[Redacted]
Penetration Test

SECURITY VULNERABILITIES ANALYSIS REPORT

Site:	Redacted
Date:	June 26, 2024
Classification:	Confidential
Prepared by:	Cybersecurity Assessment Team Fast Pen Tests
For:	[Redacted]

Table of Contents

Security Vulnerabilities Analysis

Summary

Vulnerability	Risk
Potential BREACH Attack Vulnerability	Moderate to High
Missing Strict-Transport-Security Header	Moderate
Missing X-Content-Type-Options Header	Low to Moderate
Uncommon Header 'fly-request-id'	Low

Potential BREACH Attack Vulnerability

Description

The Content-Encoding header is set to "deflate", which may indicate vulnerability to the BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext) attack. BREACH exploits the compression in TLS responses to potentially extract secret information from the encrypted traffic.

Risk

Moderate to High. This vulnerability is especially concerning for applications handling sensitive data and for long-lived HTTPS sessions.

Remediation

Consider implementing one or more of the following strategies:

1. Disabling HTTP compression
2. Separating secrets from user input
3. Randomizing secrets per request
4. Masking secrets (effectively randomizing by XORing with a random secret per request)
5. Protecting vulnerable pages with CSRF
6. Length hiding (by adding random number of bytes to the responses)

Missing Strict-Transport-Security Header

Description

The absence of the HTTP Strict Transport Security (HSTS) header in a TLS-enabled site has been identified. Without HSTS, the site remains vulnerable to downgrade attacks and SSL stripping, potentially allowing an attacker to intercept or modify supposedly secure communications.

Risk

Moderate. This vulnerability could lead to man-in-the-middle attacks, compromising the confidentiality and integrity of data in transit.

Remediation

Implement the Strict-Transport-Security header with an appropriate max-age value. For example: "Strict-Transport-Security: max-age=31536000; includeSubDomains". This forces

compliant browsers to use HTTPS for all connections to the domain for the specified duration, significantly enhancing transport layer security.

Missing X-Content-Type-Options Header

Description

The X-Content-Type-Options header is not set. This omission could allow the user agent to render the content of the site in a different fashion to the declared MIME type, potentially leading to MIME type confusion attacks.

Risk

Low to Moderate. Such attacks might enable malicious file execution or cross-site scripting (XSS) in certain scenarios. The risk is particularly relevant when dealing with user-uploaded content or in conjunction with other vulnerabilities.

Remediation

Set the X-Content-Type-Options header to 'nosniff'. This instructs browsers to strictly adhere to the declared content type, preventing MIME type sniffing and reducing the risk of content-type related attacks.

Uncommon Header 'fly-request-id'

Description

The presence of an uncommon header 'fly-request-id' with contents '01HTZQTRQ73E8QFC9F8CP3NCXE-iad' has been detected. While not inherently a vulnerability, non-standard headers can potentially leak information about the server infrastructure or deployment details. This could aid attackers in fingerprinting the system or tailoring their attacks.

Risk

Low. The exposure of non-standard headers generally poses minimal direct security threat but may contribute to information disclosure that could be leveraged in more sophisticated attacks.

Remediation

To mitigate this, consider removing or masking the header if it's not critical for operations. If the header is required, ensure it doesn't disclose sensitive information that could be exploited by malicious actors.

Report prepared by the Fast Pen Tests Cybersecurity Assessment Team

For questions or further information, please contact:
Cybersecurity Assessment Team
Email: cybersecurity@fastpentests.com
Phone: +1 (424) 229-2286

Classification: Confidential
Distribution limited to [Client Name] and authorized Fast Pen Tests personnel.