

DevSecOps Code Quality and Security for Salesforce

Static Code Analysis that drives Salesforce code quality and reduces vulnerabilities for speedy feature delivery, compliance and security



Salesforce code quality and security are mission-critical

Salesforce is a key driver of digital transformation, and at risk from the development supply chain. At risk, because sensitive data pervades the platform, and its use is complicated by the role of Salesforce Metadata, which encodes security roles, access controls, permissions and other platform customizations. The risk of introducing errors via Metadata is high – and directly affected by developer code quality. Poor code quality slows feature velocity and creates additional risks for compliance and security.

AutoRABIT CodeScan – Static Code Analysis built to drive Salesforce development quality, speed and security

Delivered on the AutoRABIT DevSecOps platform, AutoRABIT CodeScan’s Static Code Analysis delivers total visibility into code health from the first line written to final deployment into Production. Equipped with the most comprehensive insights for Salesforce languages and Metadata, CodeScan enables organizations to more quickly create high-quality features, evaluate and reduce outstanding technical debt, define and deliver to code standards, and meet security and compliance requirements. Deployment options for Cloud and on-premises enable organizations to take complete control over their data. This control enables data sovereignty and helps meet privacy requirements (such as GDPR). Code security standard support includes OWASP (scans for OWASP’s top 10 vulnerabilities), CWE, and SANS guidelines to add another layer of controls for high quality, highly secure code.

Salesforce Code Quality and Security are Mission Critical

IT security and regulatory compliance risks in Salesforce development are substantial and often overlooked

Sensitive information is pervasive. Repositories of operating data, customer personal information, business methods, and financial information are found throughout Salesforce environments.

Code analysis not only ensures faster, higher-quality feature delivery but reduces vulnerabilities and risks.

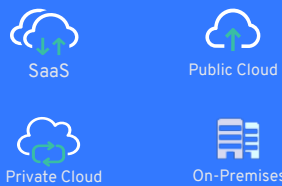
Salesforce metadata increases risk. Unique Salesforce metadata persists, inherits, and propagates – Can compromise release quality, leading to downtime and exposure of sensitive or protected data.

Scan with AutoRABIT CodeScan’s Metadata rules to help keep your Salesforce Orgs secure and clean.

AutoRABIT CodeScan supports security and compliance

- Security rules are aligned with CWE, OWASP, and SANS standards
- IDE developer tools, and vulnerability assessments for clean code at speed
- Visibility into technical debt help eliminate legacy faults and threats

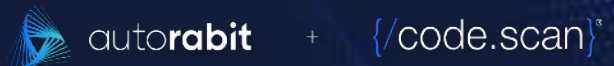
Flexible Deployment models support risk reduction, privacy mandates, cost control, and security



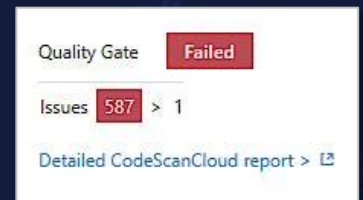
Salesforce Metadata Management addresses unique environment requirements

- Every screen update or line of code creates metadata
- Metadata properties persist, inherit, propagate and nest
- Bad metadata breaks orgs, slows development, exposes sensitive data

AutoRABIT CodeScan Empowers Salesforce DevOps Teams



- Speed development cycles
- Get higher quality, more secure code
- Reduce technical debt
- Increase Code Visibility
- Promote learning with immediate developer quality feedback



CodeScan Cloud Analysis Report

WITH CODESCAN YOU CAN ...

Reduce Technical Debt

- Over 600 rules built-in
- Detects code bugs and vulnerabilities
- Integrates directly into AutoRABIT ARM's DevSecOps CI/CD pipelines

Increase Feature Delivery Velocity and Productivity

- Speed code reviews with an automated review process
- Detects code bugs and vulnerabilities
- Integrated with your CI/CD pipeline on the AutoRABIT DevSecOps platform

Higher Quality, More Secure Code

- Integrated with popular IDE plugins to enable coders to find and fix errors as code is written
- Supports SANS, CWE and OWASP standards

Increase Code Visibility

- Dashboards and reports
- High-level analysis of code health
- 100% compatible with Salesforce languages and Metadata- Apex, Visualforce, Lightning Web Components, flows, and process builders

Categories	Vulnerabilities	Security Hotspots		
		Open	In Review	Won't Fix
A1 - Injection	1078	1	0	0
A2 - Broken Authentication	3	6	0	0
A3 - Sensitive Data Exposure	2992	1	0	0
A4 - XML External Entities (XXE)	-	-	-	-
A5 - Broken Access Control	1823	0	0	0
A6 - Security Misconfiguration	0	0	0	0
A7 - Cross-Site Scripting (XSS)	1100	0	0	0
A8 - Insecure Deserialization	27	0	0	0
A9 - Using Components with Known Vulnerabilities	-	-	-	-
A10 - Insufficient Logging & Monitoring	2	0	0	0
Not OWASP	2371	0	0	0

Security Reports

CUSTOMERS AGREE

98%

Say CodeScan helps developers write higher quality code

98%

Plan to continue using CodeScan

97%

Say CodeScan helps reduce technical debt

96%

Say CodeScan makes code reviews more productive