Security Vulnerability & Secret Scan Report

Target URL: https://tokopedia.com

Scan Date: 2025-07-03 06:07:22

Scanner Tools & Capabilities:

• **Semgrep** - Static code analysis to identify bugs, security vulnerabilities, and malicious code patterns

• **Grype** - Vulnerability scanning for dependencies based on CVE/NVD databases

• **TruffleHog** - Detection of secrets and credentials accidentally exposed in code

Supported File Types:

JavaScript (.js, .ts), Configuration (.json, .xml, .yml, .yaml, .env, .config, .ini, .properties), Text (.txt), Server-side (.py, .php, .rb, .go, .java, .cs, .cpp, .c, .h), Scripts (.sh, .bat, .ps1), Database (.sql), Containers (.dockerfile), Certificates (.pem, .key, .crt, .cer)

Executive Summary

Metric	Count
Files Scanned	175
Semgrep - Code Analysis Issues	0
• High Severity	0
• Medium Severity	0
• Low Severity	0
Grype - Dependency Vulnerabilities	0
TruffleHog - Secrets/Credentials	8

Risk Assessment

Overall Risk Level: CRITICAL

Secret Detection (TruffleHog)

TruffleHog identified 8 potential secrets in the code. This tool searches for credentials such as API keys, tokens, passwords, and other sensitive information that may have been accidentally included in code or repositories.

High Confidence Secrets

AWS Secret Key: 0123**********ABCD
File: https___www.googletagmanager.com_gtag_js_id=UA-9801603-1 (Line 330)
Scanner: Custom Regex

Medium Confidence Secrets

AWS Secret Key: 0123**********ABCD
File: https___www.googletagmanager.com_gtag_js_id=UA-9801603-1 (Line 143)
Scanner: Custom Regex
AWS Secret Key: ABCD**********klmn
File: https___www.googletagmanager.com_gtag_js_id=UA-9801603-1 (Line 244)
Scanner: Custom Regex
AWS Secret Key: eylw**********YWxz
File: https___www.googletagmanager.com_gtag_js_id=UA-9801603-1 (Line 273)
Scanner: Custom Regex
AWS Secret Key: 0123**********ABCD
File: https___www.googletagmanager.com_gtag_js_id=UA-9801603-1 (Line 326)
Scanner: Custom Regex
AWS Secret Key: 0123**********ABCD
File: https___www.googletagmanager.com_gtag_js_id=UA-9801603-1 (Line 327)
Scanner: Custom Regex
AWS Secret Key: 0123**********ABCD
File: https___www.googletagmanager.com_gtag_js_id=UA-9801603-1 (Line 329)
Scanner: Custom Regex
AWS Secret Key: 4148**********a28d
File: inline_6.js (Line 7)
Scanner: Custom Regex

Recommendations

1. Implementasikan proses secure code review sebelum deploy kode JavaScript.

2. Gunakan Content Security Policy (CSP) headers untuk mencegah serangan XSS.

3. Update secara berkala semua dependencies JavaScript ke versi terbaru yang aman.

4. [TruffleHog] Hapus semua hardcoded secrets dan gunakan environment variables atau sistem manajemen secret yang aman.

5. [TruffleHog] Implementasikan pre-commit hooks untuk mencegah secrets ter-commit ke version control.

6. [TruffleHog] Lakukan audit menyeluruh pada repositori untuk memastikan tidak ada credentials yang terekspos.