

# Black Duck Polaris Platform

An integrated, cloud-based AST solution optimized for modern DevSecOps

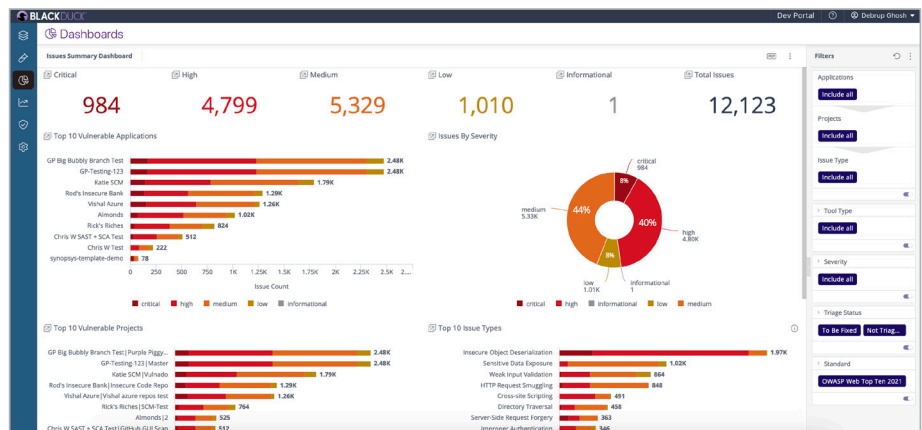
Polaris is an easy-to-use application security platform, optimized for modern DevSecOps, with the power and scalability enterprises need.

## Overview

Black Duck Polaris® Platform is an integrated, software-as-a-service (SaaS) application security platform powered by the industry's leading static application security testing (SAST), software composition analysis (SCA), and dynamic application security testing (DAST) engines. It provides fast, multitype scanning capabilities with highly accurate results triaged by Black Duck security experts. An easy-to-use and cost-effective solution that can scale with business application security needs, Polaris enables application security and development teams to collaborate in real time and meet release deadlines while managing enterprise application risk holistically.

## Key benefits

- **Flexibility.** The on-demand, integrated AppSec platform makes it easy to provision, manage, and monitor enterprise-wide scanning and assessments 24x7.
- **Scalability.** Scale application security cost-effectively. Whether your organization requires testing for a single application or thousands, Polaris delivers a unified SaaS platform to meet your needs.
- **Ease of use.** Easy onboarding, deployment, and testing from a single unified platform. Seamless integration with existing developer, test automation, and CI/CD workflows.
- **Concurrent scanning.** Concurrent scanning improves performance by allowing you to run SAST, SCA, and DAST analysis at the same time. There is no limit to the number of tests you can run.
- **Accurate findings.** Black Duck market-leading SCA, SAST, and DAST engines provide complete and highly accurate results. Expert analysis and triage for SAST results is also available to further improve results by identifying and removing false positive findings.
- **Enterprise visibility.** Polaris dashboards and reports give you a view of vulnerabilities and trends across all your teams and applications.



# Key features

## fAST Static

Polaris fAST Static allows organizations to perform automated static analysis of all codebases, making it easy for developers and testers to find potential security flaws in their code early in the software development life cycle (SDLC).

The screenshot displays the Black Duck fAST Static interface. The top navigation bar includes 'Summary', 'Issues', 'Components', 'Licenses', 'Tests', 'Branches', and 'Settings'. The 'Issues' tab is active, showing a list of 104 matching issues. The table columns are: Issue Type, Location, Filename/Origin, Tool Type, Triage Status, CWE, Vulnerability, Jira ID, and First Detected. The first issue is 'Cross-site Scripting' located in 'src/main/java/org/hdivsamples/controllers/DashboardController.java' with a severity of 'High' and a CWE of 'CWE-79'. Below the table, the 'Issue Details' section for 'Cross-site Scripting' is shown, including the location, severity, and a detailed description of the vulnerability. The description mentions that the application is vulnerable to cross-site scripting because it does not properly sanitize for context HTML PCDATA block. It also provides a list of steps to remediate the issue: 1. Reading data from an HTTP request, which is considered tainted. 2. Concatenating 'file.getOriginalFilename()' to an HTML page allows cross-site scripting, because it was not properly sanitized for context HTML PCDATA block. 3. Perform the following escaping in the following order to guard against cross-site scripting attacks with Java. For example: 'EncodeForHtml()' \* Use the 'EncodeForHtml' function from the OWASP Java Encoder. This escapes the output for HTML. 4. Printing to HTML output.

## fAST SCA

Polaris fAST SCA allows organizations to automate software composition analysis across the SDLC, providing a complete Bill of Materials (BOM) of nonvulnerable and vulnerable open source components, including licenses used, dependency trees, and origins, as well as upgrade guidance.

The screenshot displays the Black Duck fAST SCA interface. The top navigation bar includes 'Summary', 'Issues', 'Components', 'Licenses', 'Tests', and 'Settings'. The 'Components' tab is active, showing a list of 2,921 results across 36 pages. The table columns are: Security Risk, Component Name, Match Type, Usage, and License Name. The first component is 'Apache Ant 1.7.1' with a severity of 'Critical' and a license of 'LGPL-2.1+'. Below the table, the 'Component Details' section for 'Apache Ant 1.7.1' is shown, including the component description, component links, and a list of known short-term vulnerabilities. The 'Dependency Tree' section shows the component's origin and its dependencies, including 'com.synopsys.sig:norby:2021-1029-SNAPSHOT' and 'Cargo Core Ueberjar 1.2.0'. The 'Export Bill of Materials' section is also visible, showing options to export the BOM in JSON or XML format.

# FAST Dynamic

Polaris FAST Dynamic allows organizations to run quick, self-service DAST analysis of modern web applications without slowing development down. No complex configuration or setup required. Automate and scale testing of hundreds of websites easily with built-in settings to choose from.

BLACKDUCK

Dev Portal

greg patton

Insecure Shoppe > project6

Issues Tests Settings

Displaying 16 out of 16 matching issues

Triage All 16

Export All 16

Issue Type	Location	Attack Target	Triage Status	CWE	Vulnerability ID	Fix-By	First Detected
Improper Neutralization of Special Elements used in SQL Co...	https://altorj.tinfoilsecurity.com/altorj/doLogin	uid	Not Triaged	CWE-89		in 5 days	Mar 19, 2024, 1:11 AM
Improper Control of Interaction Frequency	https://altorj.tinfoilsecurity.com		Not Triaged	CWE-770		in 12 days	Mar 19, 2024, 1:11 AM
Use of Web Browser Cache Containing Sensitive Information	https://altorj.tinfoilsecurity.com/admin/		Not Triaged	CWE-525		in 28 days	Mar 19, 2024, 1:11 AM
Exposed Dangerous Method or Function	https://altorj.tinfoilsecurity.com/doSubscribe	Method	Not Triaged	CWE-749		in 28 days	Mar 19, 2024, 1:11 AM
Inadequate Encryption Strength	https://altorj.tinfoilsecurity.com/altorj/feedback.jsp	[TLS_ECDHE_RSA_WITH...	Not Triaged	CWE-326		in 28 days	Mar 19, 2024, 1:11 AM
Insufficient Verification of Data Authenticity	https://altorj.tinfoilsecurity.com/altorj/util/serverStatus...	HostName	Not Triaged	CWE-345		in 28 days	Mar 19, 2024, 1:11 AM
Cross Site Scripting - Reflected	https://altorj.tinfoilsecurity.com/altorj/util/serverStatus...	HostName	Not Triaged	CWE-79		in 28 days	Mar 19, 2024, 1:11 AM

Issue Details Evidence

Location: https://altorj.tinfoilsecurity.com/altorj/util/serverStatusCheckService.jsp?HostName=<script>alert(985510345);</script>

Issue Details

First Detected:  
Mar 19, 2024, 1:11 AM

Fix-By:  
in 28 days (Apr 18, 2024, 1:11 AM)

Issue Type:  
Cross Site Scripting - Reflected

Description:  
Reflected XSS (Non-Persistent) occurs when an injection from one request is displayed in a following response from the web server.

Tool:  
FAST-DAST

Scan Date and Time:  
Mar 20, 2024, 9:29 AM

Vulnerability: Overall Score  
6.1

Severity:  
Medium

## Expert verification and analysis

SAST scan results are reviewed with false positives removed, and critical findings prioritized for timely remediation.

## AI-enabled remediation guidance

AI-driven remediation assistance that provides concise, developer-friendly descriptions with risk information alongside specific code fix recommendations, powered by Polaris Assist.

## Seamless integrations

The easy-to-use platform provides seamless integrations with development and DevOps toolchains.

## Policy management

Customizable rules can be set up in minutes per defined business risk policy.

## Enterprise insights

Get organization-wide insights into the overall health and effective risk posture across apps and projects.

blackduck.com | 3

## Choose the Polaris offering best suited to your needs

Feature	Description	Polaris SAST Subscription	Polaris SCA Subscription	Polaris DAST Subscription	Polaris Package SCA/SAST
<b>fAST Static</b>	Automate static analysis across the SDLC	●			●
<b>fAST SCA</b>	Automate software composition analysis across the SDLC		●		●
<b>fAST Dynamic</b>	Self-serve, automated dynamic web application testing			●	
<b>Expert triage option</b>	SAST analysis results are reviewed by Black Duck security experts to assist with prioritization and false positive removal	●			●
<b>SCM integrations</b>	Quickly onboard applications directly from your repositories	●	●		●
<b>Policy management</b>	Simplify policy management through optimized rules, automating enforcement of security and risk policies	●	●	●	●
<b>Concurrent scanning</b>	Run multiple types of scans on target application simultaneously	●	●	●	●
<b>CI/CD integrations</b>	Automate application security in DevOps pipelines	●	●	●	●
<b>Flexible reports, analytics</b>	Manage risk, measure, and improve your risk posture using enterprise analytics capabilities	●	●	●	●

# Language and package manager support

## SAST languages

- Salesforce Apex
- C/C++
- C#
- DART
- Go
- Java
- JavaScript
- Kotlin
- Objective-C/C++
- PHP
- Python
- Ruby
- Swift
- TypeScript
- Visual Basic

## IaC platforms and formats

- AWS Cloud Formation
- Kubernetes
- Terraform
- YAML
- JSON

## SCA package manager support

- XML
- Apache Ivy
- BitBake
- Cargo
- Carthage
- CocoaPods
- Conan
- Conda
- CPAN
- CRAN
- Dart
- Erlang/Hex/Rebar
- Git
- Go Dep
- Gogradle
- Go Modules
- Go Vendor
- Gradle
- Hex
- Lerna
- Maven
- npm
- NuGet
- Packagist
- PEAR
- pip
- pnpm
- Poetry
- RubyGems
- SBT
- Swift and Xcode
- Yarn

## Source code management (SCM) system support

- GitHub
- GitLab
- Azure DevOps
- Bitbucket

## About Black Duck

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at [www.blackduck.com](https://www.blackduck.com).

©2025 Black Duck Software, Inc. All rights reserved. Black Duck is a trademark of Black Duck Software, Inc. in the United States and other countries. All other names mentioned herein are trademarks or registered trademarks of their respective owners. May 2025