



确保 Web 应用在整个开发周期内的安全

解决方案概述

在应用开发生命周期内和部署期间，HP Application Security Center 软件产品能及时发现安全漏洞，为安全人员、开发人员和 QA 团队节省时间和金钱。

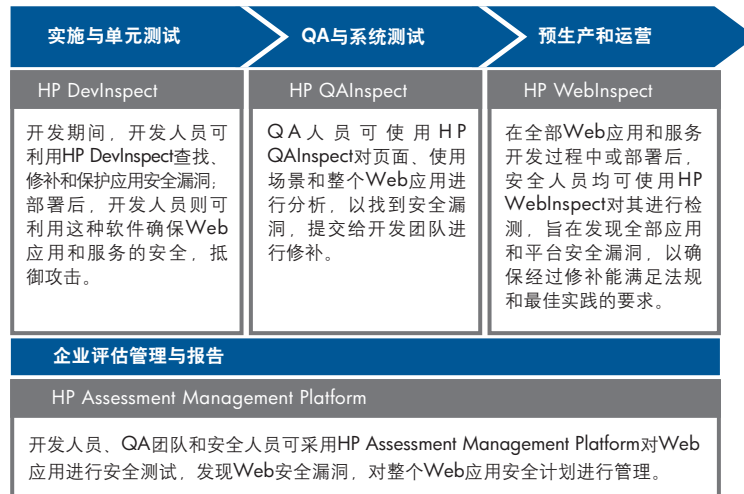
生命周期安全测试的必要性

通常从安全专家购买 Web 应用安全产品之日起，就开始实施 Web 应用安全计划。当这些安全人员着手测试和寻找安全漏洞时，他们会很快发现两个严重问题。

第一，虽然 Web 服务器或应用配置的确存在某些漏洞，但是至少 80% 的漏洞其实存在于源代码中。通常情况下，安全人员会通过开发安全漏洞报告流程，向修补漏洞的开发人员提供支持，确保开发人员和 QA 团队有效地解决问题。开发人员、QA 团队和安全人员不久就会认识到，在着手向应用添加新功能时，他们就必须开发安全代码。

HP Application Security Center 软件

惠普安全测试软件产品可提供通用安全政策定义，具备集中控制能力和访问安全信息的能力，能在从开发到生产的整个生命周期内为应用提供支持。



第二，很多企业开始意识到，仅靠一两个安全人员远远不能满足对Web应用和漏洞进行定期测试的要求。因此需要抽调全球的开发人员、QA团队及其他安全专家充实安全队伍，加大Web应用测试和修补的力度。这就对现有支持复杂、可扩展的企业Web应用安全计划的产品提出了新的要求——实现自动化。因此，那些既能提供Web应用信息及安全漏洞信息，同时又具备安全漏洞测试功能的软件解决方案成为扩展团队的必需。

而HP Application Security Center软件解决方案正是这样一款产品，因为它能在应用开发过程中及早发现安全漏洞，从而帮助安全人员、开发人员和QA团队节省时间和金钱。我们在设计软件时始终将灵活性牢记心间。部分开发和QA组织希望部署能够集成到开发和测试环境的软件。其他组织则希望部署一款集中式解决方案，帮助授权团队成员根据需要进行安全检测。很多组织采取各种组合方式，为安全人员管理整个安全计划，与开发人员、QA团队和安全专家合作提供便利。所以他们希望部署能对Web应用安全流程进行灵活定义和管理的解决方案。

HP DevInspect软件、HP QAInspect软件和HP WebInspect软件是三款分别为开发人员、QA人员和安全人员量身打造的产品。HP Assessment Management Platform软件对这些产品进行了整合，每位客户可根据自己的目的分别加以应用。如果组合应用，这三款产品则会构成一套有效的企业端到端安全测试解决方案。

安全人员

安全人员必须确保企业Web应用的安全，降低黑客恶意攻击的风险。黑客为了突破Web应用和服务的安全屏障，会通过分析传统防御体系的弱点寻找更加有效的攻击途径。在这种复杂多变的环境中，安全人员一方面要保护资产，保持应有的警惕，另一方面，还要说明Web安全和法规遵从状态。

此外，如今的安全人员还必须解决难以数计的应用、漏洞和人带来的问题。他们必须确定关键应用，统筹规划，全面管理风险，并且要为大批利益相关方提供关于企业应用安全状态的信息。他们必须对整个企业采用的、贯穿整个生命周期的评估流程进行扩展，以满足拥有该应用的开发人员、QA团队、其他安全人员及业务经理的需要。很多企业正努力通过推行主动式应用安全计划，试图在生产过程中及早发现应用漏洞，从而减少因修补漏洞产生的额外费用。实施这些计划的安全人员也希望借助先进软件帮助其协调全球团队的关系，加强管理，以降低应用风险。而对于惠普提供的两款软件产品，您既可以单独使用，也可以搭配使用，它们可以帮助您测试Web应用，管理整个安全计划。

HP WebInspect

HP WebInspect 是一款易用、可扩展、精确的 Web 应用安全评估软件。很多安全人员起初都使用 HP WebInspect 实施其应用安全检测计划，因为这款软件可协助安全专家和新手发现 Web 应用和服务中存在的高风险漏洞。HP WebInspect 解决了复杂的 Web 2.0 问题，且能找到传统扫描程序无法发现的漏洞。HP WebInspect 支持如今最复杂的 Web 应用技术，由于采用了突破性自动测试技术(包括 SCA 和同步应用扫描)，所以可以迅速、准确地发现 Web 应用的安全漏洞。

HP Assessment Management Platform

HP Assessment Management Platform 彻底简化了如今的 Web 应用安全计划。在使用 HP WebInspect 一段时间后，安全人员通常需要扩展其计划，以测试新增的 Web 应用，并提高检测频率。他们需要定期进行自动化全面检测，更频繁地进行专家手工检测。他们需要向其它地区的安全人员、开发人员和 QA 团队推广安全检测技术，及早发现并解决应用生命周期各阶段的安全问题。

除了支持全球性高级安全项目，允许相关人员获取其需要的应用安全信息，参与评估和修补流程外，HP Assessment Management Platform 还能确保安全人员行使集中控制权利。分布式 HP Assessment Management Platform 可以扩展。它拥有一个基于 Web 的界面，该界面整合了全球视野，支持多名用户在生命周期内开展协作，对整个企业的应用安全风险实施控制。开发人员、QA 团队和安全人员可将 HP Assessment Management Platform 视为一个黑盒评估工具在整个企业内使用，以抢在黑客之前发现应用安全漏洞。

开发人员

如今的开发人员越来越多地使用工具确保代码安全。开发人员非常清楚，安全漏洞像其它缺陷一样会对安全构成威胁。因此及早发现安全漏洞可以避免后期修补耗费的时间和金钱。现在，跨国企业拥有成千上万分布在世界各地、从事开发的人员。

很多时候，企业都会将开发任务外包给其它企业。建立普遍适用的准则，开发相应的工具，以确保代码安全这个问题始终未得到解决。惠普推出的两款产品为开发人员进行 Web 应用安全测试提供了新的途径。

HP DevInspect

HP DevInspect 可以自动发现和修补应用安全漏洞，缓解了开发人员的安全检测压力。另外，HP DevInspect 还能帮助开发人员快捷构建安全的 Web 应用，这既不影响开发进度，也不要求开发人员具备安全知识。HP DevInspect 安装在开发人员的系统中，能综合利用源代码分析和黑盒测试方式，通过全面分析，减少明显错误，并找到其它安全漏洞。

HP DevInspect 整合了以下集成开发环境(IDE)：

- Microsoft® Visual Studio 2003 和 2005
- IBM Rational Application Developer 6 和 7
- Eclipse 3.1 或更高版本
- 独立的基于 Eclipse 的工具
- Supports C#、Java™、Visual Basic、超文本标记语言 (HTML)、可扩展标记语言(XML)、简单对象访问协议 (SOAP)、Web 服务定义语言(WSDL)、JavaScript、VBScript

HP Assessment Management Platform

很多开发机构也使用 HP Assessment Management Platform，其中的开发人员根据需要使用这种工具评估其代码的安全性。开发人员可使用 HP Assessment Management Platform 检测其应用，找到可能会遭到攻击的安全漏洞。HP Assessment Management Platform 能对使用各种语言编写的所有 Web 应用进行综合检测。另外，HP Assessment Management Platform 还能利用灵活的报告功能，使开发团队与 QA 团队和安全人员共享信息与安全政策。

QA 人员

QA 团队会利用安全产品寻找 Web 应用存在的安全漏洞。过去，安全测试人员的重点始终是功能与性能。随着 Web 应用的逐渐成熟，如今，QA 团队开始对 Web 应用进行有重点的全面安全测试。QA 团队需要既能提高其自动测试能力，又能与环境实现整合的安全产品。

HP QAInspect

采用创新技术的HP QAInspect能发现黑客可能会进行攻击的安全漏洞。HP QAInspect以QA人员可以理解的方式详细报告应用的安全状态，报告内容包括按安全等级排列的漏洞列表及关于漏洞的完整描述。分析结果十分详尽，会列出黑客可能采取的攻击方式，例如跨站脚本(XSS)攻击或结构化查询语言(SQL)注入，或者列出法规(《萨班斯-奥克斯利法案》(SOX)、《医疗保险便携性及责任法案》(HIPAA)及《支付卡行业数据安全标准》(PCI))遵从漏洞，做出预测。

HP QAInspect集成了以下测试产品：

- HP Quality Center 软件
- HP WinRunner 软件和HP QuickTest Professional 软件

HP Assessment Management Platform

很多QA团队也使用HP Assessment Management Platform对应用进行安全评估。HP Assessment Management Platform可对所有Web应用进行综合检测，QA团队可利用其自动调度功能，定期执行Web安全检测。另外，HP Assessment Management Platform还能利用灵活的报告功能，帮助QA团队与开发团队、安全人员共享信息与安全政策。

完整的解决方案

全面的培训

惠普提供了一系列全面的惠普软件和IT服务管理课程。这些课程可为您提供所需要的培训，以充分发挥惠普解决方案的潜力，进一步优化您的网络和响应能力，为您带来更高的IT投资回报。

凭借30年来在全球范围内解决复杂多样的培训挑战的丰富经验，惠普对开展培训可谓了如指掌。这些丰富经验加上深厚的HP软件知识，使惠普公司能够提供最佳培训体验。如欲了解有关这些培训及其它培训课程的更多详细信息，请访问www.hp.com/learn

最明智的IT投资方式

惠普金融服务提供创新的融资和金融资产管理计划，来帮助您经济高效地购置、管理您的惠普解决方案，直至最终的产品更新换代。欲了解有关这些服务的更多信息，请联系惠普销售代表或访问：

www.hp.com/go/hpfinancialservices

联系信息

如欲就近寻找惠普软件销售部门或经销商，请访问：

www.managementsoftware.hp.com/buy

惠普服务

从软件投资中获取最大回报

惠普为您提供高品质的软件服务，以全方位满足您软件应用生命周期中的各种需求。与惠普合作，您可以获得基于标准的、模块化的、多平台软件以及惠普一流的全球服务与支持。从这些种类繁多的服务产品中——从在线自助支持到主动式关键任务服务——您可以选择最符合自己业务需求的服务。

如欲了解惠普软件服务概况，请访问：

www.managementsoftware.hp.com/service

如欲获得技术互动支持，请访问在线软件支持网站：

www.hp.com/managementsoftware/services

如欲了解有关HP Software Customer Connection (软件产品和服务一站式信息和学习门户网站)的更多信息，请访问：

www.hp.com/go/swcustomerconnection

详情请访问：www.hp.com.cn/software

或拨打支持热线：800-820-2255 转 126

Copyright © 2008 Hewlett-Packard Development Company, L.P. 本文所含信息可能随时更改，恕不另行通知。惠普产品和服务的保修条款在这些产品和服务附带的保修声明中已阐明。本文中的任何信息均不构成额外的保修条款。惠普对本文所含有的技术或编辑错误、遗漏概不负责。Java是Sun Microsystems公司在美国的商标。Microsoft是微软公司在美国的注册商标。

2008年2月中国印刷
P/N: 4AA1-5368CHP

