Dynamic Application Security Testing (DAST) Policy

AI Security Policy Framework

Current runtime scanning has uncovered three medium-severity findings that expose the organization to data leakage, content spoofing, and speculative execution attacks. Immediate remediation and hardened scanning processes are required to reduce the ...

Generated: November 13, 2025

Dynamic Application Security Testing (DAST) Policy

Policy Metadata

Policy ID	POL-DAST-2025-001
Status	Active
Created Date	2025-11-05T00:00:00Z
Last Updated	2025-11-05T00:00:00Z
Author	Security Policy Generator

Executive Summary

Current runtime scanning has uncovered three medium-severity findings that expose the organization to data leakage, content spoofing, and speculative execution attacks. Immediate remediation and hardened scanning processes are required to reduce the attack surface and align with NIST CSF and ISO 27001 controls.

Policy Statement

Purpose

To identify and remediate runtime security vulnerabilities through dynamic testing

Description

This policy defines requirements for DAST implementation, runtime security monitoring, and production security hardening

Applicability

All web applications, APIs, and internet-facing services

Enforcement

Pre-production DAST scans required before deployment to production

Exceptions

Internal-only applications may use reduced scan frequency with documented approval

Objectives

1. Identify runtime vulnerabilities before code reaches production
2. Remediate identified findings within defined timeframes

3 Maintain continuous compliance with NIST CSF and ISO 27001 security controls

Risk Assessment

Risk Metric	Value
Overall Risk Level	Medium
Critical Risks	0
High Risks	0
Medium Risks	3
Low Risks	0
Likelihood	Medium
Business Impact	Exploitation could lead to information disclosure, cross■site scripting, and

Security Controls

SC-DAST-001: Security Headers Implementation

Enforce mandatory HTTP security headers to protect against content sniffing and click-jacking.

- Update web server configuration to include X-Content-Type-Options: nosniff
- Add X-Frame-Options: SAMEORIGIN and Content-Security-Policy headers
- Automate header verification in CI/CD pipeline using a linting tool

SC-DAST-002: Cache Control and Content Hardening

Prevent sensitive or dynamic content from being stored or cached unintentionally.

- Set Cache-Control: no-store, no-cache for all dynamic endpoints
- Review and update response headers for static assets to include appropriate max-age values
- Integrate automated DAST rule to flag cacheable responses lacking proper directives

SC-DAST-003: Spectre Mitigation and Site Isolation

Apply mitigations to reduce risk from speculative execution side-channel attacks.

- Enable site-isolation features in modern browsers (e.g., Chrome's Site Isolation flag) for all public pages
- Patch underlying OS and runtime libraries to latest versions containing Spectre mitigations
- Validate mitigation effectiveness with vendor-provided test suites after each release

Remediation Actions

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

Owner: Web Operations Team | Timeline: Within 14 days

Affected Assets:

- All web front-ends
- /api/*

Success Criteria: All HTTP responses contain X-Content-Type-Options: nosniff header verified by automated scan

P2: Restrict Storable and Cacheable Content

Owner: Application Development Team | Timeline: Within 21 days

Affected Assets:

- /static/*
- /api/public/*

Success Criteria: No DAST findings for cacheable content without Cache-Control or Pragma headers

P2: Mitigate Spectre via Site Isolation

Owner: Infrastructure Security Team | Timeline: Within 30 days

Affected Assets:

- All public web applications

Success Criteria: Site Isolation enabled in browsers for all domains and OS patches applied; spectre test suite passes

Compliance Mapping

Framework	Controls
NIST CSF	• PR.IP-1 • PR.DS-2 • DE.CM-1
ISO 27001	• A.9.1.1 • A.12.6.1 • A.13.1.1 • A.14.2.9

Monitoring Requirements

- Continuous runtime security monitoring via WAF logs
- Weekly automated DAST scans on staging and production environments
- Monthly review of security-header compliance reports
- Quarterly update of Spectre mitigation status

Review Schedule

Monthly policy review and quarterly full penetration testing