SECURITY ANALYSIS REPORT

Security Analysis Report

Provider:

Client: {'name': 'Client Name', 'address': '456 Client Avenue, Suite 789, App City, 12345'}

Scan ID: ca3747e4-079a-439b-bdc8-06c362557e75

Date: 2026-02-05 15:05:51

Version: 1.0.0

CONFIDENTIAL

TABLE OF CONTENTS

1 Document Control 4

1.1 Team 4

1.2 List of Changes 4

2 Executive Summary 5

2.1 Overview 5

2.2 Identified Vulnerabilities 5

3 Methodology 7

3.1 Objective 7

3.2 Scope 7

3.3 User Accounts and Permissions 8

4 Findings 9

C1 Hardcoded JWT Token --

H1 Flask Debug Mode Enabled --

L1 Verbose Error Messages Exposing Internal Details --

5 Endpoint Security Analysis --

/register --

/login --

/verify-instagram --

/verify-instagram/ --

/request-password-reset --

/api/brand/campaigns --

/api/brand/campaigns --

/api/campaigns --

/api/campaigns/ --

/api/creator/your-campaigns --

/api/creator/submit-clip --

/api/creator/campaign-clips --

/api/creator/accepted-clip-details/ --

/api/brand/campaigns/ --

/api/creator/clip/ --

/api/admin/campaigns --

/api/admin/clip/ --

/api/admin/clip/ --

/api/creator/profile --

/api/creator/profile --
/api/brand/campaigns//image --
/api/brand/campaigns//budget --
/api/brand/campaigns//requirements --
/api/brand/campaigns//status --
/api/brand/campaigns//view_threshold --
/api/brand/campaigns//deadline --
/api/brand/campaigns//pending-payouts --
/api/brand/profile --
/api/brand/profile --
/api/admin/clip//view-count --
/api/admin/campaign//update-views --
/api/admin/analytics/campaign-performance/ --
/api/auth/google-sync --
/refresh --
/logout --
/api/health --
/create-deposit-order --
/verify-deposit --
/virtual-account --
/wallet-balance --
/allocate-budget --
/reclaim-budget --
/distribute-to-creator --
/creator-withdraw --
/creator/payout-details --
/creator/payout-details --
/creator/verify-payout-details --
/creator/withdrawals --
/creator/notifications/ --
/transactions// --
/refund-campaign --
/campaign-summary/ --
/calculate-earnings// --
/bulk-distribute --
/request-refund --
/refund-requests --
/admin/approve-refund --
/admin/reject-refund --

/refund-status/ --

/admin/refund-audit-trail --

/creator/revert-withdrawal --

6 Metrics Summary --

7 Disclaimer --

8 Appendix --

8.1 Static Appendix Section --

8.2 Tool Output --

EXECUTIVE SUMMARY

This security assessment report summarizes the findings from an analysis of the provided codebase. The review identified a critical hardcoded JWT token, a high-severity configuration issue with Flask debug mode enabled, and numerous instances of verbose error messages exposing internal system details. Addressing these vulnerabilities is crucial to prevent unauthorized access, remote code execution, and information leakage, thereby enhancing the overall security posture of the application.

Identified Vulnerabilities

ID	Title	CVSS	Page
H1	Flask Debug Mode Enabled	8.8	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. Findings within virtual environment directories (e.g., `venv/`) were generally triaged as false positives if they represented standard library or third-party package functionality not directly controlled by the application's unique business logic.

Systems in Scope

Name	IP
Application Source Code	

User Accounts

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

FINDINGS

C1 – Hardcoded JWT Token

Severity:	Critical
CVSS Score:	9.8
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Target:	tasks.py

Overview

A JSON Web Token (JWT) has been directly embedded within the `tasks.py` file. Hardcoding secrets, even for testing purposes, poses a severe security risk as it can lead to unauthorized access if the code is committed to a repository or otherwise exposed.

Details

The `token` variable on line 14 of `tasks.py` contains a full JWT string. While the surrounding code suggests it's for local testing using an environment variable `secret` for verification, the presence of the token itself in the source code is problematic. An attacker gaining access to the source code could potentially extract this token and use it if it's still valid or similar tokens are used in other environments. This bypasses proper secret management practices and increases the attack surface.

Evidence

- **Vulnerable Code:** tasks.py:14

References

- https://owasp.org/www-community/vulnerabilities/Hardcoded_credentials
- https://cheatsheetseries.owasp.org/cheatsheets/Hardcoded_Credentials_Cheat_Sheet.html

Recommendation

- Remove the hardcoded JWT token from `tasks.py`. - If a test token is required, ensure it is generated dynamically or loaded securely from an environment variable or secure configuration management system, and that it is not a token that could ever grant access to sensitive data or functions in any environment. - Implement robust secret management practices using environment variables, cloud key management services, or secure vaults. - Educate developers on the risks of hardcoding any sensitive information.

H1 – Flask Debug Mode Enabled

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:	app.py

Overview

The Flask application is configured to run with debug mode enabled, as indicated by `debug=True` in `app.run()`. This configuration is highly dangerous for production environments as it exposes a debugger interface that can allow remote code execution and sensitive information disclosure.

Details

When `debug=True`, Flask activates its interactive debugger. If a traceback occurs in the application, the debugger is accessible via the web interface. This debugger reveals sensitive information about the application's internal state, environment variables, and local variables, aiding an attacker in crafting further exploits. In some configurations or older versions, it could even allow arbitrary code execution. The `use_reloader=True` also consumes more resources and can be unstable in production.

Evidence

- **Vulnerable Code:** app.py:1872

References

- https://flask.palletsprojects.com/en/2.3.x/deploying/#debugging-problems
- https://nvd.nist.gov/vuln/detail/CVE-2016-10497

Recommendation

- **NEVER** enable `debug=True` in production environments. Ensure this setting is conditionally enabled only for development (e.g., `if os.getenv('FLASK_ENV') == 'development': app.run(debug=True)`). - For production deployments, use a production-ready WSGI server (e.g., Gunicorn, uWSGI) instead of `app.run()`. - Implement robust error logging and monitoring instead of relying on the interactive debugger.

L1 – Verbose Error Messages Exposing Internal Details

Severity:	Low
CVSS Score:	3.1
CVSS Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Target:	Multiple API endpoints

Overview

Several API endpoints return raw exception messages (`str(e)`) directly in their JSON error responses. This practice exposes internal server details, which can provide valuable information to attackers.

Details

When an unhandled exception occurs within the Flask routes, the application catches the `Exception` and returns a generic error message, but includes `str(e)` in the response. This `str(e)` can contain stack traces, database query failures, internal file paths, module names, variable values, or other implementation-specific information. Such details can help an attacker understand the application's architecture, identify vulnerable libraries, or craft more targeted attacks (e.g., SQL injection, path traversal, RCE). While not directly exploitable, it significantly lowers the bar for subsequent attacks.

Evidence

- **Vulnerable Code (Example 1):** app.py:117
- **Vulnerable Code (Example 2):** app.py:187
- **Vulnerable Code (Example 3):** app.py:210
- **Vulnerable Code (Example 4):** app.py:243
- **Vulnerable Code (Example 5):** app.py:288
- **Vulnerable Code (Example 6):** app.py:326
- **Vulnerable Code (Example 7):** app.py:385
- **Vulnerable Code (Example 8):** app.py:491
- **Vulnerable Code (Example 9):** app.py:579
- **Vulnerable Code (Example 10):** app.py:653
- **Vulnerable Code (Example 11):** app.py:718
- **Vulnerable Code (Example 12):** app.py:754
- **Vulnerable Code (Example 13):** app.py:829
- **Vulnerable Code (Example 14):** app.py:884
- **Vulnerable Code (Example 15):** app.py:931
- **Vulnerable Code (Example 16):** app.py:1022
- **Vulnerable Code (Example 17):** app.py:1075
- **Vulnerable Code (Example 18):** app.py:1109
- **Vulnerable Code (Example 19):** app.py:1155
- **Vulnerable Code (Example 20):** app.py:1194
- **Vulnerable Code (Example 21):** app.py:1226

- **Vulnerable Code (Example 22):** app.py:1255
- **Vulnerable Code (Example 23):** app.py:1286
- **Vulnerable Code (Example 24):** app.py:1317
- **Vulnerable Code (Example 25):** app.py:1354
- **Vulnerable Code (Example 26):** app.py:1450
- **Vulnerable Code (Example 27):** app.py:1478
- **Vulnerable Code (Example 28):** app.py:1509
- **Vulnerable Code (Example 29):** app.py:1576
- **Vulnerable Code (Example 30):** app.py:1631
- **Vulnerable Code (Example 31):** app.py:1729
- **Vulnerable Code (Example 32):** app.py:1756
- **Vulnerable Code (Example 33):** app.py:1808
- **Vulnerable Code (Example 34):** app.py:1812
- **Vulnerable Code (Example 35):** routes\payments.py:115
- **Vulnerable Code (Example 36):** routes\payments.py:186
- **Vulnerable Code (Example 37):** routes\payments.py:343
- **Vulnerable Code (Example 38):** routes\payments.py:430
- **Vulnerable Code (Example 39):** routes\payments.py:554
- **Vulnerable Code (Example 40):** routes\payments.py:729
- **Vulnerable Code (Example 41):** routes\payments.py:817
- **Vulnerable Code (Example 42):** routes\payments.py:867
- **Vulnerable Code (Example 43):** routes\payments.py:927
- **Vulnerable Code (Example 44):** routes\payments.py:989
- **Vulnerable Code (Example 45):** routes\payments.py:1023
- **Vulnerable Code (Example 46):** routes\payments.py:1105
- **Vulnerable Code (Example 47):** routes\payments.py:1197
- **Vulnerable Code (Example 48):** routes\payments.py:1264
- **Vulnerable Code (Example 49):** routes\payments.py:1358
- **Vulnerable Code (Example 50):** routes\payments.py:1529
- **Vulnerable Code (Example 51):** routes\payments.py:1623
- **Vulnerable Code (Example 52):** routes\payments.py:1690
- **Vulnerable Code (Example 53):** routes\payments.py:1804
- **Vulnerable Code (Example 54):** routes\payments.py:1865
- **Vulnerable Code (Example 55):** routes\payments.py:1934
- **Vulnerable Code (Example 56):** routes\payments.py:2014
- **Vulnerable Code (Example 57):** routes\payments.py:2088

References

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

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

Recommendation

- Avoid exposing raw exception messages or stack traces to end-users. - Implement custom error handling that provides generic, user-friendly error messages (e.g., "An unexpected error occurred. Please try again later."). - Log detailed exception information securely on the server side for debugging and monitoring purposes. - Ensure that sensitive data is never included in error messages, even in development environments, as it can still be leaked.

ENDPOINT SECURITY ANALYSIS

This section provides a detailed security-oriented analysis of the identified API endpoints, including authentication mechanisms, data handling characteristics, potential security risks, and regulatory compliance considerations.

Endpoint Path	/register
HTTP Methods	POST
Source Location	: 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 register endpoint, allowing unauthorized user creation.

  Potential Attack Scenario:

  An attacker could create multiple fake user accounts to disrupt the service or perform other malicious activities.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of authentication on user registration can lead to unauthorized access and data integrity issues, violating trust service criteria.
ISO/IEC 27001	Yes	high	Absence of access control for registration bypasses security policies and potentially compromises user data.
CSA STAR	Yes	high	Insecure registration process can lead to account takeover and unauthorized data access, impacting the security posture.

Security Assessment Notes

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

References

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

Endpoint Path	/login
HTTP Methods	POST
Source Location	: 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, potentially allowing unauthorized access to user accounts.

  Potential Attack Scenario:

  An attacker could bypass authentication and gain access to user accounts without valid credentials.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of authentication on login is a severe security vulnerability, directly impacting the integrity and confidentiality of user data.
ISO/IEC 27001	Yes	high	Absence of authentication for login is a critical failure in access control, leading to unauthorized access.
CSA STAR	Yes	high	Bypassing login authentication exposes user accounts and sensitive data, leading to potential breaches.

Security Assessment Notes

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

References

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

Endpoint Path	/verify-instagram
HTTP Methods	POST
Source Location	: 192
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	This endpoint does not appear to handle sensitive data or have direct compliance implications based on the provided information.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/verify-instagram/
HTTP Methods	POST
Source Location	: 192
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	This endpoint does not appear to handle sensitive data or have direct compliance implications based on the provided information.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/request-password-reset
HTTP Methods	POST
Source Location	: 224
Authentication Required	No
Risk Severity	High
CVSS Score	7.5

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (medium): Authentication is missing for password reset request, potentially allowing attackers to initiate resets for other users.

  Potential Attack Scenario:

  An attacker could flood the system with password reset requests for various users, causing denial of service or facilitating account takeover attempts.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Lack of authentication on password reset can lead to unauthorized access attempts and compromise account security.
ISO/IEC 27001	Yes	medium	Weak access control for password reset functionality can be exploited to compromise user accounts.
CSA STAR	Yes	medium	Insecure password reset mechanisms can lead to account compromise and unauthorized access.

Security Assessment Notes

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

References

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

Endpoint Path	/api/brand/campaigns
HTTP Methods	POST
Source Location	: 248
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/brand/campaigns
HTTP Methods	GET
Source Location	: 292
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/campaigns
HTTP Methods	GET
Source Location	: 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, potentially exposing campaign data to unauthorized users.

  Potential Attack Scenario:

  An attacker could access a list of all campaigns, potentially gaining insights into ongoing marketing efforts or sensitive campaign details.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Exposing campaign data without authentication can lead to unauthorized disclosure of information.
ISO/IEC 27001	Yes	medium	Lack of access control for retrieving campaign data can lead to information leakage.
CSA STAR	Yes	medium	Unauthorized access to campaign data can compromise business intelligence and competitive advantage.

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/
HTTP Methods	GET
Source Location	: 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, potentially exposing campaign data to unauthorized users.

  Potential Attack Scenario:

  An attacker could enumerate campaign IDs and access details of specific campaigns they are not authorized to view.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Exposing campaign data without authentication can lead to unauthorized disclosure of information.
ISO/IEC 27001	Yes	medium	Lack of access control for retrieving specific campaign data can lead to information leakage.
CSA STAR	Yes	medium	Unauthorized access to campaign data can compromise business intelligence and competitive advantage.

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
HTTP Methods	GET
Source Location	: 495
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/creator/submit-clip
HTTP Methods	POST
Source Location	: 583
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/creator/campaign-clips
HTTP Methods	GET
Source Location	: 657
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/creator/accepted-clip-details/
HTTP Methods	GET
Source Location	: 722
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/brand/campaigns/
HTTP Methods	DELETE, OPTIONS
Source Location	: 761
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/creator/clip/
HTTP Methods	DELETE, OPTIONS
Source Location	: 833
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/admin/campaigns
HTTP Methods	GET
Source Location	: 888
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/admin/clip/
HTTP Methods	PUT
Source Location	: 935
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/admin/clip/
HTTP Methods	DELETE, OPTIONS
Source Location	: 1026
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/creator/profile
HTTP Methods	GET
Source Location	: 1079
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/creator/profile
HTTP Methods	PUT
Source Location	: 1113
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/brand/campaigns//image
HTTP Methods	PUT, OPTIONS
Source Location	: 1159
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/brand/campaigns//budget
HTTP Methods	PUT
Source Location	: 1198
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/brand/campaigns//requirements
HTTP Methods	PUT
Source Location	: 1230
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/brand/campaigns//status
HTTP Methods	PUT
Source Location	: 1259
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/brand/campaigns//view_threshold
HTTP Methods	PUT
Source Location	: 1290
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/brand/campaigns//deadline
HTTP Methods	PUT
Source Location	: 1321
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/brand/campaigns//pending-payouts
HTTP Methods	GET
Source Location	: 1358
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/brand/profile
HTTP Methods	GET
Source Location	: 1455
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/brand/profile
HTTP Methods	PUT
Source Location	: 1482
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/admin/clip//view-count
HTTP Methods	PUT
Source Location	: 1514
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/admin/campaign//update-views
HTTP Methods	PUT
Source Location	: 1580
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/admin/analytics/campaign-performance/
HTTP Methods	GET
Source Location	: 1635
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/auth/google-sync
HTTP Methods	POST
Source Location	: 1738
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/refresh
HTTP Methods	POST
Source Location	: 1816
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/logout
HTTP Methods	DELETE
Source Location	: 1832
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	No specific risks identified that directly violate SOC 2 controls based on the provided data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/api/health
HTTP Methods	GET
Source Location	: 1843
Authentication Required	No
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (low): Authentication is missing for the health check endpoint. While generally considered safe, it's good practice to secure all endpoints.

  Potential Attack Scenario:

  An attacker could potentially use this endpoint to probe for system availability information, though it typically poses a low risk.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	No	low	Health check endpoints are typically not subject to strict compliance requirements unless they expose sensitive operational data.
ISO/IEC 27001	No	low	No specific risks identified that directly violate ISO 27001 controls based on the provided data.
CSA STAR	No	low	No specific risks identified that directly violate CSA STAR controls based on the provided data.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/creator/withdrawals
HTTP Methods	GET
Source Location	: 933
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/creator/notifications/
HTTP Methods	GET
Source Location	: 995
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

Endpoint Path	/transactions//
HTTP Methods	GET
Source Location	: 1030
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	0.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

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

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint requires authentication, which is a baseline security control.
ISO/IEC 27001	Yes	low	Endpoint has authentication, aligning with access control requirements.
CSA STAR	Yes	low	Authentication is present, contributing to a secure cloud environment.

Security Assessment Notes

CVSS Vector: None

References

METRICS SUMMARY

Total Findings: 3

Severity	Count
CRITICAL	**1**
HIGH	**1**
MEDIUM	**0**
LOW	**28**

DISCLAIMER

This report is generated by an automated security analysis tool.

BUSINESS RISK ADVICE

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

No specific business risk advice was generated for this report.