



GUIDE

SecureFlag Platform: **A Comprehensive Guide to Integrations**



SecureFlag offers a suite of plugins and APIs to provide contextual remediation guidance, integrate with Learning Management Systems, tailor training programs based on detected vulnerabilities and much more.

Single Sign-On & User Provisioning	2
SCORM Integration for Learning Management Systems	2
Just-in-Time Training	3
Jira Integration	3
Azure Boards Integration	4
GitLab Integration	5
GitHub Integration	6
SonarQube Integration	7
OpenAPI Third-Party Integration	8
SARIF Integration	9
SecureFlag REST APIs	9

Single Sign-On & User Provisioning

SecureFlag offers a seamless and secure user authentication, supporting integrations with SAML or OAuth-based identity providers. Furthermore, the availability of SCIM for automated provisioning further streamlines user management, offering an efficient, scalable, and secure solution to facilitate smooth operations and an enhanced user experience.

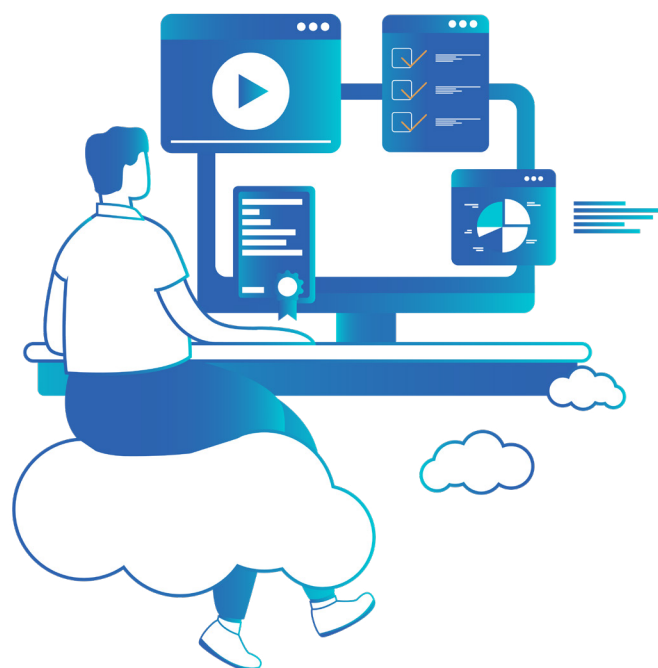


Single Sign On (SSO)

SCORM Integration for Learning Management Systems

Through this integration, organizations can enhance the delivery and tracking of learning experiences.

Our Learning Management Systems integration allows for centralized reporting and analytical insights into learning paths, and it also fosters an enriched learning culture, providing employees with a one-stop solution for all their learning needs.



Just-in-Time Training

SecureFlag offers a wide range of integrations to provide just-in-time training resources that empower and support software developers during their vulnerability remediation tasks. Approaching secure coding training in a manner whereby it is instilled as a critical part of the whole development lifecycle not only streamlines the remediation process but also significantly reduces the time and cost associated with vulnerability fixes.

Jira Integration

SecureFlag's integration with Jira provides contextual security training directly within your Jira issues. When a security vulnerability is identified, SecureFlag provides a link to the relevant training resource, guiding developers through the remediation process with practical, hands-on labs. This integration ensures that developers are equipped with the necessary knowledge to handle identified vulnerabilities, reducing overall remediation time and cost. [Read more](#)

XML entity expansion present in configuration export

 Attach  Create subtask  Link issue  

Description

Reported by an independent researcher yesterday, validated this morning and needs a fix ASAP.

Steps to reproduce:

1. Log into a site as a user with admin permissions and add any marketplace app whilst inspecting network calls with the browser developer console
2. Copy the POST request for adding an app and resend it with the name:

```
1 a</name><<!--
2 <!DOCTYPE foo [
```

SecureFlag Knowledge Base



SecureFlag

XML Entity Expansion

Click [here](#) to find a XML Entity Expansion training lab

Description

XML External Entity Expansion (also referred to as XXE) attacks are used against applications that process XML input by exploiting XML external entity support. By supplying hostile

Azure Boards Integration

The SecureFlag Azure Boards plugin allows for the seamless integration of SecureFlag's contextual security training within your Azure Boards. This integration enables developers to access relevant, hands-on labs and comprehensive instructions to resolve specific vulnerabilities within the relevant programming language. [Read more](#)



SQL Injection

Start SQL Injection Lab



Description

A SQL Injection is not a new or overly complicated type of attack, yet it continues to sit atop the OWASP Top Ten Application Security Risks after more than 20 years of it having been publicly utilized. This is primarily due to its inherent relative ease of use, coupled with its severity of impact when directed toward the staggeringly high number of websites with poorly written, vulnerable code.

SQL is a query language that is designed to access, modify, and delete data stored in relational databases. Numerous web applications and websites use SQL databases as their method of data storage. Applications with a higher prevalence of older functional interfaces such as PHP and ASP are relatively more susceptible to SQL Injection flaws than applications based on more recent technologies.

Applications are vulnerable to attacks when user-supplied data is not validated, filtered for escape characters or sanitized by the application.

An attacker can use SQL Injection to manipulate an SQL query via the input data from the client to the application, thus forcing the SQL server to execute an unintended operation constructed using untrusted input.

Impact

A successful SQL Injection attack can result in a malicious user gaining complete access to all data in a database server with the ability to execute

GitLab Integration

SecureFlag's integration with GitLab provides developers with a comprehensive understanding of identified issues and guides them through the remediation process via practical, hands-on labs. Upon detecting a vulnerability via GitLab scans, SecureFlag steps in to equip developers with the necessary knowledge and skills to handle the identified vulnerabilities, thus reducing remediation time and cost. [Read more](#)

Broken Authentication

Broken Authorization

Broken Cryptography

Code Injection

Cross-Site Request Forgery

Cross-Site Scripting

Inadequate Input Validation

Insufficient Logging

NoSQL Injection

SQL Injection

SQL Injection Vulnerability

SQL Injection in .NET

SQL Injection in ABAP

SQL Injection in Android

SQL Injection in Go Lang

SQL Injection in Java

SQL Injection in NodeJS

SQL Injection in PHP

SQL Injection in Python

SQL Injection in Ruby

Search SecureFlag Security Knowledge Base

SQL Injection / SQL Injection Vulnerability / SQL Injection in Java

SQL Injection in Java

SecureFlag

Play Java Labs on this vulnerability with SecureFlag!

Prevention

Java provides the `PreparedStatement` method of the `Connection` object database to perform parameterized queries on most of the database technologies available.

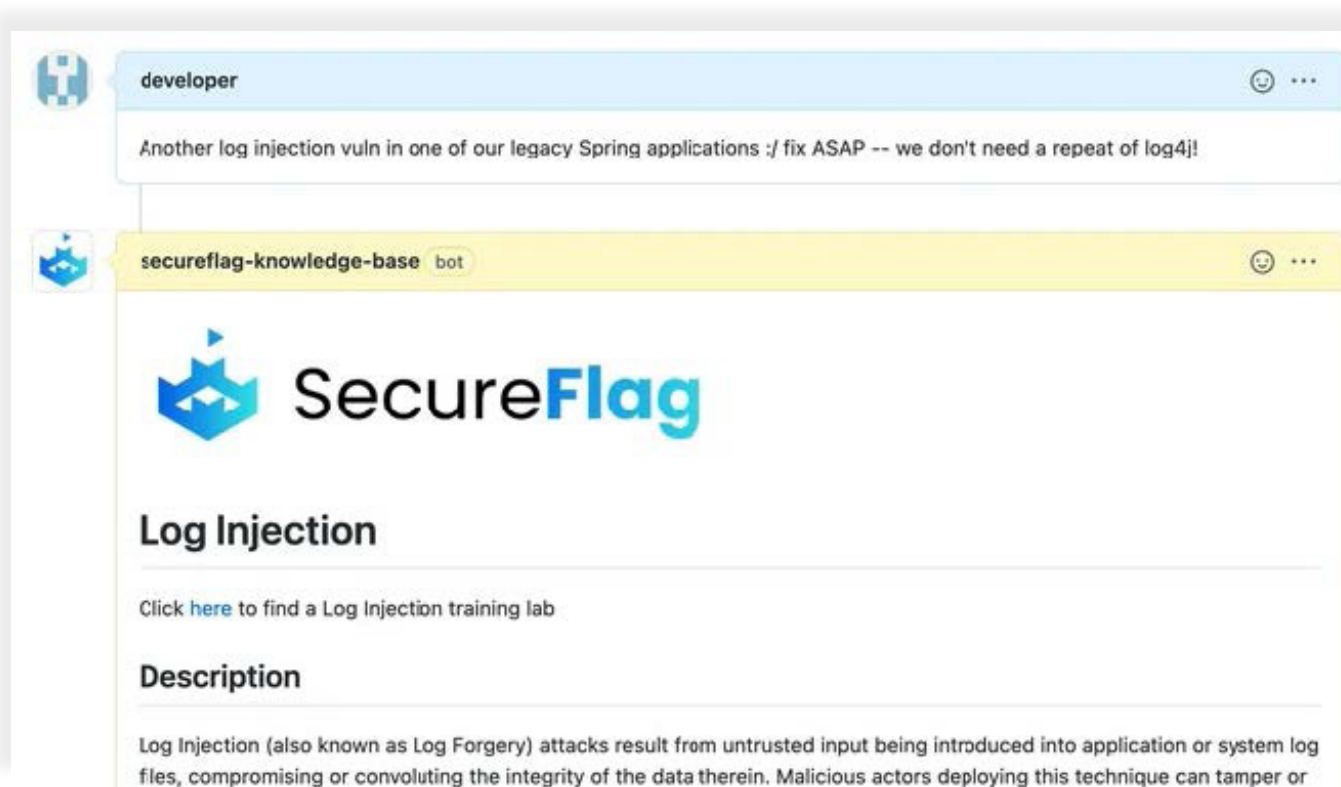
```
String custid = request.getParameter("id");
String query = "SELECT account_number, account_balance FROM customer_data WHERE account_owner_id = ?"
PreparedStatement pstmt = connection.prepareStatement( query );
pstmt.setString( 1, custid);
ResultSet results = pstmt.executeQuery( );
```

Vulnerable example

The following snippet contains a Java application that runs an SQL query to resolve the host supplied by the user.

GitHub Integration

SecureFlag's GitHub integration provides vulnerability remediation and testing advice directly in the developer's issues and pull requests. It also recommends relevant training labs comprising live development environments, ensuring that your team is not only operating efficiently but also deepening their secure coding proficiency [Read more](#)



SonarQube Integration

SecureFlag's integration with SonarQube provides on-demand remediation techniques, recommended hands-on labs, remediation advice, and example code. The plugin adds an additional project page that enumerates over SonarQube's recently detected vulnerabilities and security hotspots to fetch relevant information from the SecureFlag knowledge base.

[Read more](#)



Knowledge Base

Recent Issues

Issue

[Handle the following exception that could be thrown by "sendError": IOException.](#)

[Handle the following exception that could be thrown by "sendRedirect": IOException.](#)

[Handle the following exception that could be thrown by "sendRedirect": IOException.](#)

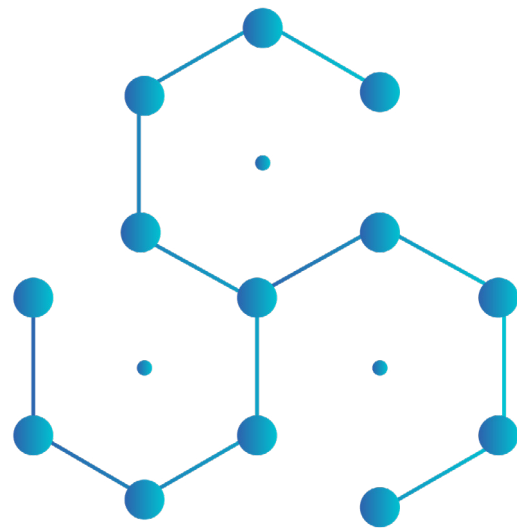
OpenAPI Third-Party Integration

SecureFlag's OpenAPI allows customers and third-party vendors to seamlessly integrate with SecureFlag content and labs, delivering just-in-time security training to their customers. This integration enables software applications to consume SecureFlag's Security Knowledge Base, providing just-in-time training information to developers on how to fix vulnerabilities and offering an example lab in which the developer can practice before performing the remediation. [Read more](#)



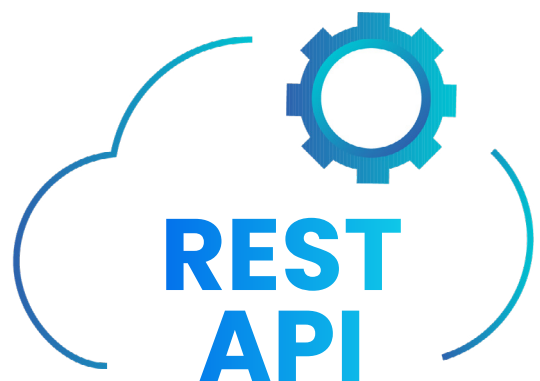
SARIF Integration

SecureFlag also supports integration with the Static Analysis Results Interchange Format (SARIF), a widely adopted standard for representing the results from static analysis tools. This integration allows SecureFlag to ingest vulnerability data from a multitude of static analysis tools that output in the SARIF format. By leveraging this integration, developers can receive contextually relevant, hands-on training based on the vulnerabilities identified by these tools. The SARIF integration enhances the efficiency of the remediation process and ensures developers learn from real-world, relevant security issues identified in their codebase.



SecureFlag REST APIs

In addition to these integrations, SecureFlag also offers a vast collection of restful APIs to further streamline security training processes and make it even easier for customers' teams to access SecureFlag's resources. Through the APIs it is possible to manage users, teams, assignments, retrieve metrics & much more.





Contact us to get started

www.secureflag.com