SECURITY ANALYSIS REPORT

Generated By

Backstage Rookie

Provider: Backstage Rookie

contact - swarajdarekar9@gmail.com

Client: heaven Darekar

darekarheaven@gmail.com

Scan ID: 89420f17-09cc-480a-aa1b-62d892c81850

Date: 2026-02-10 12:50:34

Version: 1.0.0

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This security assessment identified several critical and high-severity vulnerabilities within the application, alongside important medium and low-severity issues. The most significant risks stem from exposed debug functionalities in a Flask application, which could lead to remote code execution, and the use of a vulnerable third-party dependency. Additionally, the widespread practice of exposing raw exception details in API responses and the absence of request timeouts for external calls present further avenues for exploitation and service disruption. Addressing these findings is crucial for enhancing the application's overall security posture and reducing its attack surface.

Identified Vulnerabilities

ID	Title	CVSS	Page
C1	Flask Debug Mode Enabled in Production Configuration	9.8	
H1	Hardcoded JWT Token in Test Script	7.3	
H2	Vulnerable aiohttp Dependency (Request Smuggling)	7.5	
M1	Missing Request Timeouts for External API Calls	6.5	
L1	Verbose Error Messages Exposing Internal Details	3.7	

METHODOLOGY

Introduction

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

Objective

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

Scope

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

Systems in Scope

Name	IP

User Accounts

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

FINDINGS

C1 – Flask Debug Mode Enabled in Production Configuration

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: Flask Application Configuration

Overview

The Flask application is configured to run with debug mode enabled, which exposes the Werkzeug debugger. This debugger can allow attackers to execute arbitrary code on the server if they can trigger an unhandled exception.

Details

Line 1872 in `app.py` shows `app.run(debug=True, ...)`. In a production environment, this setting is extremely dangerous as it can lead to remote code execution (RCE) by presenting an interactive debugger traceback on internal server errors. This allows an attacker to inspect local variables, execute arbitrary Python code, and potentially gain full control over the server. This is a severe security misconfiguration that must be remediated immediately.

Evidence

- **app.py:1872:** Flask app initiated with debug=True. `app.run(debug=True, port=5000, use_reloader=True)`

References

- https://flask.palletsprojects.com/en/latest/config/#debug-mode
- https://owasp.org/www-community/Weaknesses/W-CWE-215

Recommendation

- Disable Flask debug mode (`debug=False`) for all production deployments. - Use a production-ready WSGI server (e.g., Gunicorn, uWSGI) to serve the Flask application, which typically handles error logging and serves requests more robustly. - Implement proper error handling and logging without exposing sensitive traceback information to clients. - Use environment variables or configuration files to control debug settings based on the deployment environment.

Prompt to Solve the Vulnerability:

In app.py at line 1872, the Flask application is run with 'debug=True'. To fix this critical vulnerability, change 'debug=True' to 'debug=False' for production environments. It is recommended to manage this setting using an environment variable (e.g., 'FLASK_ENV') and only enable debug mode in development environments. For example, you could replace `app.run(debug=True, ...)` with `if os.environ.get('FLASK_ENV') == 'development': app.run(debug=True, ...) else: app.run(debug=False, ...)` and use a production-grade WSGI server.

H1 – Hardcoded JWT Token in Test Script

Severity: High

CVSS Score: 7.3

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

Target: tasks.py

Overview

A JSON Web Token (JWT) is directly hardcoded within `tasks.py`, intended for testing purposes. Although the JWT signing key is loaded from an environment variable, the hardcoded token itself is a sensitive piece of information.

Details

Line 14 of `tasks.py` contains a full JWT string. While the context suggests this is used for debugging and verifying the `JWT_SECRET_KEY` from `.env`, hardcoding active or expired JWTs is a security risk. If this script is accidentally included in a production build, or if the token itself was generated from a production system, it could lead to token reuse, data leakage, or provide attackers with insights into the JWT structure and potential vulnerabilities. It also presents a risk if the associated secret key is ever compromised, making the hardcoded token potentially valid again.

Evidence

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

References

- https://owasp.org/www-community/Weaknesses/W-CWE-798

Recommendation

- Avoid hardcoding any sensitive data, including JWT tokens, even in test scripts. - For testing JWT verification, consider using mock tokens, dynamically generated tokens, or a dedicated testing framework that manages test credentials securely. - Ensure that test-specific files containing sensitive data are excluded from production deployments and version control systems. - Rotate any secret keys associated with hardcoded tokens if there's a risk they were from a production system.

Prompt to Solve the Vulnerability:

In tasks.py, at line 14, a JWT token is hardcoded. To remove this hardcoded secret, instead of assigning a literal string to the 'token' variable, consider loading it from a secure source like an environment variable (similar to how 'secret' is loaded), or generate a synthetic token dynamically if the purpose is purely for testing the JWT decoding logic. For example, if you need a static token for a test, ensure it's a dummy token with no real-world implications, or load it from a test-specific configuration file that is not committed to version control.

H2 – Vulnerable aiohttp Dependency (Request Smuggling)

Severity: High

CVSS Score: 7.5

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

Target: Application Dependencies

Overview

The application uses `aiohttp` version 3.11.10, which is affected by CVE-2025-53643, a request smuggling vulnerability.

Details

`aiohttp` version 3.11.10 is vulnerable to a request smuggling attack if used without its C extensions (pure Python version) or with `AIOHTTP_NO_EXTENSIONS` enabled. This vulnerability arises from improper parsing of HTTP request trailer sections, allowing an attacker to bypass security mechanisms like firewalls or proxy protections by "smuggling" malicious requests within legitimate ones. This can lead to unauthorized access, cache poisoning, or bypassing security controls.

Evidence

- **dependency_file:** Vulnerable dependency `aiohttp==3.11.10` identified, associated with CVE-2025-53643.

References

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

Recommendation

- Upgrade `aiohttp` to a patched version that addresses CVE-2025-53643. Refer to the provided patch link for details on the fix. - Regularly audit all project dependencies for known vulnerabilities using tools like `pip-audit` or `Snyk`. - Ensure that `aiohttp` is installed with its C extensions in production environments unless explicitly required not to, as the vulnerability primarily impacts the pure Python version.

Prompt to Solve the Vulnerability:

The dependency 'aiohttp==3.11.10' is vulnerable to CVE-2025-53643 (Request Smuggling). To remediate this, update 'aiohttp' to a version that includes the fix. For example, if a fix is available in `aiohttp>=3.12.0`, update your `requirements.txt` or `pyproject.toml` file to specify this version, then run your dependency installer (e.g., `pip install -U aiohttp` or `pip install -r requirements.txt`).

M1 – Missing Request Timeouts for External API Calls

Severity: Medium

CVSS Score: 6.5

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

Target: External API Integrations

Overview

Several outbound HTTP requests made using the `requests` library lack explicit timeout configurations, which can lead to hanging connections and potential denial-of-service.

Details

Calls to `requests.post` and `requests.get` (e.g., lines 90, 136, 663 in `routes\payments.py`) are made without specifying a `timeout` parameter. If the external Cashfree API (or any other external service) becomes unresponsive or slow, these requests could indefinitely block the server process, consuming resources and potentially leading to application unresponsiveness or a denial-of-service condition for legitimate users. This can impact the reliability and availability of the service.

Evidence

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

References

- https://requests.readthedocs.io/en/latest/user/advanced/#timeouts
- https://owasp.org/www-community/Weaknesses/W-CWE-770

Recommendation

- Add a `timeout` parameter to all `requests` calls to specify how long the client should wait for a response. - The timeout should include both the connect timeout (time to establish the connection) and the read timeout (time to wait for the first byte of the response). - Choose appropriate timeout values based on the expected response times of the external APIs and the application's tolerance for delays.

Prompt to Solve the Vulnerability:

In routes\payments.py, at lines 90, 136, and 663, 'requests' calls are made without a 'timeout' parameter. To prevent hanging connections and improve resilience, add a 'timeout' argument to each 'requests.post' and 'requests.get' call. For example, change `requests.post(url, ...)` to `requests.post(url, ..., timeout=(5, 10))` where the first value is the connect timeout and the second is the read timeout (in seconds). Adjust these values based on the expected behavior of the external API.

L1 – Verbose Error Messages Exposing Internal Details

Severity: Low

CVSS Score: 3.7

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

Target: API Error Handling

Overview

The application's API endpoints consistently return raw Python exception messages (`str(e)`) in their error responses, potentially exposing internal application details, data structures, or execution paths to clients.

Details

Across numerous API endpoints in `app.py` and `routes\payments.py`, `except Exception as e:` blocks catch broad exceptions and return `{'msg': '...', 'error': str(e)}`. This practice is dangerous because `str(e)` can contain stack traces, database query failures, path information, or even fragments of data that were being processed at the time of the error. Such information can aid attackers in understanding the application's internals, identifying potential attack vectors, or exploiting other vulnerabilities. While the `msg` field provides a generic message, the `error` field directly exposes implementation details.

Evidence

- **app.py:117:** `return jsonify({'msg': 'Registration failed', 'error': str(e)}), 500`
- **app.py:187:** `return jsonify({'msg': 'Login failed', 'error': str(e)}), 500`
- **app.py:210:** `return jsonify({'msg': 'Failed to update profile', 'error': str(e)}), 500`
- **app.py:243:** `return jsonify({'msg': 'Failed to send reset email', 'error': str(e)}), 500`
- **app.py:288:** `return jsonify({'msg': 'Failed to create campaign', 'error': str(e)}), 500`
- **app.py:326:** `return jsonify({'msg': 'Failed to fetch campaigns', 'error': str(e)}), 500`
- **app.py:385:** `return jsonify({'msg': 'Failed to fetch campaigns', 'error': str(e)}), 500`
- **app.py:491:** `return jsonify({'msg': 'Failed to fetch campaign details', 'error': str(e)}), 500`
- **app.py:579:** `return jsonify({'msg': 'Failed to fetch creator campaigns', 'error': str(e)}), 500`
- **app.py:653:** `return jsonify({'msg': 'Failed to submit clip', 'error': str(e)}), 500`
- **app.py:718:** `return jsonify({'msg': 'Failed to fetch clips', 'error': str(e)}), 500`
- **app.py:754:** `return jsonify({'msg': 'Failed to fetch accepted clip details', 'error': str(e)}), 500`
- **app.py:829:** `return jsonify({'msg': 'Failed to delete campaign', 'error': str(e)}), 500`
- **app.py:884:** `return jsonify({'msg': 'Failed to delete clip', 'error': str(e)}), 500`
- **app.py:931:** `return jsonify({'msg': 'Failed to fetch campaigns', 'error': str(e)}), 500`
- **app.py:1022:** `return jsonify({'msg': 'Failed to update clip', 'error': str(e)}), 500`
- **app.py:1075:** `return jsonify({'msg': 'Failed to delete clip', 'error': str(e)}), 500`
- **app.py:1109:** `return jsonify({'msg': 'Failed to fetch creator profile', 'error': str(e)}), 500`
- **app.py:1155:** `return jsonify({'msg': 'Failed to update creator profile', 'error': str(e)}), 500`
- **app.py:1194:** `return jsonify({'msg': 'Failed to update campaign image', 'error': str(e)}), 500`
- **app.py:1226:** `return jsonify({'msg': 'Failed to update campaign budget', 'error': str(e)}), 500`
- **app.py:1255:** `return jsonify({'msg': 'Failed to update campaign requirements', 'error': str(e)}), 500`
- **app.py:1286:** `return jsonify({'msg': 'Failed to update campaign status', 'error': str(e)}), 500`
- **app.py:1317:** `return jsonify({'msg': 'Failed to update campaign view threshold', 'error': str(e)}), 500`
- **app.py:1354:** `return jsonify({'msg': 'Failed to update campaign deadline', 'error': str(e)}), 500`
- **app.py:1450:** `return jsonify({'msg': 'Failed to retrieve pending payouts', 'error': str(e)}), 500`
- **app.py:1478:** `return jsonify({'msg': 'Failed to fetch brand profile', 'error': str(e)}), 500`
- **app.py:1509:** `return jsonify({'msg': 'Failed to update brand profile', 'error': str(e)}), 500`
- **app.py:1576:** `return jsonify({'msg': 'Failed to update view count', 'error': str(e)}), 500`
- **app.py:1631:** `return jsonify({'msg': 'Failed to update campaign views', 'error': str(e)}), 500`
- **app.py:1729:** `return jsonify({'msg': 'Failed to retrieve analytics', 'error': str(e)}), 500`
- **app.py:1756:** `return jsonify({'msg': 'Failed to sync Google user: could not retrieve user data', 'error': str(e)}), 500`
- **app.py:1808:** `return jsonify({'msg': 'Sync failed due to database error', 'error': str(e)}), 500`
- **app.py:1812:** `return jsonify({'msg': 'Sync failed', 'error': str(e)}), 500`
- **routes\payments.py:115:** `return jsonify({'msg': 'Internal server error', 'error': str(e)}), 500`
- **routes\payments.py:186:** `return jsonify({'msg': 'Verification failed', 'error': str(e)}), 500`
- **routes\payments.py:343:** `return jsonify({'msg': 'Allocation failed', 'error': str(e)}), 500`
- **routes\payments.py:430:** `return jsonify({'msg': 'Reclaim failed', 'error': str(e)}), 500`
- **routes\payments.py:554:** `return jsonify({'msg': 'Distribution failed', 'error': str(e)}), 500`
- **routes\payments.py:729:** `return jsonify({'msg': 'Withdrawal failed', 'error': str(e)}), 500`
- **routes\payments.py:817:** `return jsonify({'msg': 'Failed to save payout details', 'error': str(e)}), 500`
- **routes\payments.py:867:** `return jsonify({'msg': 'Failed to retrieve payout details', 'error': str(e)}), 500`

- **routes\payments.py:927:** `return jsonify({'msg': 'Failed to verify payout details', 'error': str(e)}), 500`
- **routes\payments.py:989:** `return jsonify({'msg': 'Failed to retrieve withdrawal history', 'error': str(e)}), 500`
- **routes\payments.py:1023:** `return jsonify({'msg': 'Failed to retrieve notifications', 'error': str(e)}), 500`
- **routes\payments.py:1105:** `return jsonify({'msg': 'Failed to retrieve transactions', 'error': str(e)}), 500`
- **routes\payments.py:1197:** `return jsonify({'msg': 'Refund failed', 'error': str(e)}), 500`
- **routes\payments.py:1264:** `return jsonify({'msg': 'Failed to retrieve campaign summary', 'error': str(e)}), 500`
- **routes\payments.py:1358:** `return jsonify({'msg': 'Failed to calculate earnings', 'error': str(e)}), 500`
- **routes\payments.py:1529:** `return jsonify({'msg': 'Bulk distribution failed', 'error': str(e)}), 500`
- **routes\payments.py:1623:** `return jsonify({'msg': 'Failed to request refund', 'error': str(e)}), 500`
- **routes\payments.py:1690:** `return jsonify({'msg': 'Failed to retrieve refund requests', 'error': str(e)}), 500`
- **routes\payments.py:1804:** `return jsonify({'msg': 'Failed to approve refund', 'error': str(e)}), 500`
- **routes\payments.py:1865:** `return jsonify({'msg': 'Failed to reject refund', 'error': str(e)}), 500`
- **routes\payments.py:1934:** `return jsonify({'msg': 'Failed to retrieve refund status', 'error': str(e)}), 500`
- **routes\payments.py:2014:** `return jsonify({'msg': 'Failed to retrieve refund audit trail', 'error': str(e)}), 500`
- **routes\payments.py:2088:** `return jsonify({'msg': 'Failed to revert withdrawal', 'error': str(e)}), 500`

References

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

Recommendation

- Implement a centralized error handling mechanism to catch exceptions globally and present generic error messages to end-users. - Log full exception details (including stack traces) securely on the server side for debugging purposes, but never expose them directly in API responses. - Define specific, user-friendly error messages for different types of failures, rather than relying on raw exception strings. - Avoid broad `except Exception as e:` blocks; instead, catch more specific exceptions to handle errors gracefully and provide targeted responses.

Prompt to Solve the Vulnerability:

Across app.py and routes\payments.py, many API endpoints return raw exception messages using 'str(e)'. To prevent sensitive data exposure, refactor error handling to return only generic messages to the client. Instead of `return jsonify({'msg': 'Failed...', 'error': str(e)}), 500`, change it to `return jsonify({'msg': 'An unexpected error occurred. Please try again later.'}), 500` and log the detailed exception (`print(f"Error: {str(e)}")` or use a proper logging library) on the server side.

ENDPOINT SECURITY ANALYSIS

Endpoint Path /register

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for the registration endpoint, allowing unauthorized users to register.

  Potential Attack Scenario:

  An attacker could register a large number of fake accounts to disrupt the service or perform other malicious activities.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of authentication on user registration can lead to unauthorized access and control of user accounts, violating principles of access control.
ISO/IEC 27001	Yes	high	Inadequate access control for user registration can lead to unauthorized creation of accounts, impacting information security.
CSA STAR	Yes	high	Missing authentication controls for user registration is a fundamental security weakness that could be exploited.

Security Assessment Notes

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

References

- https://nvd.nist.gov/vuln/detail/CVE-2021-44228
- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Endpoint Path /login

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for the login endpoint, allowing unauthorized users to log in.

  Potential Attack Scenario:

  An attacker could gain unauthorized access to user accounts by submitting credentials without proper authentication.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of authentication on login endpoint allows unauthorized access, violating principles of identity verification and access control.
ISO/IEC 27001	Yes	high	Absence of authentication on login is a critical security flaw that compromises user authentication and access control.
CSA STAR	Yes	high	Missing authentication on login is a severe security risk that can lead to account compromise.

Security Assessment Notes

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

References

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

Endpoint Path /verify-instagram

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication is present, which aligns with SOC 2 requirements for access control.
ISO/IEC 27001	Yes	low	The presence of authentication supports the security control objectives of ISO/IEC 27001.
CSA STAR	Yes	low	Authentication mechanisms are in place, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /verify-instagram/

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

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication is present, which aligns with SOC 2 requirements for access control.
ISO/IEC 27001	Yes	low	The presence of authentication supports the security control objectives of ISO/IEC 27001.
CSA STAR	Yes	low	Authentication mechanisms are in place, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /request-password-reset

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (medium): Password reset functionality should ideally require some form of authentication or verification to prevent abuse.

  Potential Attack Scenario:

  An attacker could flood the system with password reset requests for various accounts, potentially leading to denial of service or attempts to guess user information if responses are not carefully handled.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Weaknesses in password reset flows can impact the security of user credentials and account access.
ISO/IEC 27001	Yes	medium	Insecure password reset mechanisms can weaken authentication controls and potentially lead to unauthorized access.

Regulation	Applicable	Risk Level	Reason
CSA STAR	Yes	medium	The security of password reset processes is crucial for maintaining user account integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication is present, aligning with SOC 2 principles for access control.
ISO/IEC 27001	Yes	low	The use of authentication supports access control measures required by ISO/IEC 27001.
CSA STAR	Yes	low	Authenticated access helps ensure that only authorized users can create campaigns.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures that only authorized users can retrieve campaign data.
ISO/IEC 27001	Yes	low	Access control through authentication is a key part of ISO/IEC 27001 compliance for data retrieval.
CSA STAR	Yes	low	Requiring authentication for accessing campaign data enhances security and accountability.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/campaigns

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (medium): This endpoint retrieves campaign data but does not appear to have authentication, potentially exposing sensitive campaign information.

  Potential Attack Scenario:

  An unauthorized user could access a list of all campaigns, potentially revealing business strategies or sensitive project details.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Exposure of campaign data without proper authentication can violate principles of confidentiality and data protection.
ISO/IEC 27001	Yes	medium	Lack of access control on sensitive campaign data can lead to information leakage and non-compliance.
CSA STAR	Yes	medium	Publicly accessible campaign data without authorization is a security concern.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/campaigns/

Endpoint Path	/api/campaigns/
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 388

Authentication Required	No
Risk Severity	Low
CVSS Score	N/A

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (medium): Retrieving specific campaign details without authentication could expose sensitive information.

  Potential Attack Scenario:

  An attacker could query specific campaign IDs to gather detailed information about ongoing projects or financial data.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Unauthorized access to specific campaign details can compromise data confidentiality.
ISO/IEC 27001	Yes	medium	Lack of access control for detailed campaign information poses a risk to information security.
CSA STAR	Yes	medium	Exposing campaign details without authentication is a security concern.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/your-campaigns

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures creators can only view their own campaigns, supporting data segregation.
ISO/IEC 27001	Yes	low	Access control for creator data is consistent with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Ensuring creators can only access their own campaign data improves security.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/submit-clip

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for submitting clips ensures accountability.
ISO/IEC 27001	Yes	low	Authentication for content submission is a good practice for data integrity.
CSA STAR	Yes	low	Ensuring authenticated submissions helps maintain the integrity of submitted content.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/campaign-clips

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures creators can only view clips associated with their campaigns.
ISO/IEC 27001	Yes	low	Access control for creator-submitted clips is in line with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for accessing campaign clips enhances data privacy.

Security Assessment Notes

CVSS Vector:

References

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

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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 ensures that only authorized users can access specific clip details.
ISO/IEC 27001	Yes	low	Access control for clip details aligns with ISO/IEC 27001 requirements.
CSA STAR	Yes	low	Authenticated access to clip details enhances data security.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns/

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

CVSS Score	N/A

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for deleting campaigns ensures data integrity and prevents unauthorized data loss.
ISO/IEC 27001	Yes	low	Secure deletion of campaign data with authentication is consistent with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for deleting campaigns protects against unauthorized modification or deletion of data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/clip/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated deletion of clips prevents unauthorized data removal.
ISO/IEC 27001	Yes	low	Secure deletion of creator content with authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for deleting clips protects against unauthorized data modification.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/admin/campaigns

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access for administrators ensures only authorized personnel can view campaign data.
ISO/IEC 27001	Yes	low	Role-based access control for administrative functions is a key security measure under ISO/IEC 27001.
CSA STAR	Yes	low	Restricting access to administrative campaign data improves overall system security.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/admin/clip/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated administrative access for updating clips ensures data integrity and prevents unauthorized modifications.
ISO/IEC 27001	Yes	low	Secure administrative controls for modifying clip data align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for administrative clip updates protects against unauthorized data changes.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/admin/clip/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated administrative deletion of clips ensures data integrity and prevents unauthorized removal.
ISO/IEC 27001	Yes	low	Secure administrative controls for deleting clip data align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for administrative clip deletion protects against unauthorized data loss.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/profile

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures creators can only view their own profile information.
ISO/IEC 27001	Yes	low	Access control for personal data aligns with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Protecting creator profile information through authentication is a standard security practice.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/creator/profile

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for updating creator profiles ensures that only the owner can modify their data.
ISO/IEC 27001	Yes	low	Secure modification of personal data with authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for profile updates protects against unauthorized changes to personal information.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//image

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for updating campaign images ensures data integrity and prevents unauthorized modifications.
ISO/IEC 27001	Yes	low	Secure administrative controls for modifying campaign assets align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for campaign image updates protects against unauthorized data changes.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//budget

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for updating campaign budgets ensures data integrity and prevents unauthorized financial modifications.
ISO/IEC 27001	Yes	low	Secure administrative controls for modifying campaign financial data align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for budget updates protects against unauthorized financial changes.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//requirements

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for updating campaign requirements ensures data integrity and prevents unauthorized modifications.
ISO/IEC 27001	Yes	low	Secure administrative controls for modifying campaign requirements align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for requirement updates protects against unauthorized data changes.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//status

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for updating campaign status ensures data integrity and prevents unauthorized modifications.
ISO/IEC 27001	Yes	low	Secure administrative controls for modifying campaign status align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for status updates protects against unauthorized campaign state changes.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//view_threshold

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for updating view thresholds ensures data integrity and prevents unauthorized modifications.
ISO/IEC 27001	Yes	low	Secure administrative controls for modifying campaign thresholds align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for threshold updates protects against unauthorized campaign metric manipulation.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/campaigns//deadline

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for updating campaign deadlines ensures data integrity and prevents unauthorized modifications.
ISO/IEC 27001	Yes	low	Secure administrative controls for modifying campaign deadlines align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for deadline updates protects against unauthorized campaign timeline manipulation.

Security Assessment Notes

CVSS Vector:

References

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

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures that only authorized users can view pending payout information.
ISO/IEC 27001	Yes	low	Access control for financial data aligns with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Protecting payout information through authentication is a standard security practice.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/profile

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures brand users can only view their own profile information.
ISO/IEC 27001	Yes	low	Access control for brand profile data aligns with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Protecting brand profile information through authentication is a standard security practice.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/brand/profile

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for updating brand profiles ensures that only the owner can modify their data.
ISO/IEC 27001	Yes	low	Secure modification of brand profile data with authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for profile updates protects against unauthorized changes to brand information.

Security Assessment Notes

CVSS Vector:

References

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

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated administrative access for updating clip view counts ensures data integrity and prevents tampering.
ISO/IEC 27001	Yes	low	Secure administrative controls for modifying clip metrics align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for view count updates protects against unauthorized manipulation of clip statistics.

Security Assessment Notes

CVSS Vector:

References

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

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated administrative access for updating campaign view counts ensures data integrity and prevents tampering.
ISO/IEC 27001	Yes	low	Secure administrative controls for modifying campaign metrics align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for view count updates protects against unauthorized manipulation of campaign statistics.

Security Assessment Notes

CVSS Vector:

References

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

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated administrative access for analytics ensures that only authorized personnel can view campaign performance data.
ISO/IEC 27001	Yes	low	Role-based access control for accessing sensitive analytics data aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Restricting access to campaign analytics data through authentication improves overall system security.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/auth/google-sync

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for Google sync ensures that only authorized users can link their accounts.
ISO/IEC 27001	Yes	low	Secure integration with third-party services like Google via authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for third-party integrations like Google sync protects user data.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /refresh

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated refresh token mechanism supports secure session management.
ISO/IEC 27001	Yes	low	Secure token management is important for session security under ISO/IEC 27001.
CSA STAR	Yes	low	Authenticated token refreshing helps maintain secure user sessions.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /logout

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated logout ensures proper session termination, aligning with access control principles.
ISO/IEC 27001	Yes	low	Secure session management, including logout, is part of ISO/IEC 27001 security controls.
CSA STAR	Yes	low	Authenticated logout helps prevent session hijacking.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /api/health

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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 generally acceptable if they do not expose sensitive system information.
ISO/IEC 27001	Yes	low	Availability monitoring through health checks is a standard operational practice.
CSA STAR	Yes	low	Health check endpoints are common for monitoring service availability.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /create-deposit-order

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for creating deposit orders ensures that only authorized users can initiate financial transactions.
ISO/IEC 27001	Yes	low	Secure handling of financial transactions through authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for financial operations protects against unauthorized transactions.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /verify-deposit

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated verification of deposits ensures the integrity of financial transactions.
ISO/IEC 27001	Yes	low	Secure verification processes for financial data align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for deposit verification protects financial data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /virtual-account

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access to virtual account details ensures that only authorized users can view financial information.
ISO/IEC 27001	Yes	low	Access control for financial account details aligns with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Protecting virtual account information through authentication is a standard security practice.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /wallet-balance

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures users can only view their own wallet balance.
ISO/IEC 27001	Yes	low	Access control for financial information aligns with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Protecting wallet balance information through authentication is a standard security practice.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /allocate-budget

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for budget allocation ensures that only authorized users can manage financial resources.
ISO/IEC 27001	Yes	low	Secure handling of financial allocations through authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for budget allocation protects financial data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /reclaim-budget

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for budget reclamation ensures that only authorized users can reclaim funds.
ISO/IEC 27001	Yes	low	Secure handling of financial reclamation through authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for budget reclamation protects financial data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /distribute-to-creator

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for distributing funds to creators ensures that only authorized entities can initiate payments.
ISO/IEC 27001	Yes	low	Secure handling of creator payments through authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for creator payouts protects financial data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator-withdraw

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for creator withdrawals ensures that only authorized creators can initiate payouts.
ISO/IEC 27001	Yes	low	Secure handling of creator withdrawal requests through authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for creator withdrawals protects financial data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/payout-details

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for saving payout details ensures that only authorized creators can manage their financial information.
ISO/IEC 27001	Yes	low	Secure handling of sensitive payout details through authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for payout detail management protects financial data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/payout-details

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures creators can only view their own payout details.
ISO/IEC 27001	Yes	low	Access control for sensitive financial payout information aligns with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Protecting payout details through authentication is a standard security practice.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/verify-payout-details

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated verification of payout details ensures that only authorized creators can confirm their financial information.
ISO/IEC 27001	Yes	low	Secure verification processes for sensitive payout data align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for payout detail verification protects financial data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/withdrawals

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures creators can only view their own withdrawal history.
ISO/IEC 27001	Yes	low	Access control for financial transaction history aligns with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Protecting withdrawal history through authentication is a standard security practice.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/notifications/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures creators can only retrieve their own notifications.
ISO/IEC 27001	Yes	low	Access control for user notifications aligns with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Protecting notification data through authentication is a standard security practice.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /transactions//

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures users can only view their own transaction history.
ISO/IEC 27001	Yes	low	Access control for transaction data aligns with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Protecting transaction history through authentication is a standard security practice.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /refund-campaign

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for refund requests ensures that only authorized users can initiate a refund process.
ISO/IEC 27001	Yes	low	Secure handling of refund processes through authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for refund requests protects financial data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /campaign-summary/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures users can only view summaries of campaigns they are authorized to see.
ISO/IEC 27001	Yes	low	Access control for campaign summary data aligns with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Protecting campaign summary information through authentication is a standard security practice.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /calculate-earnings//

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures that creators can only calculate their own earnings.
ISO/IEC 27001	Yes	low	Access control for financial earnings data aligns with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Protecting earnings calculation through authentication is a standard security practice.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /bulk-distribute

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for bulk distribution ensures that only authorized administrators can initiate mass payments.
ISO/IEC 27001	Yes	low	Secure handling of bulk financial distributions through authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for bulk distribution protects financial data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /request-refund

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for refund requests ensures that only authorized users can initiate a refund process.
ISO/IEC 27001	Yes	low	Secure handling of refund processes through authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for refund requests protects financial data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /refund-requests

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures users can only view their own refund requests or those they are authorized to see (e.g., admin).
ISO/IEC 27001	Yes	low	Access control for refund request data aligns with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Protecting refund request information through authentication is a standard security practice.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /admin/approve-refund

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated administrative approval of refunds ensures that only authorized personnel can process financial reversals.
ISO/IEC 27001	Yes	low	Secure administrative controls for financial refund processing align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for refund approval protects financial data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /admin/reject-refund

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated administrative rejection of refunds ensures that only authorized personnel can process financial reversals.
ISO/IEC 27001	Yes	low	Secure administrative controls for financial refund processing align with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for refund rejection protects financial data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /refund-status/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated access ensures users can only view the status of refunds they are authorized to see.
ISO/IEC 27001	Yes	low	Access control for refund status information aligns with ISO/IEC 27001 principles.
CSA STAR	Yes	low	Protecting refund status information through authentication is a standard security practice.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /admin/refund-audit-trail

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: application/json

Status Codes: 200

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	Authenticated administrative access for audit trails ensures that only authorized personnel can view sensitive operational logs.
ISO/IEC 27001	Yes	low	Role-based access control for accessing audit logs is a key security measure under ISO/IEC 27001.
CSA STAR	Yes	low	Restricting access to audit trail data through authentication improves overall system security.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /creator/revert-withdrawal

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authenticated access for reverting withdrawals ensures that only authorized actions can be taken on financial transactions.
ISO/IEC 27001	Yes	low	Secure handling of financial transaction modifications through authentication aligns with ISO/IEC 27001.
CSA STAR	Yes	low	Authentication for reverting withdrawals protects financial data integrity.

Security Assessment Notes

CVSS Vector:

References

METRICS SUMMARY

Total Findings: 5

Severity	Count
CRITICAL	1
HIGH	2
MEDIUM	1
LOW	1

BUSINESS RISK ADVICE

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

Disable Flask Debug Mode and Secure Environment Configuration (Priority: Immediate)

Description: The application runs with 'debug=True' at the entry point, exposing an interactive debugger to the public internet.

Why it Matters: Enables unauthenticated Remote Code Execution (RCE), allowing full server takeover and data breach.

Recommended Actions:

- Change 'app.run(debug=True)' to 'app.run(debug=False)' in app.py.
- Use environment variables (e.g., FLASK_DEBUG=0) to control behavior across environments.
- Enforce the use of a production-grade WSGI server like Gunicorn or uWSGI.

Expected Outcome: Elimination of the RCE attack vector and Werkzeug traceback exposure.

Remediate Hardcoded Secrets and Rotate Credentials (Priority: Immediate)

Description: An active or valid-structured JWT token is hardcoded in tasks.py, and the JWT secret key is likely compromised due to exposure in test scripts.

Why it Matters: Allows attackers to bypass authentication or gain unauthorized access to creator/brand accounts.

Recommended Actions:

- Delete the hardcoded JWT string from tasks.py line 14 immediately.
- Rotate the JWT_SECRET_KEY across all environments (production, staging, dev).
- Implement a Secret Management solution (e.g., AWS Secrets Manager, HashiCorp Vault, or encrypted .env files) for all sensitive strings.

Expected Outcome: Revocation of compromised credentials and prevention of token-based lateral movement.

Patch Critical Dependency Vulnerabilities (Priority: Short-Term)

Description: The current version of aiohttp (3.11.10) is susceptible to HTTP Request Smuggling (CVE-2025-53643).

Why it Matters: Attackers can bypass security controls, poison caches, or hijack user sessions by desynchronizing proxy/server communications.

Recommended Actions:

- Update aiohttp to version 3.12.0 or higher in requirements.txt.
- Verify the presence of C-extensions in production builds to mitigate the pure-Python desync risk.
- Run 'pip-audit' to identify and remediate secondary nested dependency risks.

Expected Outcome: Protection against desynchronization attacks and smuggling-based security bypasses.

Enforce Authentication on Data-Exposing Endpoints (Priority: Short-Term)

Description: Sensitive endpoints like /api/campaigns and campaign detail lookups lack JWT decorators, exposing business data.

Why it Matters: Unauthorized data harvesting of campaign strategies and creator details leads to business intelligence leakage.

Recommended Actions:

- Apply @jwt_required() decorators to all GET endpoints in the /api/campaigns/ tree.
- Enforce strict Rate Limiting on /login and /register to prevent credential stuffing and account creation abuse.
- Implement Object-Level Access Control (OLAC) to ensure creators can only see their own non-public data.

Expected Outcome: Compliance with SOC 2/ISO 27001 access control requirements and prevention of data scraping.

Sanitize API Error Responses (Priority: Short-Term)

Description: Global use of str(e) in exception handling exposes internal stack traces, database schemas, and file paths.

Why it Matters: Facilitates reconnaissance for attackers, enabling them to map the internal architecture and find injection points.

Recommended Actions:

- Implement a centralized @app.errorhandler(Exception) to catch all unhandled errors.
- Replace str(e) in jsonify responses with generic user-friendly messages like 'Internal Server Error'.
- Direct detailed exception messages only to secure server-side logs (e.g., Python logging module).

Expected Outcome: Elimination of information disclosure vulnerabilities across 50+ identified endpoints.

Implement Network Resilience and Timeouts (Priority: Mid-Term)

Description: Outbound HTTP requests to external payment APIs (Cashfree) are missing connection and read timeouts.

Why it Matters: Unresponsive external services can cause thread exhaustion, leading to Application Denial of Service (DoS).

Recommended Actions:

- Update all 'requests.post' and 'requests.get' calls to include the 'timeout' parameter (e.g., timeout=(3.05, 15)).
- Implement retry logic with exponential backoff for critical payment verification paths.
- Monitor outbound request latency to identify failing external dependencies early.

Expected Outcome: Improved application availability and resilience against upstream service failures.

Institutionalize Secure Development Lifecycle (SDLC) (Priority: Long-Term)

Description: The presence of debug mode and hardcoded secrets in production-cloned code indicates a gap in the automated security pipeline.

Why it Matters: Prevents the re-introduction of high-severity vulnerabilities in future feature releases.

Recommended Actions:

- Integrate Static Analysis Security Testing (SAST) tools (e.g., Semgrep, Bandit) into the CI/CD pipeline.
- Implement a 'Secret Scanning' hook (e.g., Gitleaks) to block commits containing tokens or keys.
- Establish a mandatory peer security review for all changes involving authentication or payment logic.

Expected Outcome: Reduced risk of regression and significantly lower Mean Time to Remediate (MTTR) for new flaws.