Application Security Testing Stack Up: StackHawk versus Netsparker

To make the most out of application security testing, you're going to need the right platform to back you up. Ideally, whatever tooling you go with will make it easier to find and fix bugs before they hit production, and integrate seamlessly with whatever tools you are already using in your CI/CD pipeline.

We have put together a quick comparison guide to make sure whatever product you buy, you get the right set of capabilities to modernize your application security testing.

Feature	STACKHAWK	ri
Dynamic Security Testing Scanner	✅	✅
Server Side HTML Scanning	✅	✅
Single Page Application Scanning	✅	✅
REST API Scanning	✅	✅
GraphQL API Scanning	✅	❌
Authenticated Scanning	✅	⚠️
Scan History and Reporting	✅	✅
Language Agnostic	✅	✅
Infrastructure Agnostic	✅	❌
Deployed via Docker	✅	❌
Automated CI/CD Scanning Pre-Deployment Modern DAST tooling should allow for scans wherever your application is deployed in CI/CD.	✅	❌
Local Development Scanning Ability to run scans in a local development environment to find potential vulnerabilities before opening a pull request or validate CI/CD findings.	✅	❌
Recreate Findings via cURL Command Auto generated cURL commands that equip developers to quickly reproduce and debug scan findings.	✅	❌
Manage Config as Code Configuration managed with version control and scalable overlays via yaml.	✅	❌
Built for Microservice Scanning Find vulnerabilities in the underlying microservices so that you can fix them quickly, before deploying to the production application.	✅	❌

Still Not Sure?

If you're looking for information on something not mentioned in this guide check out our docs or schedule a live demo at StackHawk.com. We offer a free, no credit card required 14-day trial to make sure our platform offers you everything that you need. No buyer's remorse here!