SaaS Development Creates Critical Vulnerabilities

Introducing DigitSec S4: a DevSecOps solution for Salesforce

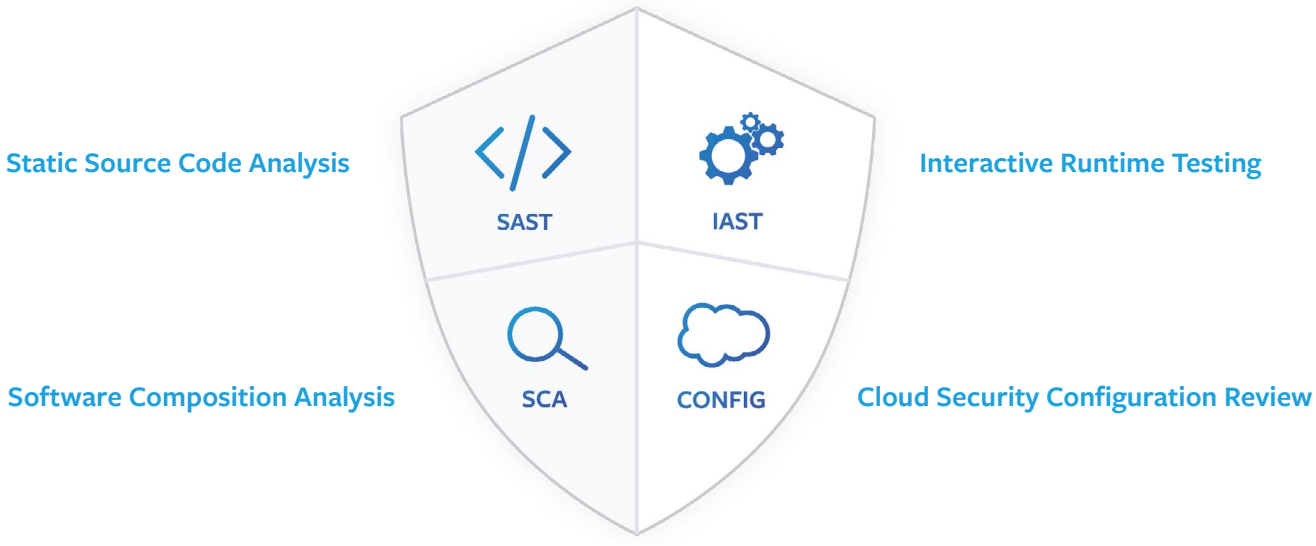
Overview

Salesforce is a feature-rich software-as-a-service (SaaS) platform designed to be developed and customized based on each enterprise's business needs. Yet when customers develop and customize Salesforce to improve data access, they are growing its attack surface, increasing risk of a data breach, and violating its default compliance status.

There are thousands of high-risk SaaS vulnerabilities which are exploitable with commonly available hacking tools. These vulnerabilities are hard to detect because most widely available security solutions were architected for general-purpose application security testing (AST), and don't address the unique vulnerabilities created by SAAS customization and development.

Security teams have responded by assembling an ad hoc patchwork of tools, each incapable of providing comprehensive and continuous AST for Salesforce development. This kluge grows complexity with the addition of each tool, as well as increases compliance risks. While the best way forward is the adoption of DevSecOps for Salesforce, integrating the kluge of existing tools into a continuous integration & deployment (CI/CD) pipeline is impractical, inefficient, and extremely difficult to accomplish.

The solution is the DigitSec SaaS Security Scanner™ - S4 for Salesforce™ - the only full-spectrum continuous application security testing (CAST) platform purpose-built to find Salesforce vulnerabilities with its four integrated scans for fast and effortless detection:



By seamlessly integrating full-spectrum CAST, DigitSec S4 accelerates development and reduces security compliance risks while significantly reducing false positives by up to 90%. . In under an hour, security and DevOps teams can shift security left, establishing DevSecOps for Salesforce and implementing comprehensive CAST in the CI/CD pipeline.

SaaS Development Introduces Hard to Detect Vulnerabilities

Salesforce custom development is necessary to the efficient operation of most enterprises and key to increasing productivity. Yet Salesforce development substantially increases cyber risk by introducing new attack vectors which are hard to detect with traditional AST solutions.

Whether downloading apps from the AppExchange, writing custom code, installing third-party software libraries, or altering configuration settings, users unknowingly grow their Salesforce attack surface with ongoing development and customization. This added complexity further increases costs, heightens cyber and compliance risks, and delays development critical to operating efficiency.

Protecting user data is a joint responsibility between Salesforce and its users, but Salesforce is not responsible for any security vulnerabilities created by user development and customization. Users must validate and fix any development-related vulnerabilities if they wish to maintain a secure and compliant Salesforce environment.

In a Salesforce development project, we typically see the following types of modifications:

- **Anonymous data** coming from the internet utilizing the Web-to-Lead or Web-to-Case Salesforce feature. While this feature enables business teams, it also creates new attack vectors.
- **Custom Apex controllers** to handle user data and execute workloads. If the Apex controllers are not properly protected against common attacks, they can lead to a data exfiltration.
- **Third-party tools and integrations** are common to most Salesforce developments. This is an attack vector which is often ignored and can cause severe damage to the confidentiality and integrity of data in Salesforce.
- **Enabling Guest User accounts** can potentially expose Salesforce data to anonymous internet users if not checked for security misconfigurations.

These are just a few examples to illustrate that without proper consideration to security, common Salesforce development can lead to security vulnerabilities posing risk to data and compliance standards.

This means static source code, third-party software libraries, runtime execution, and configuration settings all need to be checked regularly and thoroughly to maintain a strong application security posture in Salesforce. However, most available tools and solutions were not designed to address Salesforce customization vulnerabilities and thus introduce more delay, complexity, expense and risk. Let's review the current state of tools used to address the problem.

General Purpose AST Tools Increase Cost & Risk and Delay Development

There are numerous static application security testing (SAST) tools available but only a few source code scanners are capable of analyzing Salesforce Apex code. Source code scanners generally produce 30%-70% false positives, so they need to be augmented with other AST tools. Standalone SAST reports waste developers' valuable time with constant false alarms.

Dynamic application security testing (DAST) and interactive application security testing (IAST) tools are then used for runtime execution analysis. IAST can be leveraged to verify that the bugs discovered during source code analysis (SAST) are exploitable, thus significantly reducing the false positives by up to 90%.

Software composition analysis (SCA) tools can discover Common Vulnerabilities and Exposures (CVE) in third-party software libraries, yet none are optimized for the Salesforce environment.

Finally, among a handful of Salesforce configuration review tools available, none specifically addresses application security, so they are of limited use for comprehensive AST as well.

Salesforce Security Issues	S4	Apex SAST tools	DAST/IAST tools
CRUD/FLS Flaws (Authorization Bypass)	✓	✓	
Reflected Cross-site Scripting (XSS)	✓	✓	✓
Stored Cross-site Scripting (XSS)	✓		
DOM Based Cross-site Scripting (XSS)	✓	✓	✓
Lightning Components (DOM & CRUD)	✓	✓	
Lightning Components (CSP & XSS)	✓		
SOQL & SOSL Injection	✓	✓	
Cross-site Request Forgery (CSRF)	✓	✓	
Common Vulnerabilities & Exposures (CVE)	✓		
Weak Session Management	✓		
Weak Integration Endpoints	✓		
Weak Password Controls	✓		✓
Clickjacking Attacks	✓		✓
Access Control (Excessive Permissions)	✓		
Weak Cryptography	✓	✓	

In summary, none of the general-purpose AST tools are effective measures for comprehensively testing SaaS applications and addressing the unique security challenges during and following Salesforce custom development.

Outdated Processes for Today's SaaS Environments

Professional security assessments and application penetration tests are likely to produce the most thorough results for finding security vulnerabilities. However, manual assessments are expensive and disruptive, and are generally only performed annually. For legacy line-of-business applications which are rarely updated, manual assessments may be sufficient; but for SaaS environments where agile development is producing updates weekly or monthly, annual point-in-time assessments are no longer effective application security coverage.

The ad hoc assembly of AST tools and processes needed to compensate for the weaknesses of each tool not only wastes time and money, but increases the risks of violating compliance frameworks, including GDPR, ISO-27001, PCI-DSS, HIPAA, Japan-APPI, and CCPA. It also makes shifting security left and the implementation of DevSecOps unfeasible.

Traditional software development lifecycle (SDLC) does not prioritize security testing. In the fast-moving world of SaaS, security needs to be shifted left and made paramount. Today, the secure development lifecycle (SDL) prioritizes security as core to the entire software creation process, not only reducing risk, but significantly reducing cost with proactive remediation.

To mitigate these risks, application security testing must shift left and be a continuous process.

Shift Security Left into DevOps

Shifting security left in the development process empowers developers to fix vulnerabilities, before they become a problem in production that can lead to exposure of sensitive data. Securing applications during the development process reduces risk and cost while at the same time accelerates the pace of deployment. Yet the kluge of AST tools makes it nearly impossible to integrate into a CI/CD pipeline for Salesforce, undermining security posture with extra cost and complexity, while delaying the development process.

IBM found that the cost to fix an error found after product release was 4 to 5 times higher than if it's uncovered during the design phase, and up to 100 times more expensive than if it's identified in the maintenance phase.

To shift left, Salesforce AST needs to be purpose-built for the seamless, integrated, and full-spectrum detection of vulnerabilities related to customer development and customization.

Purpose-Built for Salesforce DevSecOps with Full-Spectrum Detection

The DigitSec SaaS Security Scanner - S4 for Salesforce - is the only continuous application security testing (CAST) platform purpose-built to enable DevSecOps in the CI/CD pipeline for Salesforce. S4 automates full-spectrum CAST coverage, integrating static source code analysis (SAST), interactive runtime testing (IAST), software composition analysis (SCA), and cloud security configuration review.

No other AST platform seamlessly integrates these capabilities into a single, easy to implement process, allowing teams to establish DevSecOps for Salesforce in under an hour. S4 empowers developers and security teams to collaborate on reducing risk and cost, while increasing agility.

There is no need to settle for high cost, complexity, and development delays when it comes to securing your sensitive Salesforce data; instead, you can conduct full-spectrum analysis quickly, easily and often...without slowing down your teams.

Do you require Security and Compliance for Salesforce? Need DevSecOps now? Get S4.

For more information, contact us at **info@digitsec.com** or visit **www.digitsec.com**.

digitsec

DigitSec, Inc.
214 1st Avenue South, Suite 803
Seattle, WA, 98104, USA
+1 206.659.9521
info@digitsec.com

About DigitSec

DigitSec is a security software company with the only continuous application security testing (CAST) platform purpose-built for Salesforce DevSecOps. DigitSec's patented SaaS Security Scanner™ platform - S4 for Salesforce™- automates and integrates static source code analysis (SAST), software composition analysis (SCA), interactive runtime testing (IAST), and cloud security configuration review, allowing organizations to implement DevSecOps in their CI/CD pipeline in under an hour. S4 strengthens your Salesforce security posture and reduces corporate compliance risk by accelerating your secure software development lifecycle.