



HP web application security across the development lifecycle

Solution brief



HP Application Security Center software products help security professionals, developers and quality assurance (QA) teams save time and money by catching security defects as early in the application development lifecycle as possible and throughout deployment, saving you time and money.

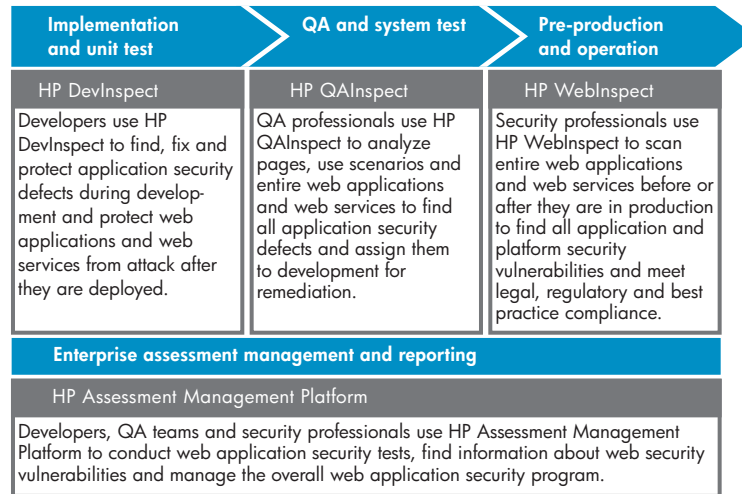
The need for lifecycle security testing

Web application security initiatives usually begin with security experts purchasing a web application security product. As these security professionals begin testing and finding security vulnerabilities, they quickly discover two important challenges.

First, while some of the vulnerabilities do exist in the web server or application configuration, at least 80 percent of the vulnerabilities they find are actually in the source code. Security professionals often respond by developing a process of reporting security defects to developers, supporting developers during the fix process and confirming that defects are resolved with developers and QA teams. It doesn't take long before the developers, QA teams and security professionals realize that they need to develop secure code from the beginning while new functionality is being built into the applications.

HP Application Security Center software

HP security testing software products provide common security policy definitions, centralized permissions control and web access to security information, and they support the complete application lifecycle from development to production.



Secondly, many organizations are discovering that they have too many web applications and vulnerabilities for only one or two security professionals to test regularly. Security professionals need to extend their team with developers, QA teams and additional security experts around the world who can conduct additional web application testing and remediation efforts. This presents a new set of automation requirements for products that can support a sophisticated, scalable enterprise web application security program. Extended teams need software solutions that provide information about web applications and their security vulnerabilities while giving them the ability to test their applications for security defects.

HP Application Security Center software solutions help security professionals, developers and QA teams save time and money by catching security defects as early in the application development lifecycle as possible. Our software is designed with flexibility in mind. Some development and QA organizations want to deploy software that is integrated into the development and testing environments. Others want a centralized solution for authorized team members to conduct security tests as needed. Many organizations implement a combined approach in which security professionals manage the overall security program, working with developers, QA teams and security experts. They need flexible solutions to define and manage web application security processes.

HP DevInspect software, HP QAInspect software and HP WebInspect software are designed for developers, QA professionals and security professionals respectively. HP Assessment Management Platform software brings these products together and can be leveraged by each

audience for different purposes. When used together, these products provide an effective end-to-end security testing solution for your enterprise.

Security professionals

Security professionals must secure enterprise web applications and reduce the risk of malicious attacks from hackers. Hackers are constantly finding new ways around traditional defenses in order to break into web applications and web services. While protecting assets and maintaining security awareness in this complex, fast-changing environment, security professionals must also demonstrate the state of your web security and regulatory compliance.

Today's security professionals must also address an overwhelming number of applications, vulnerabilities and people around the world. They must identify critical applications, maintain a holistic risk management view and give numerous stakeholders visibility into the state of application security across the enterprise. They must scale their assessment processes across the enterprise and throughout the lifecycle to developers, QA teams, other security professionals and business managers who own the applications. Many organizations are striving for proactive application security programs that find vulnerabilities early in the lifecycle to avoid the excessive costs associated with fixing defects in production applications. The security professionals driving these programs need sophisticated software to help them coordinate a global team of people and manage and mitigate application risk. HP offers two software products that can be used separately or together to test web applications and manage your overall security program.

HP WebInspect

HP WebInspect is easy-to-use, extensible and accurate web application security assessment software. Many security professionals begin their application security testing programs with HP WebInspect, which enables both security experts and security novices to identify critical, high-risk security vulnerabilities in web applications and web services. HP WebInspect addresses the complexity of Web 2.0 and identifies vulnerabilities that are undetectable by traditional scanners. HP WebInspect supports today's most complex web application technologies with breakthrough testing innovations, including simultaneous crawl and audit (SCA) and concurrent application scanning, resulting in fast and accurate automated web application security.

HP Assessment Management Platform

HP Assessment Management Platform fully addresses the complexities of today's web application security programs. After using HP WebInspect for a short time, security professionals often need to scale their program to test additional web applications and perform tests more frequently. They need both automated and scheduled penetration testing and more manual expert tests. They need to extend security testing to additional security professionals around the globe as well as developers and QA teams, who address security early in the application lifecycle.

HP Assessment Management Platform supports an advanced global security program that allows multiple participants to get the application security information they need and participate in the assessment and remediation process, while letting security professionals maintain centralized control. HP Assessment Management Platform is distributed and scalable. It provides a web-based interface for a consolidated global view, supporting multi-user lifecycle collaboration and control of application security risk throughout the enterprise. Developers, QA teams and security professionals can use HP Assessment Management Platform as a black box assessment tool across the enterprise to target vulnerabilities that hackers can exploit.

Developers

Developers are increasingly using products to help them code more securely. Developers know that security defects are like other defects. Catching security defects early eliminates the time and expense associated with later-stage patches. Today's global organizations have thousands of developers dispersed all over the world.

In many cases, development is outsourced to third-party vendors. Establishing common practices and tools for secure coding is an ever-present challenge. HP offers two products that present different options for developers to test their web applications for security.

HP DevInspect

HP DevInspect simplifies security for developers by automatically finding and fixing application security defects. HP DevInspect also helps developers build secure web applications and web services quickly and easily, without affecting schedules or requiring security expertise. HP DevInspect is installed on an individual developer's system and, using a hybrid analysis approach, combines source code analysis with black box testing to reduce false positives and find additional security defects.

HP DevInspect integrates with the following integrated development environments (IDEs):

- Microsoft® Visual Studio 2003 and 2005
- IBM Rational Application Developer 6 and 7
- Eclipse 3.1 or higher
- Also available as a standalone, Eclipse-based tool
- Supports C#, Java™, Visual Basic, hypertext markup language (HTML), extensible markup language (XML), Simple Object Access Protocol (SOAP), web service definition language (WSDL), JavaScript, VBScript

HP Assessment Management Platform

Many development organizations also use HP Assessment Management Platform, which developers can use to conduct assessments of their code as needed. Developers can use HP Assessment Management Platform to conduct black box testing of their application, targeting only exploitable security defects. HP Assessment Management Platform conducts comprehensive tests for all web applications, regardless of the language in which they are built. HP Assessment Management Platform also includes flexible reporting capabilities that let development teams share information and security policies with QA teams and security professionals.

QA professionals

QA teams use security products to help them find security defects in web applications. Security testers have always focused on functionality and performance. Now that web applications are maturing, QA teams are conducting more focused and comprehensive security testing on web applications. QA teams need products that augment their automated tests and integrate into their environments.

HP QAInspect

HP QAInspect applies innovative techniques to identify security defects from the hacker's perspective. HP QAInspect reports on vulnerabilities with detailed security knowledge in a way that QA professionals can understand with a concise, prioritized list of vulnerabilities and thorough vulnerability descriptions. Analysis results yield detailed information on possible types of attacks, including cross-site scripting (XSS) or structured query language (SQL) injection, as well as on compliance issues related to regulations, such as Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA) and payment card industry (PCI) standards.

HP QAInspect integrates with the following testing products:

- HP Quality Center software
- HP WinRunner software and HP QuickTest Professional software

HP Assessment Management Platform

Many QA teams also use HP Assessment Management Platform to assess their applications. HP Assessment Management Platform conducts comprehensive tests for all web applications, and its automatic scheduling capability lets QA teams schedule regular web security tests. HP Assessment Management Platform also includes comprehensive reporting capabilities that help QA teams share information and security policies with development teams and security professionals.

A complete solution

Comprehensive training

HP provides a comprehensive curriculum of HP Software and IT Service Management courses. These offerings provide the training you need to realize the full potential of your HP solutions, increase your network optimization and responsiveness, and achieve better return on your IT investments.

With more than 30 years experience meeting complex education challenges worldwide, HP knows training. This experience, coupled with unique insights into HP Software products, positions HP to deliver the optimum training experience. For more information about these and other educational courses, visit www.hp.com/learn.

The smartest way to invest in IT

HP Financial Services provides innovative financing and financial asset management programs to help you cost-effectively acquire, manage and ultimately retire your HP solutions. For more information on these services, contact your HP sales representative or visit www.hp.com/go/hpfinancialservices.

Contact information

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

HP Services

Get the most from your software investment

HP provides high-quality software services that address all aspects of your software application lifecycle needs. With HP, you have access to standards-based, modular, multi-platform software coupled with global services and support. The wide range of HP service offerings—from online self-solve support to proactive mission-critical services—enables you to choose the services that best match your business needs.

For an overview of HP software services, visit www.managementsoftware.hp.com/service.

To access technical interactive support, visit Software Support Online at www.hp.com/managementsoftware/services.

To learn more about HP Software Customer Connection, a one-stop information and learning portal for software products and services, visit www.hp.com/go/swcustomerconnection.

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

© Copyright 2007 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. Java is a U.S. trademark of Sun Microsystems, Inc. Microsoft is a U.S. registered trademark of Microsoft Corporation.

4AA1-5368ENW, September 2007

