S4 - SaaS Security Scanner for Salesforce

Security Assurance for Custom Development on Salesforce

www.digitsec.com | contact@digitsec.com | 206.659.9521 | 214 1st Ave S, B03 Seattle, WA 98104
## Table of Contents

- Product Description ................................................................. 3
- S4 Process ................................................................................. 3
- S4 Design .................................................................................. 4
- S4 Features ............................................................................... 5
- S4 Vulnerability Coverage ...................................................... 6
- S4 Configuration Checks ......................................................... 7
- S4 Results ................................................................................. 8
- Contact Us .............................................................................. 9
Product Description

S4 - SaaS Security Scanner for Salesforce

DigitSec’s flagship product, S4, is a one-of-a-kind product designed to rapidly identify insecurities in SaaS environments. S4 identifies vulnerabilities in Apex code developed using the Force.com development environment. It is a cloud-based application and uses a combination of static code analysis and runtime testing.

S4 Process

Below is the 4-step process implemented by S4:

Review Environment Configuration
S4 for Salesforce reviews the configurations of a Salesforce org and identifies flaws

Scan Source Code
S4 uses a robust client-side static code analysis engine to create call flows to identify CRUD/FLS flaws. It uses data flow analysis to associate Visualforce components to their associated controllers.

Generate Custom Fuzzer
S4 uses white-box fuzzing to rapidly identify injection flaws within Force.com code. All vulnerabilities identified during run-time testing contain Proof of Concept (PoC) exploits. This ensures there are no false positives.

Fuzz Live Salesforce Run-time Instance
S4 launches the custom fuzzer in the installed organization and can be scaled out to as many organizations as needed. All code analyzed remains within the organization preserving intellectual property of the code base.
S4 Design

S4 can be run in both production and in a staging or test environment such as Salesforce Sandbox. The following design represents S4’s system architecture:

Salesforce Metadata API
Used to retrieve, deploy, create, update or delete customization information such as custom object definitions and page layouts.

Salesforce Tooling API
Helps you build custom development tools or apps for Lightning Platform applications.

Salesforce Database
A powerful and intuitive data persistence layer.

Static Engine
Parses your code and converts it into runnable commands.

Runtime Engine
Provides objects to Javascript so it can interact with the outside world.
S4 Key Features

Below is a list of S4’s key features:

**Static Code Analysis**
S4 uses a robust client-side static code analysis engine to create call flows to identify CRUD/FLS flaws. It uses data flow analysis to associate Visualforce components to their assoc. controllers.

**White-box Fuzz Testing**
S4 uses white-box fuzzing to rapidly identify injection flaws within cloud services. All vulnerabilities identified during runtime testing contain Proof of Concept (PoC) exploits. This ensures there are no false positives.

**Signature Based Testing**
S4 comes with various signatures, or patterns known to cause common vulnerabilities in code. Based on these different signature, S4 can uncover flaws other security scanners might miss.

**Verified Exploits**
Runtime testing allows S4 to provide verified exploits.

**Unlimited Scale Out**
S4 is installed per organization and can be scaled out to as many organizations as needed. All code analyzed remains within the organization preserving intellectual property of the code base.

**No Code Limits**
With S4, there are no limitations on the size the code base being scanned. This is to ensure your Salesforce instance will recieve an accurate and complete security review.

**Unlimited Scans**
There is no limit in regards to the number of scans you can run on a single Salesforce instance. With unlimited scans, S4 can become a part of your organizations regular security testing.

**Vulnerability Tracking**
S4 saves the different vulnerabilities it finds in cases. These cases can then be tracked in Salesforce to allow for easier analysis and remediation.

**Lightning Components**
S4 analyzes the security elements and flaws associated with Lightning components.
S4 Vulnerability Coverage

S4 offers the following vulnerability coverage:

- CRUD/FLS Flaws (Authorization Bypass)
- Reflected Cross-site Scripting
- Stored Cross-site Scripting
- DOM Based Cross-site Scripting
- Lightning Components Security
- SOQL Injection
- Cross-site Request Forgery
- Weak Session Management
- Weak Integration Endpoints
- Weak Password Controls
- Click-jacking Attacks
- Access Control (Excessive Permissions)
- Weak Cryptography

Myth vs. Fact

The cloud is a utopia where your data is always secure

The cloud is a cornucopia of low-hanging fruit for hackers
S4 Configuration Checks

S4 performs a thorough configuration review to uncover insecurity in a Salesforce deployment. The following areas are tested by S4:

**CSP Settings**
Content Security Policy (CSP) is an added layer of security that helps detect and mitigate certain types of attacks.

**CORS Settings**
Cross Origin Resource Sharing (CORS) policies allow client side content to be called by other 3rd-party sites.

**Remote Sites**
Remote Sites allow Salesforce to send and receive data on the server side from external 3rd-party sites.

**Password Controls**
S4 checks current password policies and makes recommendations on bolstering password controls.

**Weak Session Management**
Web sessions should protect hardened to protect against data disclosure.

**Excessive Permissions**
Excessive permissions in an environment can lead to data compromise.

**High Number of Administrative Users**
High percentage of administrative users create a high-risk environment.

**Cross Site Request Forgery Settings**
Cross Site Request Forgery settings protect against unauthorized data manipulation.

**Clickjack Attack Protections**
Clickjack attack protections should be enabled to protect users from phishing and other social-engineering attacks.

**Insecure Content Settings**
S4 validates that the Salesforce instance doesn’t have insecure content settings.
S4 Results

With one click, users can pull up an Application Security Report comprised of detailed findings from S4’s scan. Each finding is prioritized based on the level of risk and impact to the organization’s data. From there, S4 provides remediation recommendations and clear guidance on how to effectively fix findings.

- Application Security Report
- Severity of Findings
- Remediation Recommendations
Contact Us

Please don’t hesitate to reach out to us if you have any questions. Our team works around the clock and can answer any sales or technical questions you may have about S4.

Email
Contact@DigitSec.com

Phone
+1 206.659.9521

Address
214 1st Ave S Suite B03, Seattle, WA, 98104

Website
www.DigitSec.com

twitter.com/DigitSec_Inc
facebook.com/DigitSec/
linkedin.com/company/digit-sec/