SECURITY ANALYSIS REPORT

Generated By

Backstage Rookie

Provider: Backstage Rookie

contact - swarajdarekar9@gmail.com

Client: N/A

N/A

Scan ID: 675f22c6-a046-4336-885a-48d97badfda1

Date: 2026-02-10 13:41:22

Version: 1.0.0

TABLE OF CONTENTS

/api/admin/campaigns

/api/admin/clip/

/api/admin/clip/

/api/admin/clip/

/api/creator/profile

/api/creator/profile

/api/brand/campaigns//image

/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/

EXECUTIVE SUMMARY

This security assessment identified critical and high-severity vulnerabilities, alongside several medium and low-severity issues within the application's codebase. The most severe finding involves the application being configured with debug mode enabled, which poses an immediate and significant risk to the production environment, allowing for arbitrary code execution. Additionally, a hardcoded authentication token and a vulnerable dependency were discovered, both of which could be exploited by attackers. Numerous instances of verbose error messages indicate a potential for information leakage. Addressing these issues is crucial for enhancing the application's overall security posture and preventing potential compromise.

Identified Vulnerabilities

ID	Title	CVSS	Page
C1	Flask Debug Mode Enabled in Production	9.8	
H1	Hardcoded Authentication Token	7.5	
H2	Vulnerable Dependency: aiohttp (CVE-2025-53643)	7.5	
M1	Missing Request Timeout for External API Calls	5.3	
L1	Verbose Error Messages Exposing Internal Details	3.1	

METHODOLOGY

Introduction

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

Objective

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

Scope

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

Systems in Scope

Name	IP

User Accounts

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

FINDINGS

C1 – 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: The Flask Web Application Server

Overview

The Flask application is configured to run with `debug=True` within a potential production environment, which exposes the Werkzeug debugger. This is an extremely dangerous configuration for production systems.

Details

When `debug=True` is enabled in a Flask application, the Werkzeug debugger becomes active. This debugger is designed for development purposes and provides a powerful console that allows an attacker to execute arbitrary Python code on the server if they can trigger an uncaught exception. Gaining access to this debugger effectively grants an attacker full control over the server, leading to complete compromise of the application, data theft, and denial of service. The provided code snippet shows `app.run(debug=True, port=5000, use_reloader=True)` directly within the `if __name__ == '__main__':` block, indicating it will be started in debug mode when executed.

Evidence

- **app.py:1872:** The Flask application is run with debug mode enabled.

References

- https://flask.palletsprojects.com/en/2.3.x/config/#DEBUG
- https://www.acunetix.com/blog/web-security-zone/flask-debug-mode-vulnerability/

Recommendation

- Ensure that `debug=False` is set when deploying the Flask application to any production or publicly accessible environment. - Use environment variables or a dedicated configuration management system to manage debug settings, for example, `app.config['DEBUG'] = os.environ.get('FLASK_DEBUG') == '1'`, ensuring `FLASK_DEBUG` is not '1' in production. - Implement a robust deployment strategy that explicitly disables debug mode for production builds and environments.

Prompt to Solve the Vulnerability:

In `app.py` at line 1872, change `app.run(debug=True, ...)` to `app.run(debug=False, ...)` or, preferably, configure debug mode via an environment variable, ensuring it's `False` in production. For example, `app.run(debug=os.getenv('FLASK_DEBUG', 'False') == 'True', ...)`.

H1 – Hardcoded Authentication Token

Severity: High

CVSS Score: 7.5

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

Target: tasks.py

Overview

An authentication token (JWT) is hardcoded directly within the `tasks.py` file. While this might be intended for debugging or testing, hardcoding sensitive data like tokens poses a significant security risk.

Details

The `token` variable on line 14 of `tasks.py` contains a complete JSON Web Token. This token, even if a test token, contains claims such as issuer, subject (user ID), audience, expiration, issued at times, email, phone, and roles. Hardcoding such tokens, even for development purposes, is problematic because it exposes the internal structure of the JWT, sensitive test data, and could lead to unauthorized access or impersonation if accidentally deployed to production or if the token is still valid. It also sets a poor precedent for handling sensitive credentials.

Evidence

- **tasks.py:14:** A JWT token is hardcoded in the source code.

References

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

Recommendation

- Remove all hardcoded sensitive data, including authentication tokens, from the source code. - For testing purposes, load mock tokens from secure configuration files (e.g., `.env` or a dedicated test secrets store) that are excluded from version control. - Ensure proper environment variable loading for production secrets and configuration. - Rotate any exposed tokens or keys immediately and invalidate the hardcoded token if it was ever active in a production environment.

Prompt to Solve the Vulnerability:

In `tasks.py`, remove the hardcoded JWT token at line 14. Instead, for testing, load it from an environment variable or a secure configuration file that is not committed to version control. For example, `token = os.getenv('TEST_JWT_TOKEN')` and ensure `TEST_JWT_TOKEN` is set in your `.env` file.

H2 – Vulnerable Dependency: aiohttp (CVE-2025-53643)

Severity: High

CVSS Score: 7.5

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

Target: Application dependencies (aiohttp)

Overview

The application uses `aiohttp` version `3.11.10`, which is vulnerable to a request smuggling attack (CVE-2025-53643).

Details

The Python parser in `aiohttp` versions prior to the patch (`3.11.10` in this case) does not correctly parse trailer sections of an HTTP request. This vulnerability can be exploited to perform request smuggling attacks, potentially bypassing security controls like firewalls, reverse proxies, or web application firewalls. Successful exploitation could lead to unauthorized access to internal resources, cache poisoning, or other server-side attacks. The impact is specifically noted for pure Python `aiohttp` installations or when `AIOHTTP_NO_EXTENSIONS` is enabled.

Evidence

- **dependency_file:0:** Vulnerable dependency `aiohttp==3.11.10` with CVE-2025-53643 identified by pip-audit.

References

- https://github.com/aio-libs/aiohttp/commit/e8d774f635dc6d1cd3174d0e38891da5de0e2b6a
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-53643

Recommendation

- Upgrade `aiohttp` to a version that contains the fix for CVE-2025-53643. Refer to the provided GitHub commit link for details on the patch. - Regularly scan all project dependencies for known vulnerabilities using automated tools (e.g., `pip-audit`, Snyk, Dependabot) as part of your CI/CD pipeline. - Ensure your deployment environment always pulls the latest patched versions of dependencies to mitigate supply chain risks.

Prompt to Solve the Vulnerability:

Upgrade the `aiohttp` dependency to a version patched against CVE-2025-53643. Check the official `aiohttp` repository for the latest secure version and update your `requirements.txt` or `pyproject.toml` accordingly. For example, `pip install aiohttp --upgrade` or manually update `aiohttp==` in `requirements.txt` and run `pip install -r requirements.txt`.

M1 – Missing Request Timeout for External API Calls

Severity: Medium

CVSS Score: 5.3

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

Target: External API calls in payments routes

Overview

Multiple external API calls using the `requests` library lack explicit timeout configurations, leading to potential denial-of-service or resource exhaustion.

Details

Without a configured timeout, HTTP requests made to external services (such as the Cashfree API) can hang indefinitely if the remote server becomes unresponsive or experiences network issues. This can lead to various problems within the application, including blocking application threads/processes, exhausting available network connections, or causing overall service degradation. In a worst-case scenario, this could result in a denial-of-service condition for legitimate users, as application resources remain tied up waiting for responses that never arrive.

Evidence

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

References

- https://docs.python-requests.org/en/master/user/advanced/#timeouts

Recommendation

- Always specify a `timeout` parameter for all `requests` calls to external services to prevent indefinite hanging. - Define a reasonable timeout duration based on the expected response time and reliability of the external API, e.g., `timeout=5` for 5 seconds. - Consider separating the connection timeout from the read timeout using a tuple (e.g., `timeout=(connect_timeout, read_timeout)`) for more granular control over network behavior.

Prompt to Solve the Vulnerability:

For all `requests` calls in `routes\payments.py`, add a `timeout` parameter. For example, change `requests.post(url, json=payload, headers=headers)` to `requests.post(url, json=payload, headers=headers, timeout=5)`. Apply this to lines 90, 136, and 663. Choose an appropriate timeout duration (e.g., 5-10 seconds) based on the expected response time of the Cashfree API.

L1 – Verbose Error Messages Exposing Internal Details

Severity: Low

CVSS Score: 3.1

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

Target: API error responses across multiple endpoints

Overview

The application frequently returns raw exception messages directly in API responses when an error occurs, potentially exposing sensitive internal details.

Details

Numerous API endpoints catch general exceptions (`Exception as e`) and then include the string representation of the exception (`str(e)`) in the JSON response returned to the client. While useful for debugging during development, this practice in a production environment can inadvertently leak sensitive information about the application's internal structure, database schema, underlying libraries, or specific runtime errors. This detailed information can be valuable to an attacker during reconnaissance, helping them to identify potential attack vectors, deduce logic flows, or craft more targeted exploits.

Evidence

- **app.py:117:** Registration failed error exposes `str(e)`.
- **app.py:187:** Login failed error exposes `str(e)`.
- **app.py:210:** Failed to update profile error exposes `str(e)`.
- **app.py:243:** Failed to send reset email error exposes `str(e)`.
- **app.py:288:** Failed to create campaign error exposes `str(e)`.
- **app.py:326:** Failed to fetch campaigns error exposes `str(e)`.
- **app.py:385:** Failed to fetch campaigns error exposes `str(e)`.
- **app.py:491:** Failed to fetch campaign details error exposes `str(e)`.
- **app.py:579:** Failed to fetch creator campaigns error exposes `str(e)`.
- **app.py:653:** Failed to submit clip error exposes `str(e)`.
- **app.py:718:** Failed to fetch clips error exposes `str(e)`.
- **app.py:754:** Failed to fetch accepted clip details error exposes `str(e)`.
- **app.py:829:** Failed to delete campaign error exposes `str(e)`.
- **app.py:884:** Failed to delete clip error exposes `str(e)`.
- **app.py:931:** Failed to fetch campaigns error exposes `str(e)`.
- **app.py:1022:** Failed to update clip error exposes `str(e)`.
- **app.py:1075:** Failed to delete clip error exposes `str(e)`.
- **app.py:1109:** Failed to fetch creator profile error exposes `str(e)`.
- **app.py:1155:** Failed to update creator profile error exposes `str(e)`.
- **app.py:1194:** Failed to update campaign image error exposes `str(e)`.
- **app.py:1226:** Failed to update campaign budget error exposes `str(e)`.

- **app.py:1255:** Failed to update campaign requirements error exposes `str(e)`.
- **app.py:1286:** Failed to update campaign status error exposes `str(e)`.
- **app.py:1317:** Failed to update campaign view threshold error exposes `str(e)`.
- **app.py:1354:** Failed to update campaign deadline error exposes `str(e)`.
- **app.py:1450:** Failed to retrieve pending payouts error exposes `str(e)`.
- **app.py:1478:** Failed to fetch brand profile error exposes `str(e)`.
- **app.py:1509:** Failed to update brand profile error exposes `str(e)`.
- **app.py:1576:** Failed to update view count error exposes `str(e)`.
- **app.py:1631:** Failed to update campaign views error exposes `str(e)`.
- **app.py:1729:** Failed to retrieve analytics error exposes `str(e)`.
- **app.py:1756:** Failed to sync Google user error exposes `str(e)`.
- **app.py:1808:** Sync failed due to database error exposes `str(e)`.
- **app.py:1812:** Sync failed error exposes `str(e)`.
- **routes\payments.py:115:** Internal server error exposes `str(e)`.
- **routes\payments.py:186:** Verification failed error exposes `str(e)`.
- **routes\payments.py:343:** Allocation failed error exposes `str(e)`.
- **routes\payments.py:430:** Reclaim failed error exposes `str(e)`.
- **routes\payments.py:554:** Distribution failed error exposes `str(e)`.
- **routes\payments.py:729:** Withdrawal failed error exposes `str(e)`.
- **routes\payments.py:817:** Failed to save payout details error exposes `str(e)`.
- **routes\payments.py:867:** Failed to retrieve payout details error exposes `str(e)`.
- **routes\payments.py:927:** Failed to verify payout details error exposes `str(e)`.
- **routes\payments.py:989:** Failed to retrieve withdrawal history error exposes `str(e)`.
- **routes\payments.py:1023:** Failed to retrieve notifications error exposes `str(e)`.
- **routes\payments.py:1105:** Failed to retrieve transactions error exposes `str(e)`.
- **routes\payments.py:1197:** Refund failed error exposes `str(e)`.
- **routes\payments.py:1264:** Failed to retrieve campaign summary error exposes `str(e)`.
- **routes\payments.py:1358:** Failed to calculate earnings error exposes `str(e)`.
- **routes\payments.py:1529:** Bulk distribution failed error exposes `str(e)`.
- **routes\payments.py:1623:** Failed to request refund error exposes `str(e)`.
- **routes\payments.py:1690:** Failed to retrieve refund requests error exposes `str(e)`.
- **routes\payments.py:1804:** Failed to approve refund error exposes `str(e)`.
- **routes\payments.py:1865:** Failed to reject refund error exposes `str(e)`.
- **routes\payments.py:1934:** Failed to retrieve refund status error exposes `str(e)`.
- **routes\payments.py:2014:** Failed to retrieve refund audit trail error exposes `str(e)`.
- **routes\payments.py:2088:** Failed to revert withdrawal error exposes `str(e)`.

References

- https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html

Recommendation

- Implement custom error handling that prevents raw exception details from being exposed to the client in production environments. - Return generic, user-friendly error messages (e.g., 'An unexpected error occurred. Please try again later.') for all unhandled exceptions. - Log detailed exception information securely on the server-side for debugging purposes, using a robust logging framework that separates logs from client responses. - Consider integrating a centralized error monitoring service to capture and analyze exceptions without exposing them to end-users.

Prompt to Solve the Vulnerability:

Refactor error handling in `app.py` and `routes\payments.py` to prevent raw exception details from being returned to clients. Replace instances like `return jsonify({'msg': '...', 'error': str(e)}), 500` with generic error messages, e.g., `return jsonify({'msg': 'An internal server error occurred.'}), 500`. Ensure that `str(e)` is only used for server-side logging and not exposed in API responses. This applies to all occurrences where `str(e)` is returned in an error message.

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	10.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

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

  Potential Attack Scenario:

  Unauthorized users can register for accounts.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Missing authentication on user registration can lead to unauthorized access and data breaches, violating SOC 2 principles related to access control and security.
ISO/IEC 27001	Yes	high	Lack of authentication for registration poses a security risk, potentially allowing unauthorized account creation and violating ISO 27001 controls for access management.
CSA STAR	Yes	high	Absence of authentication on registration is a security vulnerability that could be exploited, impacting the integrity and availability of the system, relevant to CSA STAR.

Security Assessment Notes

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

References

Endpoint Path /login

Endpoint Path	/login
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 120
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

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

  Potential Attack Scenario:

  Unauthorized users can attempt to log in without proper credentials, potentially leading to brute-force attacks or credential stuffing.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Missing authentication on login can lead to unauthorized access, violating SOC 2 principles related to access control and user identification.
ISO/IEC 27001	Yes	high	Lack of authentication for login increases the risk of unauthorized access, impacting ISO 27001 controls for access management.
CSA STAR	Yes	high	Absence of authentication on login is a critical security flaw that can be exploited for unauthorized access, relevant to CSA STAR's security principles.

Security Assessment Notes

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

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	Yes	low	Authentication is present for this endpoint, aligning with SOC 2 access control requirements. Further analysis of the specific verification logic is needed.
ISO/IEC 27001	Yes	low	The endpoint appears to have authentication, which is a positive step towards ISO 27001 compliance for access control.
CSA STAR	Yes	low	Authentication is present, contributing to the security posture required by CSA STAR.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for this endpoint, aligning with SOC 2 access control requirements. Further analysis of the specific verification logic is needed.
ISO/IEC 27001	Yes	low	The endpoint appears to have authentication, which is a positive step towards ISO 27001 compliance for access control.
CSA STAR	Yes	low	Authentication is present, contributing to the security posture required by CSA STAR.

Security Assessment Notes

CVSS Vector: N/A

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	7.5

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (medium): Authentication is missing for this endpoint.

  Potential Attack Scenario:

  Without authentication, an attacker might be able to flood the system with password reset requests, potentially leading to denial-of-service or abuse of the reset mechanism.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Lack of authentication on password reset requests can be exploited, potentially violating SOC 2 principles related to secure configuration and access control.
ISO/IEC 27001	Yes	medium	Weak or missing authentication on password reset functionality can lead to account compromise, which is a concern for ISO 27001.
CSA STAR	Yes	medium	Insecure handling of password reset requests can be a vulnerability, impacting the confidentiality and integrity of user accounts, as per CSA STAR guidelines.

Security Assessment Notes

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

References

Endpoint Path /api/brand/campaigns

Endpoint Path	/api/brand/campaigns
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 248
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	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	Yes	low	Authentication is present for creating campaigns, adhering to SOC 2 access control principles.
ISO/IEC 27001	Yes	low	Authentication is implemented for campaign creation, contributing to ISO 27001's access control objectives.
CSA STAR	Yes	low	The presence of authentication for creating campaigns aligns with CSA STAR's focus on secure operations.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for listing campaigns, aligning with SOC 2 access control requirements.
ISO/IEC 27001	Yes	low	Authentication for accessing campaign lists is in place, supporting ISO 27001 objectives for information access.
CSA STAR	Yes	low	Authentication for campaign listing is implemented, contributing to secure data access as per CSA STAR.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/campaigns

Endpoint Path	/api/campaigns
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 329
Authentication Required	No
Risk Severity	High
CVSS Score	7.5

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (medium): Authentication is missing for this endpoint.

  Potential Attack Scenario:

  Unauthorized users could access all campaign data, potentially leading to information disclosure or enumeration of campaigns.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Missing authentication for accessing all campaigns could lead to unauthorized data access, impacting SOC 2 controls.
ISO/IEC 27001	Yes	medium	Lack of authentication for retrieving all campaign data might expose sensitive information, relevant to ISO 27001.
CSA STAR	Yes	medium	Exposing campaign data without authentication is a security risk that could violate CSA STAR principles regarding data protection.

Security Assessment Notes

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

References

Endpoint Path /api/campaigns/

Endpoint Path	/api/campaigns/
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 388
Authentication Required	No
Risk Severity	High
CVSS Score	7.5

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (medium): Authentication is missing for this endpoint.

  Potential Attack Scenario:

  Unauthorized users can access specific campaign details, potentially leading to information disclosure.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Missing authentication for accessing campaign details could lead to unauthorized information disclosure, impacting SOC 2 controls.
ISO/IEC 27001	Yes	medium	Lack of authentication for retrieving campaign details may expose sensitive information, relevant to ISO 27001.
CSA STAR	Yes	medium	Exposing campaign details without authentication is a security risk, potentially violating CSA STAR principles.

Security Assessment Notes

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

References

Endpoint Path /api/creator/your-campaigns

Endpoint Path	/api/creator/your-campaigns
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 495
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	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	Yes	low	Authentication is present for creators to access their campaigns, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for creator campaign access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for creator data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for submitting clips, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for clip submission supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for clip submissions is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for creators to view campaign clips, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for creator clip access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for creator clip data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for accessing accepted clip details, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for creator clip detail access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for creator clip detail data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/campaigns/

Endpoint Path	/api/brand/campaigns/
HTTP Methods	DELETE
Source Location	..\Mipoe-Backend\app.py - 761
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	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	Yes	low	Authentication is present for deleting campaigns, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for campaign deletion supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for campaign deletion is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/campaigns/

Endpoint Path	/api/brand/campaigns/
HTTP Methods	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	Yes	low	Authentication is present for OPTIONS requests, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for OPTIONS requests supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for OPTIONS requests is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/creator/clip/

Endpoint Path	/api/creator/clip/
HTTP Methods	DELETE
Source Location	..\Mipoe-Backend\app.py - 833
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	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	Yes	low	Authentication is present for deleting clips, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for clip deletion supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for clip deletion is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/creator/clip/

Endpoint Path	/api/creator/clip/
HTTP Methods	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	Yes	low	Authentication is present for OPTIONS requests, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for OPTIONS requests supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for OPTIONS requests is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for admin access to campaigns, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for administrative campaign access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for admin access to campaign data is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for admin clip updates, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for administrative clip modification supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for admin modification of clip data is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/admin/clip/

Endpoint Path	/api/admin/clip/
HTTP Methods	DELETE
Source Location	..\Mipoe-Backend\app.py - 1026
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	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	Yes	low	Authentication is present for admin clip deletion, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for administrative clip deletion supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for admin deletion of clip data is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/admin/clip/

Endpoint Path	/api/admin/clip/
HTTP Methods	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	Yes	low	Authentication is present for OPTIONS requests, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for OPTIONS requests supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for OPTIONS requests is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for accessing creator profiles, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for creator profile access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for creator profile data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for updating creator profiles, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for creator profile updates supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for creator profile data updates is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/campaigns//image

Endpoint Path	/api/brand/campaigns//image
HTTP Methods	PUT
Source Location	..\Mipoe-Backend\app.py - 1159

Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	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	Yes	low	Authentication is present for updating campaign images, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for campaign image updates supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for campaign image updates is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/campaigns//image

Endpoint Path	/api/brand/campaigns//image
HTTP Methods	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	Yes	low	Authentication is present for OPTIONS requests, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for OPTIONS requests supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for OPTIONS requests is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for updating campaign budgets, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for campaign budget updates supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for campaign budget updates is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for updating campaign requirements, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for campaign requirements updates supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for campaign requirements updates is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for updating campaign status, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for campaign status updates supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for campaign status updates is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for updating campaign view thresholds, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for campaign view threshold updates supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for campaign view threshold updates is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for updating campaign deadlines, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for campaign deadline updates supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for campaign deadline updates is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for accessing pending payouts, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for pending payout access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for pending payout data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for accessing brand profiles, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for brand profile access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for brand profile data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for updating brand profiles, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for brand profile updates supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for brand profile data updates is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for admin clip view count updates, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for administrative clip view count updates supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for admin modification of clip view counts is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for admin campaign view count updates, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for administrative campaign view count updates supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for admin modification of campaign view counts is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for accessing campaign performance analytics, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for administrative analytics access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for administrative access to analytics data is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for Google sync, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for Google sync supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for Google sync is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for token refresh, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for token refresh supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for token refresh is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for logout, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for logout supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for logout is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/health

Endpoint Path	/api/health
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 1843
Authentication Required	No
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Health check endpoints are typically not authenticated, but sensitive information should not be exposed.
ISO/IEC 27001	Yes	low	Health check endpoints generally do not require authentication, provided no sensitive operational details are exposed.
CSA STAR	Yes	low	Health endpoints are usually public; the focus is on not revealing sensitive operational data.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for creating deposit orders, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for deposit order creation supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for deposit order creation is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for verifying deposits, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for deposit verification supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for deposit verification is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for retrieving virtual account information, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for virtual account access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for virtual account data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for retrieving wallet balance, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for wallet balance access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for wallet balance data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for budget allocation, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for budget allocation supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for budget allocation is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for budget reclamation, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for budget reclamation supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for budget reclamation is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for distributing funds to creators, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for creator distributions supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for creator distributions is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for creator withdrawals, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for creator withdrawals supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for creator withdrawals is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for saving payout details, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for saving payout details supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for saving payout details is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for retrieving payout details, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for retrieving payout details supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for retrieving payout details is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for verifying payout details, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for verifying payout details supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for verifying payout details is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for retrieving withdrawal history, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for withdrawal history access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for withdrawal history data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for retrieving creator notifications, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for creator notification access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for creator notification data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for retrieving transaction history, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for transaction history access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for transaction history data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for refund requests, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for refund requests supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for refund requests is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for campaign summaries, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for campaign summary access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for campaign summary data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for calculating earnings, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for earnings calculation supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for earnings calculation is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for bulk distribution, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for bulk distribution supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for bulk distribution is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for requesting refunds, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for refund requests supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for refund requests is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for retrieving refund requests, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for refund request access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for refund request data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for approving refunds, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for refund approval supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for refund approval is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for rejecting refunds, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for refund rejection supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for refund rejection is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for retrieving refund status, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for refund status access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for refund status data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for accessing refund audit trails, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for refund audit trail access supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for refund audit trail data access is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

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	Yes	low	Authentication is present for reverting withdrawals, aligning with SOC 2 access control.
ISO/IEC 27001	Yes	low	Authentication for withdrawal reversion supports ISO 27001's information access controls.
CSA STAR	Yes	low	Implementing authentication for withdrawal reversion is consistent with CSA STAR's security principles.

Security Assessment Notes

CVSS Vector: N/A

References

METRICS SUMMARY

Total Findings: 5

Severity	Count
CRITICAL	1
HIGH	2
MEDIUM	1
LOW	1

BUSINESS RISK ADVICE

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

No specific business risk advice was generated for this report.

DISCLAIMER

This report is generated by an automated security analysis tool.