Fortify WebInspect (DAST)

Fortify WebInspect is a dynamic application security testing (DAST) tool that identifies application vulnerabilities in deployed web applications and services.

Fortify WebInspect by OpenText™ is an automated DAST solution that provides comprehensive vulnerability detection and helps security professionals and QA testers identify security vulnerabilities and configuration issues. It does this by simulating real-world external security attacks on a running application to identify issues and prioritize them for root-cause analysis. Fortify WebInspect by OpenText has numerous REST APIs to benefit integration and has the flexibility to be managed through an intuitive UI or run completely via automation. Fortify WebInspect also has a single, cohesive method of defining authentication, whether it be static, dynamic, or pulling tokens from macros.

Product Highlights

Automation with Integration
Fortify WebInspect can be run as a fully-automated solution to meet DevOps and scaling needs, and integrate with the SDLC without adding additional overhead.

- REST APIs help achieve a tighter integration and help automate scans and check whether compliance requirements have been met.
- Leverage prebuilt integrations for OpenText™ Application Lifecycle Management (ALM) and OpenText™ Quality Center, and other security testing and management systems.

- Powerful integrations allow teams to re-use existing scripts and tools. Fortify WebInspect can easily integrate with any Selenium script.
- Scan RESTful web services: supports Swagger and OData formats via WISwag command line tool, enabling Fortify WebInspect to fit into any DevOps pipeline.
- Base settings: ScanCentral Admin can pre-configure a scan template and provide that to users to scan their apps—no security knowledge needed.
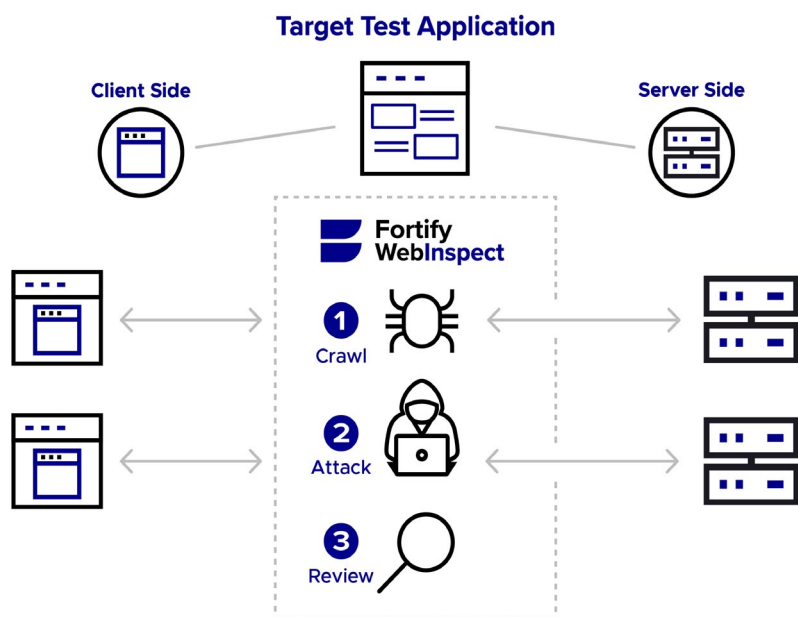
Key Features

Functional Application Security Testing (FAST)
Don't be limited by IAST! FAST can take all the functional tests and use those in the same way IAST does, but then it keeps crawling. Even if a functional test misses something, FAST won't miss it.

Hacker-Level Insights
View findings such as client-side frameworks and the version numbers—findings that could become vulnerabilities if not updated.

HAR Files for Workflow Macros
Fortify WebInspect can use HAR files for workflow scanning, ensuring important content is covered during scans.

Manage Enterprise Application Security Risk
Monitor trends within an application and take action on the most critical vulnerabilities first to meet DevOps needs.

Flexible Deployment
Start quickly and scale as needed with the flexibility of on-premise, SaaS, or AppSec-as-a-service.

Compliance Management
Pre-configured policies and reports for all major compliance regulations related to web application security, including PCI DSS, DISA STIG, NIST 800-53, ISO 27K, OWASP, and HIPAA.

Increase Speed with Horizontal Scaling
Horizontal scaling creates little versions of Fortify WebInspect using Kubernetes that just focus on processing JavaScript. This allows the scans to work in parallel, allowing for much faster scans.

Scan Any API for Improved Accuracy
WebInspect allows users to configure API scanning to cover any authentication scenario with GraphQL, gRPC, SOAP, Postman, and Swagger. It also allows users to automatically pull bearer tokens from an identity provider.

Client-side Software Composition
Client-side Software Composition Analysis (SCA) provides CVEs of client-side libraries, health data of open source projects, and an exportable CycloneDX SBOM.

Key Benefits

Find Vulnerabilities Faster and Earlier

Fortify WebInspect can be tuned and optimized for your application to find vulnerabilities faster and earlier in the SDLC. Enhance scan with agent technology that expands the coverage of the attack surface and detects additional types of vulnerabilities.

- Fortify WebInspect Agent integrates dynamic testing and runtime analysis to enhance your findings and scope. It identifies vulnerabilities by crawling more of the app, expanding coverage of the attack surface, and exposing exploits better than dynamic testing alone.

Prioritization with advanced technologies:

- Run custom policies that are tuned towards high speed with policy manager.
- Simultaneous crawl and audit.
- Deduplication: Reduce number of attacks sent, by avoiding scanning the same class/function in a different part of the app.
- Redundant Page Detection allows for reduced scan times.
- Fix vulnerabilities faster as devs are provided with line of code detail and return stack trace info.
- Fortify WebInspect continues to scan, even in two-factor authentication (2FA) environments.

Save Time with Automation and Agent Technology

- Save time and resources with features like redundant page detection, automated macro generations, incremental scanning, and containerized delivery.
- Optimize the scanning process, increase speed, and improve accuracy.

Crawl Modern Frameworks and Web Technologies

Fortify WebInspect crawls modern frameworks and web technologies with a comprehensive audit of all vulnerability classes.

- Support for the latest web technologies including HTML5, JSON, AJAX, JavaScript, HTTP2, and more.

- Test for a new class of vulnerabilities called "Out of Band" or OAST Vulnerabilities. Using the public Fortify OAST server, Fortify WebInspect can detect OAST vulns such as Log4Shell.
- Single Page Application (SPA) Detection supporting these common frameworks: Angular, AngularJS, React, GWT, Vue, Dojo, and Backbone.
- Test mobile-optimized websites as well as native web service calls.
- Fortify WebInspect provides features like automatic macro generation, macro validation, and fix validation, to enable small teams to detect and remediate vulnerabilities at scale.
- Run Linux versions of WebInspect and ScanCentral DAST through the API.

Manage Enterprise AppSec Risk with Fortify ScanCentral DAST

Manage application security risk across the enterprise with reports for remediation and management oversight. Monitor trends and take action on vulnerabilities within an application. Build an enterprise-wide AppSec program that manages and provides visibility to your risk profile via dashboards and reports, so you can confirm remediation, track metrics, trends and progress. Fortify ScanCentral DAST can be used as an orchestration platform to run hundreds of thousands of scans, enabling a small team of AppSec professionals to manage an entire organization.

- **SCDast Visualization**: View and triage DAST vulnerabilities in SCDast.
- **User and Domain Restrictions**: Centralized managed of DAST users is complex. User and Domain restrictions allow an admin to put rules in place to ensure quality scans when using ScanCentral DAST in a self-service model.
- **PostGresSQL:** MS SQL is an expensive option for a database, so PostGresSQL provides another option when installing Fortify ScanCentral DAST without sacrificing speed and quality.
- Fortify ScanCentral DAST integrates with Kubernetes for scaling sensors, giving both cost savings and ensuring each scan has a new enviroment to run on.

Connect with Us
www.opentext.com

- **Fortify ScanCentral Credential Management**: Save time and update all passwords in one place.
- **Fortify ScanCentral DAST repo integration:** Pull scan configuration artifacts from a repository at runtime, no need to update settings configurations.

About Fortify

Fortify by OpenText™ offers a comprehensive suite of products that bring holistic security and visibility to developers and AppSec professionals. Fortify provides automated integrations for any tool, anywhere in the SDLC, and a robust set of capabilities available on-premise, cloud-hosted, or as-a-service.

About Cybersecurity

OpenText™ Cybersecurity is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from OpenText™ Cybersecurity Data Security, ArcSight, and Fortify, the Cybersecurity Security Intelligence Platform uniquely delivers the advanced correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Learn more at
www.opentext.com/products/fortify-webinspect

opentext™ | Cybersecurity