

SECURITY ANALYSIS REPORT

Security Analysis Report

Provider:

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

Scan ID: ddead94c-245a-4008-8ac9-4be5cb3ce20e

Date: 2026-02-05 06:43:58

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
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

Identified Vulnerabilities

ID	Title	CVSS	Page
----	-------	------	------

METHODOLOGY

Introduction

Objective

Scope

Systems in Scope

No systems explicitly defined.

User Accounts

FINDINGS

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	None : 73
Authentication Required	No
Risk Severity	Critical
CVSS Score	9.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

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

Potential Attack Scenario:

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

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of authentication on registration can lead to unauthorized account creation, violating principles of access control and integrity.
ISO/IEC 27001	Yes	high	Missing authentication on user registration undermines the principle of verifying user identity and controlling access.
CSA STAR	Yes	high	Insecure registration processes can lead to account enumeration and abuse, impacting the security and availability of cloud services.

Security Assessment Notes

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

References

Endpoint Path	/login
HTTP Methods	POST
Source Location	None : 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 attempt brute-force attacks on login credentials or exploit vulnerabilities if authentication is not properly enforced.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Insecure login mechanisms can lead to unauthorized access, compromising confidentiality and integrity.
ISO/IEC 27001	Yes	high	Weak or missing authentication on login allows unauthorized access, failing to meet the control objective for access control.
CSA STAR	Yes	high	Inadequate authentication for login exposes the system to brute-force attacks and credential stuffing, impacting security and availability.

Security Assessment Notes

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

References

Endpoint Path	/verify-instagram
HTTP Methods	POST
Source Location	None : 192
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

Security Assessment Notes

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

References

Endpoint Path	/verify-instagram/
HTTP Methods	POST
Source Location	None : 192
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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, 194, 191, 191, 193, 193, 194, 194.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

Security Assessment Notes

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

References

Endpoint Path	/request-password-reset
HTTP Methods	POST
Source Location	None : 224
Authentication Required	No
Risk Severity	Critical
CVSS Score	8.1

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 flood the system with password reset requests for other users, leading to denial of service or facilitating social engineering attacks.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of authentication for password resets can lead to account takeover attempts and unauthorized access.
ISO/IEC 27001	Yes	high	Inadequate controls for password reset requests can lead to unauthorized access and compromise of user accounts.
CSA STAR	Yes	high	Vulnerabilities in password reset mechanisms can be exploited for account hijacking and denial of service.

Security Assessment Notes

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

References

Endpoint Path	/api/brand/campaigns
HTTP Methods	POST
Source Location	None : 248
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/brand/campaigns
HTTP Methods	GET
Source Location	None : 292
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	5.3

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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

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

Endpoint Path	/api/campaigns
HTTP Methods	GET
Source Location	None : 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 the endpoint that retrieves all campaigns.

Potential Attack Scenario:

An unauthenticated user could access sensitive campaign data, potentially leading to information disclosure.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Exposing campaign data without proper authentication could violate principles of confidentiality and lead to unauthorized access.
ISO/IEC 27001	Yes	medium	Failure to enforce access control on sensitive campaign data violates the confidentiality principle.
CSA STAR	Yes	medium	Inadequate access control for campaign data can lead to information leakage and compromise of service integrity.

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

Endpoint Path	/api/campaigns/
HTTP Methods	GET
Source Location	None : 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 the endpoint that retrieves a specific campaign by ID.

Potential Attack Scenario:

An unauthenticated user could access sensitive campaign details, leading to information disclosure.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Exposing campaign data without proper authentication could violate principles of confidentiality and lead to unauthorized access.
ISO/IEC 27001	Yes	medium	Failure to enforce access control on sensitive campaign data violates the confidentiality principle.
CSA STAR	Yes	medium	Inadequate access control for campaign data can lead to information leakage and compromise of service integrity.

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

Endpoint Path	/api/creator/your-campaigns
HTTP Methods	GET
Source Location	None : 495
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

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

Endpoint Path	/api/creator/submit-clip
HTTP Methods	POST
Source Location	None : 583
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/creator/campaign-clips
HTTP Methods	GET
Source Location	None : 657
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

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

Endpoint Path	/api/creator/accepted-clip-details/
HTTP Methods	GET
Source Location	None : 722
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

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

Endpoint Path	/api/brand/campaigns/
HTTP Methods	DELETE, OPTIONS
Source Location	None : 761
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	7.5

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, 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/creator/clip/
HTTP Methods	DELETE, OPTIONS
Source Location	None : 833
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	7.5

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, 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/admin/campaigns
HTTP Methods	GET
Source Location	None : 888
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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, 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

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

Endpoint Path	/api/admin/clip/
HTTP Methods	PUT
Source Location	None : 935
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/admin/clip/
HTTP Methods	DELETE, OPTIONS
Source Location	None : 1026
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	7.5

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.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/creator/profile
HTTP Methods	GET
Source Location	None : 1079
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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, 1080, 1080, 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

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

Endpoint Path	/api/creator/profile
HTTP Methods	PUT
Source Location	None : 1113
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/brand/campaigns//image
HTTP Methods	PUT, OPTIONS
Source Location	None : 1159
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1158, 1158, 1159, 1159, 1159, 1165, 1165, 1166, 1166, 1170, 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/brand/campaigns//budget
HTTP Methods	PUT
Source Location	None : 1198
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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, 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/brand/campaigns//requirements
HTTP Methods	PUT
Source Location	None : 1230
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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, 1231, 1235, 1235, 1229, 1229, 1231, 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/brand/campaigns//status
HTTP Methods	PUT
Source Location	None : 1259
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/brand/campaigns//view_threshold
HTTP Methods	PUT
Source Location	None : 1290
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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, 1291, 1295, 1295, 1289, 1289, 1291, 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/brand/campaigns//deadline
HTTP Methods	PUT
Source Location	None : 1321
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/brand/campaigns//pending-payouts
HTTP Methods	GET
Source Location	None : 1358
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

Authentication Analysis

This endpoint enforces authentication using a token-based mechanism. Authentication checks were detected at the following code locations: 1357, 1357, 1358, 1358, 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

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

Endpoint Path	/api/brand/profile
HTTP Methods	GET
Source Location	None : 1455
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

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

Endpoint Path	/api/brand/profile
HTTP Methods	PUT
Source Location	None : 1482
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/admin/clip//view-count
HTTP Methods	PUT
Source Location	None : 1514
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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, 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/admin/campaign//update-views
HTTP Methods	PUT
Source Location	None : 1580
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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, 1591, 1592, 1592, 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/admin/analytics/campaign-performance/
HTTP Methods	GET
Source Location	None : 1635
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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, 1640, 1641, 1641, 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

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

Endpoint Path	/api/auth/google-sync
HTTP Methods	POST
Source Location	None : 1738
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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, 1745, 1748, 1748, 1761, 1761, 1737, 1737, 1739, 1744, 1744, 1745, 1745, 1748, 1748, 1772, 1772, 1778, 1737, 1737, 1744, 1744, 1745, 1745, 1772, 1772, 1778, 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/refresh
HTTP Methods	POST
Source Location	None : 1816
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/logout
HTTP Methods	DELETE
Source Location	None : 1832
Authentication Required	Yes (token)
Risk Severity	Low
CVSS Score	3.1

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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/api/health
HTTP Methods	GET
Source Location	None : 1843
Authentication Required	No
Risk Severity	Low
CVSS Score	1.0

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	No	low	No specific compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/create-deposit-order
HTTP Methods	POST
Source Location	None : 49
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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, 48, 50, 50, 55, 55, 48, 48, 50, 50, 55, 55.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

Security Assessment Notes

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

References

Endpoint Path	/verify-deposit
HTTP Methods	POST
Source Location	None : 121
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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, 127, 120, 120, 122, 122, 127, 127, 127, 120, 120, 122, 122, 127.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

Security Assessment Notes

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

References

Endpoint Path	/virtual-account
HTTP Methods	GET
Source Location	None : 192
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

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

Endpoint Path	/wallet-balance
HTTP Methods	GET
Source Location	None : 243
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

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

Endpoint Path	/allocate-budget
HTTP Methods	POST
Source Location	None : 269
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

Security Assessment Notes

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

References

Endpoint Path	/reclaim-budget
HTTP Methods	POST
Source Location	None : 349
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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, 348, 350, 350, 355, 355, 348, 348, 350, 350, 355, 355.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

Security Assessment Notes

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

References

Endpoint Path	/distribute-to-creator
HTTP Methods	POST
Source Location	None : 436
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

Security Assessment Notes

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

References

Endpoint Path	/creator-withdraw
HTTP Methods	POST
Source Location	None : 560
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

Security Assessment Notes

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

References

Endpoint Path	/creator/payout-details
HTTP Methods	POST, PUT
Source Location	None : 735
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

Security Assessment Notes

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

References

Endpoint Path	/creator/payout-details
HTTP Methods	GET
Source Location	None : 823
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

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

Endpoint Path	/creator/verify-payout-details
HTTP Methods	POST
Source Location	None : 873
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

Security Assessment Notes

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

References

Endpoint Path	/creator/withdrawals
HTTP Methods	GET
Source Location	None : 933
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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, 940, 940, 945, 945.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

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

Endpoint Path	/creator/notifications/
HTTP Methods	GET
Source Location	None : 995
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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, 994, 994, 999, 999, 1000, 1000, 1002, 1002, 1000, 1000, 1002, 1002, 1002, 1002, 1002, 1002.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

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

Endpoint Path	/transactions//
HTTP Methods	GET
Source Location	None : 1030
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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, 1035, 1038, 1042, 1038, 1042.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

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

Endpoint Path	/refund-campaign
HTTP Methods	POST
Source Location	None : 1110
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

Security Assessment Notes

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

References

Endpoint Path	/campaign-summary/
HTTP Methods	GET
Source Location	None : 1203
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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, 1217, 1202, 1202, 1215, 1215, 1217, 1217, 1202, 1202, 1215, 1215, 1217.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

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

Endpoint Path	/calculate-earnings//
HTTP Methods	GET
Source Location	None : 1270
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

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

Endpoint Path	/bulk-distribute
HTTP Methods	POST
Source Location	None : 1364
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/request-refund
HTTP Methods	POST
Source Location	None : 1535
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

Security Assessment Notes

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

References

Endpoint Path	/refund-requests
HTTP Methods	GET
Source Location	None : 1629
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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, 1636, 1636, 1641, 1641.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

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

Endpoint Path	/admin/approve-refund
HTTP Methods	POST
Source Location	None : 1696
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

Security Assessment Notes

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

References

Endpoint Path	/admin/reject-refund
HTTP Methods	POST
Source Location	None : 1810
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

Endpoint Path	/refund-status/
HTTP Methods	GET
Source Location	None : 1871
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

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.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

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

Endpoint Path	/admin/refund-audit-trail
HTTP Methods	GET
Source Location	None : 1940
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	5.3

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

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

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

Endpoint Path	/creator/revert-withdrawal
HTTP Methods	POST
Source Location	None : 2019
Authentication Required	Yes (token)
Risk Severity	Medium
CVSS Score	6.5

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.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains 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 compliance mappings identified for this endpoint based on provided information.
ISO/IEC 27001	No	low	No specific compliance mappings identified for this endpoint based on provided information.
CSA STAR	No	low	No specific compliance mappings identified for this endpoint based on provided information.

Security Assessment Notes

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

References

METRICS SUMMARY

Total Findings: 63

Severity	Count
Informational	63

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.

Enforce Authentication and Rate Limiting on Public Endpoints (Priority: Immediate)

Description: The `/register`, `/login`, and `/request-password-reset` endpoints are critically exposed due to missing authentication and rate-limiting. This allows unconstrained access and potential automated abuse.

Why it Matters: Unauthenticated access to these core user management functions creates severe risks for account enumeration, brute-force attacks, spam registration, and denial of service. This violates fundamental access control and integrity principles required by SOC 2, ISO/IEC 27001, and CSA STAR.

Recommended Actions:

- Implement robust, distributed rate-limiting for `/register`, `/login`, and `/request-password-reset` to prevent automated attacks (e.g., IP-based limits, CAPTCHA integration).
- Ensure strong password policies (complexity, length, entropy) are enforced server-side for `/register` and `/login`.
- For `/request-password-reset`, implement token-based, single-use, time-limited reset links, and provide generic success messages to prevent user enumeration.
- Review the necessity of `/register` being completely public; consider alternative secure user onboarding methods if applicable.

Expected Outcome: Critical reduction in automated account abuse, brute-force login attempts, and unauthorized password resets. Improved platform resilience and compliance with core security controls.

Harden JWT Token Implementation and Lifecycle Management (Priority: Short-Term)

Description: Numerous endpoints across the application and payments module rely on JWTs for authentication. While JWT usage is detected, the scan does not detail the robustness of their implementation, indicating a potential area for hardening.

Why it Matters: Improper JWT handling, such as weak secret keys, lack of signature/expiration validation, or insufficient revocation mechanisms, can lead to unauthorized access, session hijacking, and privilege escalation. This directly impacts confidentiality and integrity.

Recommended Actions:

- Verify that JWTs are signed with strong, cryptographically secure secrets (e.g., HMAC-SHA256 or better) that are securely stored (e.g., in environment variables, a secrets management service) and rotated regularly.
- Implement comprehensive server-side validation for all incoming JWTs, checking signature integrity, expiration, issuer, audience, and 'not before' claims.
- Establish and enforce a robust JWT revocation mechanism (e.g., a blacklist/denylist service) for logouts, password changes, or suspected token compromise.
- Ensure all JWT transmission occurs exclusively over HTTPS to prevent interception and tampering.
- Avoid embedding sensitive or excessive user data in JWT payloads; prefer minimal identifiers and fetch necessary data from secure backend sources.

Expected Outcome: Enhanced session security, prevention of unauthorized access through compromised or forged tokens, and improved data confidentiality during authenticated user interactions.

Implement Strict Object-Level Authorization Checks (Priority: Short-Term)

Description: Many authenticated endpoints accept resource IDs (e.g., `campaign_id`, `clip_id`, `user_id`, `refund_id`) in their paths, indicating potential for Broken Access Control if not properly validated. The LLM's 'medium' severity on authenticated GET/POST/PUT endpoints suggests a general concern for unauthorized data access.

Why it Matters: Absence of thorough object-level authorization (OLA) can lead to Horizontal Privilege Escalation (users accessing other users' data) or Vertical Privilege Escalation (users accessing privileged functions). This is a critical OWASP Top 10 vulnerability (Broken Access Control) with direct compliance implications for data confidentiality.

Recommended Actions:

- Enforce granular authorization checks on every API endpoint that accesses specific resources, ensuring the authenticated user (identified from their JWT) is authorized to access the requested resource.
- Verify that the user's role and ownership attributes explicitly match the resource's owner or that they possess the necessary permissions for the requested action (e.g., only a brand can modify its own campaign).
- Implement a centralized authorization library or service to consistently apply access control logic across all relevant endpoints.
- Conduct a thorough manual review and penetration testing focused on IDOR (Insecure Direct Object References) and privilege escalation across all authenticated and resource-specific endpoints.
- Map defined user roles (e.g., 'brand', 'creator', 'admin') to specific API endpoint permissions and enforce these mappings rigorously.

Expected Outcome: Elimination of unauthorized data access and manipulation across all resource-specific endpoints, ensuring data integrity and compliance with 'need-to-know' access principles.

Standardize and Implement Comprehensive Input Validation (Priority: Mid-Term)

Description: The presence of generic 'body' fields in multiple request payloads implies diverse and potentially complex input structures. Without explicit findings, the robustness of input validation cannot be guaranteed, leaving the application vulnerable to various injection attacks.

Why it Matters: Lack of strict input validation allows attackers to inject malicious payloads (e.g., SQL injection, Cross-Site Scripting (XSS), command injection) or submit malformed data that can lead to unexpected application behavior, data corruption, or denial of service. This is a primary concern in the OWASP Top 10.

Recommended Actions:

- Implement strict, whitelist-based input validation for all parameters received by the API (path, query, and request body).
- Validate all user-supplied data against expected data types, formats, lengths, and acceptable character sets.
- Utilize parameterized queries or Object-Relational Mappers (ORMs) consistently across the application to prevent SQL injection vulnerabilities.
- Ensure proper output encoding is applied to all user-controlled data before it is rendered back to a client (e.g., HTML encoding for web pages, JSON encoding for API responses) to prevent XSS and other rendering attacks.
- Adopt a robust data validation library or framework that supports schema validation for API request bodies.

Expected Outcome: Significant mitigation of injection vulnerabilities, improved data integrity, reduced risk of application crashes due to malformed inputs, and a more robust and secure API surface.

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

Description: Effective security visibility is critical for detecting and responding to threats. The current scan output does not provide insight into the existing logging, monitoring, and alerting capabilities of the application.

Why it Matters: Inadequate logging hinders the ability to detect security incidents, track unauthorized activities, and conduct effective forensic analysis post-breach. Without robust monitoring and alerting, security events may go unnoticed for extended periods, increasing the potential impact of an attack. This is a key requirement for SOC 2 and ISO/IEC 27001 compliance.

Recommended Actions:

- Implement centralized logging for all critical application security events, including authentication attempts (success/failure), authorization failures, sensitive data access, configuration changes, and API errors.
- Ensure logs contain essential context such as timestamp, source IP address, authenticated user ID, event type, and relevant object identifiers (e.g., 'campaign_id', 'clip_id').
- Integrate application logs with a Security Information and Event Management (SIEM) system or a similar real-time monitoring platform.
- Configure specific, actionable alerts for suspicious activities (e.g., multiple failed login attempts, unusual access patterns, high rates of API errors, administrative actions by non-admins) with clear escalation procedures.
- Regularly review and analyze logs for anomalies, indicators of compromise, and compliance adherence.

Expected Outcome: Improved capabilities for real-time threat detection, faster incident response, enhanced forensic investigation, and sustained compliance with audit trail and security monitoring requirements.

Integrate Security into the Software Development Lifecycle (SDLC) (Priority: Long-Term)

Description: The presence of fundamental vulnerabilities like missing authentication suggests an opportunity to embed security practices earlier and more consistently throughout the entire development process.

Why it Matters: Shifting security considerations to the left in the SDLC significantly reduces the cost and effort of remediation, improves the overall security posture of the application, and fosters a security-aware development culture. This is a cornerstone of modern security programs and a requirement for achieving higher compliance maturity.

Recommended Actions:

- Establish and enforce a Secure Development Lifecycle (SDLC) framework that integrates security activities into each phase, from design to deployment.
- Implement mandatory security training for all developers, focusing on current threat landscapes (e.g., OWASP Top 10), secure coding practices, and specific framework vulnerabilities.
- Conduct threat modeling exercises for new features and architectural changes to identify and mitigate security risks at the design phase.
- Integrate automated security testing tools (e.g., Static Application Security Testing - SAST, Dynamic Application Security Testing - DAST, Software Composition Analysis - SCA) into the CI/CD pipeline.
- Perform regular security code reviews and peer reviews with a dedicated security focus to catch vulnerabilities before they reach production.

Expected Outcome: A more inherently secure application with fewer vulnerabilities, reduced remediation costs, improved developer security awareness, and a stronger overall security posture across the product lifecycle.