IT314 - SOFTWARE ENGINEERING

Penetration Testing

Group ID: 6
Topic: Online Blogging Platform

1	202201008	Smruti Parmar
2	202201014	Deep Patel
3	202201030	Jainil Patel
4	202201034	Harshit Kumar
5	202201037	Rishi Patel
6	202201041	Dhriti Goenka
7	202201080	Kanishk Kunj
8	202201083	Sahil Vaghasiya
9	202201090	Denil Antala

Under Guidance of :
Prof Saurabh Tiwari

Security Observation Report for Blogging Platform

Website Observed: https://it-314-g6-blogging-platform.vercel.app
Observation Tool: ZAP (Zed Attack Proxy)

Executive Summary:

During the observation of the blogging platform, various security concerns were identified, ranging from high to low severity. The most critical issue found was the exposure of cloud metadata, which could potentially leak sensitive information. Other significant issues include the absence of important security headers like the Content Security Policy (CSP), Anti-Clickjacking protection, and improper cross-domain configurations.

Security Observations Summary:

High-Risk Observation:

- **Cloud Metadata Exposure**:
  - **Observation**: The platform appears to expose sensitive cloud metadata that can be accessed publicly. This poses a significant risk, as attackers could use this data to gain unauthorized access or perform other malicious activities.
  - **Potential Impact**: If exploited, attackers could gain access to cloud service information, including API credentials and instance data, which could lead to a breach of platform integrity or data exfiltration.

Medium-Risk Observations:

- **Missing Content Security Policy (CSP) Header**:
  - **Observation**: The platform does not implement a CSP header, which leaves it vulnerable to Cross-Site Scripting (XSS) and other content injection attacks.
  - **Potential Impact**: Without a CSP, malicious scripts could be injected into the platform's pages, leading to potential data theft, user manipulation, or further attacks.
- **Cross-Domain Misconfiguration**:
  - **Observation**: The platform is not properly configured to handle cross-domain requests, which could allow attackers to make unauthorized requests to external resources or manipulate data.
  - **Potential Impact**: Improper cross-domain configurations could expose the platform to security vulnerabilities such as Cross-Site Request Forgery (CSRF) or unauthorized API access.
- **Missing Anti-Clickjacking Header**:
  - **Observation**: The site does not include headers to prevent clickjacking attacks. This could allow attackers to trick users into clicking on hidden or misleading elements on the platform.
  - **Potential Impact**: Attackers could create malicious websites that embed the platform in hidden frames, causing users to perform actions unknowingly.

Low-Risk Observations:

- **Server Leaks Version Information**:
    - **Observation**: The server reveals its version information in HTTP headers, which can help attackers target known vulnerabilities in that specific version of the software.
    - **Potential Impact**: Version information exposure could help attackers identify vulnerabilities specific to the version in use, enabling targeted exploits.
- **Strict-Transport-Security (HSTS) Header Not Set**:
    - **Observation**: The platform does not have the HSTS header set, which means that attackers could potentially perform man-in-the-middle (MITM) attacks.
    - **Potential Impact**: Without HSTS, an attacker could downgrade an HTTPS connection to HTTP, intercepting sensitive data transmitted between the user and the platform.
- **Unix Timestamp Disclosure**:
    - **Observation**: Unix timestamps are visible in some responses, potentially disclosing operational data about the platform.
    - **Potential Impact**: The exposure of timestamps could give attackers insights into the platform's internal structure or behavior, potentially aiding in further attacks.

Informational Observation:

- **Caching Practices**:
    - **Observation**: Suspicious caching behaviors were identified, where certain sensitive data may be inadvertently cached, leading to potential exposure.
    - **Potential Impact**: Improper caching could allow sensitive information to be stored in caches, potentially accessible by unauthorized users.

ZAP Scanning Report

Generated with ZAP on Mon 2 Dec 2024, at 12:44:22

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Contents

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- https://fonts.googleapis.com
- http://ciscobinary.openh264.org
- http://o.pki.goog
- http://ocsp.digicert.com
- http://r11.o.lencr.org
- http://r10.o.lencr.org
- https://it-314-g6-blogging-platform.vercel.app

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (8.3%)	1 (8.3%)
	Medium	0 (0.0%)	1 (8.3%)	2 (16.7%)	0 (0.0%)	3 (25.0%)
	Low	0 (0.0%)	2 (16.7%)	1 (8.3%)	1 (8.3%)	4 (33.3%)
	Informational	0 (0.0%)	0 (0.0%)	2 (16.7%)	2 (16.7%)	4 (33.3%)
	Total	0 (0.0%)	3 (25.0%)	5 (41.7%)	4 (33.3%)	12 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://o.pki.goog	0 (0)	0 (0)	1 (1)	0 (1)
	https://it-314-g6-blogging-platform.vercel.app	1 (1)	3 (4)	3 (7)	4 (11)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Cloud Metadata Potentially Exposed	High	1 (8.3%)
Content Security Policy (CSP) Header Not Set	Medium	11 (91.7%)
Cross-Domain Misconfiguration	Medium	30 (250.0%)
Total		12

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	1 (8.3%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	4 (33.3%)
Strict-Transport-Security Header Not Set	Low	11 (91.7%)
Timestamp Disclosure - Unix	Low	62 (516.7%)
X-Content-Type-Options Header Missing	Low	32 (266.7%)
Information Disclosure - Suspicious Comments	Informational	16 (133.3%)
Modern Web Application	Informational	16 (133.3%)
Re-examine Cache-control Directives	Informational	1 (8.3%)
Retrieved from Cache	Informational	345 (2,875.0%)
Total		12

Alerts

Risk=High, Confidence=Low (1)

https://it-314-g6-blogging-platform.vercel.app (1)

Cloud Metadata Potentially Exposed (1)

▶ GET https://it-314-g6-blogging-platform.vercel.app/latest/meta-data/

Risk=Medium, Confidence=High (1)

https://it-314-g6-blogging-platform.vercel.app (1)

Content Security Policy (CSP) Header Not Set (1)

▶ GET https://it-314-g6-blogging-platform.vercel.app/sitemap.xml

Risk=Medium, Confidence=Medium (2)

https://it-314-g6-blogging-platform.vercel.app (2)

Cross-Domain Misconfiguration (1)

▶ GET https://it-314-g6-blogging-platform.vercel.app/logo.png

Missing Anti-clickjacking Header (1)

▶ GET https://it-314-g6-blogging-platform.vercel.app/

Risk=Low, Confidence=High (2)

http://o.pki.goog (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

▶ POST http://o.pki.goog/s/wr3/yvU

https://it-314-g6-blogging-platform.vercel.app (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://it-314-g6-blogging-platform.vercel.app/

Risk=Low, Confidence=Medium (1)

https://it-314-g6-blogging-platform.vercel.app (1)

X-Content-Type-Options Header Missing (1)

▶ GET https://it-314-g6-blogging-platform.vercel.app/_next/static/chunks/pages/_error-7a92967bea80186d.js

Risk=Low, Confidence=Low (1)

https://it-314-g6-blogging-platform.vercel.app (1)

Timestamp Disclosure - Unix (1)

▶ GET https://it-314-g6-blogging-platform.vercel.app/_next/static/chunks/main-983f20789698fa48.js

Risk=Informational, Confidence=Medium (2)

https://it-314-g6-blogging-platform.vercel.app (2)

Modern Web Application (1)

▶ GET https://it-314-g6-blogging-platform.vercel.app/robots.txt

Retrieved from Cache (1)

▶ GET https://it-314-g6-blogging-platform.vercel.app/_next/static/chunks/pages/_error-7a92967bea80186d.js

Risk=Informational, Confidence=Low (2)

https://it-314-g6-blogging-platform.vercel.app (2)

Information Disclosure - Suspicious Comments (1)

▶ GET https://it-314-g6-blogging-platform.vercel.app/robots.txt

Re-examine Cache-control Directives (1)

▶ GET https://it-314-g6-blogging-platform.vercel.app/

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

Cloud Metadata Potentially Exposed

Source	raised by an active scanner (Cloud Metadata Potentially Exposed)
Reference	▪ https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/

Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy ▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html ▪ https://www.w3.org/TR/CSP/ ▪ https://w3c.github.io/webappsec-csp/ ▪ https://web.dev/articles/csp ▪ https://caniuse.com/#feat=contentsecuritypolicy ▪ https://content-security-policy.com/

Cross-Domain Misconfiguration

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264
WASC ID	14
Reference	▪ https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	200
WASC ID	13
Reference	▪ https://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) ▪ https://www.troyhunt.com/shhh-dont-let-your-response-headers/

Strict-Transport-Security Header Not Set

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15

Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html ▪ https://owasp.org/www-community/Security_Headers ▪ https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security ▪ https://caniuse.com/stricttransportsecurity ▪ https://datatracker.ietf.org/doc/html/rfc6797

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
WASC ID	13
Reference	▪ https://cwe.mitre.org/data/definitions/200.html

X-Content-Type-Options Header Missing

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	693
WASC ID	15
Reference	▪ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-

developer/compatibility/gg622941(v=vs.85)

- https://owasp.org/www-community/Security_Headers

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200
WASC ID	13

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

Re-examine Cache-control Directives

Source	raised by a passive scanner (Re-examine Cache-control Directives)
CWE ID	525
WASC ID	13
Reference	- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching - https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control - https://grayduck.mn/2021/09/13/cache-control-recommendations/

Retrieved from Cache

Source raised by a passive scanner (Retrieved from Cache)

Reference

- https://tools.ietf.org/html/rfc7234
- https://tools.ietf.org/html/rfc7231
- https://www.rfc-editor.org/rfc/rfc9110.html