generic 'Internal Server Error' message and a unique correlation ID.
- Configure server-side logging (e.g., using Python's logging module or Sentry) to capture full traces for internal debugging only.

Expected Outcome: Prevention of information disclosure through API responses.

Enforce Resource Timeouts on Outbound Calls (Priority: Short-Term)

Description: External API calls (e.g., Cashfree) are made without defined timeouts, risking thread exhaustion.

Why it Matters: A slow or unresponsive third-party service will cause the application to hang, leading to a self-inflicted Denial of Service (DoS).

Recommended Actions:

- Update all 'requests.get' and 'requests.post' calls in routes/payments.py to include a 'timeout' parameter (e.g., timeout=5).
- Implement a circuit breaker pattern for critical external payment integrations.
- Configure Gunicorn/uWSGI worker timeouts to match expected application response times.

Expected Outcome: Improved application availability and resilience against external service degradation.

Hardening Production Infrastructure (Priority: Mid-Term)

Description: The application is currently configured for a development environment rather than a secure production stack.

Why it Matters: Development servers (app.run) are not designed for security or concurrency and lack essential protection layers.

Recommended Actions:

- Transition from 'app.run()' to a production WSGI server like Gunicorn or uWSGI.
- Deploy a Reverse Proxy (Nginx/Apache) in front of the application to handle SSL/TLS termination and request filtering.
- Set the 'Secure' and 'HttpOnly' flags on all session and authentication cookies.

Expected Outcome: Alignment with SOC 2/ISO 27001 requirements for secure system configuration.

Integrate Continuous Security (DevSecOps) (Priority: Long-Term)

Description: Security vulnerabilities were found manually/post-development, indicating a gap in the secure development lifecycle.

Why it Matters: Proactive security reduces remediation costs and ensures compliance persistence (SOC 2, CSA STAR).

Recommended Actions:

- Integrate Static Application Security Testing (SAST) tools into the CI/CD pipeline to block commits containing secrets.
- Perform regular Software Composition Analysis (SCA) to identify and patch vulnerable dependencies.
- Establish an automated secret scanning routine for all code repositories.

Expected Outcome: Sustained security posture and automated prevention of recurring critical vulnerabilities.