

SECURITY TESTING METHODOLOGY

WHITEPAPER

July 2025

© 2025 Software AG. All rights reserved.

softwareAG
A SOFTWARE GMBH BRAND

1 Introduction

We at Software AG are cognizant of the growing concerns stemming from security-related incidents and share the same discontent as our customers. We understand that security is imperative to any organization and hence we are committed to employing reliable industry standard practices to ensure security is ingrained at every level of activity surrounding the organization.

Application Security is the discipline of processes, tools and practices aiming to protect applications/ products from vulnerabilities throughout the secure software development life cycle. Effective security practices are important to find, fix and prevent security issues within the applications/ products. It is of immense importance to a company to protect itself and its customers from the constant threat of being hacked.

Security testing plays a key role in identifying, understanding, and rectifying vulnerabilities using various techniques. This paper provides an overview of the product security testing methodologies in use at Software AG.

2 Security Testing Methodology

Software AG suite is made up of components that are used to design, execute, and manage integration solutions. The components fall into three basic categories: design-time components, run-time components, and administrative components.

All the components of Software AG products, where applicable, are tested for security flaws using the following methodologies:

- Design review
- Penetration Testing
- Dynamic Analysis
- Static Analysis
- Third party Components Security Scanning
- Container Security Scanning

2.1 Penetration Testing

Penetration testing of an application or product is a method of evaluating the security level of a computer system or network by simulating an attack from attackers (any person who does not have credentials or authorization to access the systems) and malicious insiders (users who have some access rights to the systems).

© 2025 Software GmbH. All rights reserved.

At Software AG, various activities are involved in pentesting the components and finding potential vulnerabilities that could result from poor or improper:

- Session management
- Data validation
- Business logic
- Multitenancy
- Input/output validation such as cross-site scripting, and SQL injection
- Application specific issues
- Configuration

2.1.1 Dynamic Analysis

Dynamic testing is an important part of application security. This involves the evaluation of an application by executing it in real-time. The focus is to find security vulnerabilities in the application during run time.

In order to identify potential vulnerabilities, a dynamic test involves testing the application by using the web UI. For dynamic security testing, source code access is not required. The general approach is to find vulnerabilities by conducting the attack just like any external attacker would do.

At Software AG, we use dynamic security scanning tools that facilitate the automated detection of security vulnerabilities. Dynamic scanning tools can look for a wide variety of vulnerabilities which primarily include:

- OWASP Top-10
- OWASP IoT Top 10
- OWASP API Top 10
- CWE Top 25 vulnerabilities
- NIST guidelines

2.2 Static Analysis

Static analysis involves testing the application without executing or running it. This type of security testing is complimentary to dynamic testing as it has distinct advantages where-in we identify security flaws by scanning the source code directly. For example, it can evaluate both web and non-web applications from source code and can detect flaws in the software's inputs and outputs that cannot be seen through dynamic web scanning alone.

At Software AG, we use industry recognized static analysis tools to review the program code and search for application coding flaws or other malicious code that could give attackers access to critical company data or customer information.

The scans are done at regular intervals as well as part of the build pipeline. We have an integrated approach of feeding the findings back to the respective development teams which will help in mitigating potential security threats early in the development lifecycle. We perform quality gate checks before releasing our products to ensure that there are no high or critical vulnerabilities left unaddressed.

© 2025 Software GmbH. All rights reserved.

2.3 Third-Party Component Security Scanning

Software AG employs proven solutions for identifying vulnerable 3rd party components at various stages of the SDLC. We have an approval process in place to check the authenticity of the new third-party component when it is newly introduced into our product ecosystem. Later during the development phase, we have a process that is devised and integrated into sandboxes to scan the product artifacts.

Additionally, to provide early feedback the scan is integrated into the product build pipelines. This scanning is performed on a regular basis to monitor new vulnerabilities in third-party components, and we also perform quality gate checks before releasing our products to ensure that there are no high or critical vulnerable libraries. Post-release we continue scanning the released version to identify and address new vulnerabilities.

2.4 Container Security Scanning

At Software AG, we have industry recognized tools and practices in place to scan the docker images at various levels in the complete development cycle. Starting locally, when the base image is mirrored, we scan the respective image to check for vulnerabilities. Then, continuous scanning is performed at all the different stages and through the end of the CI/CD pipeline to provide early feedback.

Towards the end of the release, as a part of quality gate check we perform scans on the release candidate images for known vulnerabilities before deployed to production or released for customers. Post release we continue scanning the published images to identify and address new vulnerabilities.

3 Communications

Software AG publishes Early warning alerts for security issues on a quarterly basis in Empower. This ensures that the customers are notified about the available security fixes for the respective products and versions. The necessary information about the fixes can be seen in the Product Fixes Section in Empower (https://empower.softwareag.com/KnowledgeCenter/Product_Fixes/default.aspx).

To get Early warning updates, customers are encouraged to subscribe to it in Empower (https://empower.softwareag.com/Preferences/ManageMySubscriptions/earlywarnings.aspx).

© 2025 Software GmbH. All rights reserved.

4 Internal and External Penetration Testing

Product suite undergoes internal penetration testing activity before the release. The findings of these assessments must be addressed prior to releasing the product and this data is verified at the quality gate check during release.

5 Other Security Related Activities

Some of the additional activities Software AG undertakes to maximize the security of our products include:

- Training developers to write secure code.
- We subscribe to industry standard newsletters like US-CERT, many Hacker news forums, and other vendor specific security alerts & advisories etc. to be continuously updated on the new threats and attack trends.

6 Feedback

If you have feedback or questions on this whitepaper, please send an email to devsecurity@softwareag.com

© 2025 Software GmbH. All rights reserved.