HP QAInspect software

Data sheet

HP QAInspect software allows quality assurance (QA) professionals to incorporate fully-automated Web application security testing into your overall test management process without the need for specialized security knowledge and without the risk of slowing aggressive product release schedules.

Standardize security as part of your testing process

With more than one million new Web applications being launched each month and successful hacker attacks in the news each week, application security is no longer an afterthought. With an increased focus on application security, security and operations professionals are finding security vulnerabilities in production Web applications. These vulnerabilities are usually traced to defects in the source code and assigned back to development for remediation and quality assurance (QA) for regression testing.

Many organizations now realize that security must be a priority during development and QA. Development and QA teams are learning that Web application security vulnerabilities must be treated like other software defects. QA professionals know they can save organizations time and money by identifying these security defects early in the software lifecycle—long before Web applications are deployed in production environments. However, most QA professionals are not security experts and need help in identifying security defects within their existing processes and tools.

HP QAInspect software provides comprehensive security management for QA teams. It applies innovative techniques to identify security defects from the hacker's perspective. HP QAInspect reports on those vulnerabilities with detailed security knowledge in a way that you can understand with a concise prioritized list of vulnerabilities and thorough vulnerability descriptions. These detailed results yield information on the possible types of attacks, such as cross-site scripting (XSS) or structured query language (SQL) injection, as well as on compliance issues related to regulations, such as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry (PCI) Data Security Standard (DSS).

Execute application security tests within a familiar environment
The HP QAInspect user interface is embedded within HP Quality Center interface for ease of use.
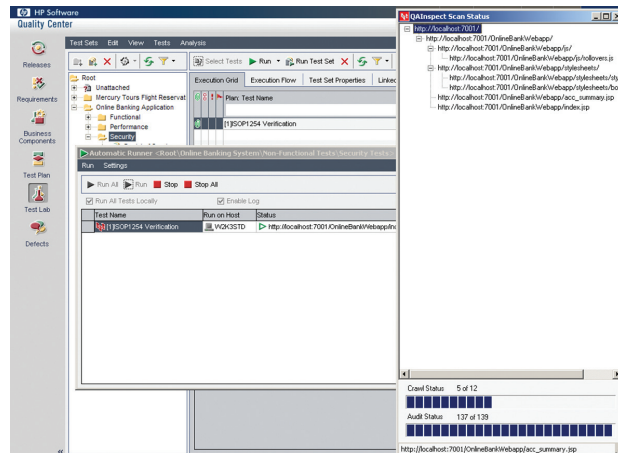
Get comprehensive security management

Security vulnerabilities should be treated like any other software defect. HP QAInspect helps you save time and money by finding security defects early and providing the information you need to work with developers to fix them quickly and prevent potential attacks in production. As a result, you can reduce your organizational risk dramatically.

Integrate security testing into your testing environment
HP QAInspect features deep and intuitive integrations. It is designed to fit naturally with the way you work so that security testing becomes as familiar as functional and performance testing. You can perform security testing of your applications without ever leaving your testing environment and automatically manage security defects using your preferred testing solution.

Analyze today's modern applications
Most application scanners are designed for legacy Web technologies and lack the intelligence required to scan emerging Web 2.0 applications that use Ajax, SOAP, JavaScript, and Flash technologies. HP QAInspect has been architected to analyze today's Web application technologies, supporting complicated sites.

Get comprehensive, accurate and fast results
HP QAInspect includes several breakthrough innovations for accuracy, including simultaneous crawl and audit (SCA) and Intelligent Engines features. Simultaneous crawl and audit combines the application crawl and audit phases into a single fluid process. The scan is refined based on real-time audit findings, resulting in a comprehensive view of the Web application's attack surface.

Patent-pending Intelligent Engines technology from HP analyzes applications in a structured and logical approach, creating targeted, intelligent attacks based on the applications' behaviors and environments. HP QAInspect combines these sophisticated, groundbreaking assessment technologies with known Web application vulnerabilities in SecureBase. Its new architecture provides broader coverage for today's Web applications and results an accurate and fast assessment.

Support legal and regulatory compliance
HP QAInspect includes detailed reports that show how you should change your Web applications to meet regulatory standards. In addition, you can create new policies or customize existing ones with the Policy and Compliance Manager feature. HP QAInspect contains policies for more than 20 laws, regulations, and best practices including:

- California SB 1386
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- ISO 17799
- PCI Data Security Standard
- OWASP Top Ten

Share knowledge and data
HP QAInspect provides pre-packaged Web application security expertise that keeps up with the latest known vulnerabilities and hacker techniques. You can improve your security expertise while securing applications using SecureBase, a leading knowledgebase of application security vulnerabilities and best practices for fixing them. HP security experts find and capture known security vulnerabilities and constantly research the next generation of Web application threats to populate the knowledgebase.

Knowledge of a highly skilled security professional in your QA team
HP QAInspect delivers the security knowledge needed to quickly fix and remediate the security vulnerabilities including best practices and coding examples.
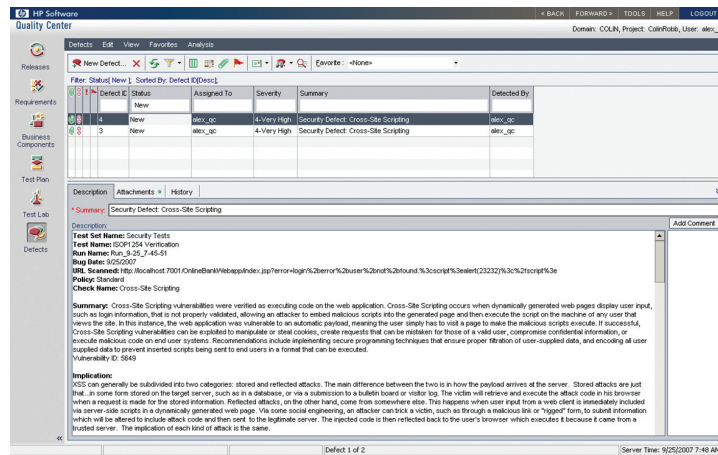
HP QAInspect checks for:

Data injection and manipulation attacks
- Reflected 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)

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

Server and general HTTP
- 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
- Ajax auditing
- WebDAV auditing
- File enumeration
- Information disclosure
- Directory and path traversal
- Spam gateway detection
- Brute force authentication attacks
- Known application and platform vulnerabilities

Integrate across your enterprise
HP QAInspect integrates with HP Assessment Management Platform software for enterprise-wide, distributed assessment capabilities. HP Assessment Management Platform provides a scalable, organization-wide view of application security with centralized control over user permissions, security policies, and remote scanning administration.

Part of a lifecycle approach to application security

HP QAInspect is part of HP Application Security Center, a comprehensive suite of products and services that support the entire Web application lifecycle, from development to ongoing operations management and auditing. These security products identify vulnerabilities early in the software lifecycle and help prevent new vulnerabilities from being introduced throughout the life of the application. These products are designed to foster collaboration among developers, security professionals, and QA teams. Trustworthy software becomes possible only when security becomes a standard requirement in the entire development process.

Tight integration with HP quality management products

HP QAInspect is tightly integrated with HP Quality Center products, letting you analyze Web applications within your existing testing framework.

HP QAInspect lets you plan, configure, execute, and manage automated Web application security from HP Quality Center software. You can leverage existing HP Quality Center software features for your security tests. Using pre-built assessment technology that automatically integrates with HP Quality Center, you can save time and identify security vulnerabilities quickly and easily.

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 a team made up of the industry's leading security researchers dedicated to being at the forefront of Web application vulnerability discovery and innovation. Comprised of acclaimed authors and spokespeople, this team's 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 with the HP SmartUpdate function, giving you the additional knowledge and skills within your security program.

Key features and benefits

Sophisticated integration
- Integrate with HP quality management solutions: Integrate with HP Quality Center
- Integrate defect reporting results: See security defects reported alongside functional defects in HP Quality Center
- Identify concise, prioritized vulnerabilities: Prioritize vulnerabilities based on business risk
- Get quick time to value with an embedded user interface: Use the scan configuration user interface in HP Quality Center

Detailed reporting and compliance
- Run high-level management reports: Show a snapshot of your enterprise-wide security status, using either HP Quality Center or HP QAInspect reporting technologies
- Create detailed reports for development and QA: Customize reports for development and QA teams

3

- Run comprehensive compliance reports: Run compliance reports for all major regulatory standards, including PCI, SOX, and HIPAA, using scan data

- Get trend analysis and security readiness reporting: Watch application security trends

Innovative assessment technology

- Get simultaneous crawl and audit (SCA): Produce faster scans and more accurate results through the combined application crawl and audit process

- Have broader coverage, reduced false negatives: Reduce false negatives using scan technology built specifically for today's complex applications

- Support IPv6: Support your IPv6-enabled networks and hosts

For more information

To learn more about HP WebInspect software, visit **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

4AA1-5362ENW Rev. 1, April 2009