DigitSec, Inc.

Stopping Hackers in Their Tracks

How S4 identified over 2000 vulnerabilities in a public, tech company's Salesforce environment.

S4 - SaaS Security Scanner for Salesforce

S4 - SaaS Security Scanner for Salesforce (S4), is a security tool developed by DigitSec, Inc. that protects Salesforce organizations from hackers and data breaches. S4 does this by utilizing static code analysis and runtime testing to identify threats and vulnerabilities in Apex code written in the Force.com development environment. As the leading SaaS application security provider, S4 is committed to providing scans which are both robust and thorough. In accordance with that, S4 can be easily scaled out for large organizations and provides Proof of Concept (PoC) exploits for all injection flaws uncovered.

Identifying risks to data in Salesforce with S4

A public tech company known for its ability to manage digital transactions securely has been customizing and developing on Salesforce since 2008. When the General Data Protection Regulation (GDPR) came into effect in late May of 2018, the company's internal security team reached out to DigitSec, Inc. to perform a security scan of their entire Salesforce environment. They had previously relied on a third-party to handle all of their Salesforce customizations, but were not sure whether or not the third-party has used security best practices during the development process. DigitSec, Inc. was chosen to perform the scan, due to S4's ability to analyze all code directly in the organization.

The GDPR is a legal framework that sets guidelines for the collection and processing of personal information of idividuals within the European Union.

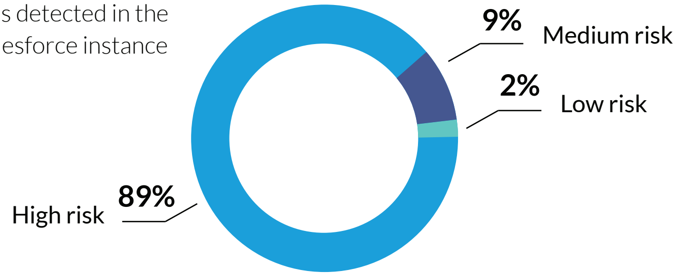
Failure to meet GDPR compliance can result in fines as large as £20 million or 4% or your company's annual global turnover - whichever is higher.

Within hours of launching its security scan of the company's Salesforce environment, S4 was able to rapidly identify over 2000 threats to their data. S4's speed and efficiency stems from its unique application of static code analysis and runtime testing. Static code analysis is used by creating call flows to identify CRUD/FLS flaws. Runtime testing plays a role by utilizing white-box fuzzing to identify injection flaws. After these flaws are identified, they are backed up with Proof of Concept (PoC) exploits to ensure there are no false positives.

S4 uncovered the following risks and vulnerabilities

In total, S4 discovered 1820 high risk issues, 192 medium risk issues, and 42 low risk issues. Among the medium and low risk issues, the risks identified ranged from injection flaws to misconfigurations. The 1820 high risk issues included authorization bypass, injection flaws, cross-site request forgery, cross-site scripting, insecure APIs, and weak credentials. High risk issues are vulnerabilities S4 recommends be dealt with immediately. These are easy target areas for hackers and security openings which if exploited, could have a disastrous result for the company involved.

Types of issues detected in the company's Salesforce instance



S4 provides remediation recommendations

Once the company realized their Salesforce data was in danger, they further enlisted the help of S4 in order to fully understand the threats uncovered and learn how to fix the issues effectively. S4 was able to do this by providing clear vulnerability tracking in Salesforce, and by matching each threat uncovered with an expert remediation recommendation. This allowed the company's internal security team to work through the threats in the order of most importance and resolve each threat with confidence.

Because of the internal security team's diligence in complying with GDPR regulations and S4's robust security scanning, the company escaped imminent threats to their data in Salesforce.

Engagement overview

- Company had been customizing and developing on Salesforce for 10 years
- Company relied on a 3rd party developer who did not use security best-practices
- 2054 total risks and vulnerabilities discovered
- Expert remediation recommendations provided for each threat
- 1 less company at risk from an attack on their Salesforce data