SECURITY ANALYSIS REPORT

Security Analysis Report

Provider:

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

Scan ID: c1cc6df8-566c-4b78-8ceb-4c7984bd8f72

Date: 2026-02-05 15:51:35

Version: 1.0.0

TABLE OF CONTENTS

/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 ..... --

EXECUTIVE SUMMARY

The security assessment of the provided repository identified several key vulnerabilities requiring immediate attention. A critical misconfiguration allows the Flask application to run in debug mode, exposing the Werkzeug debugger which can lead to remote code execution. Additionally, the application's interactions with external payment APIs lack proper timeout configurations, potentially leading to denial-of-service conditions. Finally, verbose error messages are returned to clients, which could aid attackers in gaining insights into the application's internal structure and potential weaknesses.

Identified Vulnerabilities

ID	Title	CVSS	Page
C1	Flask Debug Mode Enabled in Production	9.8	1872
M1	Missing Request Timeout for External API Calls	5.3	90
L1	Verbose Error Messages Exposing Internal Details	3.7	117

METHODOLOGY

Introduction

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

Objective

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

Scope

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

Systems in Scope

No systems explicitly defined.

User Accounts

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

FINDINGS

C1 – Flask Debug Mode Enabled in Production

Severity: Critical

CVSS Score: 9.8

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

Target: Web application server

Overview

The application is configured to run Flask with `debug=True` in what appears to be a production environment. This critically exposes the Werkzeug debugger, which includes an interactive console that allows for arbitrary code execution on the server. This vulnerability can lead to complete system compromise if exploited by an attacker.

Details

The `app.run(debug=True, ...)` call in `app.py` is intended for development environments. In a production setting, enabling debug mode exposes the Werkzeug debugger, which presents an interactive Python shell on unhandled exceptions. An attacker can use this shell to execute arbitrary Python commands, access sensitive environment variables, read or modify files, and potentially escalate privileges to achieve full remote code execution (RCE) on the host server.

Evidence

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

References

- https://flask.palletsprojects.com/en/2.3.x/deploying/
- https://owasp.org/www-community/vulnerabilities/Remote_Code_Execution

Recommendation

- Ensure `debug=False` when deploying the Flask application to any production or publicly accessible environment. - Utilize a production-ready WSGI server (e.g., Gunicorn, uWSGI) to serve the Flask application, which inherently prevents the direct exposure of the Werkzeug debugger. - Configure robust logging for production to capture errors and application state without relying on debug output exposed to clients.

M1 – Missing Request Timeout for External API Calls

Severity: Medium

CVSS Score: 5.3

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

Target: External API integrations (Cashfree API)

Overview

The application makes multiple calls to external APIs without specifying a timeout. This can cause the application to hang indefinitely if the external service becomes unresponsive or experiences high latency, potentially leading to denial-of-service (DoS) conditions and resource exhaustion on the server.

Details

Several instances of `requests.post()` and `requests.get()` are used to interact with the Cashfree payment gateway API. When no `timeout` parameter is provided, the `requests` library will wait indefinitely for a response from the external server. If the Cashfree API is slow, unresponsive, or experiencing an outage, these calls will block the application's processes, consuming server resources and potentially leading to unresponsive endpoints, degraded performance, or even application crashes. This can impact application availability and user experience.

Evidence

- **routes\payments.py:90:** Call to `requests.post` for creating Cashfree orders without a timeout.
- **routes\payments.py:136:** Call to `requests.get` for checking Cashfree order status without a timeout.
- **routes\payments.py:663:** Call to `requests.post` for Cashfree payouts without a timeout.

References

- https://docs.python-requests.org/en/latest/user/advanced/#timeouts
- https://owasp.org/www-community/attacks/Denial_of_Service

Recommendation

- Always specify a `timeout` parameter for all `requests` calls to external services. A reasonable timeout duration should be chosen based on the expected response time of the external API. - Implement robust error handling and retry mechanisms with exponential backoff for external API integrations to gracefully handle temporary network issues or service unavailability. - Consider implementing circuit breaker patterns to prevent cascading failures when an external service is consistently unavailable.

L1 – Verbose Error Messages Exposing Internal Details

Severity: Low

CVSS Score: 3.7

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

Target: API error responses

Overview

The application's API endpoints directly expose raw Python exception messages (`str(e)`) to clients in their error responses. This practice can inadvertently leak sensitive internal system details, code structure, or operational information, which could be leveraged by attackers for reconnaissance and further exploitation.

Details

Numerous API routes implement generic exception handling (`except Exception as e:`) and then include `str(e)` directly within the JSON error response (e.g., `{'msg': '...', 'error': str(e)}`). While logging these exceptions internally (`print(f"... error: {str(e)}")`) is good for debugging, exposing raw exception strings to end-users can reveal stack traces, database query failures, file paths, or other technical details about the server's environment or the application's internal workings. This information can be highly valuable to an attacker attempting to understand the system and identify potential attack vectors.

Evidence

- **app.py:117:** Returns `str(e)` on registration failure.
- **app.py:187:** Returns `str(e)` on login failure.
- **app.py:210:** Returns `str(e)` on profile update failure.
- **app.py:243:** Returns `str(e)` on password reset email failure.
- **app.py:288:** Returns `str(e)` on campaign creation failure.
- **app.py:326:** Returns `str(e)` on listing campaigns failure.
- **app.py:385:** Returns `str(e)` on fetching all campaigns failure.
- **app.py:491:** Returns `str(e)` on fetching campaign details failure.
- **app.py:579:** Returns `str(e)` on fetching creator campaigns failure.
- **app.py:653:** Returns `str(e)` on clip submission failure.
- **app.py:718:** Returns `str(e)` on fetching creator clips failure.
- **app.py:754:** Returns `str(e)` on fetching accepted clip details failure.
- **app.py:829:** Returns `str(e)` on campaign deletion failure.
- **app.py:884:** Returns `str(e)` on clip deletion failure.
- **app.py:931:** Returns `str(e)` on admin fetching campaigns failure.
- **app.py:1022:** Returns `str(e)` on admin updating clip failure.
- **app.py:1075:** Returns `str(e)` on admin deleting clip failure.
- **app.py:1109:** Returns `str(e)` on fetching creator profile failure.
- **app.py:1155:** Returns `str(e)` on updating creator profile failure.
- **app.py:1194:** Returns `str(e)` on updating campaign image failure.

- **app.py:1226:** Returns `str(e)` on updating campaign budget failure.
- **app.py:1255:** Returns `str(e)` on updating campaign requirements failure.
- **app.py:1286:** Returns `str(e)` on updating campaign status failure.
- **app.py:1317:** Returns `str(e)` on updating campaign view threshold failure.
- **app.py:1354:** Returns `str(e)` on updating campaign deadline failure.
- **app.py:1450:** Returns `str(e)` on retrieving pending payouts failure.
- **app.py:1478:** Returns `str(e)` on fetching brand profile failure.
- **app.py:1509:** Returns `str(e)` on updating brand profile failure.
- **app.py:1576:** Returns `str(e)` on updating clip view count failure.
- **app.py:1631:** Returns `str(e)` on updating campaign views failure.
- **app.py:1729:** Returns `str(e)` on retrieving analytics failure.
- **app.py:1756:** Returns `str(e)` on Google user sync failure (user data retrieval).
- **app.py:1808:** Returns `str(e)` on Google user sync database error.
- **app.py:1812:** Returns `str(e)` on generic Google user sync failure.
- **routes\payments.py:115:** Returns `str(e)` on internal server error during order creation.
- **routes\payments.py:186:** Returns `str(e)` on deposit verification failure.
- **routes\payments.py:343:** Returns `str(e)` on budget allocation failure.
- **routes\payments.py:430:** Returns `str(e)` on budget reclaim failure.
- **routes\payments.py:554:** Returns `str(e)` on funds distribution failure.
- **routes\payments.py:729:** Returns `str(e)` on creator withdrawal failure.
- **routes\payments.py:817:** Returns `str(e)` on saving payout details failure.
- **routes\payments.py:867:** Returns `str(e)` on retrieving payout details failure.
- **routes\payments.py:927:** Returns `str(e)` on verifying payout details failure.
- **routes\payments.py:989:** Returns `str(e)` on retrieving withdrawal history failure.
- **routes\payments.py:1023:** Returns `str(e)` on retrieving creator notifications failure.
- **routes\payments.py:1105:** Returns `str(e)` on retrieving transactions failure.
- **routes\payments.py:1197:** Returns `str(e)` on campaign refund failure.
- **routes\payments.py:1264:** Returns `str(e)` on retrieving campaign summary failure.
- **routes\payments.py:1358:** Returns `str(e)` on calculating creator earnings failure.
- **routes\payments.py:1529:** Returns `str(e)` on bulk distribution failure.
- **routes\payments.py:1623:** Returns `str(e)` on requesting refund failure.
- **routes\payments.py:1690:** Returns `str(e)` on retrieving refund requests failure.
- **routes\payments.py:1804:** Returns `str(e)` on approving refund failure.
- **routes\payments.py:1865:** Returns `str(e)` on rejecting refund failure.
- **routes\payments.py:1934:** Returns `str(e)` on retrieving refund status failure.
- **routes\payments.py:2014:** Returns `str(e)` on retrieving refund audit trail failure.
- **routes\payments.py:2088:** Returns `str(e)` on reverting failed withdrawal failure.

References

- https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure
- https://flask.palletsprojects.com/en/2.3.x/errorhandling/

Recommendation

- Replace generic `str(e)` in all API error responses with generic, user-friendly messages that do not reveal internal details. For example, 'An unexpected error occurred. Please try again later.' or a specific, non-technical message like 'Login failed. Please check your credentials.' - Implement a centralized error handling mechanism (e.g., Flask's `app.errorhandler`) to ensure consistent, secure, and user-friendly error responses across the entire application. - Ensure that detailed exception information and stack traces are only logged server-side for internal debugging and monitoring, and are never exposed directly to clients. - For API errors, consider returning standardized error codes or structured, predefined error objects instead of raw exception messages.

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

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 registration endpoint.

  Potential Attack Scenario:

  An attacker could register unauthorized accounts or abuse the registration process.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of authentication on user registration can lead to unauthorized access and control issues, impacting system integrity and availability.
ISO/IEC 27001	Yes	high	Unauthorized access and modification are potential risks due to missing authentication on user registration, affecting confidentiality, integrity, and availability.
CSA STAR	Yes	high	Insecure registration process can lead to account misuse and unauthorized access, impacting data security and privacy controls.

Security Assessment Notes

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

References

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

Endpoint Path /login

Endpoint Path	/login
HTTP Methods	POST
Source Location	[redacted] : 120
Authentication Required	No
Risk Severity	Critical
CVSS Score	9.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

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

  Potential Attack Scenario:

  An attacker could potentially bypass authentication mechanisms and gain unauthorized access to user accounts.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Missing authentication on login can lead to unauthorized access, compromising account security and data integrity.
ISO/IEC 27001	Yes	high	Bypassing authentication can lead to unauthorized access, impacting confidentiality, integrity, and availability of information.
CSA STAR	Yes	high	Lack of proper authentication controls on login can lead to unauthorized access and potential account compromise.

Security Assessment Notes

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

References

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

Endpoint Path /verify-instagram

Endpoint Path	/verify-instagram
HTTP Methods	POST
Source Location	[redacted] : 192
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	This endpoint appears to handle verification which may involve sensitive data. Proper authentication and authorization controls are in place.
ISO/IEC 27001	Yes	low	Authentication and authorization measures seem to be implemented, contributing to the protection of information.
CSA STAR	Yes	low	Authentication mechanisms are present, which is a fundamental security control for cloud services.

Security Assessment Notes

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

References

Endpoint Path /verify-instagram/

Endpoint Path	/verify-instagram/
HTTP Methods	POST
Source Location	: 192
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	This endpoint appears to handle verification which may involve sensitive data. Proper authentication and authorization controls are in place.
ISO/IEC 27001	Yes	low	Authentication and authorization measures seem to be implemented, contributing to the protection of information.
CSA STAR	Yes	low	Authentication mechanisms are present, which is a fundamental security control for cloud services.

Security Assessment Notes

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

References

Endpoint Path /request-password-reset

Endpoint Path	/request-password-reset
HTTP Methods	POST
Source Location	: 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, potentially leading to denial-of-service or exploiting vulnerabilities in the reset process.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	high	Lack of authentication on password reset requests can lead to account takeovers and denial-of-service attacks.
ISO/IEC 27001	Yes	high	Absence of authentication for password reset can allow unauthorized initiation of password changes, compromising account security.
CSA STAR	Yes	high	Unauthenticated password reset requests can be exploited for account hijacking and denial of service.

Security Assessment Notes

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

References

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

Endpoint Path /api/brand/campaigns

Endpoint Path	/api/brand/campaigns
HTTP Methods	POST
Source Location	: 248
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for creating campaigns appears to have authentication, which is a necessary control.
ISO/IEC 27001	Yes	low	Authentication is present for creating campaigns, contributing to authorized actions and data integrity.
CSA STAR	Yes	low	Authentication is confirmed for campaign creation, aligning with access control principles.

Security Assessment Notes

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

References

Endpoint Path /api/brand/campaigns

Endpoint Path	/api/brand/campaigns
HTTP Methods	GET
Source Location	: 292
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for listing campaigns has authentication, which is appropriate for accessing potentially sensitive campaign data.
ISO/IEC 27001	Yes	low	Authentication for listing campaigns helps ensure that only authorized users can view this information.
CSA STAR	Yes	low	Authentication for retrieving campaign data is a standard security practice.

Security Assessment Notes

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

References

Endpoint Path /api/campaigns

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 the /api/campaigns GET endpoint.

  Potential Attack Scenario:

  Unauthorized users might access campaign data they should not see.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Exposure of campaign data without authentication can lead to unauthorized access and potential data breaches.
ISO/IEC 27001	Yes	medium	Lack of authentication for accessing campaign data poses a risk to confidentiality and authorized access.
CSA STAR	Yes	medium	Unauthenticated access to campaign information could violate data privacy and 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

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

Endpoint Path /api/campaigns/

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 the /api/campaigns/ GET endpoint.

  Potential Attack Scenario:

  Unauthorized users might access specific campaign data they should not see.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	medium	Exposure of specific campaign data without authentication can lead to unauthorized access.
ISO/IEC 27001	Yes	medium	Lack of authentication for accessing individual campaign data poses a risk to confidentiality.
CSA STAR	Yes	medium	Unauthenticated access to specific campaign details could compromise data privacy.

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/Insecure_Direct_Object_Reference

Endpoint Path /api/creator/your-campaigns

Endpoint Path	/api/creator/your-campaigns
HTTP Methods	GET
Source Location	: 495
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for creator's campaigns has authentication, which is appropriate for accessing user-specific data.
ISO/IEC 27001	Yes	low	Authentication for creator-specific data ensures that only the creator can access their campaigns.
CSA STAR	Yes	low	Authentication protects creator's campaign data from unauthorized access.

Security Assessment Notes

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

References

Endpoint Path /api/creator/submit-clip

Endpoint Path	/api/creator/submit-clip
HTTP Methods	POST
Source Location	: 583
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for submitting clips has authentication, ensuring only authorized creators can submit content.
ISO/IEC 27001	Yes	low	Authentication for clip submission prevents unauthorized content from being added.
CSA STAR	Yes	low	Authentication controls are in place for submitting creator content.

Security Assessment Notes

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

References

Endpoint Path /api/creator/campaign-clips

Endpoint Path	/api/creator/campaign-clips
HTTP Methods	GET
Source Location	: 657
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for retrieving campaign clips has authentication, ensuring only authorized users can access this data.
ISO/IEC 27001	Yes	low	Authentication protects the confidentiality of campaign clips.
CSA STAR	Yes	low	Authentication is required to access creator clips associated with a campaign.

Security Assessment Notes

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

References

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

Endpoint Path	/api/creator/accepted-clip-details/
HTTP Methods	GET
Source Location	: 722
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for accepted clip details has authentication, ensuring data privacy for creators.
ISO/IEC 27001	Yes	low	Authentication protects the confidentiality of accepted clip details.
CSA STAR	Yes	low	Authentication is necessary to access specific details of submitted clips.

Security Assessment Notes

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

References

Endpoint Path /api/brand/campaigns/

Endpoint Path	/api/brand/campaigns/
HTTP Methods	DELETE, OPTIONS
Source Location	: 761
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for deleting campaigns has authentication, ensuring only authorized users can perform this action.
ISO/IEC 27001	Yes	low	Authentication is crucial for preventing unauthorized deletion of campaign data.
CSA STAR	Yes	low	Authentication controls are in place for deleting campaign resources.

Security Assessment Notes

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

References

Endpoint Path /api/creator/clip/

Endpoint Path	/api/creator/clip/
HTTP Methods	DELETE, OPTIONS
Source Location	[redacted] : 833
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for deleting clips has authentication, ensuring only authorized creators can delete their content.
ISO/IEC 27001	Yes	low	Authentication is necessary to prevent unauthorized deletion of creator clips.
CSA STAR	Yes	low	Authentication controls are in place for deleting creator-specific data.

Security Assessment Notes

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

References

Endpoint Path /api/admin/campaigns

Endpoint Path	/api/admin/campaigns
HTTP Methods	GET
Source Location	: 888
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Admin endpoint for campaigns has authentication, ensuring only authorized administrators can access this data.
ISO/IEC 27001	Yes	low	Authentication for administrative access to campaign data is critical for maintaining system integrity.
CSA STAR	Yes	low	Authentication is confirmed for admin access to campaign data.

Security Assessment Notes

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

References

Endpoint Path /api/admin/clip/

Endpoint Path	/api/admin/clip/
HTTP Methods	PUT
Source Location	: 935
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Admin endpoint for updating clips has authentication, ensuring only authorized administrators can modify clip data.
ISO/IEC 27001	Yes	low	Authentication for updating clip data maintains integrity and prevents unauthorized modifications.
CSA STAR	Yes	low	Authentication is confirmed for admin updates to clip information.

Security Assessment Notes

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

References

Endpoint Path /api/admin/clip/

Endpoint Path	/api/admin/clip/
HTTP Methods	DELETE, OPTIONS
Source Location	[redacted] : 1026
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Admin endpoint for deleting clips has authentication, ensuring only authorized administrators can perform this action.
ISO/IEC 27001	Yes	low	Authentication is necessary to prevent unauthorized deletion of clip data by administrators.
CSA STAR	Yes	low	Authentication controls are in place for admin deletion of clips.

Security Assessment Notes

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

References

Endpoint Path /api/creator/profile

Endpoint Path	/api/creator/profile
HTTP Methods	GET
Source Location	: 1079
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for creator profile has authentication, ensuring only the creator can access their profile information.
ISO/IEC 27001	Yes	low	Authentication protects the privacy and integrity of creator profile data.
CSA STAR	Yes	low	Authentication is confirmed for accessing creator profile details.

Security Assessment Notes

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

References

Endpoint Path /api/creator/profile

Endpoint Path	/api/creator/profile

HTTP Methods	PUT
Source Location	[redacted] : 1113
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for updating creator profile has authentication, ensuring only the creator can modify their profile.
ISO/IEC 27001	Yes	low	Authentication for updating profile data prevents unauthorized modifications.
CSA STAR	Yes	low	Authentication controls are in place for updating creator profile information.

Security Assessment Notes

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

References

Endpoint Path /api/brand/campaigns//image

Endpoint Path	/api/brand/campaigns//image
HTTP Methods	PUT, OPTIONS

Source Location	: 1159
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for updating campaign image has authentication, ensuring only authorized users can modify campaign assets.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized modification of campaign images, maintaining data integrity.
CSA STAR	Yes	low	Authentication controls are in place for updating campaign visual assets.

Security Assessment Notes

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

References

Endpoint Path /api/brand/campaigns//budget

Endpoint Path	/api/brand/campaigns//budget
HTTP Methods	PUT
Source Location	: 1198

Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for updating campaign budget has authentication, ensuring only authorized users can modify budget.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized modification of campaign budgets, maintaining financial integrity.
CSA STAR	Yes	low	Authentication controls are in place for updating campaign budget information.

Security Assessment Notes

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

References

Endpoint Path /api/brand/campaigns//requirements

Endpoint Path	/api/brand/campaigns//requirements
HTTP Methods	PUT
Source Location	: 1230
Authentication Required	Yes (unknown)

Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for updating campaign requirements has authentication, ensuring only authorized users can modify requirements.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized modification of campaign requirements, maintaining data integrity.
CSA STAR	Yes	low	Authentication controls are in place for updating campaign requirement information.

Security Assessment Notes

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

References

Endpoint Path /api/brand/campaigns//status

Endpoint Path	/api/brand/campaigns//status
HTTP Methods	PUT
Source Location	[redacted] : 1259
Authentication Required	Yes (unknown)
Risk Severity	Low

CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for updating campaign status has authentication, ensuring only authorized users can change campaign status.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized changes to campaign status, maintaining operational integrity.
CSA STAR	Yes	low	Authentication controls are in place for updating campaign status.

Security Assessment Notes

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

References

Endpoint Path /api/brand/campaigns//view_threshold

Endpoint Path	/api/brand/campaigns//view_threshold
HTTP Methods	PUT
Source Location	: 1290
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for updating view threshold has authentication, ensuring only authorized users can modify this setting.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized changes to view thresholds, maintaining campaign control.
CSA STAR	Yes	low	Authentication controls are in place for updating campaign view threshold.

Security Assessment Notes

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

References

Endpoint Path /api/brand/campaigns//deadline

Endpoint Path	/api/brand/campaigns//deadline
HTTP Methods	PUT
Source Location	[redacted] : 1321
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for updating campaign deadline has authentication, ensuring only authorized users can modify deadlines.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized changes to campaign deadlines, maintaining project timelines.
CSA STAR	Yes	low	Authentication controls are in place for updating campaign deadline information.

Security Assessment Notes

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

References

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

Endpoint Path	/api/brand/campaigns//pending-payouts
HTTP Methods	GET
Source Location	: 1358
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for pending payouts has authentication, ensuring only authorized personnel can view financial payout data.
ISO/IEC 27001	Yes	low	Authentication protects the confidentiality of financial payout information.
CSA STAR	Yes	low	Authentication is confirmed for accessing pending payout details.

Security Assessment Notes

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

References

Endpoint Path /api/brand/profile

Endpoint Path	/api/brand/profile
HTTP Methods	GET
Source Location	[redacted] : 1455
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for brand profile has authentication, ensuring only authorized users can access brand information.
ISO/IEC 27001	Yes	low	Authentication protects the privacy and integrity of brand profile data.
CSA STAR	Yes	low	Authentication is confirmed for accessing brand profile details.

Security Assessment Notes

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

References

Endpoint Path /api/brand/profile

Endpoint Path	/api/brand/profile
HTTP Methods	PUT
Source Location	[redacted] : 1482
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for updating brand profile has authentication, ensuring only authorized users can modify brand information.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized modifications to brand profile data.
CSA STAR	Yes	low	Authentication controls are in place for updating brand profile information.

Security Assessment Notes

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

References

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

Endpoint Path	/api/admin/clip//view-count
HTTP Methods	PUT
Source Location	[redacted] : 1514
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Admin endpoint for updating clip view count has authentication, ensuring only authorized administrators can modify this metric.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized manipulation of clip view counts, maintaining data integrity.
CSA STAR	Yes	low	Authentication controls are in place for updating clip view counts by administrators.

Security Assessment Notes

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

References

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

Endpoint Path	/api/admin/campaign//update-views
HTTP Methods	PUT
Source Location	[redacted] : 1580
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Admin endpoint for updating campaign view count has authentication, ensuring only authorized administrators can modify this metric.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized manipulation of campaign view counts, maintaining data integrity.
CSA STAR	Yes	low	Authentication controls are in place for updating campaign view counts by administrators.

Security Assessment Notes

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

References

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

Endpoint Path	/api/admin/analytics/campaign-performance/
HTTP Methods	GET
Source Location	[redacted] : 1635
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Admin endpoint for campaign performance analytics has authentication, ensuring only authorized administrators can access this data.
ISO/IEC 27001	Yes	low	Authentication for accessing performance analytics protects sensitive business data.
CSA STAR	Yes	low	Authentication is confirmed for retrieving campaign performance analytics.

Security Assessment Notes

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

References

Endpoint Path /api/auth/google-sync

Endpoint Path	/api/auth/google-sync
HTTP Methods	POST
Source Location	[redacted] : 1738
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for Google sync has authentication, ensuring that only authorized users can sync their Google data.
ISO/IEC 27001	Yes	low	Authentication protects the integrity and confidentiality of data synced from Google accounts.
CSA STAR	Yes	low	Authentication is confirmed for synchronizing with Google services.

Security Assessment Notes

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

References

Endpoint Path /refresh

Endpoint Path	/refresh
HTTP Methods	POST
Source Location	: 1816
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for refreshing tokens has authentication, ensuring only valid sessions can obtain new tokens.
ISO/IEC 27001	Yes	low	Authentication for token refresh prevents unauthorized session continuation.
CSA STAR	Yes	low	Authentication is confirmed for token refresh operations.

Security Assessment Notes

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

References

Endpoint Path /logout

Endpoint Path	/logout
HTTP Methods	DELETE
Source Location	: 1832
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Logout endpoint has authentication, ensuring that only authenticated users can log out.
ISO/IEC 27001	Yes	low	Authentication for logout ensures proper termination of authenticated sessions.
CSA STAR	Yes	low	Authentication is confirmed for logout functionality.

Security Assessment Notes

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

References

Endpoint Path /api/health

Endpoint Path	/api/health
HTTP Methods	GET
Source Location	[redacted] : 1843
Authentication Required	No
Risk Severity	Low
CVSS Score	2.7

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 /api/health GET endpoint.

  Potential Attack Scenario:

  While typically for monitoring, an unauthenticated health check could potentially reveal system information that might be useful for further reconnaissance if not properly secured.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Health check endpoints are often exposed for monitoring purposes and may not require authentication. However, care should be taken not to reveal sensitive system information.
ISO/IEC 27001	Yes	low	Exposing health status is common. The main concern is that it does not leak sensitive operational details.
CSA STAR	Yes	low	Health endpoints are generally acceptable without authentication if they do not disclose sensitive data.

Security Assessment Notes

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

References

Endpoint Path /create-deposit-order

Endpoint Path	/create-deposit-order
HTTP Methods	POST
Source Location	[redacted] : 49
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for creating deposit orders has authentication, ensuring only authorized users can initiate financial transactions.
ISO/IEC 27001	Yes	low	Authentication is critical for preventing unauthorized financial transactions and ensuring data integrity.
CSA STAR	Yes	low	Authentication controls are in place for creating financial transaction orders.

Security Assessment Notes

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

References

Endpoint Path /verify-deposit

Endpoint Path	/verify-deposit
HTTP Methods	POST
Source Location	: 121
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for verifying deposits has authentication, ensuring that only authorized users can verify financial transactions.
ISO/IEC 27001	Yes	low	Authentication is crucial for ensuring the integrity and authorized verification of financial deposits.
CSA STAR	Yes	low	Authentication controls are in place for verifying financial deposit transactions.

Security Assessment Notes

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

References

Endpoint Path /virtual-account

Endpoint Path	/virtual-account
HTTP Methods	GET
Source Location	[redacted] : 192
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for virtual account information has authentication, ensuring only authorized users can access these financial details.
ISO/IEC 27001	Yes	low	Authentication protects the confidentiality of virtual account information.
CSA STAR	Yes	low	Authentication is confirmed for retrieving virtual account details.

Security Assessment Notes

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

References

Endpoint Path /wallet-balance

Endpoint Path	/wallet-balance
HTTP Methods	GET
Source Location	[redacted] : 243
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for wallet balance has authentication, ensuring only the user can view their financial balance.
ISO/IEC 27001	Yes	low	Authentication protects the confidentiality of user wallet balances.
CSA STAR	Yes	low	Authentication is confirmed for retrieving wallet balance information.

Security Assessment Notes

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

References

Endpoint Path /allocate-budget

Endpoint Path	/allocate-budget
HTTP Methods	POST
Source Location	: 269
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for allocating budget has authentication, ensuring only authorized users can manage budgets.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized allocation of budgets, maintaining financial control.
CSA STAR	Yes	low	Authentication controls are in place for budget allocation.

Security Assessment Notes

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

References

Endpoint Path /reclaim-budget

Endpoint Path	/reclaim-budget
HTTP Methods	POST
Source Location	: 349
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for reclaiming budget has authentication, ensuring only authorized users can reclaim funds.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized reclamation of budgets, maintaining financial control.
CSA STAR	Yes	low	Authentication controls are in place for budget reclamation.

Security Assessment Notes

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

References

Endpoint Path /distribute-to-creator

Endpoint Path	/distribute-to-creator
HTTP Methods	POST
Source Location	: 436
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for distributing funds to creators has authentication, ensuring only authorized parties can initiate payments.
ISO/IEC 27001	Yes	low	Authentication is essential for preventing unauthorized financial distributions to creators.
CSA STAR	Yes	low	Authentication controls are in place for creator payment distributions.

Security Assessment Notes

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

References

Endpoint Path /creator-withdraw

Endpoint Path	/creator-withdraw
HTTP Methods	POST
Source Location	[redacted] : 560
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for creator withdrawals has authentication, ensuring only authorized creators can initiate withdrawals.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized withdrawal requests, protecting financial assets.
CSA STAR	Yes	low	Authentication controls are in place for creator withdrawal requests.

Security Assessment Notes

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

References

Endpoint Path /creator/payout-details

Endpoint Path	/creator/payout-details
HTTP Methods	POST, PUT
Source Location	: 735
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for saving payout details has authentication, ensuring only authorized creators can manage their payout information.
ISO/IEC 27001	Yes	low	Authentication protects the integrity and confidentiality of creator payout details.
CSA STAR	Yes	low	Authentication controls are in place for saving creator payout details.

Security Assessment Notes

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

References

Endpoint Path /creator/payout-details

Endpoint Path	/creator/payout-details
HTTP Methods	GET
Source Location	: 823
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for retrieving payout details has authentication, ensuring only authorized creators can access their payout information.
ISO/IEC 27001	Yes	low	Authentication protects the confidentiality of creator payout details.
CSA STAR	Yes	low	Authentication is confirmed for retrieving creator payout details.

Security Assessment Notes

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

References

Endpoint Path /creator/verify-payout-details

Endpoint Path	/creator/verify-payout-details
HTTP Methods	POST
Source Location	: 873
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for verifying payout details has authentication, ensuring only authorized creators can verify their information.
ISO/IEC 27001	Yes	low	Authentication ensures the integrity and authorized verification of creator payout details.
CSA STAR	Yes	low	Authentication controls are in place for verifying creator payout details.

Security Assessment Notes

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

References

Endpoint Path /creator/withdrawals

Endpoint Path	/creator/withdrawals
HTTP Methods	GET
Source Location	[redacted] : 933
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for withdrawal history has authentication, ensuring only the creator can view their withdrawal records.
ISO/IEC 27001	Yes	low	Authentication protects the confidentiality of creator withdrawal history.
CSA STAR	Yes	low	Authentication is confirmed for retrieving creator withdrawal history.

Security Assessment Notes

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

References

Endpoint Path /creator/notifications/

Endpoint Path	/creator/notifications/
HTTP Methods	GET
Source Location	[redacted] : 995
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for creator notifications has authentication, ensuring only the specified creator can access their notifications.
ISO/IEC 27001	Yes	low	Authentication protects the confidentiality of creator notifications.
CSA STAR	Yes	low	Authentication is confirmed for retrieving creator-specific notifications.

Security Assessment Notes

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

References

Endpoint Path /transactions//

Endpoint Path	/transactions//
HTTP Methods	GET
Source Location	[redacted] : 1030
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for transactions has authentication, ensuring only authorized users can view transaction history.
ISO/IEC 27001	Yes	low	Authentication protects the confidentiality and integrity of transaction data.
CSA STAR	Yes	low	Authentication is confirmed for retrieving transaction records.

Security Assessment Notes

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

References

Endpoint Path /refund-campaign

Endpoint Path	/refund-campaign
HTTP Methods	POST
Source Location	: 1110
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for refunding campaigns has authentication, ensuring only authorized users can initiate refunds.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized refund requests, maintaining financial integrity.
CSA STAR	Yes	low	Authentication controls are in place for campaign refund requests.

Security Assessment Notes

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

References

Endpoint Path /campaign-summary/

Endpoint Path	/campaign-summary/
HTTP Methods	GET
Source Location	[redacted] : 1203
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for campaign summary has authentication, ensuring only authorized users can view campaign details.
ISO/IEC 27001	Yes	low	Authentication protects the confidentiality of campaign summary data.
CSA STAR	Yes	low	Authentication is confirmed for retrieving campaign summary information.

Security Assessment Notes

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

References

Endpoint Path /calculate-earnings//

Endpoint Path	/calculate-earnings//
HTTP Methods	GET
Source Location	: 1270
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for calculating earnings has authentication, ensuring only authorized creators can view their earnings.
ISO/IEC 27001	Yes	low	Authentication protects the confidentiality of creator earnings data.
CSA STAR	Yes	low	Authentication is confirmed for calculating and retrieving creator earnings.

Security Assessment Notes

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

References

Endpoint Path /bulk-distribute

Endpoint Path	/bulk-distribute
HTTP Methods	POST
Source Location	[redacted] : 1364
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for bulk distribution has authentication, ensuring only authorized users can initiate mass payments.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized bulk financial distributions, maintaining financial control.
CSA STAR	Yes	low	Authentication controls are in place for bulk distribution operations.

Security Assessment Notes

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

References

Endpoint Path /request-refund

Endpoint Path	/request-refund
HTTP Methods	POST
Source Location	[redacted] : 1535
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for requesting refunds has authentication, ensuring only authorized users can submit refund requests.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized refund requests, maintaining financial integrity.
CSA STAR	Yes	low	Authentication controls are in place for refund requests.

Security Assessment Notes

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

References

Endpoint Path /refund-requests

Endpoint Path	/refund-requests
HTTP Methods	GET
Source Location	[redacted] : 1629
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for retrieving refund requests has authentication, ensuring only authorized users can view this information.
ISO/IEC 27001	Yes	low	Authentication protects the confidentiality of refund request data.
CSA STAR	Yes	low	Authentication is confirmed for retrieving refund requests.

Security Assessment Notes

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

References

Endpoint Path /admin/approve-refund

Endpoint Path	/admin/approve-refund
HTTP Methods	POST
Source Location	[redacted] : 1696
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Admin endpoint for approving refunds has authentication, ensuring only authorized administrators can approve financial transactions.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized approval of refunds, maintaining financial integrity.
CSA STAR	Yes	low	Authentication controls are in place for administrative refund approval.

Security Assessment Notes

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

References

Endpoint Path /admin/reject-refund

Endpoint Path	/admin/reject-refund
HTTP Methods	POST
Source Location	: 1810
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Admin endpoint for rejecting refunds has authentication, ensuring only authorized administrators can reject financial transactions.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized rejection of refunds, maintaining system integrity.
CSA STAR	Yes	low	Authentication controls are in place for administrative refund rejection.

Security Assessment Notes

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

References

Endpoint Path /refund-status/

Endpoint Path	/refund-status/
HTTP Methods	GET
Source Location	[redacted] : 1871
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for refund status has authentication, ensuring only authorized users can view refund status.
ISO/IEC 27001	Yes	low	Authentication protects the confidentiality of refund status information.
CSA STAR	Yes	low	Authentication is confirmed for retrieving refund status.

Security Assessment Notes

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

References

Endpoint Path /admin/refund-audit-trail

Endpoint Path	/admin/refund-audit-trail
HTTP Methods	GET
Source Location	[redacted] : 1940
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Admin endpoint for refund audit trail has authentication, ensuring only authorized administrators can access audit logs.
ISO/IEC 27001	Yes	low	Authentication protects the integrity and confidentiality of audit trail data.
CSA STAR	Yes	low	Authentication is confirmed for retrieving refund audit trail information.

Security Assessment Notes

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

References

Endpoint Path /creator/revert-withdrawal

Endpoint Path	/creator/revert-withdrawal
HTTP Methods	POST
Source Location	[redacted] : 2019
Authentication Required	Yes (unknown)
Risk Severity	Low
CVSS Score	4.0

Authentication Analysis

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

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes:

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
SOC 2	Yes	low	Endpoint for reverting failed withdrawals has authentication, ensuring only authorized users can perform this action.
ISO/IEC 27001	Yes	low	Authentication prevents unauthorized reversion of withdrawals, maintaining financial system integrity.
CSA STAR	Yes	low	Authentication controls are in place for reverting failed withdrawals.

Security Assessment Notes

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

References

METRICS SUMMARY

Total Findings: 3

Severity	Count
CRITICAL	1
HIGH	0
MEDIUM	1
LOW	1

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.

Disable Flask Debug Mode in Production (Priority: Immediate)

Description: The Flask application is configured to run with debug mode enabled, exposing the Werkzeug debugger's interactive console to the internet.

Why it Matters: This is a critical misconfiguration that allows an attacker to execute arbitrary code remotely on the server, leading to complete system compromise, data exfiltration, and disruption of service.

Recommended Actions:

- Set `debug=False` when initializing and running the Flask application in all production or publicly accessible environments.
- Utilize a production-ready WSGI server (e.g., Gunicorn, uWSGI) to serve the Flask application, which inherently prevents direct exposure of the Werkzeug debugger.
- Implement environment-specific configurations to ensure debug mode is never enabled in non-development environments.
- Conduct a post-remediation scan to verify the debugger is no longer exposed.

Expected Outcome: Elimination of a critical remote code execution (RCE) vector and significant reduction of the application's attack surface.

Enforce Robust Authentication and Rate Limiting for Core User Endpoints (Priority: Immediate)

Description: Critical user management endpoints (`/register`, `/login`, `/request-password-reset`) are identified as missing adequate authentication and/or rate-limiting controls.

Why it Matters: The absence of proper controls on these endpoints enables attackers to perform account enumeration, brute-force attacks, unauthorized account creation, and denial-of-service against password reset functionalities. This directly impacts SOC 2, ISO/IEC 27001, and CSA STAR compliance requirements for access control and system integrity.

Recommended Actions:

- Implement robust rate limiting for `/register`, `/login`, and `/request-password-reset` endpoints to prevent automated and high-volume abuse.
- Integrate CAPTCHA or reCAPTCHA challenges for `/register` and `/request-password-reset` to deter automated script attacks.
- Ensure strong authentication mechanisms (e.g., JWT, OAuth) are correctly implemented and enforced for `/login`, preventing bypass techniques.
- Review all authentication logic for common vulnerabilities such as SQL injection or insecure credential handling.

Expected Outcome: Prevention of unauthorized account creation, mitigation of brute-force and account enumeration attacks, and improved resilience against DoS on authentication-related services.

Configure Timeouts for All External API Calls (Priority: Short-Term)

Description: The application makes multiple calls to external APIs, specifically the Cashfree payment gateway, without specifying a timeout parameter, leading to indefinite waits for unresponsive services.

Why it Matters: Uncontrolled external API call durations can cause application processes to hang indefinitely, leading to resource exhaustion, degraded performance, and denial-of-service conditions for legitimate users, thereby impacting application availability.

Recommended Actions:

- Mandate the inclusion of a `timeout` parameter with a carefully chosen duration for all `requests.post()` and `requests.get()` calls to external services.
- Implement specific exception handling for `requests.exceptions.Timeout` to gracefully manage unresponsive external services, ensuring an appropriate response is returned to the client.
- Introduce robust retry mechanisms with exponential backoff for transient network issues or API unavailability to improve reliability without blocking the application indefinitely.
- Regularly review and adjust timeout durations based on external API performance and business requirements.

Expected Outcome: Enhanced application resilience against third-party service failures, improved system stability, and prevention of cascading denial-of-service impacts.

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

Description: The application's API endpoints directly expose raw Python exception messages (`str(e)`) to clients in their error responses, revealing internal system details across numerous routes.

Why it Matters: This information leakage provides attackers with valuable insights into the application's internal structure, potential technologies used, and specific failure points, which can be leveraged for reconnaissance and subsequent targeted exploitation.

Recommended Actions:

- Replace all occurrences of `str(e)` in API error responses with generic, user-friendly messages (e.g., 'An unexpected error occurred. Please try again later.' or specific, non-technical messages).
- Implement a centralized error handling mechanism (e.g., Flask's `app.errorhandler`) to ensure consistent, secure, and non-verbose error responses across the entire application.
- Ensure that detailed exception information and full stack traces are captured only in secure, server-side logs for internal debugging and monitoring, and are never exposed directly to clients.
- Return standardized error codes and predefined, structured error objects for API errors instead of raw exception details.

Expected Outcome: Elimination of sensitive information disclosure in error messages, reduction of the attack surface, and improved attacker reconnaissance resistance.

Review and Harden Access Controls for Public-Facing Endpoints (Priority: Mid-Term)

Description: Endpoints such as `/api/campaigns` and `/api/campaigns/` are identified as missing authentication, potentially exposing sensitive campaign data. The `/api/health` endpoint also lacks authentication.

Why it Matters: Even if initially deemed public, endpoints revealing campaign data without proper authorization can leak proprietary business information, competitor insights, or user-specific details. An unauthenticated health check, if not carefully implemented, can provide reconnaissance data about system architecture or internal state. This violates core principles of data confidentiality and access control fundamental to SOC 2, ISO/IEC 27001, and CSA STAR.

Recommended Actions:

- Conduct a thorough audit of all endpoints currently lacking explicit authentication to determine if sensitive or proprietary data could be accessed by unauthorized parties.
- For endpoints exposing campaign data (e.g., `/api/campaigns/`), enforce appropriate authentication (e.g., API keys, JWT) and robust authorization (e.g., role-based access control) to ensure only authorized users can view specific campaign details.
- For the health check endpoint (`/api/health`), ensure responses contain only minimal, non-sensitive operational status information and do not reveal internal system or configuration details, even if remaining unauthenticated for monitoring purposes.
- Implement fine-grained authorization checks for all authenticated endpoints to prevent insecure direct object references (IDOR).

Expected Outcome: Minimized unauthorized data exposure, strengthened access control posture across the application's API surface, and enhanced data confidentiality.

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

Description: The findings suggest a reactive approach to error handling and monitoring, without explicit detailing of a comprehensive strategy for centralized logging, proactive monitoring, or automated alerting for security events.

Why it Matters: Effective logging and monitoring are crucial for the early detection of security incidents, unauthorized access attempts, system anomalies, and performance bottlenecks. Robust logging provides necessary audit trails for compliance (SOC 2, ISO/IEC 27001, CSA STAR) and forensic investigations. A lack thereof hinders incident response capabilities.

Recommended Actions:

- Implement a centralized logging system (e.g., ELK stack, Splunk, cloud-native logging services) to aggregate all application, security, and infrastructure logs from all components.
- Define and configure clear monitoring metrics and thresholds for unusual activity, failed authentication attempts, high error rates, resource utilization, and suspicious API access patterns.
- Establish an automated alerting framework that notifies appropriate security and operations teams immediately upon detecting suspicious activities, critical system failures, or policy violations.
- Ensure logs capture essential context for security events (e.g., user ID, source IP, timestamp, action performed, request details) while redacting any sensitive user data before logging.

Expected Outcome: Improved visibility into application behavior, faster incident detection and response times, and stronger adherence to security auditing requirements.

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

Description: The presence of fundamental vulnerabilities like Remote Code Execution and widespread authentication issues indicates that security considerations may not be systematically integrated throughout the entire development process.

Why it Matters: Shifting security 'left' in the development lifecycle significantly reduces the cost and effort of remediation, prevents the introduction of new vulnerabilities, and builds a more robust, secure application from the ground up. This is essential for continuous compliance and establishing a mature security posture.

Recommended Actions:

- Provide mandatory and recurring security training for all developers, focusing on secure coding practices, common vulnerability patterns (e.g., OWASP Top 10), and threats relevant to Flask/Python applications.
- Integrate Static Application Security Testing (SAST) tools into the CI/CD pipeline to automatically scan code for vulnerabilities during development and before merge.
- Incorporate Dynamic Application Security Testing (DAST) into pre-production and staging environments to identify runtime vulnerabilities and API security issues under operational conditions.
- Establish mandatory security review gates, including manual code reviews by security experts or peer security champions, before deployment to production environments.
- Implement threat modeling exercises early in the design phase for new features and applications to proactively identify and mitigate security risks.

Expected Outcome: A proactive security culture, significant reduction in the introduction of new vulnerabilities, and a measurable increase in the overall security maturity of the application.