Fortify WebInspect (DAST)

Fortify WebInspect is a dynamic application security testing (DAST) tool that identifles 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

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
Get a complete story around APIs, whether it's SOAP, Rest, Swagger, OpenAPI, Postman, GraphQL, or gRPC.

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.