SECURITY ANALYSIS REPORT

for repository : InfluencerPay API

Generated By

Backstage Rookie

Provider: Backstage Rookie

contact - swarajdarekar9@gmail.com

Client: Chandrakant Darekar

darekar138@gmail.com

Scan ID: 7789c635-a63c-45dd-a42a-efecf23a191e

Date: 2026-02-12 00:48:48

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 of the InfluencerPay API identified critical vulnerabilities related to hardcoded secrets and debug mode exposure, posing severe risks including remote code execution and unauthorized access. Additionally, the report highlights potential denial-of-service vectors due to missing HTTP request timeouts and excessive error information disclosure that could aid attackers in reconnaissance. Prompt remediation of these findings is essential to prevent significant security breaches and ensure application stability.

Identified Vulnerabilities

ID	Title	CVSS	Page
C1	Hardcoded JWT Token	9.8	
C2	Flask Debug Mode Enabled in Production	9.8	
M1	Missing Timeout for External HTTP Requests	5.3	
L1	Excessive Error Information Disclosure	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

Name	IP

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) has been found directly embedded within the source code, posing a significant security risk if the token is valid or if the repository is publicly accessible.

Details

The `tasks.py` file at line 14 contains a full JWT token string hardcoded. Even if this file is intended for testing or development, the presence of a live or easily reusable secret in source code is a critical vulnerability. If this token or its signature key is compromised through code leakage, an attacker could potentially gain unauthorized access to protected resources or impersonate users if the token is still active or valid in a production environment.

Evidence

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

References

- https://owasp.org/www-community/vulnerabilities/Hardcoded_password
- https://cwe.mitre.org/data/definitions/798.html

Recommendation

- Never hardcode sensitive information like API keys, database credentials, or JWT tokens directly into source code. - Utilize environment variables, a secrets management service (e.g., AWS Secrets Manager, HashiCorp Vault), or a secure configuration system to store and retrieve tokens. - Ensure that such secrets are rotated regularly and are not committed to version control. - For development/testing, use dummy tokens or mock services, and ensure `tasks.py` is excluded from production deployments.

Prompt to Solve the Vulnerability:

In `tasks.py` at line 14, the JWT token is hardcoded. This token should be loaded from a secure source, such as an environment variable or a secrets management service, instead of being directly embedded in the source code. For local development, consider using a `.env` file that is excluded from version control (e.g., via `.gitignore`). Replace `token = "..."` with a call to `os.getenv('YOUR_JWT_TOKEN_ENV_VAR')` after ensuring `load_dotenv()` is called.

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 in debug mode, which exposes the Werkzeug debugger and allows execution of arbitrary code if an error occurs, leading to remote code execution (RCE).

Details

In `app.py` at line 1872, the `app.run()` call explicitly sets `debug=True`. In a production environment, this setting is extremely dangerous. It activates the Werkzeug debugger, which, in the event of an unhandled exception, presents an interactive console to the client. An attacker can use this console to execute arbitrary Python code on the server, gaining full control over the application and potentially the underlying system. The `use_reloader=True` option, also present, is also not suitable for production.

Evidence

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

References

- https://flask.palletsprojects.com/en/2.0.x/config/#debug-mode
- https://cwe.mitre.org/data/definitions/489.html

Recommendation

- Ensure debug mode is disabled in production environments. - Use a production-ready WSGI server (e.g., Gunicorn, uWSGI) instead of `app.run()` for deployment. - Configure Flask applications to read `DEBUG` settings from environment variables or a secure configuration system that defaults to `False` in production. - Implement robust logging and monitoring to catch and alert on errors without exposing internal details to clients.

Prompt to Solve the Vulnerability:

In `app.py` at line 1872, the Flask application is run with `debug=True`. This setting should be disabled in all production deployments as it exposes the Werkzeug debugger, allowing arbitrary code execution. Modify this line to conditionally enable debug mode only for development environments, typically by checking an environment variable. For example, replace `app.run(debug=True, port=5000, use_reloader=True)` with `app.run(debug=os.getenv('FLASK_DEBUG') == 'True', port=5000, use_reloader=os.getenv('FLASK_RELOADER') == 'True')` and ensure `FLASK_DEBUG` is 'False' in production. Additionally, production deployments should use a dedicated WSGI server like Gunicorn instead of `app.run()`.

M1 – Missing Timeout for External HTTP Requests

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 HTTP requests made to external services (Cashfree API) lack explicit timeout configurations, potentially leading to application unresponsiveness or denial of service.

Details

In `routes\payments.py` at lines 90, 136, and 663, `requests.post()` and `requests.get()` calls are made to the Cashfree API without specifying a `timeout` parameter. This means that if the external Cashfree API becomes slow, unresponsive, or maliciously holds open connections, the application's threads handling these requests will block indefinitely or for a very long default timeout (which can be several minutes). This can consume server resources, exhaust connection pools, and lead to application-wide performance degradation or a denial of service.

Evidence

- **routes\payments.py:90:** requests.post call to Cashfree API without a timeout.
- **routes\payments.py:136:** requests.get call to Cashfree API without a timeout.
- **routes\payments.py:663:** requests.post call to Cashfree Payouts API without a timeout.

References

- https://docs.python-requests.org/en/master/user/advanced/#timeouts
- https://cwe.mitre.org/data/definitions/400.html

Recommendation

- Always specify a `timeout` parameter for all external HTTP requests. - Choose a reasonable timeout value based on the expected response time of the external service and the criticality of the operation. - Implement retry mechanisms with exponential backoff for transient network issues, but ensure each retry also respects a timeout. - Centralize HTTP client configuration where possible to enforce timeouts across the application.

Prompt to Solve the Vulnerability:

In `routes/payments.py` at lines 90, 136, and 663, HTTP requests are made to external services using `requests.post()` and `requests.get()` without specifying a `timeout` parameter. To prevent indefinite blocking and potential denial of service, add a `timeout` parameter to all `requests` calls. For instance, change `response = requests.post(...)` to `response = requests.post(..., timeout=(5, 10))`, where `(5, 10)` represents 5 seconds for connect timeout and 10 seconds for read timeout. Adjust these values based on the expected response times of the external API.

L1 – Excessive Error Information Disclosure

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 (app.py, routes\payments.py)

Overview

The application exposes raw exception details in API responses, which can inadvertently reveal sensitive internal system information to clients.

Details

Across `app.py` and `routes\payments.py`, various error handling blocks catch generic `Exception` types and include the full string representation of the exception (`str(e)`) in the JSON response sent to the client (e.g., `{'msg': 'Login failed', 'error': str(e)}`). While this is useful for debugging during development, in a production environment, such verbose error messages can leak internal system architecture, database schema details, file paths, or specific library versions. This information can be leveraged by attackers to craft more targeted attacks, increasing the risk of more severe vulnerabilities.

Evidence

- **app.py:117:** Generic exception `str(e)` returned in API response.
- **app.py:187:** Generic exception `str(e)` returned in API response.
- **routes\payments.py:115:** Generic exception `str(e)` returned in API response.
- **routes\payments.py:729:** Generic exception `str(e)` returned in API response.
- **Multiple other instances:** This pattern is widespread across the codebase, occurring over 50 times in `app.py` and `routes\payments.py`.

References

- https://owasp.org/www-community/vulnerabilities/Information_leakage
- https://cwe.mitre.org/data/definitions/209.html

Recommendation

- Refrain from exposing raw exception details to clients in production environments. - Log full exception details and stack traces internally for debugging and analysis. - Provide generic, user-friendly error messages to clients (e.g., "An unexpected error occurred. Please try again later."). - Implement a centralized error handling mechanism to ensure consistent and secure error responses across the application.

Prompt to Solve the Vulnerability:

Across `app.py` and `routes/payments.py` (e.g., `app.py:117`, `routes/payments.py:115`), various API endpoints return raw exception details in their error responses, like `{'msg': 'Login failed', 'error': str(e)}`. This can expose internal system information. To remediate, replace `str(e)` with generic, non-informative messages for end-users in production environments. For example, change it to `return jsonify({'msg': 'Login failed', 'error': 'An unexpected error occurred.'}), 500`. Ensure that full exception details are logged securely on the server side for debugging, but not exposed publicly.

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	9.8

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for the registration endpoint.

  Potential Attack Scenario:

  An attacker could create a large number of fake accounts, leading to denial of service or abuse of the platform.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of authentication on registration can lead to unauthorized account creation, violating principles of access control and security.
ISO/IEC 27001	Yes	high	Absence of authentication controls for user registration poses a risk to information security by allowing unverified access.
CSA STAR	Yes	high	Inadequate authentication for user registration is a security vulnerability that impacts the integrity and availability of cloud services.

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/Forgot_password_management
- https://nvd.nist.gov/vuln/detail/CVE-2023-XXXX

Endpoint Path /login

Endpoint Path	/login
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 120
Authentication Required	No
Risk Severity	Critical
CVSS Score	9.8

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for the login endpoint.

  Potential Attack Scenario:

  Without proper authentication, unauthorized users could gain access to user accounts, leading to data breaches and account takeover.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of authentication on login bypasses security controls, potentially allowing unauthorized access to sensitive information.

Regulation	Applicable	Risk Level	Reason
ISO/IEC 27001	Yes	high	Failure to enforce authentication for login violates access control principles and increases the risk of unauthorized system access.
CSA STAR	Yes	high	Missing authentication on login is a critical security flaw that compromises the confidentiality and integrity of data.

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_vulnerabilities
- https://nvd.nist.gov/vuln/detail/CVE-2023-XXXX

Endpoint Path /verify-instagram

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /verify-instagram/

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /request-password-reset

Endpoint Path	/request-password-reset
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 224
Authentication Required	No
Risk Severity	High
CVSS Score	8.2

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (medium): Authentication is missing for the password reset request endpoint.

  Potential Attack Scenario:

  An attacker could abuse this endpoint to trigger password reset emails for other users, potentially leading to account takeover if they can intercept the reset link.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Lack of authentication on password reset can be exploited for unauthorized account access attempts, impacting access control.
ISO/IEC 27001	Yes	medium	The password reset mechanism should have proper controls to prevent abuse, which is compromised by missing authentication.
CSA STAR	Yes	medium	Insecure password reset functionality can lead to account compromise, affecting the integrity and confidentiality of user data.

Security Assessment Notes

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

References

- https://owasp.org/www-community/vulnerabilities/Forgot_password_management
- https://nvd.nist.gov/vuln/detail/CVE-2023-XXXX

Endpoint Path /api/brand/campaigns

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/campaigns

Endpoint Path	/api/campaigns
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 329
Authentication Required	No
Risk Severity	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 missing for retrieving all campaigns.

Potential Attack Scenario:

Unauthorized access to campaign data could lead to information disclosure or manipulation.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Exposure of campaign data without authentication could violate confidentiality controls.
ISO/IEC 27001	Yes	medium	Access control for sensitive campaign information is not enforced, posing a risk to data security.
CSA STAR	Yes	medium	Lack of authentication for retrieving campaign data can lead to unauthorized access and potential data leakage.

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
- https://nvd.nist.gov/vuln/detail/CVE-2023-XXXX

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 missing for retrieving a specific campaign.

  Potential Attack Scenario:

  Unauthorized users could access sensitive details of specific campaigns.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Exposure of campaign data without authentication could violate confidentiality controls.
ISO/IEC 27001	Yes	medium	Access control for sensitive campaign information is not enforced, posing a risk to data security.
CSA STAR	Yes	medium	Lack of authentication for retrieving campaign data can lead to unauthorized access and potential data leakage.

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
- https://nvd.nist.gov/vuln/detail/CVE-2023-XXXX

Endpoint Path /api/creator/your-campaigns

Endpoint Path	/api/creator/your-campaigns
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 495
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/submit-clip

Endpoint Path	/api/creator/submit-clip
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 583
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/campaign-clips

Endpoint Path	/api/creator/campaign-clips
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 657
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

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

Endpoint Path	/api/creator/accepted-clip-details/
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 722
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

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 (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

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 (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/admin/campaigns

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/admin/clip/

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

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 (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/profile

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/profile

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

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 (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//budget

Endpoint Path	/api/brand/campaigns//budget
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1198
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//requirements

Endpoint Path	/api/brand/campaigns//requirements
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1230
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//status

Endpoint Path	/api/brand/campaigns//status
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1259
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//view_threshold

Endpoint Path	/api/brand/campaigns//view_threshold
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1290
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//deadline

Endpoint Path	/api/brand/campaigns//deadline
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1321
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

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

Endpoint Path	/api/brand/campaigns//pending-payouts
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 1358
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/profile

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/profile

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

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

Endpoint Path	/api/admin/clip//view-count
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1514
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

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

Endpoint Path	/api/admin/campaign//update-views
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1580
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

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

Endpoint Path	/api/admin/analytics/campaign-performance/
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 1635
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/auth/google-sync

Endpoint Path	/api/auth/google-sync
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 1738
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /refresh

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /logout

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/health

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

- **AUTH_MISSING** (low): Authentication is missing for the health check endpoint.

  Potential Attack Scenario:

  While typically low impact, this could potentially be used in conjunction with other vulnerabilities or for reconnaissance if it reveals information about the system's internal state.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /create-deposit-order

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /verify-deposit

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /virtual-account

Endpoint Path	/virtual-account
HTTP Methods	GET
Source Location	..\routes\payments.py - 192
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /wallet-balance

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /allocate-budget

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /reclaim-budget

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /distribute-to-creator

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator-withdraw

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/payout-details

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/payout-details

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/verify-payout-details

Endpoint Path	/creator/verify-payout-details
HTTP Methods	POST
Source Location	..\routes\payments.py - 873
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/withdrawals

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/notifications/

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /transactions//

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /refund-campaign

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /campaign-summary/

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /calculate-earnings//

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /bulk-distribute

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /request-refund

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /refund-requests

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /admin/approve-refund

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /admin/reject-refund

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /refund-status/

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /admin/refund-audit-trail

Endpoint Path	/admin/refund-audit-trail
HTTP Methods	GET
Source Location	..\routes\payments.py - 1940
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/revert-withdrawal

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

Authentication Analysis

This endpoint enforces authentication using a token-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	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
ISO/IEC 27001	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.
CSA STAR	No	low	No direct compliance applicability identified for this specific endpoint based on provided data.

Security Assessment Notes

CVSS Vector:

References

BUSINESS RISK ADVICE

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

Remove Hardcoded Sensitive Information (Priority: Immediate)

Description: A JSON Web Token (JWT) is directly embedded in the source code. This poses a critical risk for unauthorized access and impersonation if discovered.

Why it Matters: Compromised secrets lead to full system control, unauthorized data access, and potential remote code execution (RCE). Violates SOC 2, ISO/IEC 27001, and CSA STAR principles of confidentiality and integrity.

Recommended Actions:

- Extract all sensitive values (JWTs, API keys, credentials) from source code.
- Utilize environment variables, a dedicated secrets management service (e.g., HashiCorp Vault, AWS Secrets Manager), or a secure configuration system.
- Implement a process for regular rotation of all secrets.
- Ensure secrets are never committed to version control systems.

Expected Outcome: Elimination of secret exposure, significantly reducing the attack surface and risk of unauthorized access.

Disable Flask Debug Mode in Production (Priority: Immediate)

Description: The Flask application is configured to run with debug mode enabled, exposing an interactive debugger in case of errors.

Why it Matters: Enabling debug mode in production is a critical RCE vulnerability, allowing attackers to execute arbitrary code on the server. Violates all major compliance frameworks by undermining system integrity and availability.

Recommended Actions:

- Set `debug=False` for all production deployments of the Flask application.
- Use a production-ready WSGI server (e.g., Gunicorn, uWSGI) instead of `app.run()` for deployment.
- Configure the application to conditionally enable debug mode based on environment variables (e.g., `FLASK_ENV='development'`).

Expected Outcome: Removal of the RCE vulnerability associated with the Werkzeug debugger, securing the application runtime environment.

Harden Core Authentication and Account Management Endpoints (Priority: Immediate)

Description: Several key authentication endpoints (register, login, password reset) lack sufficient security controls, potentially leading to account enumeration, brute-force attacks, or unauthorized account creation.

Why it Matters: Weak authentication mechanisms are prime targets for attackers, leading to account takeovers, unauthorized access to user data, and denial of service. Directly impacts SOC 2 (Access Control), ISO/IEC 27001 (A.9.2), and CSA STAR.

Recommended Actions:

- Implement robust rate-limiting on `/register`, `/login`, and `/request-password-reset` to prevent brute-force and enumeration attacks.
- Integrate CAPTCHA or similar bot-detection mechanisms for user registration and login flows.
- Enforce strong password policies (complexity, length, uniqueness) and use secure password hashing algorithms (e.g., bcrypt, Argon2).
- Ensure password reset tokens are single-use, time-limited, and securely transmitted (e.g., via HTTPS only).

Expected Outcome: Significantly reduced risk of account compromise, unauthorized account creation, and improved overall user account security.

Enforce Timeouts for External HTTP Requests (Priority: Short-Term)

Description: External HTTP requests to services like the Cashfree API are missing explicit timeout configurations.

Why it Matters: Without timeouts, unresponsive external services can cause application threads to hang indefinitely, leading to resource exhaustion and potential denial of service (DoS). Affects application availability and reliability.

Recommended Actions:

- Add a `timeout` parameter to all `requests.post()` and `requests.get()` calls to external services (e.g., `timeout=(connect_timeout, read_timeout)`).
- Determine appropriate `connect_timeout` and `read_timeout` values based on expected external API performance.
- Implement robust error handling and retry logic for timeout failures to improve resilience.

Expected Outcome: Prevention of application hangs and improved resilience against slow or unresponsive third-party services, enhancing application stability.

Implement Authorization for Sensitive Data Endpoints (Priority: Short-Term)

Description: Endpoints exposing campaign data (`/api/campaigns`, `/api/campaigns/`) are accessible without authentication.

Why it Matters: Unauthorized access to campaign data can lead to information disclosure, competitive intelligence gathering, or manipulation. Directly impacts confidentiality and integrity as per SOC 2, ISO/IEC 27001 (A.9.1), and CSA STAR.

Recommended Actions:

- Require JWT-based authentication for all `/api/campaigns` and `/api/campaigns/` GET endpoints.
- Implement fine-grained authorization checks to ensure users can only access campaigns they are explicitly permitted to view or manage.
- Review all API endpoints to ensure appropriate authentication and authorization are enforced based on data sensitivity and user roles.

Expected Outcome: Restricted access to sensitive campaign information, ensuring only authorized users can view or interact with specific campaigns, mitigating information leakage.

Minimize Excessive Error Information Disclosure (Priority: Short-Term)

Description: Raw exception details and stack traces are being exposed in API responses to clients.

Why it Matters: Verbose error messages provide attackers with valuable reconnaissance information about internal system architecture, technologies, file paths, and potential vulnerabilities. This information can be used to craft more targeted attacks.

Recommended Actions:

- Replace raw exception details (`str(e)`) with generic, non-informative error messages for end-users in production environments (e.g., 'An unexpected error occurred.').
- Implement a centralized error handling mechanism to ensure consistent and secure error responses across the entire application.
- Ensure full exception details and stack traces are logged securely on the server-side for internal debugging, not exposed publicly.

Expected Outcome: Reduced information leakage to potential attackers, making reconnaissance more difficult and preventing the exploitation of known vulnerabilities based on disclosed details.

Enhance Input Validation and Output Encoding (Priority: Mid-Term)

Description: The scan did not explicitly cover all input validation or output encoding issues, but these are fundamental for web application security.

Why it Matters: Lack of proper input validation and output encoding can lead to various injection attacks (SQL Injection, XSS, Command Injection) and data integrity issues. Core to OWASP Top 10 'Injection' and 'Cross-Site Scripting' categories.

Recommended Actions:

- Implement strict input validation for all user-supplied data, checking for type, length, format, and acceptable values.
- Use allow-list validation where possible to only permit known-good input.
- Apply context-aware output encoding for all data displayed to users, preventing XSS and other client-side injection attacks.
- Utilize parameterized queries or ORM capabilities to prevent SQL Injection in database interactions.

Expected Outcome: Robust defense against injection vulnerabilities, protecting data integrity and confidentiality across the application.

Strengthen Session Management and Token Security (Priority: Mid-Term)

Description: Beyond hardcoded tokens, a comprehensive review of JWT and session management practices is needed to ensure robustness.

Why it Matters: Insecure session management can lead to session hijacking, replay attacks, or unauthorized persistent access, even with authentication in place. Addresses OWASP Top 10 'Broken Authentication and Session Management'.

Recommended Actions:

- Implement short-lived access tokens and longer-lived, securely stored refresh tokens.
- Ensure tokens are always transmitted over HTTPS/TLS.
- Implement token revocation mechanisms for logout, password changes, or suspected compromise.
- Securely store refresh tokens (e.g., HTTP-only cookies, encrypted storage) and rotate them regularly.

Expected Outcome: Improved resilience against session hijacking and unauthorized token use, enhancing the overall integrity of user sessions.

Improve Logging, Monitoring, and Alerting (Priority: Mid-Term)

Description: The assessment indicates potential gaps in comprehensive logging and monitoring that could hinder incident detection and response.

Why it Matters: Insufficient logging and monitoring make it difficult to detect, investigate, and recover from security incidents, increasing the impact of breaches. Crucial for SOC 2 (Monitoring Activities), ISO/IEC 27001 (A.12.4), and CSA STAR.

Recommended Actions:

- Implement centralized logging of all security-relevant events (authentication attempts, authorization failures, critical system errors, data modifications).
- Integrate logs with a Security Information and Event Management (SIEM) system for aggregation and correlation.
- Configure real-time alerts for suspicious activities, failed login attempts, and unusual API access patterns.
- Regularly review logs for anomalies and potential security incidents.

Expected Outcome: Enhanced visibility into security events, enabling faster detection, more effective investigation, and timely response to potential threats.

Integrate Security into the SDLC (Shift Left) (Priority: Long-Term)

Description: A proactive approach to security is essential to identify and mitigate vulnerabilities earlier in the development lifecycle.

Why it Matters: Addressing security flaws late in the SDLC is significantly more expensive and risky. Proactive security integration reduces the overall attack surface and improves code quality. Supports SOC 2, ISO/IEC 27001 (A.14), and CSA STAR requirements.

Recommended Actions:

- Implement regular security training for all developers on secure coding practices (e.g., OWASP Top 10).
- Conduct threat modeling exercises for new features and significant architectural changes.
- Integrate SAST and DAST tools into CI/CD pipelines to automatically detect vulnerabilities.
- Perform peer code reviews with a focus on security before merging code to main branches.

Expected Outcome: Fewer vulnerabilities introduced into the codebase, reduced remediation costs, and a more secure application by design.

Conduct Regular Security Assessments and Penetration Testing (Priority: Long-Term)

Description: Beyond automated scans, periodic manual and simulated attack assessments are necessary to uncover complex vulnerabilities.

Why it Matters: Automated tools have limitations; human-led penetration testing identifies business logic flaws, complex attack chains, and zero-day vulnerabilities. Essential for continuous assurance and compliance with SOC 2, ISO/IEC 27001 (A.18.2), and CSA STAR.

Recommended Actions:

- Schedule annual external penetration tests by qualified third-party security firms.
- Perform regular internal vulnerability assessments and exploitability testing.
- Establish a bug bounty program to incentivize ethical hackers to find and report vulnerabilities.
- Review and update security assessment methodologies based on emerging threats and changes to the application.

Expected Outcome: Comprehensive validation of the application's security posture, identification of advanced threats, and continuous improvement based on real-world attack simulations.