AI Security Policies

Executive Summary - Problems & Solutions

Generated: November 13, 2025

Dynamic Application Security Testing (DAST) Policy

Problem

Risk Level: Medium | Findings: 0 Critical, 0 High, 3 Medium, 0 Low

Impact: Exploitation could lead to information disclosure, cross-site scripting, and reduced confidence in service integrity, potentially impacting customer trust and regulatory compliance.

Required Actions

P2: Add Missing X-Content-Type-Options Header

Timeline: Within 14 days | Owner: Web Operations Team

P2: Restrict Storable and Cacheable Content

Timeline: Within 21 days | Owner: Application Development Team

P2: Mitigate Spectre via Site Isolation

Timeline: Within 30 days | Owner: Infrastructure Security Team

Static Application Security Testing (SAST) Policy

Problem

Risk Level: Low | Findings: 0 Critical, 0 High, 0 Medium, 1 Low

Impact: A low-severity, unknown vulnerability could lead to minor information disclosure if left unaddressed, but the impact on core business operations is limited.

Required Actions

P3: Review and fix unknown security report analysis finding

Timeline: Within 14 days | Owner: Backend Development Team

Software Composition Analysis (SCA) Policy

Problem

Risk Level: High | Findings: 0 Critical, 16 High, 14 Medium, 3 Low

Impact: Data breach, service disruption, or loss of intellectual property.

Required Actions

P0: Patch all high-severity vulnerable dependencies

Timeline: Immediate (0-7 days) | Owner: DevOps Team

P1: Upgrade medium-severity dependencies with known exploits

Timeline: Within 30 days | Owner: Application Development Leads

P2: Review low-severity and license-risk dependencies

Timeline: Within 60 days | Owner: Legal & Compliance