

# AI-Powered Security Policy Report

Generated: 2025-11-06 16:17:25

## 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 could allow malicious actors to inject malicious code, potentially leading to unauthorized access, data theft, or disruption of services. The affected systems include web applications, and the impacted users are all individuals who interact with these applications. If exploited, this vulnerability could result in significant reputational damage, financial loss, and compromise of sensitive information.

### \*\*COMPLIANCE MAPPING\*\*

This policy aligns with the following compliance requirements:

- NIST CSF: PR.DS-5 (Data Protection), DE.AE-3 (Anomaly 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, 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 web applications
- Implementation of Content Security Policy (CSP) header

- Regular code reviews to identify and address potential vulnerabilities
- Success criteria: All web applications must be reviewed and updated to use secure URL generation methods, and CSP headers must be implemented.
- Validation methods: Code reviews, penetration testing, and vulnerability scanning will be used to validate compliance with this policy.

#### **\*\*REMEDIATION PLAN\*\***

To address the identified vulnerability, the following technical actions are required:

- Review and update the 'profile.html' file to use secure URL generation methods
- Implement CSP headers in all web applications
- Responsible party: Dev Lead
- Timeline: 2 weeks
- Verification steps: Code review, re-scan, and penetration testing will be conducted to verify remediation.

#### **\*\*MONITORING AND DETECTION\*\***

To detect similar vulnerabilities in the future, the following measures will be implemented:

- Regular code reviews and vulnerability scanning
- Logging and alerting requirements: All security-related logs will be monitored, and alerts will be triggered in case of potential security incidents
- Continuous monitoring strategies: The organization will conduct regular penetration testing, code reviews, and vulnerability scanning to identify and address potential security vulnerabilities.