SECURITY ANALYSIS REPORT

Generated By

Backstage Rookie

Provider: Backstage Rookie

contact - swarajdarekar9@gmail.com

Client: swaraj darekar

swarajdarekar9@gmail.com

Scan ID: 80df7f4a-8465-4da3-823a-87f82e327912

Date: 2026-02-10 19:28:47

Version: 1.0.0

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This security assessment identified several critical, high, and medium-severity vulnerabilities within the application, alongside numerous low-severity issues related to verbose error reporting. The findings indicate a need for improved security practices, particularly concerning secret management, debug configurations, external API call resilience, and information disclosure in error messages. Addressing these issues is crucial for protecting sensitive data, maintaining application availability, and preventing potential system compromise.

Identified Vulnerabilities

ID	Title	CVSS	Page
C1	Hardcoded JWT Secret/Token	9.8	
H1	Flask Debug Mode Enabled in Production	8.8	
M1	Missing Request Timeout for External API Calls	6.5	
L1	Verbose Error Messages Exposing Internal Details	3.1	

METHODOLOGY

Introduction

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

Objective

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

Scope

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

Systems in Scope

Name	IP

User Accounts

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

FINDINGS

C1 – Hardcoded JWT Secret/Token

Severity: Critical

CVSS Score: 9.8

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

Target: Application source code

Overview

A sensitive JSON Web Token (JWT) is hardcoded directly into the `tasks.py` file, representing a severe security misconfiguration.

Details

The `token` variable on line 14 of `tasks.py` contains a complete JWT. While the context suggests this might be for testing token verification, the presence of such a token (or, by extension, a hardcoded signing key) in source code is a critical security vulnerability. If this token or a related signing key were to be a production secret, an attacker could use it to impersonate users, bypass authentication mechanisms, or forge valid tokens, leading to full system compromise. Even as an example, it sets a dangerous precedent for handling sensitive information.

Evidence

- **tasks.py:14:** Hardcoded JWT token assigned to variable 'token'. python 13: # 3. The exact token you received from login (I copied it from your message) 14: token = "eyJhbGciOiJIUzI1NiIsImtpZCI6IkRUK3NRQURhd0Uwdm9RbkwiLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodHRwczovL2Frd2VtZWZld2ZtenhlZ2lkZXNsLnN1cGFiYXNlLmNvL2F1dGgvdjEi 15:

References

- https://owasp.org/www-project-top-ten/2021/A04_2021-Insecure_Design
- https://owasp.org/www-community/vulnerabilities/Hardcoded_password

Recommendation

- Immediately remove the hardcoded JWT token from the source code. - Ensure all sensitive credentials, tokens, and keys are loaded from secure environment variables or a dedicated secret management service (e.g., AWS Secrets Manager, HashiCorp Vault, Azure Key Vault). - Implement strict access controls for configuration files and environment variables. - Rotate any exposed tokens or keys immediately. - Educate developers on secure secret management practices to prevent similar issues in the future.

Prompt to Solve the Vulnerability:

In `tasks.py` at line 14, remove the hardcoded JWT token `token = "eyJhbGciOiJIUzI1NiIs..."`. Instead, any necessary token for testing or development should be loaded dynamically from secure environment variables, such as `token = os.getenv('EXAMPLE_JWT_TOKEN')`, or generated on-the-fly, and never committed to version control. If this token represents a secret key, replace it with `secret = os.getenv('JWT_SECRET_KEY')` ensuring `JWT_SECRET_KEY` is never hardcoded.

H1 – Flask Debug Mode Enabled in Production

Severity: High

CVSS Score: 8.8

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

Target: Application deployment configuration

Overview

The Flask application is configured to run with `debug=True` in the main execution block, a setting highly dangerous for production environments.

Details

Running a Flask application with `debug=True` enables the Werkzeug debugger, which can allow an attacker to execute arbitrary Python code on the server if the debugger pin is compromised or guessed. This can lead to full system compromise, including data exfiltration, modification, and denial of service. While convenient for development, this configuration should never be deployed to a production environment. The `if __name__ == '__main__':` block suggests this might be for local development, but it poses a significant risk if not properly excluded or controlled in production builds.

Evidence

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

References

- https://flask.palletsprojects.com/en/2.0.x/config/#DEBUG
- https://owasp.org/www-project-top-ten/2021/A05_2021-Security_Misconfiguration

Recommendation

- Ensure that `debug=True` is explicitly disabled when deploying to production. Use environment variables (e.g., `FLASK_ENV='production'`) to conditionally control this setting. - Configure a robust production server (e.g., Gunicorn, uWSGI) to serve the Flask application, which typically disables debug mode by default and handles application processes more securely. - Remove or guard the `if __name__ == '__main__':` block's `app.run(debug=True)` call in production deployments, perhaps using a conditional check for the `FLASK_ENV` environment variable. - Implement strict logging and monitoring for production environments to detect unusual activity.

Prompt to Solve the Vulnerability:

In `app.py` at line 1872, change `app.run(debug=True, port=5000, use_reloader=True)` to `app.run(debug=False, port=5000, use_reloader=False)`. Ideally, this line should be conditionally executed only in development environments, for example: `if os.getenv('FLASK_ENV') == 'development': app.run(debug=True, ...)` and production deployments should use a WSGI server like Gunicorn.

M1 – Missing Request Timeout 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:H

Target: External API integrations

Overview

Multiple HTTP requests made to external services (specifically Cashfree API) do not specify a timeout parameter.

Details

When making HTTP requests to external services, failing to specify a timeout can lead to the application hanging indefinitely if the external service is slow, unresponsive, or experiencing network issues. This can exhaust server resources (threads, memory, connections), leading to denial of service (DoS) for legitimate users as the application becomes unresponsive while waiting for external replies. Such a vulnerability can significantly impact application availability and user experience, especially in a technology-driven SaaS environment where external dependencies are common.

Evidence

- **routes\payments.py:90:** requests.post call without a timeout. python 89: # 3. Call Cashfree API 90: response = requests.post(91: f"{CASHFREE_BASE_URL}/orders", 92: headers=get_cashfree_headers(), 93: json=payload 94:)
- **routes\payments.py:136:** requests.get call without a timeout. python 135: # 1. Check Status from Cashfree 136: response = requests.get(137: f"{CASHFREE_BASE_URL}/orders/{order_id}", 138: headers=get_cashfree_headers() 139:)
- **routes\payments.py:663:** requests.post call without a timeout. python 662: 663: payout_response = requests.post(payout_api_url, json=cashfree_payout_payload, headers=cashfree_headers) 664:

References

- https://docs.python-requests.org/en/master/user/advanced/#timeouts
- https://owasp.org/www-project-top-ten/2021/A07_2021-Identification_and_Authentication_Failures#api-abuse

Recommendation

- Add a `timeout` parameter to all `requests.post` and `requests.get` calls. The timeout value should be a reasonable duration based on the expected response time of the external API. - Implement robust error handling around external API calls, including specific handling for `requests.exceptions.Timeout`. - Consider using a circuit breaker pattern for critical external dependencies to prevent cascading failures and provide graceful degradation.

Prompt to Solve the Vulnerability:

For each `requests.post` or `requests.get` call identified, add a `timeout` parameter. For example, change `response = requests.post(url, ...)` to `response = requests.post(url, ..., timeout=10)` (where 10 is seconds). Similarly, for `response = requests.get(url, ...)`, change it to `response = requests.get(url, ..., timeout=10)`. A suitable timeout value should be chosen based on the expected behavior and latency of the external API, ensuring it's not excessively long.

L1 – Verbose Error Messages Exposing Internal Details

Severity: Low

CVSS Score: 3.1

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

Target: Application API endpoints

Overview

Multiple API endpoints return raw exception messages directly to the client in case of an error, potentially exposing sensitive information.

Details

Exposing raw exception details (e.g., via `str(e)`) in API responses can inadvertently reveal sensitive information about the application's internal architecture, database schema, file paths, or other system-level configurations. This information, while useful for debugging during development, can be leveraged by malicious actors to craft more targeted attacks, such as SQL injection, path traversal, or to understand the application's technology stack for further exploitation. This practice violates the principle of least privilege in information disclosure, making it easier for attackers to enumerate vulnerabilities. This is particularly prevalent across numerous payment and core application routes.

Evidence

- **app.py:117:** Error message exposing str(e). python 115: except Exception as e: 116: print(f"Registration error: {str(e)}") 117: return jsonify({'msg': 'Registration failed', 'error': str(e)}), 500
- **app.py:187:** Error message exposing str(e). python 185: print(f"Login error: {str(e)}") 186: # This will now only print real errors, or the final network error if all retries failed 187: return jsonify({'msg': 'Login failed', 'error': str(e)}), 500
- **app.py:210:** Error message exposing str(e). python 208: result['msg'] = 'Instagram account verified and linked.' 209: except Exception as e: 210: return jsonify({'msg': 'Failed to update profile', 'error': str(e)}), 500
- **app.py:243:** Error message exposing str(e). python 241: except Exception as e: 242: print(f"Reset password error: {str(e)}") 243: return jsonify({'msg': 'Failed to send reset email', 'error': str(e)}), 500
- **app.py:288:** Error message exposing str(e). python 286: except Exception as e: 287: print(f"Create campaign error: {str(e)}") 288: return jsonify({'msg': 'Failed to create campaign', 'error': str(e)}), 500
- **app.py:326:** Error message exposing str(e). python 324: except Exception as e: 325: print(f"List campaigns error: {str(e)}") 326: return jsonify({'msg': 'Failed to fetch campaigns', 'error': str(e)}), 500
- **app.py:385:** Error message exposing str(e). python 383: except Exception as e: 384: print(f"Get all campaigns error: {str(e)}") 385: return jsonify({'msg': 'Failed to fetch campaigns', 'error': str(e)}), 500
- **app.py:491:** Error message exposing str(e). python 489: except Exception as e: 490: print(f"Get campaign by ID error: {str(e)}") 491: return jsonify({'msg': 'Failed to fetch campaign details', 'error': str(e)}), 500
- **app.py:579:** Error message exposing str(e). python 577: except Exception as e: 578: print(f"Get creator campaigns error: {str(e)}") 579: return jsonify({'msg': 'Failed to fetch creator campaigns', 'error': str(e)}), 500
- **app.py:653:** Error message exposing str(e). python 651: except Exception as e: 652: print(f"Submit clip error: {str(e)}") 653: return jsonify({'msg': 'Failed to submit clip', 'error': str(e)}), 500
- **app.py:718:** Error message exposing str(e). python 716: except Exception as e: 717: print(f"Get creator clips for campaign error: {str(e)}") 718: return jsonify({'msg': 'Failed to fetch clips', 'error': str(e)}), 500
- **app.py:754:** Error message exposing str(e). python 752: except Exception as e: 753: print(f"Get accepted clip details error: {str(e)}") 754: return jsonify({'msg': 'Failed to fetch accepted clip details', 'error': str(e)}), 500
- **app.py:829:** Error message exposing str(e). python 827: except Exception as e: 828: print(f"Delete campaign error: {str(e)}") 829: return jsonify({'msg': 'Failed to delete campaign', 'error': str(e)}), 500
- **app.py:884:** Error message exposing str(e). python 882: except Exception as e: 883: print(f"Delete clip error: {str(e)}") 884: return jsonify({'msg': 'Failed to delete clip', 'error': str(e)}), 500
- **app.py:931:** Error message exposing str(e). python 929: except Exception as e: 930: print(f"Admin get campaigns error: {str(e)}") 931: return jsonify({'msg': 'Failed to fetch campaigns', 'error': str(e)}), 500
- **app.py:1022:** Error message exposing str(e). python 1020: except Exception as e: 1021: print(f"Admin update clip error: {str(e)}") 1022: return jsonify({'msg': 'Failed to update clip', 'error': str(e)}), 500
- **app.py:1075:** Error message exposing str(e). python 1073: except Exception as e: 1074: print(f"Admin delete clip error: {str(e)}") 1075: return jsonify({'msg': 'Failed to delete clip', 'error': str(e)}), 500
- **app.py:1109:** Error message exposing str(e). python 1107: except Exception as e: 1108: print(f"Get creator profile error: {str(e)}") 1109: return jsonify({'msg': 'Failed to fetch creator profile', 'error': str(e)}), 500
- **app.py:1155:** Error message exposing str(e). python 1153: except Exception as e: 1154: print(f"Update creator profile error: {str(e)}") 1155: return jsonify({'msg': 'Failed to update creator profile', 'error': str(e)}), 500
- **app.py:1194:** Error message exposing str(e). python 1192: except Exception as e: 1193: print(f"Update campaign image error: {str(e)}") 1194: return jsonify({'msg': 'Failed to update campaign image', 'error': str(e)}), 500
- **app.py:1226:** Error message exposing str(e). python 1224: except Exception as e: 1225: print(f"Update campaign budget error: {str(e)}") 1226: return jsonify({'msg': 'Failed to update campaign budget', 'error': str(e)}), 500
- **app.py:1255:** Error message exposing str(e). python 1253: except Exception as e: 1254: print(f"Update campaign requirements error: {str(e)}") 1255: return jsonify({'msg': 'Failed to update campaign requirements', 'error': str(e)}), 500
- **app.py:1286:** Error message exposing str(e). python 1284: except Exception as e: 1285: print(f"Update campaign status error: {str(e)}") 1286: return jsonify({'msg': 'Failed to update campaign status', 'error': str(e)}), 500

- **app.py:1317:** Error message exposing str(e). python 1315: except Exception as e: 1316: print(f"Update campaign view threshold error: {str(e)}") 1317: return jsonify({'msg': 'Failed to update campaign view threshold', 'error': str(e)}), 500
- **app.py:1354:** Error message exposing str(e). python 1352: except Exception as e: 1353: print(f"Update campaign deadline error: {str(e)}") 1354: return jsonify({'msg': 'Failed to update campaign deadline', 'error': str(e)}), 500
- **app.py:1450:** Error message exposing str(e). python 1448: except Exception as e: 1449: print(f"Get pending payouts error: {str(e)}") 1450: return jsonify({'msg': 'Failed to retrieve pending payouts', 'error': str(e)}), 500
- **app.py:1478:** Error message exposing str(e). python 1476: except Exception as e: 1477: print(f"Get brand profile error: {str(e)}") 1478: return jsonify({'msg': 'Failed to fetch brand profile', 'error': str(e)}), 500
- **app.py:1509:** Error message exposing str(e). python 1507: except Exception as e: 1508: print(f"Update brand profile error: {str(e)}") 1509: return jsonify({'msg': 'Failed to update brand profile', 'error': str(e)}), 500
- **app.py:1576:** Error message exposing str(e). python 1574: except Exception as e: 1575: print(f"Update view count error: {str(e)}") 1576: return jsonify({'msg': 'Failed to update view count', 'error': str(e)}), 500
- **app.py:1631:** Error message exposing str(e). python 1629: except Exception as e: 1630: print(f"Update campaign views error: {str(e)}") 1631: return jsonify({'msg': 'Failed to update campaign views', 'error': str(e)}), 500
- **app.py:1729:** Error message exposing str(e). python 1727: except Exception as e: 1728: print(f"Get campaign performance analytics error: {str(e)}") 1729: return jsonify({'msg': 'Failed to retrieve analytics', 'error': str(e)}), 500
- **app.py:1756:** Error message exposing str(e). python 1754: except Exception as e: 1755: print(f"Error fetching user from Supabase in google_sync: {e}") 1756: return jsonify({'msg': 'Failed to sync Google user: could not retrieve user data', 'error': str(e)}), 500
- **app.py:1808:** Error message exposing str(e). python 1806: # If it's a different API error, report it 1807: print(f"Google sync API error: {str(e)}") 1808: return jsonify({'msg': 'Sync failed due to database error', 'error': str(e)}), 500
- **app.py:1812:** Error message exposing str(e). python 1810: # Catch any other general exceptions 1811: print(f"Google sync generic error: {str(e)}") 1812: return jsonify({'msg': 'Sync failed', 'error': str(e)}), 500
- **routes\payments.py:115:** Error message exposing str(e). python 113: except Exception as e: 114: print(f"[Server Error]: {str(e)}") 115: return jsonify({'msg': 'Internal server error', 'error': str(e)}), 500
- **routes\payments.py:186:** Error message exposing str(e). python 184: except Exception as e: 185: print(f"[Verification Error]: {str(e)}") 186: return jsonify({'msg': 'Verification failed', 'error': str(e)}), 500
- **routes\payments.py:343:** Error message exposing str(e). python 341: except Exception as e: 342: print(f"Allocate budget error: {str(e)}") 343: return jsonify({'msg': 'Allocation failed', 'error': str(e)}), 500
- **routes\payments.py:430:** Error message exposing str(e). python 428: except Exception as e: 429: print(f"Reclaim budget error: {str(e)}") 430: return jsonify({'msg': 'Reclaim failed', 'error': str(e)}), 500
- **routes\payments.py:554:** Error message exposing str(e). python 552: except Exception as e: 553: print(f"Distribution error: {str(e)}") 554: return jsonify({'msg': 'Distribution failed', 'error': str(e)}), 500
- **routes\payments.py:729:** Error message exposing str(e). python 727: except Exception as e: 728: print(f"Withdrawal error: {str(e)}") 729: return jsonify({'msg': 'Withdrawal failed', 'error': str(e)}), 500
- **routes\payments.py:817:** Error message exposing str(e). python 815: except Exception as e: 816: print(f"Save payout details error: {str(e)}") 817: return jsonify({'msg': 'Failed to save payout details', 'error': str(e)}), 500
- **routes\payments.py:867:** Error message exposing str(e). python 865: except Exception as e: 866: print(f"Get payout details error: {str(e)}") 867: return jsonify({'msg': 'Failed to retrieve payout details', 'error': str(e)}), 500
- **routes\payments.py:927:** Error message exposing str(e). python 925: except Exception as e: 926: print(f"Verify payout details error: {str(e)}") 927: return jsonify({'msg': 'Failed to verify payout details', 'error': str(e)}), 500
- **routes\payments.py:989:** Error message exposing str(e). python 987: except Exception as e: 988: print(f"Get withdrawal history error: {str(e)}") 989: return jsonify({'msg': 'Failed to retrieve withdrawal history', 'error': str(e)}), 500
- **routes\payments.py:1023:** Error message exposing str(e). python 1021: except Exception as e: 1022: print(f"Get creator notifications error: {str(e)}") 1023: return jsonify({'msg': 'Failed to retrieve notifications', 'error': str(e)}), 500
- **routes\payments.py:1105:** Error message exposing str(e). python 1103: except Exception as e: 1104: print(f"Get transactions error: {str(e)}") 1105: return jsonify({'msg': 'Failed to retrieve transactions', 'error': str(e)}), 500
- **routes\payments.py:1197:** Error message exposing str(e). python 1195: except Exception as e: 1196: print(f"Refund error: {str(e)}") 1197: return jsonify({'msg': 'Refund failed', 'error': str(e)}), 500
- **routes\payments.py:1264:** Error message exposing str(e). python 1262: except Exception as e: 1263: print(f"Get campaign summary error: {str(e)}") 1264: return jsonify({'msg': 'Failed to retrieve campaign summary', 'error': str(e)}), 500
- **routes\payments.py:1358:** Error message exposing str(e). python 1356: except Exception as e: 1357: print(f"Calculate earnings error: {str(e)}") 1358: return jsonify({'msg': 'Failed to calculate earnings', 'error': str(e)}), 500
- **routes\payments.py:1529:** Error message exposing str(e). python 1527: except Exception as e: 1528: print(f"Bulk distribute error: {str(e)}") 1529: return jsonify({'msg': 'Bulk distribution failed', 'error': str(e)}), 500
- **routes\payments.py:1623:** Error message exposing str(e). python 1621: except Exception as e: 1622: print(f"Request refund error: {str(e)}") 1623: return jsonify({'msg': 'Failed to request refund', 'error': str(e)}), 500
- **routes\payments.py:1690:** Error message exposing str(e). python 1688: except Exception as e: 1689: print(f"Get refund requests error: {str(e)}") 1690: return jsonify({'msg': 'Failed to retrieve refund requests', 'error': str(e)}), 500
- **routes\payments.py:1804:** Error message exposing str(e). python 1802: except Exception as e: 1803: print(f"Approve refund error: {str(e)}") 1804: return jsonify({'msg': 'Failed to approve refund', 'error': str(e)}), 500
- **routes\payments.py:1865:** Error message exposing str(e). python 1863: except Exception as e: 1864: print(f"Reject refund error: {str(e)}") 1865: return jsonify({'msg': 'Failed to reject refund', 'error': str(e)}), 500
- **routes\payments.py:1934:** Error message exposing str(e). python 1932: except Exception as e: 1933: print(f"Get refund status error: {str(e)}") 1934: return jsonify({'msg': 'Failed to retrieve refund status', 'error': str(e)}), 500

- **routes\payments.py:2014:** Error message exposing str(e). python 2012: except Exception as e: 2013: print(f"Get refund audit trail error: {str(e)}") 2014: return jsonify({'msg': 'Failed to retrieve refund audit trail', 'error': str(e)}), 500
- **routes\payments.py:2088:** Error message exposing str(e). python 2086: except Exception as e: 2087: print(f"Revert withdrawal error: {str(e)}") 2088: return jsonify({'msg': 'Failed to revert withdrawal', 'error': str(e)}), 500

References

- https://owasp.org/www-project-top-ten/2021/A05_2021-Security_Misconfiguration#information-disclosure
- https://cwe.mitre.org/data/definitions/209.html

Recommendation

- Implement custom error handling that returns generic, user-friendly error messages to the client. - Log detailed exception information internally on the server for debugging purposes, but never expose it directly to end-users. - Consider a global error handler for the Flask application to catch unhandled exceptions and return a standardized, non-verbose error response. - Avoid including `str(e)` in `jsonify` responses that go to clients, replacing it with a more general message like 'An unexpected error occurred'.

Prompt to Solve the Vulnerability:

For each instance of `return jsonify({'msg': '...', 'error': str(e)}), 500`, replace `str(e)` with a generic, non-technical error message. For example, change `return jsonify({'msg': 'Registration failed', 'error': str(e)}), 500` to `return jsonify({'msg': 'Registration failed. An unexpected error occurred. Please try again later.'}), 500`. The detailed `str(e)` should only be logged 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 user registration endpoint.

  Potential Attack Scenario:

  An attacker could create unauthorized user accounts, potentially for spamming, phishing, or other malicious activities.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of authentication on registration can lead to unauthorized access and misuse of the system, violating principles of access control and integrity.
ISO/IEC 27001	Yes	high	Inadequate access control mechanisms, specifically for user registration, can compromise the confidentiality and integrity of user data.
CSA STAR	Yes	high	Absence of proper authentication controls for user creation increases the risk of unauthorized account provisioning, impacting system security and trustworthiness.

Security Assessment Notes

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

References

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

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.

  Potential Attack Scenario:

  An attacker could potentially brute-force credentials or exploit unauthenticated access to gain unauthorized entry into the system.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of proper authentication on login directly violates access control principles, allowing unauthorized access and compromising system security.
ISO/IEC 27001	Yes	high	Insecure authentication for login can lead to unauthorized access to information, violating confidentiality and integrity.
CSA STAR	Yes	high	Failure to implement robust authentication for login poses a significant risk to the security of user accounts and the overall system.

Security Assessment Notes

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

References

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

Endpoint Path /verify-instagram

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	The endpoint appears to have authentication implemented, which aligns with SOC 2 principles for access control.
ISO/IEC 27001	Yes	low	The presence of authentication suggests adherence to access control policies required by ISO 27001.
CSA STAR	Yes	low	Authentication on this endpoint contributes to a secure cloud environment, as generally expected by CSA STAR.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /verify-instagram/

Endpoint Path	/verify-instagram/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	The endpoint appears to have authentication implemented, which aligns with SOC 2 principles for access control.
ISO/IEC 27001	Yes	low	The presence of authentication suggests adherence to access control policies required by ISO 27001.
CSA STAR	Yes	low	Authentication on this endpoint contributes to a secure cloud environment, as generally expected by CSA STAR.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /request-password-reset

Endpoint Path	/request-password-reset
HTTP Methods	POST
Source Location	..\Mipoe-Backend\app.py - 224
Authentication Required	No
Risk Severity	Critical
CVSS Score	8.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

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

  Potential Attack Scenario:

  An attacker could initiate password resets for other users, potentially leading to account takeover if email verification is weak or bypassed.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Unauthenticated password reset functionality can be exploited for account takeover, violating principles of access control and integrity.
ISO/IEC 27001	Yes	high	Inadequate protection of the password reset process can lead to unauthorized access to user accounts, compromising confidentiality.
CSA STAR	Yes	high	Vulnerabilities in password reset mechanisms can be exploited for account hijacking, posing a significant security risk in cloud services.

Security Assessment Notes

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

References

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

Endpoint Path /api/brand/campaigns

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication is present, indicating an effort to control access to campaign creation.
ISO/IEC 27001	Yes	low	The endpoint requires authentication, which is a standard control for protecting sensitive operations like campaign creation.
CSA STAR	Yes	low	Proper authentication for creating campaigns helps maintain data integrity and security in the cloud environment.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/campaigns

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication is present for retrieving campaign data, aligning with access control requirements.
ISO/IEC 27001	Yes	low	The requirement for authentication ensures that only authorized users can access campaign information.
CSA STAR	Yes	low	Authentication for accessing campaign data contributes to data confidentiality and security.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/campaigns

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (medium): Authentication is missing for retrieving all campaigns.

  Potential Attack Scenario:

  An attacker could potentially access sensitive campaign information if the endpoint is not intended to be public.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Publicly accessible campaign data could violate confidentiality requirements if not intended, impacting SOC 2 compliance.
ISO/IEC 27001	Yes	medium	Exposure of potentially sensitive campaign information without proper authorization contravenes information security principles.
CSA STAR	Yes	medium	Unrestricted access to campaign data could lead to information leakage, affecting the security posture required by CSA STAR.

Security Assessment Notes

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

References

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

Endpoint Path /api/campaigns/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (medium): Authentication is missing for retrieving a specific campaign by ID.

  Potential Attack Scenario:

  An attacker could potentially access sensitive campaign details of other users if authorization checks are not properly implemented after authentication (or if authentication is expected).

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Lack of authentication could lead to unauthorized access to specific campaign data, violating confidentiality.
ISO/IEC 27001	Yes	medium	Accessing specific campaign data without authentication can compromise information security.
CSA STAR	Yes	medium	Unsecured access to individual campaign data can lead to data leakage.

Security Assessment Notes

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

References

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

Endpoint Path /api/creator/your-campaigns

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication is present, ensuring only authorized creators can access their own campaigns.
ISO/IEC 27001	Yes	low	Access control is enforced through authentication, protecting creator-specific data.
CSA STAR	Yes	low	Secure access to creator campaign data is maintained through authentication.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/creator/submit-clip

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized creators can submit clips.
ISO/IEC 27001	Yes	low	Access control for submitting clips is managed through authentication.
CSA STAR	Yes	low	Secure submission of clips is facilitated by authentication.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/creator/campaign-clips

Endpoint Path	/api/creator/campaign-clips
HTTP Methods	GET
Source Location	..\Mipoe-Backend\app.py - 657

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures that only authorized creators can view clips associated with their campaigns.
ISO/IEC 27001	Yes	low	Access control is enforced through authentication, protecting creator-specific data.
CSA STAR	Yes	low	Secure access to creator campaign clip data is maintained through authentication.

Security Assessment Notes

CVSS Vector: N/A

References

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

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures that only authorized creators can view details of accepted clips.
ISO/IEC 27001	Yes	low	Access control is enforced through authentication, protecting clip details.
CSA STAR	Yes	low	Secure access to clip details is maintained through authentication.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/campaigns/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication is present for deleting campaigns, ensuring only authorized actions.
ISO/IEC 27001	Yes	low	Access control via authentication prevents unauthorized deletion of campaigns.
CSA STAR	Yes	low	Secure deletion of campaign data is ensured through authentication.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/creator/clip/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication is present for deleting clips, ensuring only authorized actions.
ISO/IEC 27001	Yes	low	Access control via authentication prevents unauthorized deletion of clips.
CSA STAR	Yes	low	Secure deletion of clip data is ensured through authentication.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/admin/campaigns

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Admin access to campaigns is protected by authentication.
ISO/IEC 27001	Yes	low	Proper access control for administrative functions is maintained.
CSA STAR	Yes	low	Secure administrative access to campaign data.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/admin/clip/

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

CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication protects administrative updates to clips.
ISO/IEC 27001	Yes	low	Access control via authentication is enforced for administrative modifications.
CSA STAR	Yes	low	Secure administrative updates to clip data.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/admin/clip/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication is present for administrative deletion of clips, ensuring control.
ISO/IEC 27001	Yes	low	Access control via authentication prevents unauthorized administrative deletions.
CSA STAR	Yes	low	Secure administrative deletion of clip data.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/creator/profile

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures creators can only access their own profile information.
ISO/IEC 27001	Yes	low	Access control via authentication protects creator profile data.
CSA STAR	Yes	low	Secure access to creator profile data is maintained through authentication.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/creator/profile

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures creators can only update their own profile information.
ISO/IEC 27001	Yes	low	Access control via authentication protects creator profile data from unauthorized modification.
CSA STAR	Yes	low	Secure modification of creator profile data.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/campaigns//image

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication protects brand campaign image updates.
ISO/IEC 27001	Yes	low	Access control ensures only authorized users can update campaign images.
CSA STAR	Yes	low	Secure updates to brand campaign assets.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/campaigns//budget

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication protects brand campaign budget updates.
ISO/IEC 27001	Yes	low	Access control ensures only authorized users can update campaign budgets.
CSA STAR	Yes	low	Secure updates to brand campaign financial data.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/campaigns//requirements

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication protects brand campaign requirement updates.
ISO/IEC 27001	Yes	low	Access control ensures only authorized users can update campaign requirements.
CSA STAR	Yes	low	Secure updates to brand campaign operational details.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/campaigns//status

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication protects brand campaign status updates.
ISO/IEC 27001	Yes	low	Access control ensures only authorized users can update campaign status.
CSA STAR	Yes	low	Secure updates to brand campaign operational status.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/campaigns//view_threshold

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication protects brand campaign view threshold updates.
ISO/IEC 27001	Yes	low	Access control ensures only authorized users can update campaign view thresholds.
CSA STAR	Yes	low	Secure updates to brand campaign performance metrics.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/campaigns//deadline

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication protects brand campaign deadline updates.
ISO/IEC 27001	Yes	low	Access control ensures only authorized users can update campaign deadlines.
CSA STAR	Yes	low	Secure updates to brand campaign timelines.

Security Assessment Notes

CVSS Vector: N/A

References

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

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized users can view pending payouts for campaigns.
ISO/IEC 27001	Yes	low	Access control via authentication protects sensitive financial payout information.
CSA STAR	Yes	low	Secure access to financial payout data.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/profile

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures brands can only access their own profile information.
ISO/IEC 27001	Yes	low	Access control via authentication protects brand profile data.
CSA STAR	Yes	low	Secure access to brand profile data is maintained through authentication.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/brand/profile

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures brands can only update their own profile information.
ISO/IEC 27001	Yes	low	Access control via authentication protects brand profile data from unauthorized modification.
CSA STAR	Yes	low	Secure modification of brand profile data.

Security Assessment Notes

CVSS Vector: N/A

References

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

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication protects administrative updates to clip view counts.
ISO/IEC 27001	Yes	low	Access control via authentication is enforced for administrative modifications.
CSA STAR	Yes	low	Secure administrative updates to clip metrics.

Security Assessment Notes

CVSS Vector: N/A

References

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

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication protects administrative updates to campaign view counts.
ISO/IEC 27001	Yes	low	Access control via authentication is enforced for administrative modifications.
CSA STAR	Yes	low	Secure administrative updates to campaign metrics.

Security Assessment Notes

CVSS Vector: N/A

References

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

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized administrators can access campaign performance analytics.
ISO/IEC 27001	Yes	low	Access control via authentication protects sensitive analytics data.
CSA STAR	Yes	low	Secure access to campaign performance analytics.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/auth/google-sync

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication is present for Google synchronization, securing user data.
ISO/IEC 27001	Yes	low	Secure integration with Google services via authenticated access.
CSA STAR	Yes	low	Authenticated data synchronization with external services like Google.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /refresh

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication is present for token refresh operations, maintaining session security.
ISO/IEC 27001	Yes	low	Secure token management through authenticated refresh.
CSA STAR	Yes	low	Protected token lifecycle management.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /logout

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only the logged-in user can log out.
ISO/IEC 27001	Yes	low	Secure session termination through authenticated logout.
CSA STAR	Yes	low	Proper session management via authenticated logout.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /api/health

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Health check endpoints are typically not considered a high risk if they do not expose sensitive information.
ISO/IEC 27001	Yes	low	Health checks are operational endpoints and do not typically pose security risks if designed correctly.
CSA STAR	Yes	low	Health check endpoints are standard for monitoring cloud service availability.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /create-deposit-order

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized users can create deposit orders, aligning with access control principles.
ISO/IEC 27001	Yes	low	Secure financial transactions are managed through authenticated endpoints.
CSA STAR	Yes	low	Authentication for payment processing contributes to secure cloud operations.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /verify-deposit

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized actions for verifying deposits.
ISO/IEC 27001	Yes	low	Secure verification of financial transactions.
CSA STAR	Yes	low	Authentication for financial transaction verification.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /virtual-account

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized users can access virtual account information.
ISO/IEC 27001	Yes	low	Access control protects sensitive financial information.
CSA STAR	Yes	low	Secure access to virtual account details.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /wallet-balance

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures users can only view their own wallet balances.
ISO/IEC 27001	Yes	low	Access control protects sensitive financial information.
CSA STAR	Yes	low	Secure access to wallet balance information.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /allocate-budget

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized users can allocate budget.
ISO/IEC 27001	Yes	low	Access control protects financial budget management.
CSA STAR	Yes	low	Secure allocation of financial resources.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /reclaim-budget

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized users can reclaim budget.
ISO/IEC 27001	Yes	low	Access control protects financial budget management.
CSA STAR	Yes	low	Secure reclamation of financial resources.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /distribute-to-creator

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized actions for distributing funds to creators.
ISO/IEC 27001	Yes	low	Secure financial distribution processes are managed through authenticated endpoints.
CSA STAR	Yes	low	Authentication for creator payments contributes to secure cloud operations.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /creator-withdraw

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized creators can initiate withdrawals.
ISO/IEC 27001	Yes	low	Access control protects financial withdrawal processes.
CSA STAR	Yes	low	Secure withdrawal of funds by creators.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /creator/payout-details

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures creators can only manage their own payout details.
ISO/IEC 27001	Yes	low	Access control protects sensitive financial payout information.
CSA STAR	Yes	low	Secure management of creator payout details.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /creator/payout-details

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures creators can only view their own payout details.
ISO/IEC 27001	Yes	low	Access control protects sensitive financial payout information.
CSA STAR	Yes	low	Secure access to creator payout details.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /creator/verify-payout-details

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized creators can verify their payout details.
ISO/IEC 27001	Yes	low	Access control protects sensitive financial payout information.
CSA STAR	Yes	low	Secure verification of creator payout details.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /creator/withdrawals

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures creators can only view their own withdrawal history.
ISO/IEC 27001	Yes	low	Access control protects sensitive financial withdrawal history.
CSA STAR	Yes	low	Secure access to creator withdrawal history.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /creator/notifications/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures creators can only access their own notifications.
ISO/IEC 27001	Yes	low	Access control protects notification data.
CSA STAR	Yes	low	Secure access to creator notifications.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /transactions//

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures users can only view their own transaction history.
ISO/IEC 27001	Yes	low	Access control protects sensitive financial transaction data.
CSA STAR	Yes	low	Secure access to transaction history.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /refund-campaign

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized users can request refunds for campaigns.
ISO/IEC 27001	Yes	low	Access control protects financial refund processes.
CSA STAR	Yes	low	Secure refund requests for campaigns.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /campaign-summary/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized users can access campaign summaries.
ISO/IEC 27001	Yes	low	Access control protects sensitive campaign summary data.
CSA STAR	Yes	low	Secure access to campaign summaries.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /calculate-earnings//

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures creators can only calculate their own earnings for a campaign.
ISO/IEC 27001	Yes	low	Access control protects sensitive financial calculation data.
CSA STAR	Yes	low	Secure calculation of creator earnings.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /bulk-distribute

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized actions for bulk distribution.
ISO/IEC 27001	Yes	low	Secure financial distribution processes are managed through authenticated endpoints.
CSA STAR	Yes	low	Authentication for bulk payments contributes to secure cloud operations.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /request-refund

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized users can request refunds.
ISO/IEC 27001	Yes	low	Access control protects financial refund processes.
CSA STAR	Yes	low	Secure refund requests.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /refund-requests

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures users can only view their own refund requests (or relevant ones based on role).
ISO/IEC 27001	Yes	low	Access control protects sensitive refund request data.
CSA STAR	Yes	low	Secure access to refund request information.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /admin/approve-refund

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized administrators can approve refunds.
ISO/IEC 27001	Yes	low	Access control protects financial approval processes.
CSA STAR	Yes	low	Secure administrative approval of refunds.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /admin/reject-refund

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized administrators can reject refunds.
ISO/IEC 27001	Yes	low	Access control protects financial rejection processes.
CSA STAR	Yes	low	Secure administrative rejection of refunds.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /refund-status/

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures users can only check the status of refunds they are authorized for.
ISO/IEC 27001	Yes	low	Access control protects sensitive refund status information.
CSA STAR	Yes	low	Secure access to refund status.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /admin/refund-audit-trail

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized administrators can access the refund audit trail.
ISO/IEC 27001	Yes	low	Access control protects sensitive audit trail information.
CSA STAR	Yes	low	Secure access to audit trails for financial operations.

Security Assessment Notes

CVSS Vector: N/A

References

Endpoint Path /creator/revert-withdrawal

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Authentication ensures only authorized users can revert withdrawals.
ISO/IEC 27001	Yes	low	Access control protects financial transaction modifications.
CSA STAR	Yes	low	Secure reversion of financial transactions.

Security Assessment Notes

CVSS Vector: N/A

References

METRICS SUMMARY

Total Findings: 4

Severity	Count
CRITICAL	1
HIGH	1
MEDIUM	1
LOW	1

BUSINESS RISK ADVICE

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

Eliminate Hardcoded Sensitive Data (Priority: Immediate)

Description: A sensitive JSON Web Token (JWT) is hardcoded directly into the `tasks.py` file, posing a critical security risk by exposing production secrets or dangerous examples.

Why it Matters: Hardcoded secrets allow attackers to bypass authentication, impersonate users, and achieve full system compromise, violating data confidentiality and integrity requirements of SOC 2, ISO/IEC 27001, and CSA STAR.

Recommended Actions:

- Immediately remove the hardcoded JWT token from `tasks.py:14`.
- Implement a secure secret management solution (e.g., environment variables, dedicated secret management service like AWS Secrets Manager or HashiCorp Vault) for all sensitive credentials, tokens, and keys.
- Rotate any tokens or keys that may have been exposed through the hardcoded value.

Expected Outcome: Sensitive tokens and keys are securely managed, preventing direct compromise through source code exposure and enhancing overall system integrity.

Disable Flask Debug Mode in Production (Priority: Immediate)

Description: The Flask application is configured to run with `debug=True` in a way that risks its activation in production environments, exposing the Werkzeug debugger.

Why it Matters: Enabling debug mode in production allows attackers to execute arbitrary Python code on the server, leading to full system compromise. This constitutes a severe security misconfiguration, impacting all compliance frameworks.

Recommended Actions:

- Modify `app.py:1872` to unconditionally set `debug=False` for production deployments.
- Configure a production-ready WSGI server (e.g., Gunicorn, uWSGI) to serve the Flask application, which inherently manages debug settings more securely.
- Utilize environment variables (e.g., `FLASK_ENV`) to conditionally enable debug mode only in development environments.

Expected Outcome: The production environment is protected from remote code execution vulnerabilities associated with debug mode, significantly reducing the attack surface.

Strengthen User Account Security Controls (Priority: Immediate)

Description: Endpoints for `/register`, `/login`, and `/request-password-reset` are identified as high-risk due to implied vulnerabilities that allow for unauthorized account creation or account takeover attempts.

Why it Matters: Without robust controls, these critical entry points are susceptible to brute-force attacks, account enumeration, and spam, leading to unauthorized access, account takeover, and system abuse. This directly impacts access control and user data integrity, critical for SOC 2, ISO/IEC 27001, and CSA STAR.

Recommended Actions:

- Implement rate limiting on `/register`, `/login`, and `/request-password-reset` to prevent brute-force and enumeration attacks.
- Integrate CAPTCHA or other anti-bot mechanisms to deter automated account creation and password reset abuse.
- Enforce strong password policies and implement account lockout mechanisms after multiple failed login attempts.
- Ensure password reset mechanisms utilize robust, expiring tokens and require multi-factor authentication where possible.

Expected Outcome: User account registration, login, and password reset processes are hardened against automated abuse, reducing the risk of unauthorized access and account compromise.

Enforce Request Timeouts for External API Calls (Priority: Short-Term)

Description: Multiple HTTP requests to external services (e.g., Cashfree API) lack defined timeout parameters, risking indefinite hanging and resource exhaustion.

Why it Matters: Uncontrolled external API calls can lead to application unresponsiveness, denial-of-service (DoS) conditions, and resource exhaustion, severely impacting application availability and reliability.

Recommended Actions:

- Add a `timeout` parameter to all `requests.post` and `requests.get` calls in `routes\payments.py` (e.g., `timeout=10` seconds, adjusted based on service expectations).
- Implement comprehensive error handling, specifically for `requests.exceptions.Timeout`, to gracefully manage unresponsive external services.
- Consider adopting a circuit breaker pattern for critical external dependencies to prevent cascading failures.

Expected Outcome: Application resilience and availability are improved by preventing indefinite hangs, ensuring graceful degradation and efficient resource management during external service outages or delays.

Standardize Non-Verbose Error Responses (Priority: Short-Term)

Description: The application returns raw exception messages, including `str(e)`, directly in API responses across numerous endpoints, potentially exposing internal details.

Why it Matters: Verbose error messages can inadvertently reveal sensitive information about the application's internal architecture, database schema, or file paths, which can be leveraged by attackers for targeted exploitation and reconnaissance.

Recommended Actions:

- Replace all instances of `str(e)` in `jsonify` responses that are returned to clients with generic, user-friendly error messages (e.g., 'An unexpected error occurred.').
- Implement a centralized error handling mechanism for the Flask application to ensure all unhandled exceptions return a standardized, non-verbose response.
- Ensure detailed exception information is logged internally on the server for debugging purposes, but never exposed to end-users.

Expected Outcome: Information disclosure is minimized, making it harder for attackers to gather intelligence about the application's internal workings and reducing the risk of further exploitation.

Implement Granular Authorization Checks (Priority: Mid-Term)

Description: Review current authentication and authorization logic, particularly for endpoints like `/api/campaigns` (GET) and `/api/campaigns/` (GET), which are currently unauthenticated and flagged as medium risk.

Why it Matters: Inadequate authorization can lead to unauthorized users accessing or modifying data they should not have access to (horizontal or vertical privilege escalation), compromising data confidentiality and integrity. This is a critical component of access control for SOC 2, ISO/IEC 27001, and CSA STAR compliance.

Recommended Actions:

- Thoroughly review all endpoints to confirm the intended access level (public vs. authenticated) and implement authorization logic to verify that the requesting user has the necessary permissions for the requested resource.
- For public endpoints like `/api/campaigns`, explicitly confirm that the data exposed is non-sensitive and intended for public viewing.
- Integrate a robust role-based access control (RBAC) mechanism where different user roles have distinct permissions.

Expected Outcome: Fine-grained access control is enforced across the application, preventing unauthorized data access, modification, and privilege escalation.

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

Description: A proactive measure to defend against common web vulnerabilities, ensuring all user-supplied data is safe before processing and display.

Why it Matters: Lack of proper input validation and output encoding leads to vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), and other injection attacks, compromising data integrity, confidentiality, and potentially leading to full system compromise. This directly addresses multiple OWASP Top 10 risks.

Recommended Actions:

- Implement strict, allow-list based server-side input validation for all user-supplied data, ensuring it conforms to expected formats, types, and lengths.
- Apply context-sensitive output encoding (e.g., HTML entity encoding, URL encoding, JavaScript encoding) to all user-controlled data before it is rendered in web pages or API responses.

Expected Outcome: The application is significantly hardened against injection vulnerabilities and XSS, protecting backend systems and client-side users from malicious input.

Integrate Security into SDLC (Priority: Long-Term)

Description: Establish a comprehensive Secure Software Development Lifecycle (SSDLC) to prevent the introduction of new vulnerabilities and systematically improve the application's security posture.

Why it Matters: Shifting security left in the development process significantly reduces the cost and effort of remediation, fosters a security-aware culture, and ensures continuous compliance with regulatory requirements (SOC 2, ISO/IEC 27001, CSA STAR).

Recommended Actions:

- Mandate regular security awareness training for all developers and engineers.
- Integrate automated security testing tools (SAST, DAST, SCA) into the CI/CD pipeline to catch vulnerabilities early.
- Perform threat modeling for new features and significant architectural changes.
- Conduct periodic manual security assessments, such as penetration testing and code reviews.

Expected Outcome: A proactive, systematic approach to security reduces the likelihood of future vulnerabilities, improves code quality, and embeds security as a core component of the development culture.