AI-Powered Security Policy Report

Generated: 2025-11-06 16:17:10

Total Vulnerabilities Scanned: 1
• SAST: 1
• SCA: 0
• DAST: 0

LLM Models Used:

• LLaMA 3.3 70B (Groq) - SAST/SCA
• LLaMA 3.1 8B Instant (Groq) - DAST

Policy #1: SAST

Title: Var In Href
Severity: MEDIUM
LLM: LLaMA 3.3 70B

POLICY IDENTIFIER
SP-2024-001: Cross-Site Scripting (XSS) Protection Policy

RISK STATEMENT
The organization is at risk of cross-site scripting (XSS) attacks due to the use of template variables in anchor tags with the 'href' attribute. This vulnerability allows malicious actors to input the 'javascript:' URI, potentially leading to unauthorized access, data theft, or system compromise. The affected systems include the NodeGoat application, and the impacted users are those accessing the profile.html page. If exploited, this vulnerability could result in significant business consequences, including reputational damage, financial loss, and compromised customer trust.

COMPLIANCE MAPPING
This policy aligns with the following compliance requirements:
- NIST CSF: PR.DS-5 (Data Protection), DE.CM-1 (Anomalous Activity Detection)
- ISO 27001: A.8.23 (Web filtering), A.8.8 (Management of technical vulnerabilities), A.8.7 (Protection against malware), A.8.16 (Monitoring activities)
- Industry standards: OWASP A7:2021 (Cross-Site Scripting), CWE-79 (Improper Neutralization of Input During Web Page Generation)

POLICY REQUIREMENTS
To mitigate the risk of XSS attacks, the following security controls must be implemented:
- Use of 'url_for()' or 'url' filter to safely generate URLs in the NodeGoat application
- Implementation of a Content Security Policy (CSP) header to define allowed sources of content

- Regular code reviews to ensure secure coding practices
- Success criteria: No detected XSS vulnerabilities in the NodeGoat application, validated through regular security scans and penetration testing

REMEDIATION PLAN
To remediate this vulnerability, the following technical actions are required:
- Review and fix the vulnerable code in the profile.html page (line 78)
- Responsible party: Dev Lead
- Timeline: 2 weeks
- Verification steps: Code review, re-scan using a vulnerability scanner, and penetration testing to ensure the fix is effective

MONITORING AND DETECTION
To detect similar vulnerabilities in the future, the organization will:
- Implement logging and alerting for suspicious activity, including anomalous URL requests
- Conduct regular security scans and penetration testing to identify potential vulnerabilities
- Continuously monitor the NodeGoat application for signs of XSS attacks, using tools such as web application firewalls (WAFs) and intrusion detection systems (IDS)
- Perform regular code reviews to ensure secure coding practices and adherence to this policy.