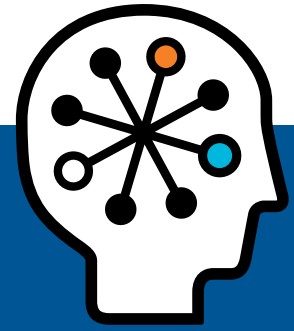




HP WebInspect Software

Data sheet



HP WebInspect software is an industry leading Web application security assessment software designed to thoroughly analyze today's complex Web applications. It delivers fast scanning capabilities, broad assessment coverage, extensive vulnerability knowledge, and accurate Web application scanning results.

The leader in Web application security assessment

HP WebInspect addresses the complexity of Web 2.0 and identifies security vulnerabilities that are undetectable by traditional scanners. Catering to both security professionals and security novices alike, HP WebInspect easily tackles today's most complex Web application technologies, including JavaScript, Adobe® Flash, Ajax, and SOAP. It utilizes break-through testing innovations by HP, which results in fast, accurate, and automated Web application security tests.

HP WebInspect's extensive security knowledge gives areas of an organization, which are new to application security, the ability to bring the extensive knowledge of a highly trained security professional to their fingertips. Fully backed by the HP Web Security Research Group and HP SmartUpdate, HP WebInspect makes sure you are testing for the latest known vulnerabilities in your applications before the hackers do.

Identify and remediate security vulnerabilities in your Web applications and services

HP WebInspect is easy-to-use, extensible, and accurate Web application security assessment software. HP WebInspect gives security professionals and novices

the power and knowledge to easily identify and remediate critical and high-risk security vulnerabilities in your Web applications and Web services.

Support your latest application environments

Most application scanners are designed for legacy Web technologies and lack the intelligence required to scan the complexities of today's Web 2.0 applications. HP WebInspect leads the way in intelligent scanning allowing you to assess your entire application and their architecture. Web 2.0 Innovations of HP WebInspect include:

- **Adobe® Flash:** In an industry first, HP WebInspect addresses security vulnerabilities that exist within applications using Adobe® Flash technologies. HP WebInspect will find Adobe® Shockwave Flash (SWF) files, decompile them, and then perform static analysis on the resulting ActionScript 3 code, detecting vulnerabilities such as insecure programming practices, insecure application deployment, Adobe® "best practices" violations, and information disclosures.
- **JavaScript/Ajax:** Heavy client-side JavaScript applications have changed the game when it comes to application security assessment. HP WebInspect's superior technology will trace and record code paths through the JavaScript, fully analyzing how the application changes from the user's perspective as well as watch the Ajax requests and then make attacks to the server-side application accordingly to reveal vulnerabilities.

The knowledge for application security success

HP WebInspect brings the intellect and knowledge of a highly skilled security professional to your organization enabling your teams to accurately assess your organization's Web applications for security vulnerabilities. HP WebInspect is easy to configure and use with its intuitive wizard interface allowing even the security novice to execute a fully automated Web application assessment quickly.

Figure 1: WebInspect Scan Dashboard

The WebInspect scan dashboard delivers real-time scan results visualizing a deep understanding of the scan taking place

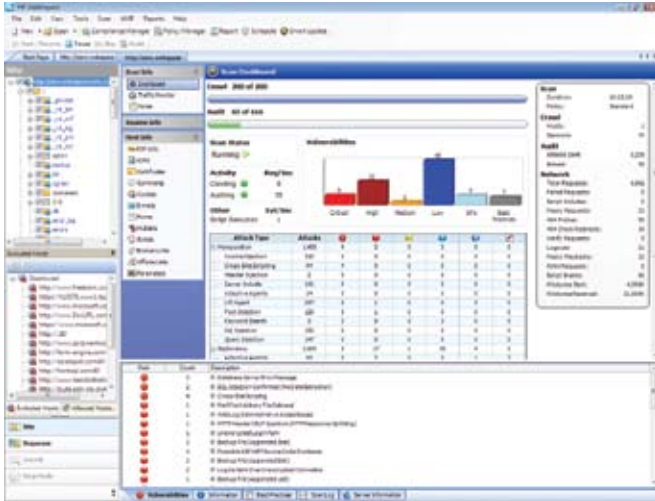
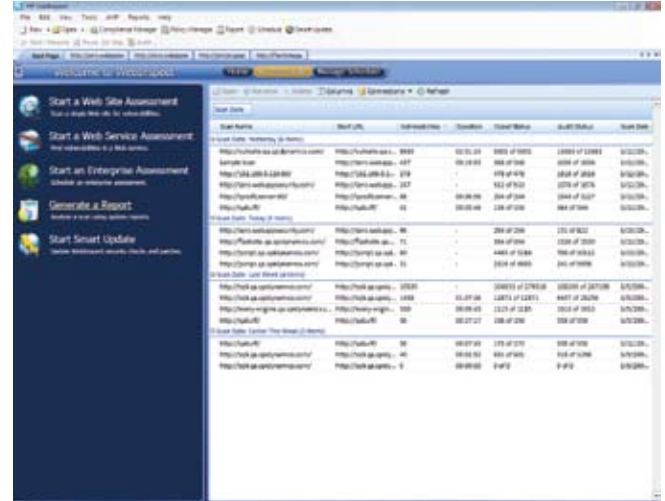


Figure 2: WebInspect Scan Database

Easily manage and view your scan results and history



HP WebInspect doesn't just discover security vulnerabilities quickly and accurately, but it also delivers the security knowledge needed to fix and remediate the issues. 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 remediate the issue.

Deliver knowledge to stakeholders across the business

HP WebInspect has the most powerful reporting system in the industry, 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 easy-to-use 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. The reporting capabilities are not just limited to the scan analysis or details from the knowledge base, HP WebInspect can also include data from external sources providing full enterprise-grade reporting.

It is important for you to be able to easily integrate HP WebInspect into your existing defect remediation processes and provide detailed knowledge needed by developers so that they can quickly fix vulnerabilities. HP WebInspect integrates out-of-the-box with the industry leading HP Quality Center software as well as IBM® Rational® ClearQuest® software.

Easily address legal and regulatory compliance

With the increase in Web application attacks have also come many additional legal, regulatory, and best practice requirements related to application security that need to be adhered to. 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 regulations and 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 major law, regulation, and best practices, including the Payment Card Industry Data Security Standard (PCI DSS), Open Web Application Security Project (OWASP) Top 10, ISO 17799, ISO 27001, Health Insurance Portability and Accountability Act (HIPAA), and many more.

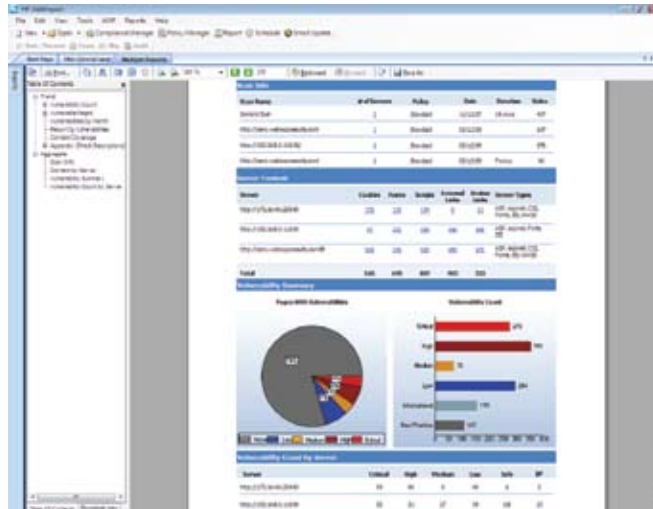
Do more with less

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 percent decrease in application security research costs, a 56 percent improvement in application security assessment activities as well as a 36 percent reduction in the total cost of audit and compliance¹. 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 makes sure you can maximize the use of your valuable time, lower the cost of security vulnerability assessment and remediation, while minimizing the risk of your Web applications to your business.

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

Figure 3: WebInspect Trend Reporting

View and analyze vulnerability trends over time, which allows an organization to track their progress, efficiency, and make improvements



Build an enterprise-wide application security program

HP WebInspect integrates with HP Assessment Management Platform (AMP) software for enterprise-wide and distributed assessment capabilities. HP AMP 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 business decisions. HP AMP also allows you to easily add and integrate other solutions across the entire application lifecycle, including HP DevInspect 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 AMP is also available in a Software as a Service (SaaS) model so organizations can instantly get up and running, and see a very quick time-to-value.

HP Web Security Research Group

All HP Application Security Center software is backed by the HP Web Security Research Group. The HP Web Security Research Group is made up of industry's leading security researchers dedicated to being at the forefront of Web application vulnerability discovery and innovation. The team consists of acclaimed authors and spokespeople. Their extensive research not only provides the latest innovations in Web application vulnerability assessment but also regular and timely updates to all HP Application

Security Center Products. This is done through the HP SmartUpdate function, giving you the additional knowledge and skills within your security program.

Key features and benefits

Innovative assessment technology

- Statically analyze client-side Adobe Flash applications
- Produce faster scans and more accurate results through the Simultaneous Crawl and Audit (SCA) technology
- Reduce false negatives and broaden coverage using scan technology built specifically for today's complex applications
- Reduce false positives using Intelligent Engines designed to imitate a hacker's methodology
- Increase testing throughput with support for multiple concurrent scans
- Enter a URL, username, and password to quickly initiate a simple scan for immediate results
- Innovative scan profiler assists you in optimizing the scan configuration to maximize the effectiveness and accuracy of the scan
- Depth-first crawling option for websites that enforce order-dependent navigation
- Fingerprinting of Web framework using Smart Assessment technology to reduce unnecessary attacks

HP WebInspect checks for: Data injection and manipulation attacks

- Reflected cross-site scripting (XSS)
- Persistent 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

Uncomplicated usability

- Walk through a wizard to setup a scan, or jump right in with 'Scan Now' option
- View scan results within seconds of starting an assessment
- Review and control multiple scans and reports through a tabbed interface
- Submit false positive reports and other feedback directly and securely to HP in just a few clicks
- Create macros to record testing steps and login procedures and test them before starting the scan
- Develop custom attacks quickly and easily using the custom check wizard

True enterprise reporting and compliance

- 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, and polished appearance
- Tailor reports for the reader to focus on issues that matter most to them
- Run compliance reports for all major regulatory standards, including PCI, ISO, and HIPAA
- Analyze application security trends and readiness

Key integrations

- Integrate into your defect management processes with out-of-the-box integrations with HP Quality Center and IBM® Rational® ClearQuest® software
- Integrate into your enterprise application security management process with an out-of-the-box integration with HP AMP software or utilize extensive XML output functionality
- Include information from external data sources in your reports through 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
- **SOAP editor:** 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 Secure Socket Layer (SSL) analysis
- **Traffic monitor:** monitor every HTTP request and response sent during the crawl and audit

For more information

To learn more about HP WebInspect software, go to www.hp.com/go/securitysoftware

Contact information

To find an HP Software sales office or reseller near you, visit www.managementsoftware.hp.com/buy

Technology for better business outcomes

To learn more, visit www.hp.com/go/securitysoftware

© Copyright 2007–2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. Windows Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

4AA1-5363ENW Rev. 1, April 2009

