

第三部分: 应用安全最佳实践指南

应用安全综合业务指南 (三步骤系列)



目录

简介	3
利用惠普应用安全成熟度模型, 实施最佳实践	3
应用安全成熟度模型	4
第0级 — 特例	4
第1级 — 风险意识	5
第2级 — 生命周期基本计划	6
第3级 — 企业视图	7
第4级 — 卓越中心	8
总结	10
附录A. 惠普应用安全: 覆盖应用生命周期的解决方案	11

简介

软件是全球经济的循环系统。它管理着我们的金融交易、跟踪港口集装箱中的产品、监控病人的生命体征，总之可以完成大量重要任务。创新的软件开发技术正在改变我们对互联网的看法、重塑企业形象并创建新的关键业务。从Web 2.0到云计算，软件不仅在推动全球变更的发展，同时也加快了变更速度。

无论您处于哪个行业，势必都会通过企业内部的软件开发计划、外包开发，或商用软件战略采购，受到这些趋势的影响。您创建新市场、获得竞争优势、提高运营和通信效率等目标，也与您引入的创新软件技术息息相关。

获得这些软件业务优势的主要因素在于确保软件安全实施。停滞不前固然不是明智的选择，但对软件质量和安全采取的措施不当也会给企业带来不必要的风险，而且会导致企业陷入进退维谷的尴尬境地。

21世纪第一个十年末，软件行业已经积累了确保软件质量和安全所需的大量专业知识。我们发现，软件安全领域的成功企业对该问题采取了完整生命周期方法，并做出了一个计划级承诺。

本白皮书是惠普应用安全（商业培训系列）三步骤中的第三部分，旨在帮助管理人员了解应用安全对其业务的重要性。我们建议您了解全部三个部分的内容：

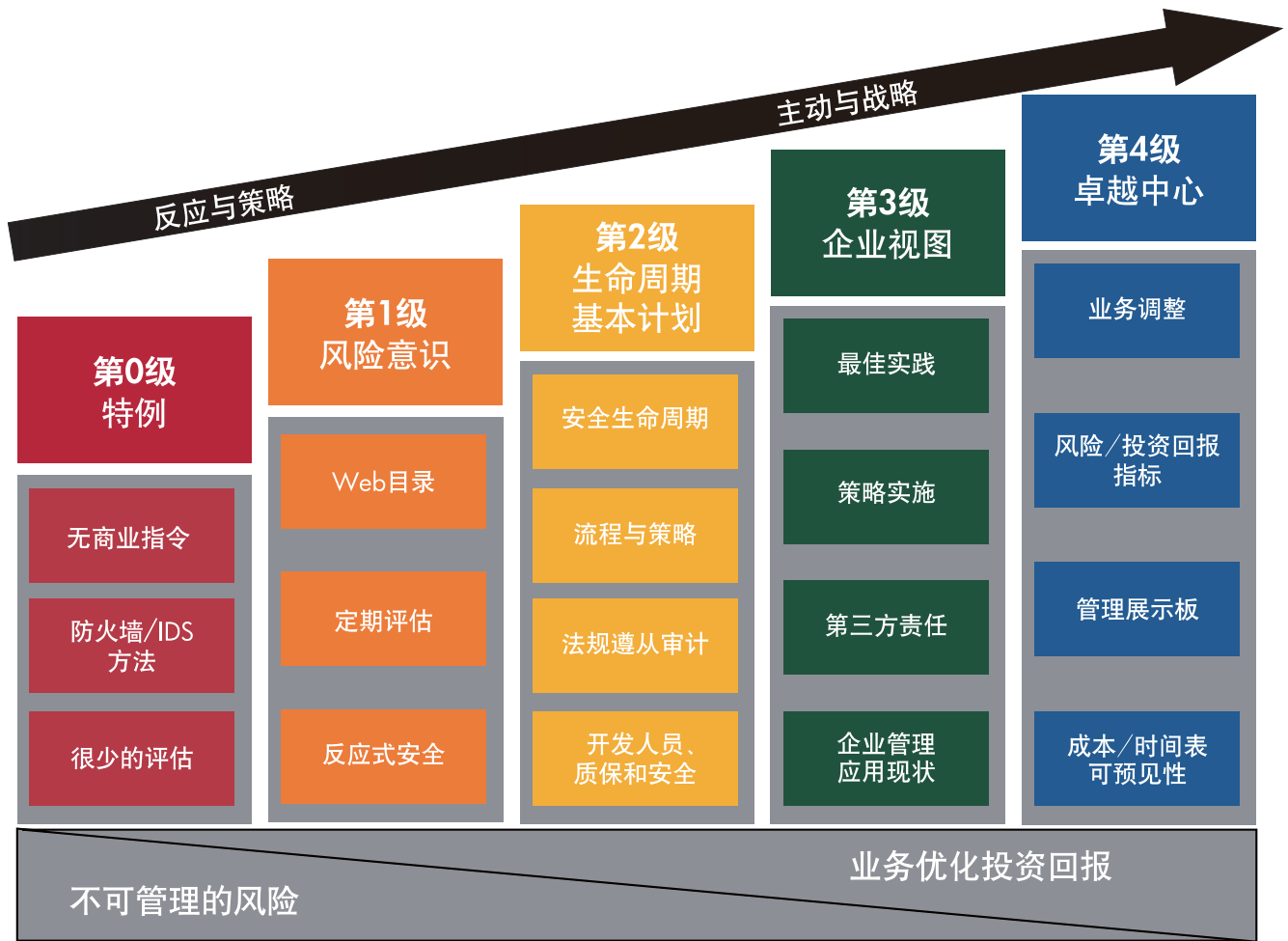
- **第一部分：**应用安全指令
- **第二部分：**应用安全综合业务承诺
- **第三部分：**利用惠普应用安全成熟度模型，实施最佳实践

利用惠普应用安全成熟度模型，实施最佳实践

为应用安全做出计划级承诺是一项综合活动，可提供端到端开发生命周期覆盖能力，同时涵盖人员、流程及技术等多个领域。然而，由于每个企业都有其独特的起点、资源以及其他计划管理限制，因此为综合计划制定的线路图必须灵活。获得高水平安全计划的常用方法是通过成熟度模型寻求持续改进。惠普已经开发了应用安全成熟度模型，在不断提高的级别范围内定义了应用安全计划的主要特点。

了解本成熟度模型后，即可开发包含明确步骤的定制线路图，进而在符合您企业要求的一定时期和预算内提高您应用的安全性。

图1. 惠普应用安全成熟度模型



应用安全成熟度模型

应用安全成熟度模型包括5个级别，诠释了不断完善的应用安全计划。大多数级别均包括对典型环境的两种描述，其中一些级别可能既是通过该模型采取的消极措施，又是积极措施。更高的级别应视作上一级别推荐的所有积极措施的累积。该成熟度模型适用于不同厂商，但我们打算将HP Application Security Center软件部署在适当级别，以便企业在执行自行制定的线路图时充分了解应该采取的具体措施。欲了解有关HP Application Security Center软件的更多信息，请参见附录A。

第0级 — 特例

第0级针对根本没有应用开发安全计划的企业。

这些企业尚未意识到各种法规或其他章程中新增的大量安全指令，或者管理层轻易断定这些指令还不适用于其企业。更糟糕的是，他们尚未发现其软件中固有的安全隐患将给企业带来的风险及相关成本。当然，这些企业开发的软件也不安全，而且他们有意或无意地隐藏这些安全漏洞。在某些情况下，这些企业的管理欠佳。但通常又在其他领域注重产品质量，可以拥有强大的IT安全计划，只是没有综合考虑漏洞应用导致的严重后果。

虽然开发团队多年来一贯严肃对待常见的安全问题（身份验证、授权等），但没有实施任何具体的安全计划，而且通常认为它会减缓产品上市速度。

通常，第0级企业中的积极措施仅出自尽职尽责的个人，主要是信息安全部门员工，他们只是自行其事，没有具体的公司指令。如果您是其中一员，请关注以下建议措施：

1. 将这些措施相关的新闻和文件发送给企业中的主要利益相关者。
2. 鼓励各部门利益相关者参加研讨会或网络广播，了解应用黑客攻击。
3. 下载免费试用工具（例如HP WebInspect），以证明企业自有软件中的漏洞。您必须确保已获得企业利益相关者的许可，而且正在对生产中未使用的应用进行测试。

实际上任何第0级企业的目标都是快速升至下一级别。

第1级 — 风险意识

该级别的企业对应用安全规章制度和内部业务风险具备基本的意识。通常，支付卡行业/数据安全标准 (PCI/DSS) 和类似法规的普遍性需求推动了其发展。IT审计和外部检查人员可以为提高企业意识起到催化剂的作用。这会促使公司针对安全应用开发制定企业策略，从而限制了培训、测试及遵从标准。

安全和开发团队可以就开发人员安全意识计划展开协作。典型开发人员意识形成的过程沿袭了“Web应用黑客攻击”的模式，具有很强的初始影响力，其中开发人员会看到自己的应用或类似软件被掌握渗透测试和评估技术的培训师攻击。本演示可通过探讨导致安全漏洞（例如无法执行输入验证）的主要开发错误加以补充。提高开发人员和团队对开源Web应用安全计划 (OWASP) 10大漏洞的意识¹（与安全漏洞相关的10个常见Web应用错误），也是一大培训计划。

¹ 《2007年开源Web应用安全计划10大漏洞 — 方法》，www.owasp.org/index.php/Top_10_2007-Methodology，2008年10月检索

第1级企业通常需要一款应用安全测试工具,例如HP WebInspect。HP WebInspect可用于测试应用是否达到目前生产中可接受的安全级别,也可以在投入生产之前对新应用进行测试。由于一个版本的应用在需求收集和软件设计阶段没有具体的安全规范,因此常被称为“扩充安全”。然而,当企业使用HP WebInspect等工具时会取得特殊效果。该工具通常用于测试生产使用的应用,并能发现重大缺陷。开发人员感兴趣的是对自己的应用进行扫描,然后再进行必需的测试。HP WebInspect还能确定企业当前的应用安全状态基准,有助于我们判断开发人员的工作情况。

第1级企业在安全软件开发专用流程方面,相对而言还不够完善。通常,这些企业利用项目管理方法执行计划,但对软件开发生命周期的记录不严谨。

要达到第1级水平,企业需积极采取以下措施:

1. 记录并传达安全应用开发标准和生产前应用安全测试要求的基本策略。制定这些策略需参考适用的法规及其他指令,例如支付卡行业/数据安全标准。
2. 使用HP WebInspect等工具对应用进行测试,然后再将其用于生产。同时,该工具还有助于提高应用安全意识。
3. 应用开发人员需通过安全培训避免常见错误,例如“Web应用黑客攻击”和有关正确编码的课程。
4. 提高应用开发人员和IT安全人员对开源Web应用安全计划十大漏洞的意识。

第2级 — 生命周期基本计划

从第1级过渡到第2级需要企业在应用安全方法上进行战略转型。该级别的企业须认识到安全必须“融入”应用开发的整个生命周期,这与最终的“扩充”安全截然相反。消除软件漏洞不再是个人的专有职责,而是整个企业的责任。了解应用安全生命周期方法可以推动企业内多个重要的积极措施。

在第2级,需清晰记录企业的应用开发生命周期流程,然后将多个安全检查点重要事项融入该流程。在定义业务和功能要求流程期间确定安全要求。软件架构师需要在设计开发人员使用文档中阐明安全规范。开发人员将拥有安全的编码实践,并且其应用组件将在编码阶段进行安全测试,同时创建加速的反馈回路。质保(QA)团队将进行一套负面功能测试,确保应用除允许进行正面功能测试外,拒绝一切不安全操作。许多情况下,IT安全团队是企业中早期采用应用安全的部门,他们将促进正规记录法规遵从指令的执行并加入到生命周期测试。

技术工具的使用贯穿整个生命周期是对安全生命周期方法的进一步认识。例如,开发人员和架构师会在集成式开发环境(IDE)中使用HP DevInspect,以便进行漏洞测试。质量测试期间,质保团队将利用测试解决方案中集成的HP QAInspect,对电池安全性进行全面测试。安全团队通过HP WebInspect对应用进行生产前和生产后测试。部分第2级企业开始使用管理控制台(例如惠普评估管理平台)提供生命周期安全的整体视图。

第2级企业可扩大企业风险管理应用,从而提高重要检查点期间的决策能力。企业可以使用一些量化风险指标,例如资产价值和停机成本。第2级企业使用的大多数指标是定性指标,例如确定的高/中/低级安全漏洞。

对应用安全采取生命周期理念还可以将早期的培训计划扩展到应用开发生命周期的所有支持者。开发人员仍将参加绝大多数培训课程,以深入了解特定的开发环境。不过,全体主要利益相关者至少要参加意识培训,包括创建新应用和更新应用的各个业务部门。

企业应该通过采取积极措施,达到第2级计划成熟度:

1. 记录应用安全生命周期,清晰阐明整个生命周期的安全检查点。
2. 整个生命周期中都使用技术工具,例如适用于应用开发人员的HP DevInspect、适用于质保专家的HP QAInspect,以及用于生产前和生产后测试的HP WebInspect。
3. 企业应考虑运用管理工具(例如惠普评估管理平台),获得生命周期的整体视图。
4. 扩展培训课程,以便涵盖全体利益相关者。
5. 当决策关系到安全漏洞级别时,利用风险管理和风险指标提高决策能力。

第3级 — 企业视图

如果在构建应用安全生命周期方法架构阶段为第2级成熟度,则第3级重在填充架构并集成实践,为企业的应用安全提供真实的企业视图。

高级管理人员的支持是推动企业向第3级成熟度发展的主要驱动力。这并不意味着高级管理团队完全参与应用安全,而是需有一名成员担任应用安全计划的正式主办者,或者至少有一名其他高级管理人员是非正式拥护者和影响者。拥护者的角色随企业不同而有很大差异:他可以是首席信息官(CIO)、首席财务官(CFO)、法律顾问,甚至是将应用安全视作业务优势的营销高级管理人员。

第3级企业通过制定生命周期组件的最佳实践,构建应用安全生命周期架构。例如,企业可以鼓励或要求非常具体的加密技术,同时指定审核的加密算法、主要管理解决方案以及中央加密库,而不只是提供支持开发人员构建强大的加密模块的培训和工具。另外,企业还可以审计和修改生命周期流程,同时利用公认的质量改进流程简化应用开发流程并减少缺陷。

企业可以出色培训课程、更新的阅读清单以及所含资源的全面策略文档等信息，开发应用安全资源中心。参与应用开发的所有人员都应了解应用安全资源中心，并能够参考资源中心指南。这就需要集中管理整个计划，因此许多企业利用惠普评估管理平台提供实时、全面的应用安全计划视图，并加速流程自动化。

第3级企业通常建立多个指标，以获得持续改进。人员的测评方法有多种，例如完成的各种课程和获得的证书，也可以对特定知识的掌握程度进行测试。测试工具可以提供量化的漏洞指标和严重程度定性级别。第3级企业制定的一个关键指标系列是业务案例模型，例如总体拥有成本、平衡计分卡以及其他常见的IT衡量模型。成功的企业案例对管理层监督和保持整个应用安全计划的健康至关重要。

据调查，第3级企业不断完善和了解软件的相关性和复杂性，使其能够求助于业务合作伙伴，并将合作伙伴加入应用安全计划中。将安全责任纳入外包应用开发和商用现成 (COTS) 软件是第3级企业的一个主要特点。

企业应该通过采取积极措施，达到第3级计划成熟度：

1. 致力于采用与应用开发生命周期所有阶段相关的最佳实践。
2. 确定执行发起人。
3. 利用全面的计划信息和详细的公司策略构建应用安全资源中心。
4. 利用惠普评估管理平台等管理工具获得全面的应用生命周期信息。
5. 指出第三方责任，例如外包的开发人员和商用现成软件。前面的“确定外包和采购应用软件责任”章节对此提供了指导。
6. 开发可衡量应用安全计划财务指标的企业案例模型，例如DHS“内置安全”网站提供的计划。

第4级 — 卓越中心

该级别的企业具有更高绩效，致力于提高质量并增强软件与业务策略的一致性。第4级企业对应用安全计划已有多年研究，并对第3级计划中的基准进行了全面改进。

安全卓越中心由企业中的多个团队人员组成，他们负责定义企业安全策略和程序，衡量整体安全状态，并管理整个企业的应用安全计划进度。信息安全通常对此计划具有推动作用，但多样化参与和企业支持是成功的关键因素，并且可扩展到各业务部门 (LOB)，通常是首席财务官的办公室。安全卓越中心是整个企业的安全顾问，通常负责培训和解决复杂的安全问题。

第4级企业的一个主要指标是业务策略及其风险偏好的一致性。成熟的应用安全计划可确定开发任意安全质量级别软件所需的成本和时间范围，并能够以出色的灵敏性对不断变化的业务需求做出响应。适应新兴市场的应用可满足高回报/低风险需求，并可以在整个应用生命周期内进行快速管理。企业风险偏好可能随特定的业务计划而有很大差异，并且应用安全计划需要体现该灵活性。这一级别的企业通常了解应用安全企业案例，并通过做出基于风险的各种决策了解规避的成本（例如开发XYZ漏洞意外路径的成本是多少？）。

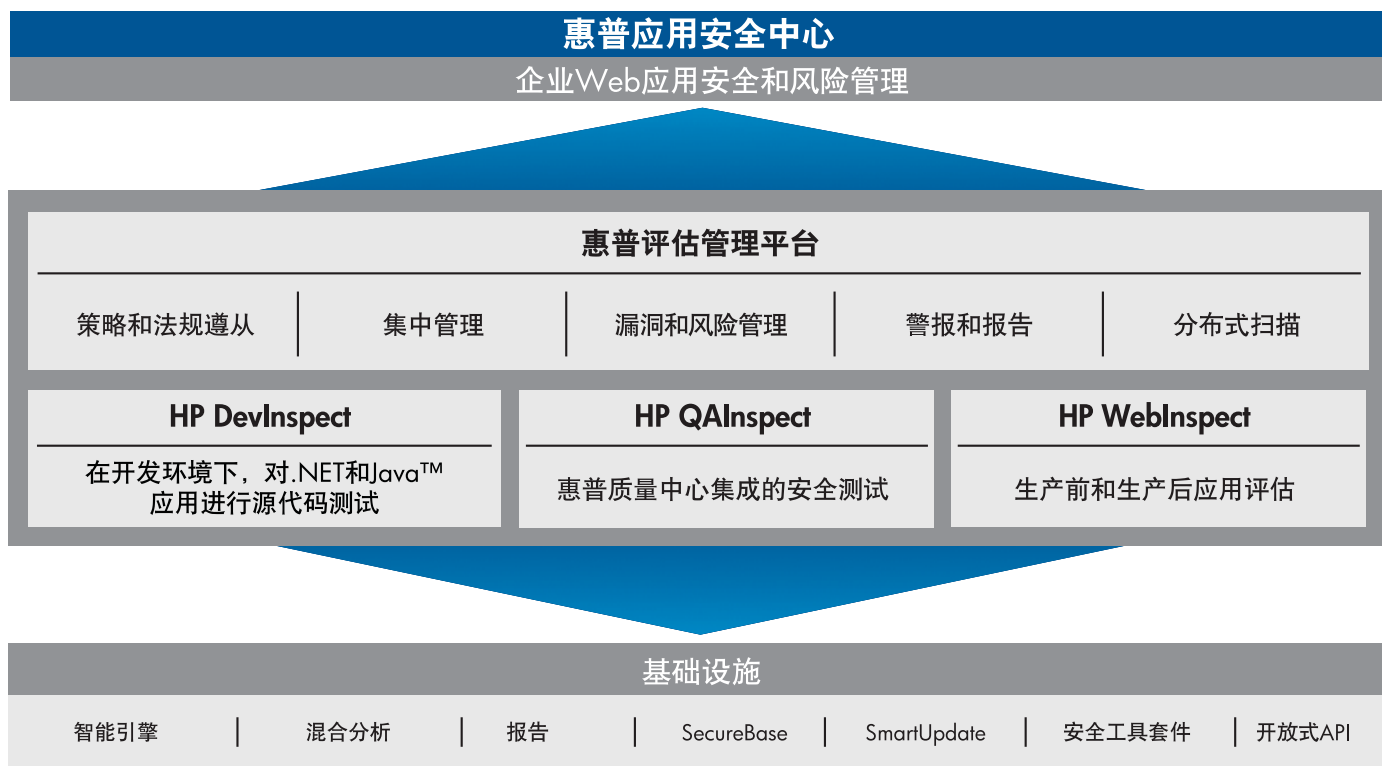
第4级企业拥有管理展示板,可以为C级管理人员报告关键指标,并及时、准确地做出决策。这些展示板用于汇聚生命周期管理软件解决方案(例如惠普评估管理平台)的数据、企业风险管理数据以及财务报告。制定治理、风险和法规遵从管理(GRC)衡量标准的企业常将这些展示板用于多种业务功能。

第4级企业的培训课程不仅拥有一套全面的应用安全课程,而且还以高效的方法充分提高学习效率。例如,安全课程线路图可帮助员工了解他们在企业中的作用,例如.NET或数据库开发人员。同时,还可帮助员工实现个人专业发展和事业目标。

最后,达到第4级成熟度的企业可以在可预测的时间内,以可预测的成本开发出具有可预测安全质量的软件。该计划自身需要说明异常和例外情况。达到第4级成熟度主要得益于对上述所有积极措施的不断改进,而不是采用一套新措施。要实现第4级成熟度,需要考虑以下几点:

1. 能否根据既定应用的风险情况调整应用安全生命周期?
2. 是否有管理人员展示板报告系统,将应用安全纳入企业主要风险和财务指标中?
3. 是否将惠普评估管理平台等应用安全管理工具集成到其他管理平台?
4. 是否有成熟度培训课程,能够为应用安全计划的主要人员提供专业发展和事业发展机会?
5. 是否有指标能够衡量多年来应用安全质量的改进?
6. 高级管理人员是否积极参与应用安全计划,以及他们是否根据企业的风险承受级别不断提供应用开发指导?

图2. 惠普应用安全中心产品和评估技术



总结

不安全软件的成本和结果缔造了强制性软件保护指令，特别是对Web应用。实施涵盖人员、流程及技术的全面应用计划需要一个线路图，以及一系列能够灵活应用于各种企业的可行措施。惠普应用安全成熟度模型是一个最佳实践方法，可为无数企业的应用提供保护。我们建议根据该5级成熟度模型对企业进行基准测试，同时按流程步骤制定高度成熟、高效的应用安全计划：

- **第0级：特例。**此级别针对根本没有应用开发安全计划的企业。此类企业内的个体支持人员需采取各种措施，加强主要利益相关者对问题的意识。通常可以按照意识程度使用HP WebInspect等工具，识别所选内部应用的安全漏洞。
- **第1级：风险意识。**针对开始将应用安全与法规要求和基本业务风险捆绑的企业。此类企业需推广开发人员教育，并定期对应用进行测试。第1级企业将采用一些应用开发最佳实践，并将其转化为企业策略。
- **第2级：生命周期基本计划。**在这一级别，企业了解在开发应用生命周期流程中创建安全性的必要性，并采取支持生命周期所有阶段的措施。例如，适用于开发人员的DevInspect、适用于质保专家的QAInspect和适用于安全专家的WebInspect等工具。这些企业拥有应用安全开发生命周期，并在制定相关决策时使用风险管理。

- **第3级：企业视图。**这些企业处于更高级别，可促进在应用生命周期内实施最佳实践，同时拥有成熟的资源中心，需要第三方应用开发人员承担责任，并设立执行发起人。第3级企业通常利用惠普评估管理平台等工具，实时提供应用安全计划的全面可视性。
- **第4级：卓越中心。**最高级别的企业将应用安全与业务相结合，并能够利用各种风险指标调整应用开发流程，以取得出色的业务成效。这些企业切实提高了企业内部和供应链内的应用开发质量。

毫无疑问，您非常有必要重视应用安全。本白皮书旨在为您提供工作线路图，解决有关如何保护软件应用的各种问题。您所面临的问题是何时采取措施？在发生影响业务运营之前还是之后？作为确定应用安全解决方案计划的一部分，我们建议您阅读此系列的其他两部分内容：

- **第一部分：应用安全指令**
- **第二部分：应用安全综合业务承诺**

惠普与惠普应用安全中心将永久提供全面的研究、最佳实践、培训、技术和产品，帮助企业制定自己的安全卓越中心和成熟的企业安全计划。

附录A. 惠普应用安全：覆盖应用生命周期的解决方案

HP Application Security Center软件产品经过精心设计，可完美集成企业整个应用生命周期的所有阶段，并不断进行更新，以准确、全面地评估网站和Web应用（包括最新的Web 2.0技术）。

以下内容对这些产品进行了简要介绍，并根据上一章节的指导原则加以定位。

HP DevInspect. HP DevInspect可以无缝实施于企业程序员使用的各种集成式开发环境（包括Microsoft® Visual Studio®、Eclipse和IBM Rational Application Developer）中，为您的团队提供易于部署、使用和实现价值的解决方案。HP Hybrid Analysis是其准专利核心，可以结合静态分析（“白箱”）与动态测试（“黑箱”）提供更精确的分析结果，因而消除了对修复对象的主观臆测。另外，HP SecureObjects作为HP DevInspect的一部分提供，可以自动纠正任何安全漏洞。开发人员的台式机上安装HP DevInspect之后，便可在生命周期的初始编码阶段修复漏洞。我们的研究显示，HP DevInspect不仅可以在关键的编码阶段减少漏洞，而且还可以为开发人员创建反馈回路，加强开发流程中对安全问题的意识。

虽然企业愿意为内部开发人员部署HP DevInspect，但需通过外包开发人员管理此工具。HP DevInspect可用于提供质量代码交付的内部重要报告，并增加外包责任。

HP QAInspect. HP QAInspect可用于针对应用开发生命周期质保测试阶段的高级安全测试。HP QAInspect直接集成到市场先进的质保解决方案——HP Quality Center，可以同时安全测试和功能测试，或作为独立的安全验证方法，所有测试和验证都在一个熟悉界面内完成。HP QAInspect的设计可轻松融入现有的质量机构和方法。从需求收集、测试规划到测试执行，HP QAInspect真正将安全作为应用质量管理的支柱。

HP WebInspect. HP WebInspect具有适合安全专家的先进边缘Web应用测试功能,能够识别Web应用中最新的高风险漏洞。该工具可以为缺乏经验的安全专家提供专业指导,同时提高资深渗透测试人员和应用安全专家的工作效率。测试的应用范围不同,企业所需的安全测试人员数量也不同。虽然这些测试人员可以通过多种技术识别安全漏洞,但在使用集成工具管理评估方面具有明显优势。HP WebInspect可以验证应用的配置,确保应用不受威胁攻击。

开发人员可使用HP DevInspect轻松修复HP WebInspect报告中检测出的漏洞。重新测试应用时,质保部门也可以标记相同的问题。应用开发生命周期标记的重复流程中,可使用常见测试套件提高生产率。

此外,HP WebInspect等工具也可用作商用现成软件的验收测试衡量标准。企业软件不断变更,并且定制流程可能会导致意外漏洞。黑盒测试更能够明确采购流程和价格及支持谈判期间的责任。

每天都能发现新漏洞。HP Web应用安全研究集团是Web应用安全研究行业的先进机构,并通过SmartUpdate对HP WebInspect进行日常更新,以对您可以持续测试最新漏洞进行验证。

HP WebInspect还可以在生中持续分析现有及新的Web应用,以降低其对业务的风险。

惠普评估管理平台。 惠普评估管理平台可用于评估和管理企业整个生命周期中的应用安全风险。安全专家利用该平台定义整个应用安全计划,其中包括安全策略、测试许可、测试时间表、运行分布式扫描等。它是HP Application Security Center的中枢,可以为企业出色的可视性、可扩展性,并控制应用安全计划。

适用于惠普应用安全的惠普软件即服务。 您是否正面临着时间、技术或成本挑战? 惠普可以帮助您或您的企业消除应用安全挑战。凭借在软件即服务 (SaaS) 方面8年的丰富经验,适用于惠普应用安全的惠普软件即服务可以创建或扩充您的安全计划,并快速减少漏洞。

惠普专业服务。 惠普提供的全套专业服务计划可满足您的各种需求,包括产品实施和培训、渗透测试、漏洞扫描和安全计划咨询服务。

惠普应用安全中心将提供更强大、更全面的解决方案,保护您的业务免受应用安全漏洞攻击。我们的产品套件可以为开发、质保和生产提供全面的应用安全生命周期方法。它是一款出色的企业解决方案,与采用成熟技术的传统安全评估方法相比,可以更快获得投资回报。

科技以推动业务成效为本

欲了解更多信息,请访问: www.hp.com/go/securitysoftware

© 2009 Hewlett-Packard Development Company, L.P.本文所含信息如有更改,恕不另行通知。惠普产品与服务的全部保修条款在此类产品和服务附带的保修声明中均已列明,本文中的任何信息均不构成额外的保修条款。惠普对于本文中所包含的技术或编辑错误、遗漏概不负责。

Java是Sun Microsystems, Inc.在美国的商标。

