HP WEBINSPECT

Quickly identify exploitable security vulnerabilities in Web applications, from development through production.

Data sheet

The leader in Web application security assessment

HP WebInspect is the industry leading Web application security assessment solution designed to thoroughly analyze today's complex Web applications and Web services for security vulnerabilities. It delivers broad technology coverage, fast scanning capabilities, extensive vulnerability knowledge, and accurate Web application scanning results. HP WebInspect is an integral part of the HP integrated security testing technologies that uncover real and relevant security vulnerabilities in a way that siloed security testing cannot.

Enable broader lifecycle adoption through security automation

HP WebInspect is dynamic application security testing software for assessing security of Web applications and Web services. HP WebInspect gives security professionals and security novices alike the power and knowledge to quickly identify and validate critical, high-risk security vulnerabilities in applications running in development, QA or production.

Increase modern Web technology coverage
Most application scanners are designed for simple, fairly static Web technologies and lack the sophistication required to scan the complexities of today's interactive, Web 2.0 applications. HP WebInspect leads the way in intelligent scanning, allowing you to assess your entire application, no matter the architecture or technology. Innovations of HP WebInspect include:

- **JavaScript/Ajax:** HP WebInspect technology will trace and record code paths through JavaScript, fully analyzing how the application changes from the user's perspective as well as watch the Ajax and web service requests and then make attacks to the server-side application accordingly to reveal vulnerabilities.
- **Adobe Flash:** HP WebInspect addresses security vulnerabilities that exist within applications using Adobe Flash technologies by decompiling Flash files and performing static analysis on the resulting code to detect vulnerabilities.

Accelerate security through more actionable information
HP WebInspect doesn't just discover security vulnerabilities that someone else needs to fix, it interactively communicates the security knowledge needed to reproduce and fix the issues. Through cooperation with HP Fortify solutions and integrations with HP Quality Center and HP Application Lifecycle Management, HP WebInspect's first-class knowledge base provides comprehensive details about the vulnerability detected, the implications of that vulnerability if it were to be exploited, as well as best-practices and coding examples necessary to quickly pinpoint and fix the issue.

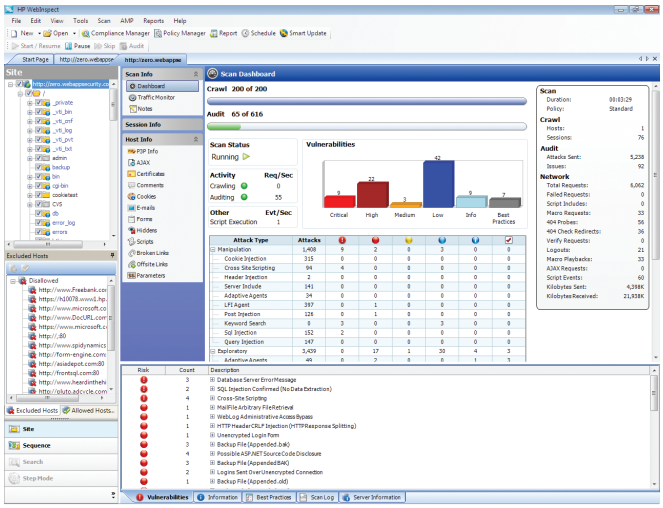
Find more vulnerabilities and fix them faster with HP WebInspect Real-Time

HP WebInspect Real-Time is a new bundled application security solution that combines the advanced dynamic application security testing technology of HP WebInspect with the real-time application security technology of HP Fortify SecurityScope for dramatically improved scan results over previous dynamic application security testing approaches.

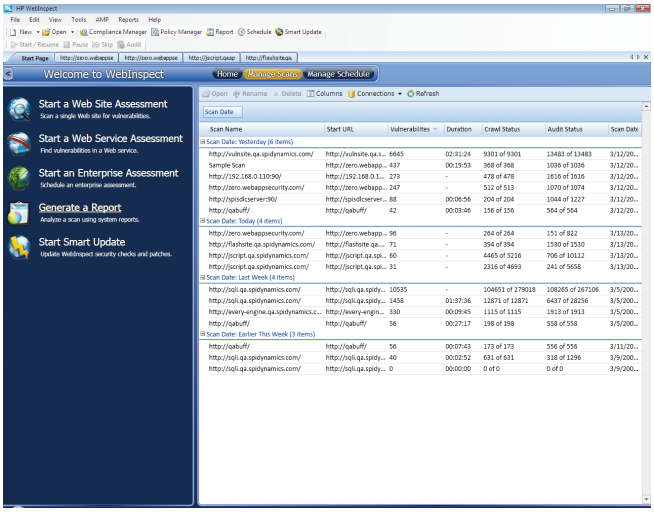
When used in conjunction with HP Fortify SecurityScope, HP WebInspect Real-Time can stimulate an application through automated, external security attacks, and then gather internal, code-level vulnerability information by observing the attacks in the code as they happen in real-time. HP WebInspect Real-Time identifies and crawls more of an application to expand the coverage of the attack surface and detect new types of vulnerabilities that can go undetected by siloed security testing technologies.

Elevate security knowledge across the business
HP WebInspect has the most powerful reporting system available, delivering a fast, flexible, and scalable instrument for communicating meaningful results from your application security assessment. In addition to the many standard report templates, HP WebInspect's simple report designer allows you to develop and generate fully customized reports that deliver the relevant knowledge to key stakeholders in a professional and polished format. HP WebInspect can also include data from external sources, providing full

WebInspect Scan Dashboard
Dashboard delivers real-time visibility into and interactivity with test results



WebInspect Scan Database
Easily manage, view and share your security test results and history



enterprise-grade reporting. HP WebInspect also features interactive vulnerability review and retest features that enhance the security team's ability to validate discovered issues and regression test fixes from development. This closed feedback loop from security testing through development improves the overall security effectiveness of application teams.

Comply with legal, regulatory, and architectural requirements

Along with the increase in Web application attacks there are now many additional legal, regulatory, and best practice requirements related to application security. HP WebInspect gives you the capabilities to easily address these additional requirements in a cost efficient manner. HP WebInspect includes detailed reports that show how your Web applications meet government regulations and industry standards, as well as what changes are required for compliance. In addition, users can create new policies or customize existing ones. The sophisticated reporting system allows you to easily create, modify, or enhance the information reported. HP WebInspect includes pre-configured policies for every relevant regulation, and best practices including the Payment Card Industry Data Security Standard (PCI DSS), OWASP Top 10, ISO 17799, ISO 27001, Health Insurance Portability and Accountability Act (HIPAA), and many more.

Leverage automation to do more with less

Every organization is faced with the challenges of doing more with less. HP WebInspect delivers the ability to drive significant results in the most efficient way. HP customers report a 60% decrease in application security research costs, a 56% improvement in application security assessment activities as well as a 36% reduction in the total cost of audit and compliance.[1] With the combination of the intuitive usability, intelligent scanning engines, first-class knowledge base, concurrent scan execution, live scan results, a tabbed workspace, and superior reporting, HP WebInspect helps you maximize the use of your valuable time, lower the cost of security vulnerability assessment and remediation, while reducing the risk of your Web applications to your business.

Build an enterprise-wide application security program

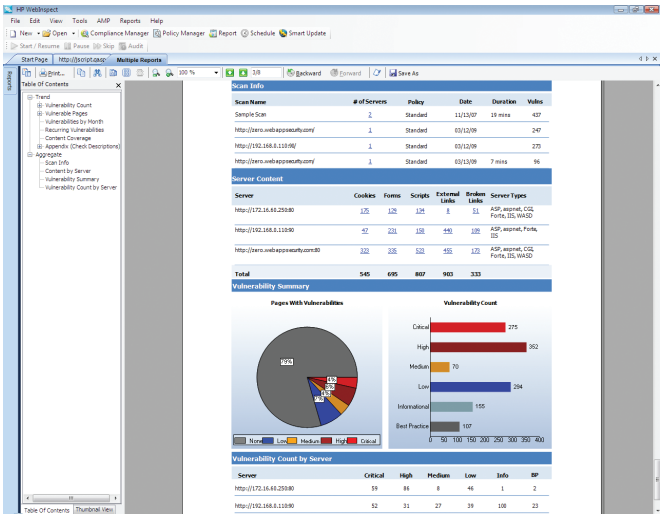
HP WebInspect integrates with HP Assessment Management Platform software for enterprise-wide, distributed assessment capabilities. HP Assessment Management Platform provides a scalable platform to assess Web applications across your entire enterprise and an organization-wide view of application security giving you the knowledge to make informed risk management decisions. HP Assessment Management Platform also allows you to easily integrate results from other solutions across the application lifecycle, including HP Fortify and HP QAInspect, as well as with other key management systems and security sources, so your business can build a mature application security program.

HP Web Security Research Group

All HP Application Security Center Software is informed by the expertise and threat intelligence from the HP Web Security Research Group. The HP Web Security Research Group is a team made up of leading security researchers dedicated to being at the forefront of web application vulnerability discovery and innovation. This team's extensive research not only provides the latest innovations in web application vulnerability assessment but also automatically generates regular and timely updates to all products via HP SmartUpdate.

[1] Quantifying the value of investments in Application Security, ROI Whitepaper, Hewlett Packard, February 2009

WebInspect Trend Reporting:
View and analyze vulnerability trends over time to track application security progress and efficiency



Key features and benefits

Innovative assessment technology

- Advanced client-side scripting technology to analyze JavaScript, Flash, and others
- Produce faster scans and more accurate results through simultaneous crawl and audit and concurrent scanning
- Advanced macro recording technology and flexible authentication handling for improved session management in complex applications
- Increase accuracy of detection using Intelligent Engines designed to imitate a hacker's methodology
- Innovative application architecture profiler assists in tuning the scan configuration and recommends improvements in site coverage and accuracy
- List-driven assessments for targeted and efficient application scanning
- Optimizations for depth-first crawling option for websites that enforce order-dependent navigation
- Fingerprinting of Web framework using Smart Scan technology to reduce unnecessary attacks

HP WebInspect Real-Time

- Integrated dynamic and real-time analysis to find more vulnerabilities and fix them faster
- Works in concert with HP Fortify SecurityScope to observe attacks at the code level during dynamic scans
- Identify and crawl more of an application to expand the coverage of the attack surface and detect new types of vulnerabilities
- Provides stack traces and line-of-code detail to confirmed vulnerabilities

Interactive vulnerability review and management

- Streamlined vulnerability review process enables user to interact with test results
- Flexible vulnerability results view for grouping and filtering of results
- Displays detailed steps to reproduce a vulnerability and show how it was identified
- Retest a single vulnerability by re-executing the series of steps to validate or regression test a fix
- Enter manual findings and attach screenshots and documents to test results for better context and communication
- Persist test results across scans

Advanced web services security testing

- Support for complex data types for rendering advanced WSDLs and specifying test data
- Automatically discover and audit web services embedded in an application
- Focused web service attacks and fuzzing
- Web Service Security Designer tool for configuring web service security tests

Refined and simple usability

- Quickly initiate simple or regression scans with minimal configuration for immediate results
- Walk through an intuitive wizard to setup a scan and begin reviewing results within seconds
- Review and control multiple simultaneous scans and reports through a tabbed interface
- Submit false positive reports and other feedback directly and securely to HP in just a couple clicks
- Create reusable, componentized macros to record testing steps and login procedures
- Develop custom attacks and policies quickly and easily using the custom check wizard

Actionable remediation and compliance reports

- Run compliance reports for all major regulatory standards, including PCI, SOX, ISO, and HIPAA
- Create flexible, extensible, and scalable reports that match your business
- Simplify repetitive report generation through report templates
- Customize fonts, colors, and backgrounds with the style editor allowing you to generate scan reports with a professional, polished appearance
- Assess application security trends and readiness

Key integrations

- Integrate into your defect management processes with out-of-the-box integrations with HP Quality Center
- Integrate into your enterprise application security management process with an out-of-the-box integration with HP Assessment Management Platform software
- Extensive data export via XML for open integration with other security management systems
- Include information from external data sources in your reports via ODBC, SQL, or XML connections

Advanced tools for penetration testers (HP Security Toolkit)

- **Report Designer:** allows you to create new reports or customize the ones from HP, combine external data sources, edit the style, and create custom user input
- **SQL injector:** extract entire databases by using SQL injection vulnerabilities
- **Cookie cruncher:** analyze the strength of cookies to avoid session hijacking
- **Encoder:** translate different encryption and encoding standards
- **HTTP editor:** create and edit raw HTTP requests
- **Regex editor:** test and build regular expressions
- **Web Service Test Designer:** generate and edit raw Web services requests
- **Web Fuzzer:** identify buffer overflows using HTTP fuzzing or modify input variables
- **Web Proxy:** view every request and server response while browsing a site
- **WebBrute:** test the strength of login forms or Web and proxy authentication systems
- **WebDiscovery:** identify and discover which Web servers and Web applications are behind which ports
- **Server analyzer:** identify a Web server or device and perform deep SSL analysis
- **Traffic monitor:** monitor every HTTP request and response sent during the crawl and audit

For more information

Learn more about application security; visit:
www.hp.com/go/securitysoftware

Connect with peers and HP Software experts; visit:
www.hp.com/go/swcommunity

HP Fortify Software Security Center

HP WebInspect is a part of the HP Fortify Software Security Center suite, a comprehensive solution for automating and managing an application security program in the enterprise. HP Fortify Software Security Center proactively eliminates the immediate risk in legacy applications, as well as the systemic risk in application development processes.

HP WebInspect checks for:
Data injection and manipulation attacks

- Reflected cross-site scripting (XSS)
- Persistent XSS
- DOM-based XSS
- Cross-site request forgery
- SQL injection
- Blind SQL injection
- Buffer overflows
- Integer overflows
- Log injection
- Remote File Include (RFI) injection
- Server Side Include (SSI) injection
- Operating system command injection
- Local File Include (LFI)
- Parameter Redirection
- Auditing of Redirect Chains

Sessions and authentication

- Session strength
- Authentication attacks
- Insufficient authentication
- Insufficient session expiration

Server and general HTTP

- Ajax auditing
- Flash Analysis
- HTTP Header Auditing
- Detection of Client-side Technologies
- Secure Sockets Layer (SSL) certificate issues
- SSL protocols supported
- SSL ciphers supported
- Server misconfiguration
- Directory indexing and enumeration
- Denial of service
- HTTP response splitting
- Windows® 8.3 file name
- DOS device handle DoS
- Canonicalization attacks
- URL redirection attacks
- Password auto complete
- Cookie security
- Custom fuzzing
- Path manipulation—traversal
- Path truncation
- WebDAV auditing
- Web services auditing
- File enumeration
- Information disclosure
- Directory and path traversal
- Spam gateway detection
- Brute force authentication attacks
- Known application and platform vulnerabilities

4AA1-5363ENW, Created September 2007; Updated July 2011, Rev. 4