SYNOPSYS®

2023年《软件漏洞快照》报告

三年来10类最常见的Web和软件应用漏洞分析

本报告由新思科技安全测试服务部与新思科技网络安全研究中心 (CyRC) 联合编制

目录

概述 1
这些测试中发现的安全问题 1
高危和超危漏洞 2
定义漏洞的严重级别 3
新思科技安全测试服务概述 3
新思科技安全测试详解 5
渗透测试 5
DAST 6
MAST 6
漏洞概述 7
安全问题详解 9
易受攻击的第三方库的危险 14
启发和建议 15

概述

在编写该《软件漏洞快照》报告时，新思CyRC的研究人员和新思安全测试服务部的顾问使用了三年来对商业软件系统和应用进行测试的匿名数据。

新思科技测试发现了仍对Web和软件应用安全造成重大威胁的已知漏洞，尤其是以下几类最常见的漏洞：

- 信息披露/泄露和隐私
- 配置错误
- 传输层保护不足

这些测试凸显出易受攻击的第三方库带来的持续危险，以及软件开发环境对强大的软件供应链安全的需求 — 在软件开发中，超过90%的软件包含开源代码。下面的数据还显示了将应用安全测试扩展到基本静态分析之外的价值。

如果您是软件安全项目的负责人，那么，深入了解软件风险可以帮助您制定更有效的安全改进策略。如果您是从战术的角度考虑安全问题，则可以使用本报告中的信息来展示需要通过第三方协助以扩展安全测试的业务案例。

测试中发现的安全问题

在2020年，97%的测试发现了漏洞。到2021年，这一比例降至95%，而2022年进一步降至83%。我们收集的三年数据显示，92%的测试在目标应用中发现了漏洞。

总体漏洞的持续减少是一个令人鼓舞的迹象，说明开发团队在编写无误代码方面取得了进步，而且诸如代码审查、自动测试和持续集成等实践也有助于减少常见的编程错误。

此外，编程语言和集成开发环境 (IDE) 的发展也为开发者提供了一些内置的检查和工具，可以帮助他们及时发现并修复错误，避免造成严重问题。对于一些受欢迎的开源项目，许多社区也加强了代码审查，提高了代码质量标准。

然而，对于一些不太受关注或者已经过时的开源项目，就没有这么幸运了。据一些报告显示，在2022年维护的Java和JavaScript开源项目中，有近20%的项目已经停止了维护，使得这些项目面临漏洞以及被利用的风险。

发现漏洞的测试占比

高危和超危漏洞

在这三年中，27%的测试发现了高危漏洞，6.2%的测试发现了超危漏洞。其中，跨站脚本 (XSS) 在新思科技的多年测试中一直都是最常见的高危漏洞之一。同样，2020到2022年间，SQL注入一直位列最常见的超危漏洞之首。

按年份细分，我们发现在2022年的测试中，高危漏洞相比2021年略有增加（25% vs. 20%），相比2020年略有减少（25% vs. 30%），但超危漏洞 (6.7%) 均高于2021年 (4.5%) 和2020年 (6.1%)。

许多中危、高危和超危漏洞都需要多层测试才能被发现。

这些数字反映出，高危和超危漏洞过去几年一直都在增加，并在2022年达到了历史最高水平。在2022年报告的CVE中，约有80%属于中危或高危漏洞，有16%属于超危漏洞。虽然开发团队的努力使总体漏洞数量减少，但数据表明，许多中危、高危和超危漏洞都需要更强有力的测试才能被发现，如渗透测试。

	2022	2021	2020
超危	28%	54%	77%
高危	38%	46%	63%
中危	60%	64%	72%

图1. 与原始测试相比，后续重复测试中发现的漏洞的减少情况（百分比）

图1说明了动态测试，比如一些类型的渗透测试和动态应用安全测试 (DAST)，是对静态应用安全测试 (SAST) 的有效补充。通过对一些重新测试进行抽样检查（即对安装了特定修复包的软件进行快速验证），我们发现在这三年期间，客户的超危、高危和中危漏洞都在逐年减少。例如，2022年检测到的中危漏洞减少了60%，高危和超高危漏洞分别减少了38%和28%。

2020至2022年间，高危和超危漏洞的占比

定义漏洞的严重级别

漏洞的严重级别根据 CVSS v3 标准评定，反映了漏洞对网络安全构成的风险。超危漏洞的CVSS分数在9.0到10.0之间，而且有已经公开或正在被攻击者使用的漏洞或存在安全缺陷的代码，例如命令、代码和SQL注入漏洞。

高危漏洞的CVSS分数在7.0到8.9之间，通常比超危漏洞更难被利用。但是，考虑到存在此类漏洞的应用/系统的业务关键性和威胁环境等因素，高危漏洞也需要及时检查和修复。

随着越来越多的攻击者开始使用自动化漏洞利用工具，可以在几秒钟内攻击数千个系统，尤其是考虑到超过一半的漏洞在披露后一周内即被利用，因此，高危和超危漏洞必须在发现后及时修复。

应用中的安全或漏洞问题不仅会影响组织机构本身（或其客户）的业务运营，而且还会影响整个软件开发生命周期乃至整条软件供应链。

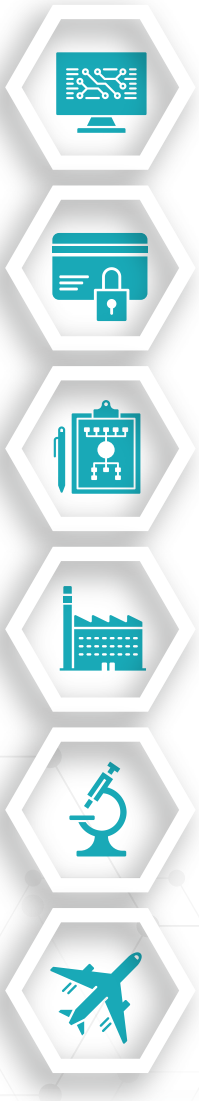
事实上，新思科技《2023年全球DevSecOps现状调查》报告指出，超过80%的受访者表示，解决严重的安全/漏洞问题已对其组织的2022-2023软件交付计划产生了影响。

新思科技安全测试服务概述

开发团队必须以前所未有的速度构建越来越复杂的软件，但训练有素的技术人员严重不足。

虽然属于不同的行业和组织，但新思科技安全测试服务部的所有客户都有一个共同需求 — 扩大测试的覆盖范围。他们要求开发团队以前所未有的速度构建越来越复杂的软件，但却面临训练有素的技术人员严重不足的问题，尤其是在软件安全方面。

本次研究涉及的行业



- 31% 软件和互联网、系统集成和相关服务、计算机和电子
- 29% 金融服务和保险
- 12% 商业服务
- 8% 制造、运输和储存、批发和分销
- 4% 医疗保健
- 6% 其他*

*包括旅游和休闲、教育、公用事业行业和公共部门。

本报告所涉及行业的三年平均值（2020至2022年）

新思科技在一份关于影响软件安全的策略、工具和实践的报告中指出，在1,000名受访者中，超过33%的受访者表示，安全培训不足是主要障碍，紧随其后的是安全人员短缺 (31%)。这33%的受访者还表示，外部顾问正在帮助其组织进行安全测试。

委托第三方安全测试人员，从客观的角度评估组织机构的安全状况，这是非常有益的。事实上，《软件安全构建成熟度模型 (BSIMM)报告》指出，在参与BSIMM项目的组织中，有超过88%聘请外部渗透测试人员来增强其安全活动，以帮助他们发现内部测试可能遗漏的问题，找出安全实践中的薄弱点。

即使您认为贵组织的安全测试覆盖范围足够，可能也需要对内部测试进行验证，确保内部安全控制是有效的。或者，您可能需要根据法规、客户或其他强制性要求而必须开展第三方评估。例如，PCI DSS 4.0第11项对定期开展渗透测试提出了明确要求。需要进行正式审计的商户和所有服务提供商都必须满足这项要求。

《健康保险可携带性与责任法案》(HIPAA) 要求医疗从业者采取技术措施保护电子健康信息的机密性和安全性。虽然HIPAA没有明确规定必须进行渗透测试或漏洞扫描，但明确规定相关组织机构必须开展风险分析，这就意味着这些组织机构必须对其安全控制措施进行测试。

HIPAA在“评估”部分特别提到了“定期技术和非技术评估”的方法。在其HIPAA指南中，美国国家标准与技术研究院 (NIST) 建议在合理和适当的情况下，应通过联合开展外部和/或内部渗透测试来满足这些技术评估要求。

在金融服务领域，金融业监管局 (FINRA) 为金融机构制定了网络安全规则，并建议定期以及在重大事件发生后开展渗透测试，例如，在公司的基础设施或访问控制机制发生重大变化之后。《格雷姆-里奇-比利利法案》(GLBA) 明确要求金融机构自2022年起（最晚到2023年6月）每年开展渗透测试和漏洞扫描，作为其安全活动的一部分。

新思科技报告显示

超过33%

在1,000名受访者中，的受访者指出，安全培训不足是主要障碍

超过31%

的受访者指出，缺乏安全人员是比较严重的问题

新思科技安全测试详解

新思科技测试是模拟真实世界的攻击者对运行中的应用进行探测，包括“黑盒”和“灰盒”测试，其目的是找出漏洞，然后根据需要进行分类和修复。黑盒测试从局外人的角度评估测试目标的安全状况，灰盒测试则是模拟有凭证的认证用户 — 本质上是在黑盒测试的基础上增加更深入的洞察。这些测试主要针对Web (82%) 和移动 (13%) 系统/应用，也涵盖少量的网络 (3.0%) 和源代码 (2.0%) 系统/应用。

渗透测试

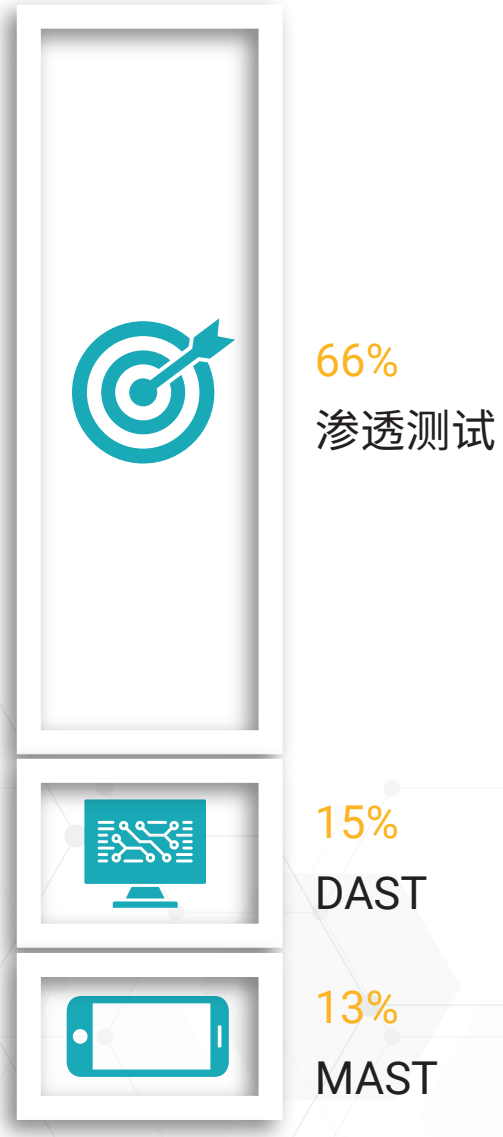
66%的测试是渗透测试—对计算机系统进行授权的模拟攻击，以评估其安全性。渗透测试人员使用与攻击者相同的工具、技术和过程来探索和展示系统中弱点对业务的影响。渗透测试检查系统是否足够强大，能否抵御来自不同位置（认证和非认证）以及各种系统角色的攻击。

外部渗透测试通常是为了满足行业法规和标准，还能带来一些额外的好处，例如客观评估贵组织的安全状况，以及准确模拟外部攻击者可能利用的潜在威胁和漏洞等。

全面的渗透测试方法对于优化风险管理至关重要。新思科技的渗透测试可能覆盖以下目标：

- Web应用。测试人员检查安全控制的有效性，寻找隐藏的漏洞、攻击模式，以及可能导致Web应用被攻破的任何其他安全缺口。
  - 移动应用/设备。测试人员采用自动测试和手动测试相结合的方式，在移动设备上运行的应用二进制文件和相应的服务器端功能中寻找漏洞。服务器端的漏洞可能包括会话管理、加密问题、身份验证和授权问题，以及其他常见的Web服务漏洞。应用二进制文件中的漏洞可能包括身份验证和授权问题、客户端信任问题、安全控制配置错误和跨平台开发框架问题。
  - 网络。这类测试旨在发现外部网络和系统中的重大安全漏洞。测试人员根据测试用例清单中的内容，对加密的传输协议、SSL证书范围和管理服务的使用等进行测试。在这三年开展的所有渗透测试中，有2.7%是网络安全渗透测试。
  - API。测试人员结合使用自动和手动测试技术，对 OWASP API Security Top 10清单中的十大严重问题进行测试，包括对象级授权失效、用户认证失效、数据暴露过度和缺乏资源/速率限制等。

过去三年开展的测试类型



专业渗透测试人员像对手一样思考和行动，为渗透测试引入了必要的人为因素，可以通过分析数据来确定攻击目标、测试系统和网站，这些都是按脚本执行测试的自动测试解决方案无法做到的。此外，有些漏洞是无法通过自动测试工具轻松检测到的，需要人工审查才能被发现。例如，手动测试是检测不安全直接对象引用（IDOR，允许攻击者访问未授权数据的问题）的唯一有效方法。

DAST

动态应用安全测试（DAST）占到三年中开展的测试总数的15%。DAST是一种应用安全（AppSec）测试方法，测试人员对运行中的应用进行检查，但不了解应用在系统级别的内部交互或设计，也没有访问或查看源程序的权限或能力。这种黑盒测试从外到内观察应用，检查其运行状态，并观察其对测试工具发起的模拟攻击的响应，据此来判断应用程序是否存在漏洞，以及是否有可能遭受真正的恶意攻击。

DAST旨在发现意料之外的结果或输出，以防其被攻击者用来攻破应用。由于DAST工具没有关于应用或源代码的内部信息，因此只能像外部黑客一样发动攻击 — 使用同样有限的应用相关知识和信息。

DAST解决方案可以发现难以通过其他安全测试检测到的运行时漏洞，例如身份验证和服务器配置错误、代码注入、SQL注入和跨站脚本错误。

正如本报告前面提到的那样，有时候，全面了解软件安全状况必须借助人工审查。新思科技的DAST评估含手动测试，以发现开箱即用工具通常无法发现的漏洞，例如与身份验证和会话管理、访问控制和信息泄露相关的一些漏洞。

MAST

在三年开展的所有测试中，移动应用安全测试（MAST）占13%。新思科技移动应用安全测试侧重于对移动客户端代码、服务器端代码和第三方库进行全面分析，无需源代码即可系统地发现和修复移动应用中的安全漏洞。新思科技采用了一系列专有的静态和动态分析工具来协同发现漏洞，并根据每个测试对象的风险状况，提供不同深度的分析，调整测试水平。

有时候，全面了解软件安全状况必须借助人工审查。

尽管移动应用的使用已经非常普及，但大多数开发和安全团队对移动安全的重视程度仍然很低。NowSecure的《MobileRiskTracker》 报告显示，公共应用商店中85%的移动应用包含一个或多个高风险漏洞，或者违反了一个或多个OWASP移动应用安全验证标准。此外，70%的移动应用会泄露隐私数据，可能触犯GDPR/CCPA等隐私法规。

漏洞概述

开放网络应用安全项目 (OWASP) Top 10和常见弱点枚举 (CWE) Top 25提供了最常见和最危险的安全漏洞清单。这两个清单都基于多种来源的数据，包括安全研究人员、漏洞数据库和安全事件报告。

OWASP Top 10清单代表了大量开发人员和 Web 应用程序安全团队对 Web 应用程序最关键的安全风险的共识。CWE Top 25清单由MITRE与SANS研究所合作创建，对25个最危险的软件漏洞进行了排名。虽然这两个清单的本意都是提高安全意识，但许多组织也将其作为安全标准来检验内部安全控制措施的效果。

OWASP Top 10清单专注于Web应用特有的安全风险，CWE Top 25清单则专注于软件缺陷和相关CWE。

如图2所示，虽然这两个清单使用的术语有所不同，但它们之间是有重叠的。例如，OWASP的“A05:2021—安全配置错误”与CWE Top 25中列出的多个弱点有关，包括CWE-798（使用了硬编码凭据）和CWE-276（默认权限不正确）。

“指纹”（探测Web应用以获取信息）可以合理地归入OWASP Top 10中的“安全日志和监控失败”或“访问控制失败”类别（我们将其归入前者），但这两个类别中都没有直接提到它。同样，指纹可能与CWE中的“向未经授权的行为者暴露敏感信息” (CWE-200) 关系最密切。如图2的第1、4、6和9行所示，在许多测试中都发现了各方面的信息泄露/泄漏问题。

公共应用商店中85%的移动应用包含一个或多个高风险漏洞。

新思科技2022年十大漏洞类别	2021年排名	2020年排名	相关的OWASP Top 10/ Mobile Top 10类别	相关的CWE(s)
1. 信息披露:信息泄露	1	1	A01:2021—访问控制失效	向未经授权的行为者暴露敏感信息 (CWE-200)。其他访问控制管理问题,包括授权缺失/错误 (CWE-863) 以及客户端/服务器端请求伪造漏洞 (CWE-918)。
2. 服务器配置错误	2	2	A05:2021—安全配置错误	安全配置错误,如 CWE-798 和 CWE-276.
3. 传输层保护不足	3	3	A05:2021—安全配置错误 M3: 传输层保护不足	安全配置错误,如 CWE-798 和 CWE-276.
4. 授权不足	4	4	A01:2021—访问控制失效 M6: 授权不足	向未经授权的行为者暴露敏感信息 (CWE-200)。其他访问控制管理问题,包括授权缺失/错误 (CWE-863) 以及客户端/服务器端请求伪造漏洞 (CWE-918)。
5. 应用配置错误	9	9	A05:2021—安全配置错误	安全配置错误,如 CWE-798 和 CWE-276.
6. 应用隐私失败	5	5	A02:2021—加密失败	向未经授权的行为者暴露敏感信息 (CWE-200)。不可信数据的反序列化 (CWE-502)。
7. 身份验证:身份验证不足	8	8	A07:2021—身份验证和认证失败	认证不正确或缺失,如 CWE-287 或 CWE-306.
8. 内容欺骗/内容注入	6	6	A03:2021—注入	SQL注入 (CWE-89),命令注入 (CWE-78和CWE-77),代码注入(CWE-94),跨站脚本 (CWE-79)。
9. 指纹敏感性	7	7	A09:2021—安全日志和监控失败	向未经授权的行为者暴露敏感信息 (CWE 200).
10. 暴露于客户端/跨站脚本攻击	不在十大漏洞范围内	10	A03:2021—注入	跨站脚本 CWE-79, 跨站请求伪造 (CWE-352).

图2. 新思科技十大漏洞类别

安全问题详解

如图2所示，漏洞类别的排名多年来基本保持不变。有趣的是，“应用配置错误”成为唯一的例外。该类别在2022年从第9位跃升到第5位，之前两年一直排在第9位。

配置错误可能发生在应用、浏览器、网络、操作系统和服务器中。例如，澳大利亚电信巨头Optus在2022年经历了一起严重的数据泄露事件，泄露了970万名客户的个人数据。造成这起事件的原因是公司的防火墙配置错误，使得第三方承包商能够访问敏感的客户数据。

人为错误通常是配置错误的最常见原因。例如，组织机构没有充分检查其应用和部署脚本，使自己容易受到攻击；测试人员在测试过程中修改了配置，但没有恢复到更安全的设置；组织机构未对新的硬件和软件进行适当的测试，无法保证其能够满足他们的安全要求。

“应用配置错误”排名上升，说明了组织机构需要使用多种安全测试工具，而不是只依赖一种测试工具。如果只使用一种测试工具，虽然在减少编码漏洞总数方面可能很有效，但并不是好的实践，尤其涉及到运行时环境时。组织机构需要使用多种测试工具来发现运行中的应用问题，如配置错误。

2022年测试中发现的十大漏洞类别如下：

1. **信息披露，又称信息泄露。**当敏感信息暴露给未授权方时，就会出现这种安全问题。例如，网站可能会因为安全配置错误而泄露用户名或财务信息等用户数据。在三年来开展的所有测试中，平均有19%的漏洞与信息泄露问题直接相关。

   OWASP团队将信息泄露归入“A01:2021-访问控制失效”类别，并指出与其他类别相比，这个类别中的漏洞最多。“向未经授权的行为者暴露敏感信息”、 “通过发送的数据暴露敏感信息”以及“跨站请求伪造”等，都是该类别中最常见的漏洞。

在三年来开展的所有测试中，平均有19%的漏洞与信息泄露问题直接相关。

2. **服务器（安全）配置错误。**服务器配置错误属于OWASP的“A05:2021-安全配置错误”类别，在三年来开展的所有测试中，这一类别平均占到漏洞总数的18%。虽然我们的研究结果集中在服务器配置错误上，但安全配置错误可以发生在应用程序堆栈的任何层级，包括网络服务、平台、Web服务器、应用服务器、数据库、框架、自定义代码和预安装的虚拟机、容器或存储器（见第5类）。这类缺陷经常允许攻击者未经授权访问系统数据或功能，有时甚至会导致整个系统被攻陷。

在三年来开展的所有测试中，平均有11%的漏洞与传输层保护不足有关。

3. **传输层保护不足。**这些安全缺陷是由于应用没有采取适当措施来保护网络流量而导致的。在身份验证期间，应用可能会使用SSL/ TLS来保护数据安全，但通常不对其他操作使用这些技术，从而使数据和会话ID暴露给第三方。

   许多移动应用都存在与传输层安全性不足相关的特定问题，以至于OWASP在其OWASP Mobile Top list中专门为其设立了一个类别。正如OWASP所指出的那样，“移动应用通常不会保护网络流量。它们可能会在身份验证期间使用SSL/TLS，但不会在其他地方使用这些技术。这种不一致性导致数据和会话ID容易被拦截。”在三年来开展的所有测试中，平均有11%的漏洞与传输层保护不足有关。

4. **授权不足。**这些漏洞可能允许用户访问他们无权访问的数据、内容或功能。当应用或系统没有正确验证用户身份或未能实施适当的访问控制时，就可能发生这种情况。

   例如，移动应用根据请求将用户角色或权限信息未经加密传输到后端系统，就属于不安全的授权。OWASP指出，IDOR漏洞的存在通常表明代码没有执行有效的授权检查。在三年来开展的所有测试中，平均有9%的漏洞与授权不足问题有关。

在三年来开展的所有测试中，平均有18%的漏洞与服务器配置错误有关。

5. **应用配置错误。**这也是一种安全配置错误，也是在OWASP十大漏洞列表中排名第五的危险漏洞。

   许多应用都有一些开发者功能，这些功能如果在部署时没有关闭，就会非常危险，比如调试和QA功能。未被适当锁定的配置文件可能以明文显示（即任何人都可以读取的未加密文本），并且配置文件中的默认设置可能并没有考虑到安全因素。在三年来开展的所有测试中，平均有5%的漏洞与应用配置错误有关。

6. **应用隐私失败。**应用隐私失败与信息泄露/披露相关，是指应用在设计、实施或修补方面存在缺陷，导致未授权的用户可以访问数据或内容，发生隐私泄露。组织机构在构建应用时，应考虑到一些隐私问题，例如：

   - 我们的开发人员是否接受过Web应用隐私方面的培训？
   - 是否编制了安全编码指南？
   - 我们的软件（包括服务器、数据库和库代码）能否及时更新？
   - 是否定期安装补丁？
   - 为确保软件中使用的第三方和开源代码是安全且最新的，我们采取了哪些措施？
   - 个人数据在完成指定任务后是否会被删除？

   在三年来开展的所有测试中，平均有5%的漏洞与隐私问题有关。

许多应用都有一些开发者功能，这些功能如果在部署时没有关闭，就会非常危险，比如调试和QA功能。

7. **身份验证不足。**以前称为“身份验证失败”，属于OWASP“A07:2021—身份验证和认证失败”类别，现在涵盖与身份验证失败相关的漏洞，例如我们列表中的第4类和第7类漏洞。在三年来开展的所有测试中，平均有5%的漏洞与身份验证不足有关。

   身份验证和授权不足是指因应用或系统没有正确验证用户身份或未能实施适当的访问控制而导致的安全漏洞。未经授权的用户可能会访问敏感信息或执行他们无权执行的操作，从而引发数据泄露和数据丢失等安全问题。

8. **内容欺骗/内容注入。**内容欺骗也称为内容注入，是一种针对用户的攻击，可能是由于Web应用中存在漏洞，无法正确处理用户提供的数据而造成的。

   当Web应用将攻击者提供的内容呈现给毫无戒心的用户时，就会发生这种情况，其发生的形式通常是可信域名下修改过的页面。OWASP指出，这类攻击经常被误解为常见的Web漏洞，几乎或根本没有业务影响。但实际上，内容欺骗攻击频繁出现在各种欺诈中，攻击者冒充合法实体诱骗用户提供登录凭证。

更令人担忧的是，内容欺骗有可能发起危险的攻击，包括代码注入和跨站脚本。三年来开展的所有测试中，平均有4%的漏洞与内容欺骗或内容注入有关。

9. **指纹敏感性。**指纹（探测Web应用以获取信息）可以给攻击者提供有价值的信息，如操作系统类型、操作系统版本、SNMP信息、域名、网络区域和VPN连接点等。三年来开展的所有测试中，平均有3%的漏洞与指纹有关。

测试中发现的许多具体的指纹类安全问题都属于微风险、低风险或中风险问题。也就是说，攻击者不能直接利用这些漏洞来访问系统或敏感数据。然而，揭示这些漏洞并不是一件徒劳无功的事情，因为即使是低风险的漏洞，也可能被用来促进攻击。

例如，在三分之一的渗透测试和近一半的DAST扫描中，持续发现了与指纹相关的一个安全问题，即冗长的服务器标识（图5）。虽然这是一个中风险漏洞，但却能够给攻击者发动攻击提供足够的信息，如服务器名称、类型和版本号等。//右图下面的文字没有翻译

在2022年测试发现的所有高风险漏洞中，有19%与跨站脚本攻击有关。

	测试发现的高危漏洞的百分比	2021年排名	2020年排名
1. 跨站脚本	19%	2	1
2. 授权不足	16%	1	2
3. 身份验证不足	6%	3	3
4. 应用配置错误	4%	6	9
5. 传输层保护不足	4%	4	5
6. 信息披露/信息泄露	3%	7	6
7. 服务器配置错误	2%	9	8
8. SQL注入	2%	8	10
9. 意外数据泄漏	1%	*	*
10. 程序验证不足	1%	*	*

* 不在十大漏洞范围内

图3. 2022年测试发现的十大高危漏洞（不包括重新测试）

	测试发现的超高危漏洞的百分比	2021年排名	2020年排名
1. SQL注入	30%	1	1
2. 授权不足	9%	2	2
3. 跨站脚本	7%	9	9
4. 身份验证不足	7%	3	3
5. 信息披露/信息泄露	6%	4	4
6. 程序验证不足	5%	8	5
7. OS命令	3%	7	7
8. 服务器配置错误	2%	*	*
9. 应用程序配置错误	2%	6	9
10. SQL注入	1%	*	*

* 不在十大漏洞范围内

图4. 2022年测试发现的十大超高危漏洞（不包括重新测试）

SQL命令注入是测试中发现的排名第一的超高危漏洞。

10. 遭遇客户端/跨站脚本攻击。跨站脚本 (XSS) 攻击是一类客户端代码注入攻击，是在新思科技三年测试中排名第一或第二的高危漏洞。攻击者试图通过在合法的网页或Web应用中注入恶意代码而在受害者的Web浏览器中执行恶意脚本。在2022年测试发现的所有高风险漏洞中，有19%与跨站脚本攻击有关（见图3）。

实施或加强诸如内容安全策略 (CSP) 之类的保护措施可以提供额外的安全层，帮助检测和缓解某些类型的攻击，包括跨站脚本和数据注入攻击（测试中发现的头号超高危漏洞，见图4）。攻击者可以使用不安全的用户数据传输（如cookie和表单），将命令注入到Web服务器上的系统Shell中，然后利用特权来破坏服务器。

许多组织都认为，CSP不安全或缺失只是低风险漏洞。然而，跨站脚本、点击劫持和跨站泄漏等攻击的频繁发生，凸显出应用CSP的必要性，尤其是可以防止恶意脚本在客户端执行的CSP — 作为第二层防线来抵御各种类型的攻击，包括跨站脚本和数据注入攻击。

脆弱的第三方库的危险

如图6所示，在新思科技开展的2022年测试中，25%的测试发现了使用易受攻击的第三方库，这与OWASP Top 10中的“A06:2021—易受攻击或过时的组件”漏洞有关。OWASP指出，无论是在客户端还是服务器端，您都必须清楚所有组件的版本，包括软件中使用的第三方和开源组件，否则，您的软件很可能会受到攻击。

	占2022年测试目标总数的百分比	2021年排名	2020年排名
1. 弱SSL/TLS配置	70%	1	4
2. 缺失Content-Security-Policy标头	43%	2	1
3. 冗长的服务器标识	37%	3	2
4. 可缓存HTTPS内容	34%	5	5
5. 未实施HTTP严格传输安全 (HSTS) 机制	34%	4	3
6. 不安全的Content-Security-Policy标头	31%	6	8
7. 弱密码策略	28%	7	7
8. 未屏蔽非公开信息数据	25%	*	*
9. 使用了易受攻击的第三方库	25%	*	*
10. 会话超时时间过长	24%	*	*

* 不在十大漏洞范围内

图5. 2022年测试发现的十大安全问题

大多数企业都不十分清楚自己的代码组成。

开源代码可以显著提升软件构建的速度和效率，这已成为现代软件的重要组成部分，深受开发者欢迎。作为经过验证的代码，开源代码便于开发者访问和使用，无需浪费时间和资源做重复工作。

然而，新思科技的年度《开源安全与风险分析报告》，显示，开源代码并非没有风险。事实上，2023年的报告显示，开源安全风险已经达到了前所未有的水平，并且大多数企业并不十分清楚自己的代码组成。

报告指出，高风险的开源漏洞在过去五年增速惊人（仅在零售和电子商务领域就增长了557%）。最重要的是，令人不安的是缺乏安全补丁和项目依赖维护（91%的项目包含了过时的开源组件）。

由于供应链攻击屡见不鲜，软件供应链安全已经成为依赖第三方软件的组织机构的主要关注点，这是几乎所有现代组织都需要面对的挑战。为了更好地管理供应链风险，越来越多的组织使用自动化工具生成软件材料清单 (SBOM)，以识别他们使用的第三方和开源软件。

从BSIMM报告中可以看出，“为软件创建物料清单”这项安全活动呈现增长趋势，证明了各组织机构都在朝着SBOM进行转变。BSIMM报告还显示，由于针对脆弱的开源项目的攻击越来越猖獗，导致“识别开源代码”和“控制开源风险”这两项活动显著增加。

由于许多公司都在同时使用数百个应用或软件系统，每个应用或软件系统本身又可能依赖成百上千个不同的第三方和开源组件，因此，他们迫切需要借助准确、最新的SBOM来有效跟踪这些组件。

启发和建议

- **实施多层安全方法。**仅依赖单一的安全测试解决方案，如静态应用安全测试 (SAST)，已经不足以满足安全需求。组织机构应实施多层安全方法，通过SAST来识别编码缺陷，通过DAST来检查运行中的应用，通过软件组成分析 (SCA) 来识别由第三方组件引入的漏洞，通过渗透测试来发现错误配置等问题以及其他测试可能遗漏的漏洞。

  新思科技《2023年全球 DevSecOps现状调查》 报告显示，44%的受访者将外部渗透测试视为安全测试的重要组成部分，也是对其他测试的有效补充。外部渗透测试的好处在于，它能从客观的第三方角度评估您的安全状况，并能准确模拟其他测试可能无法发现的潜在威胁和漏洞，以防它们被攻击者利用。

- **自动和手动安全测试相结合。**自动测试能够保证一致性和可扩展性，并节省时间和成本，而手动测试则能够增加一层洞察力和适应性，这对识别复杂和微妙的安全问题至关重要。例如，DAST作为黑盒测试（即不了解应用的内部结构）就需要开发者和安全专家验证和分析所发现的问题。

- **重视补丁管理。**保持警惕，及时修补漏洞，尤其是对第三方和开源组件。建立清晰的流程来识别、评估和快速应用补丁，有效防止漏洞利用。

> 您不知道的漏洞才是软件中最危险的漏洞。

- **实施严格的访问控制。**对应用和网络实施严格的访问控制策略。遵循最小权限原则，确保用户只拥有执行任务所需的最低访问权限。定期检查和更新应用的访问权限，防止未授权的访问。

- **将SBOM生成纳入软件开发生命周期。**您不知道的漏洞才是软件中最危险的漏洞。通过使用完整的清单来识别组件，您可以更好地了解安全状况，并且及时有效地应对漏洞问题。

- **确定是否需要补充安全测试。**您的安全团队是否具备足够的应用安全技能和资源来测试安全缺陷？是否有时间按照监管机构和客户的要求来测试软件？

- **选择能够随时随地提供专业安全测试服务的供应商。**新思科技安全测试服务部专业技能过硬、工具丰富、纪律严明，能够随时随地为您提供经济高效的支持，对任何应用开展任何深度的分析。

新思科技提供全方位的测试服务，包括渗透测试、动态应用安全测试、静态应用安全测试、移动应用安全测试、网络渗透测试、红队测试、物联网和嵌入式软件测试、以及胖客户端测试。

我们的按需测试服务可以帮助贵组织的安全测试团队提升实力。
立即联系新思科技，预约免费咨询。

SYNOPSYS®

新思科技与众不同

新思科技提供的集成解决方案，可以改变您构建和交付软件的方式，在应对业务风险的同时加速创新。与新思科技同行，您的开发人员可以在编写代码的时候快速兼顾安全。您的开发和DevSecOps团队可以在不影响速度的情况下在开发管道中自动进行安全测试。您的安全团队可以主动管理风险，并将补救工作聚焦在对贵组织最重要的事情上。我们无与伦比的专业知识可以帮助您规划和执行所需的安全计划。只有新思科技能够满足您构建可信软件的一切需求。

如需了解更多信息，请访问：www.synopsys.com/software.

SYNOPSYS®

2023年《软件漏洞快照》报告

三年来10类最常见的Web和软件应用漏洞分析

本报告由新思科技安全测试服务部与新思科技网络安全研究中心 (CyRC) 联合编制

目录

概述 1

这些测试中发现的安全问题 1

高危和超危漏洞 2

定义漏洞的严重级别 3

新思科技安全测试服务概述 3

新思科技安全测试详解 5

渗透测试 5

DAST 6

MAST 6

漏洞概述 7

安全问题详解 9

易受攻击的第三方库的危险 14

启发和建议 15

概述

在编写该《软件漏洞快照》报告时，新思CyRC的研究人员和新思安全测试服务部的顾问使用了三年来对商业软件系统和应用进行测试的匿名数据。

新思科技测试发现了仍对Web和软件应用安全造成重大威胁的已知漏洞，尤其是以下几类最常见的漏洞：

- 信息披露/泄露和隐私
- 配置错误
- 传输层保护不足

这些测试凸显出易受攻击的第三方库带来的持续危险，以及软件开发环境对强大的软件供应链安全的需求 — 在软件开发中，超过90%的软件包含开源代码。下面的数据还显示了将应用安全测试扩展到基本静态分析之外的价值。

如果您是软件安全项目的负责人，那么，深入了解软件风险可以帮助您制定更有效的安全改进策略。如果您是从战术的角度考虑安全问题，则可以使用本报告中的信息来展示需要通过第三方协助以扩展安全测试的业务案例。

测试中发现的安全问题

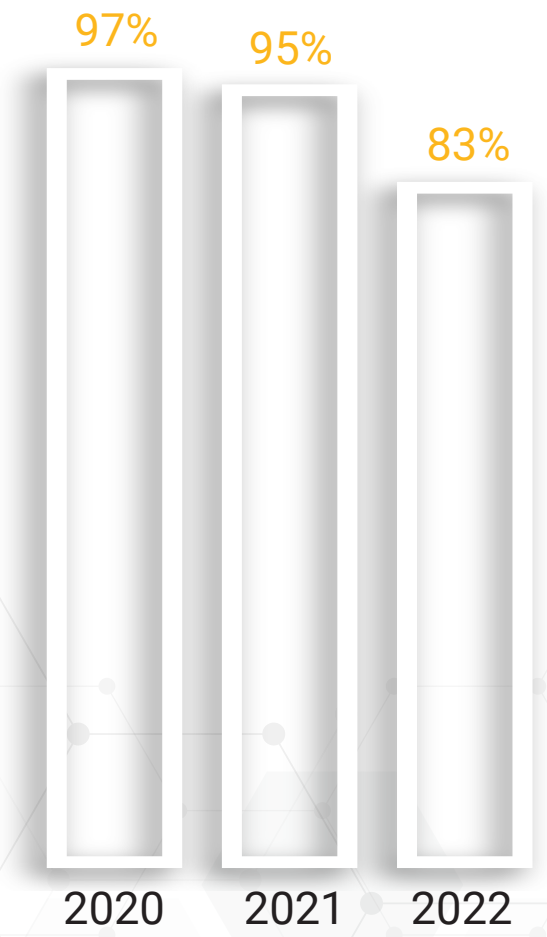
在2020年，97%的测试发现了漏洞。到2021年，这一比例降至95%，而2022年进一步降至83%。我们收集的三年数据显示，92%的测试在目标应用中发现了漏洞。

总体漏洞的持续减少是一个令人鼓舞的迹象，说明开发团队在编写无误代码方面取得了进步，而且诸如代码审查、自动测试和持续集成等实践也有助于减少常见的编程错误。

此外，编程语言和集成开发环境 (IDE) 的发展也为开发者提供了一些内置的检查和工具，可以帮助他们及时发现并修复错误，避免造成严重问题。对于一些受欢迎的开源项目，许多社区也加强了代码审查，提高了代码质量标准。

然而，对于一些不太受关注或者已经过时的开源项目，就没有这么幸运了。据一些报告显示，在2022年维护的Java和JavaScript开源项目中，有近20%的项目已经停止了维护，使得这些项目面临漏洞以及被利用的风险。

发现漏洞的测试占比



高危和超危漏洞

在这三年中，27%的测试发现了高危漏洞，6.2%的测试发现了超危漏洞。其中，跨站脚本 (XSS) 在新思科技的多年测试中一直都是最常见的高危漏洞之一。同样，2020到2022年间，SQL注入一直位列最常见的超危漏洞之首。

按年份细分，我们发现在2022年的测试中，高危漏洞相比2021年略有增加（25% vs. 20%），相比2020年略有减少（25% vs. 30%），但超危漏洞 (6.7%) 均高于2021年 (4.5%) 和2020年 (6.1%)。

许多中危、高危和超危漏洞都需要多层测试才能被发现。

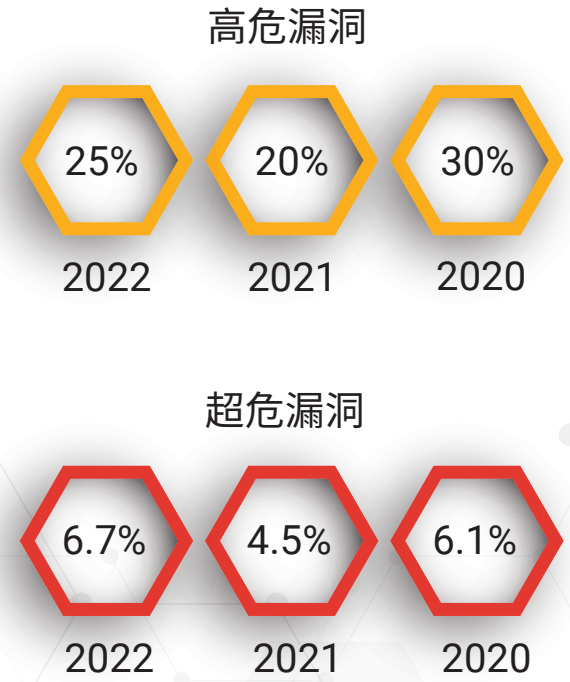
这些数字反映出，高危和超危漏洞过去几年一直都在增加，并在2022年达到了历史最高水平。在2022年报告的CVE中，约有80%属于中危或高危漏洞，有16%属于超危漏洞。虽然开发团队的努力使总体漏洞数量减少，但数据表明，许多中危、高危和超危漏洞都需要更强有力的测试才能被发现，如渗透测试。

	2022	2021	2020
超危	28%	54%	77%
高危	38%	46%	63%
中危	60%	64%	72%

图1. 与原始测试相比，后续重复测试中发现的漏洞的减少情况（百分比）

图1说明了动态测试，比如一些类型的渗透测试和动态应用安全测试 (DAST)，是对静态应用安全测试 (SAST) 的有效补充。通过对一些重新测试进行抽样检查（即对安装了特定修复包的软件进行快速验证），我们发现在这三年期间，客户的超危、高危和中危漏洞都在逐年减少。例如，2022年检测到的中危漏洞减少了60%，高危和超高危漏洞分别减少了38%和28%。

2020至2022年间，高危和超危漏洞的占比



定义漏洞的严重级别

漏洞的严重级别根据 CVSS v3 标准评定，反映了漏洞对网络安全构成的风险。超危漏洞的CVSS分数在9.0到10.0之间，而且有已经公开或正在被攻击者使用的漏洞或存在安全缺陷的代码，例如命令、代码和SQL注入漏洞。

高危漏洞的CVSS分数在7.0到8.9之间，通常比超危漏洞更难被利用。但是，考虑到存在此类漏洞的应用/系统的业务关键性和威胁环境等因素，高危漏洞也需要及时检查和修复。

随着越来越多的攻击者开始使用自动化漏洞利用工具，可以在几秒钟内攻击数千个系统，尤其是考虑到超过一半的漏洞在披露后一周内即被利用，因此，高危和超危漏洞必须在发现后及时修复。

应用中的安全或漏洞问题不仅会影响组织机构本身（或其客户）的业务运营，而且还会影响整个软件开发生命周期乃至整条软件供应链。

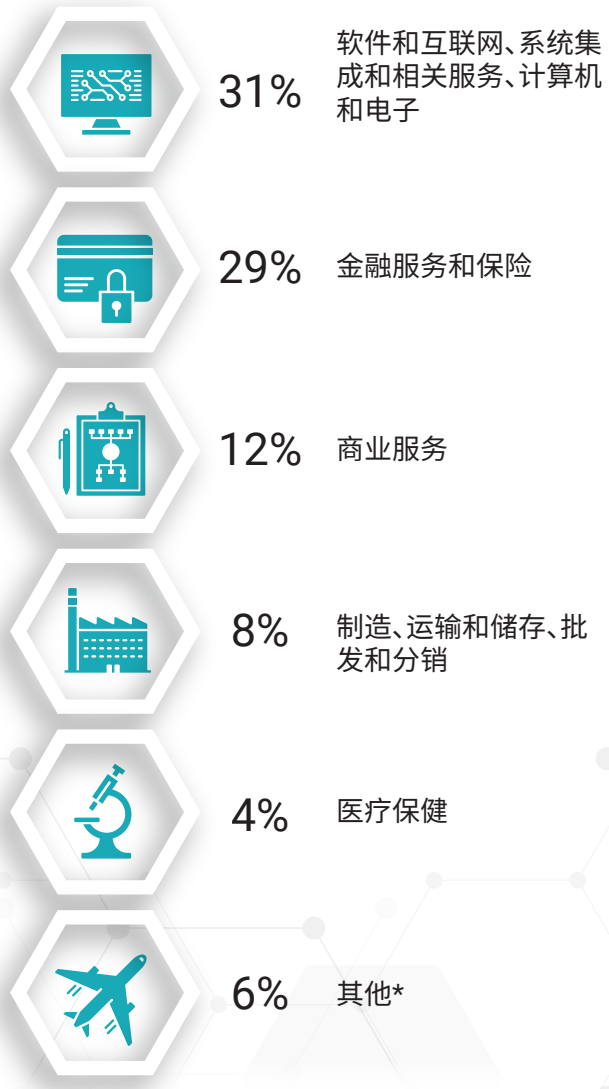
事实上，新思科技《2023年全球DevSecOps现状调查》报告指出，超过80%的受访者表示，解决严重的安全/漏洞问题已对其组织的2022-2023软件交付计划产生了影响。

新思科技安全测试服务概述

开发团队必须以前所未有的速度构建越来越复杂的软件，但训练有素的技术人员严重不足。

虽然属于不同的行业和组织，但新思科技安全测试服务部的所有客户都有一个共同需求 — 扩大测试的覆盖范围。他们要求开发团队以前所未有的速度构建越来越复杂的软件，但却面临训练有素的技术人员严重不足的问题，尤其是在软件安全方面。

本次研究涉及的行业



*包括旅游和休闲、教育、公用事业行业和公共部门。

本报告所涉及行业的三年平均值（2020至2022年）

新思科技在一份关于影响软件安全的策略、工具和实践的报告中指出，在1,000名受访者中，超过33%的受访者表示，安全培训不足是主要障碍，紧随其后的是安全人员短缺 (31%)。这33%的受访者还表示，外部顾问正在帮助其组织进行安全测试。

委托第三方安全测试人员，从客观的角度评估组织机构的安全状况，这是非常有益的。事实上，《软件安全构建成熟度模型 (BSIMM)报告》指出，在参与BSIMM项目的组织中，有超过88%聘请外部渗透测试人员来增强其安全活动，以帮助他们发现内部测试可能遗漏的问题，找出安全实践中的薄弱点。

即使您认为贵组织的安全测试覆盖范围足够，可能也需要对内部测试进行验证，确保内部安全控制是有效的。或者，您可能需要根据法规、客户或其他强制性要求而必须开展第三方评估。例如，PCI DSS 4.0第11项对定期开展渗透测试提出了明确要求。需要进行正式审计的商户和所有服务提供商都必须满足这项要求。

《健康保险可携带性与责任法案》(HIPAA) 要求医疗从业者采取技术措施保护电子健康信息的机密性和安全性。虽然HIPAA没有明确规定必须进行渗透测试或漏洞扫描，但明确规定相关组织机构必须开展风险分析，这就意味着这些组织机构必须对其安全控制措施进行测试。

HIPAA在“评估”部分特别提到了“定期技术和非技术评估”的方法。在其HIPAA指南中，美国国家标准与技术研究院 (NIST) 建议在合理和适当的情况下，应通过联合开展外部和/或内部渗透测试来满足这些技术评估要求。

在金融服务领域，金融业监管局 (FINRA) 为金融机构制定了网络安全规则，并建议定期以及在重大事件发生后开展渗透测试，例如，在公司的基础设施或访问控制机制发生重大变化之后。《格雷姆-里奇-比利利法案》(GLBA) 明确要求金融机构自2022年起（最晚到2023年6月）每年开展渗透测试和漏洞扫描，作为其安全活动的一部分。

新思科技报告显示

超过33%

在1,000名受访者中，的受访者指出，安全培训不足是主要障碍

超过31%

的受访者指出，缺乏安全人员是比较严重的问题

新思科技安全测试详解

新思科技测试是模拟真实世界的攻击者对运行中的应用进行探测，包括“黑盒”和“灰盒”测试，其目的是找出漏洞，然后根据需要进行分类和修复。黑盒测试从局外人的角度评估测试目标的安全状况，灰盒测试则是模拟有凭证的认证用户 — 本质上是在黑盒测试的基础上增加更深入的洞察。这些测试主要针对Web (82%) 和移动 (13%) 系统/应用，也涵盖少量的网络 (3.0%) 和源代码 (2.0%) 系统/应用。

渗透测试

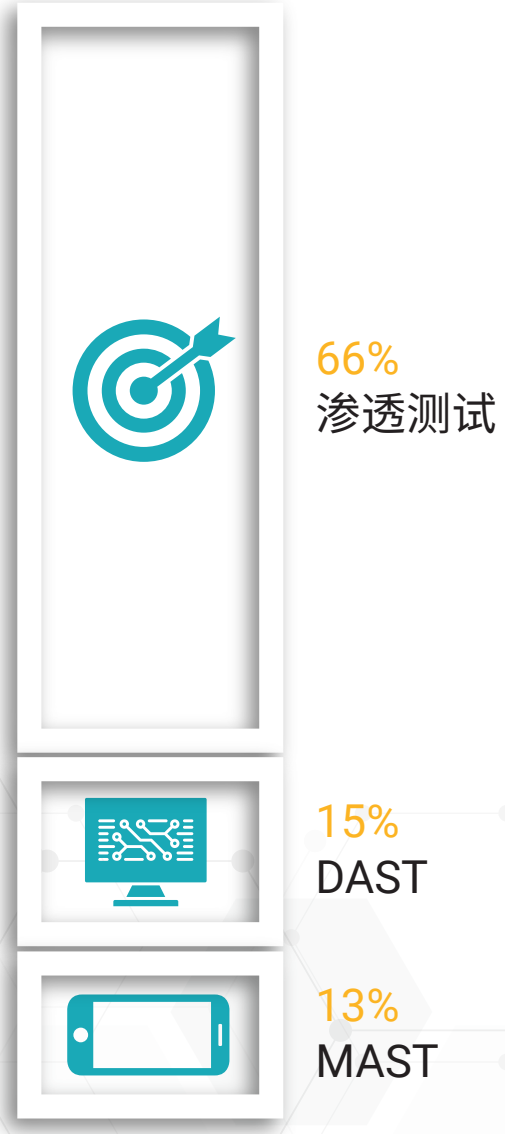
66%的测试是渗透测试—对计算机系统进行授权的模拟攻击，以评估其安全性。渗透测试人员使用与攻击者相同的工具、技术和过程来探索和展示系统中弱点对业务的影响。渗透测试检查系统是否足够强大，能否抵御来自不同位置（认证和非认证）以及各种系统角色的攻击。

外部渗透测试通常是为了满足行业法规和标准，还能带来一些额外的好处，例如客观评估贵组织的安全状况，以及准确模拟外部攻击者可能利用的潜在威胁和漏洞等。

全面的渗透测试方法对于优化风险管理至关重要。新思科技的渗透测试可能覆盖以下目标：

- Web应用。测试人员检查安全控制的有效性，寻找隐藏的漏洞、攻击模式，以及可能导致Web应用被攻破的任何其他安全缺口。
  - 移动应用/设备。测试人员采用自动测试和手动测试相结合的方式，在移动设备上运行的应用二进制文件和相应的服务器端功能中寻找漏洞。服务器端的漏洞可能包括会话管理、加密问题、身份验证和授权问题，以及其他常见的Web服务漏洞。应用二进制文件中的漏洞可能包括身份验证和授权问题、客户端信任问题、安全控制配置错误和跨平台开发框架问题。
  - 网络。这类测试旨在发现外部网络和系统中的重大安全漏洞。测试人员根据测试用例清单中的内容，对加密的传输协议、SSL证书范围和管理服务的使用等进行测试。在这三年开展的所有渗透测试中，有2.7%是网络安全渗透测试。
  - API。测试人员结合使用自动和手动测试技术，对 OWASP API Security Top 10清单中的十大严重问题进行测试，包括对象级授权失效、用户认证失效、数据暴露过度和缺乏资源/速率限制等。

过去三年开展的测试类型



专业渗透测试人员像对手一样思考和行动，为渗透测试引入了必要的人为因素，可以通过分析数据来确定攻击目标、测试系统和网站，这些都是按脚本执行测试的自动测试解决方案无法做到的。此外，有些漏洞是无法通过自动测试工具轻松检测到的，需要人工审查才能被发现。例如，手动测试是检测不安全直接对象引用（IDOR，允许攻击者访问未授权数据的问题）的唯一有效方法。

DAST

动态应用安全测试 (DAST) 占到三年中开展的测试总数的15%。DAST是一种应用安全 (AppSec) 测试方法，测试人员对运行中的应用进行检查，但不了解应用在系统级别的内部交互或设计，也没有访问或查看源程序的权限或能力。这种黑盒测试从外到内观察应用，检查其运行状态，并观察其对测试工具发起的模拟攻击的响应，据此来判断应用程序是否存在漏洞，以及是否有可能遭受真正的恶意攻击。

DAST旨在发现意料之外的结果或输出，以防其被攻击者用来攻破应用。由于DAST工具没有关于应用或源代码的内部信息，因此只能像外部黑客一样发动攻击 — 使用同样有限的应用相关知识和信息。

DAST解决方案可以发现难以通过其他安全测试检测到的运行时漏洞，例如身份验证和服务器配置错误、代码注入、SQL注入和跨站脚本错误。

正如本报告前面提到的那样，有时候，全面了解软件安全状况必须借助人工审查。新思科技的DAST评估含手动测试，以发现开箱即用工具通常无法发现的漏洞，例如与身份验证和会话管理、访问控制和信息泄露相关的一些漏洞。

MAST

在三年开展的所有测试中，移动应用安全测试 (MAST) 占13%。新思科技移动应用安全测试 侧重于对移动客户端代码、服务器端代码和第三方库进行全面分析，无需源代码即可系统地发现和修复移动应用中的安全漏洞。新思科技采用了一系列专有的静态和动态分析工具来协同发现漏洞，并根据每个测试对象的风险状况，提供不同深度的分析，调整测试水平。

有时候，全面了解软件安全状况必须借助人工审查。

尽管移动应用的使用已经非常普及，但大多数开发和安全团队对移动安全的重视程度仍然很低。NowSecure的《MobileRiskTracker》报告显示，公共应用商店中85%的移动应用包含一个或多个高风险漏洞，或者违反了一个或多个OWASP移动应用安全验证标准。此外，70%的移动应用会泄露隐私数据，可能触犯GDPR/CCPA等隐私法规。

漏洞概述

开放网络应用安全项目 (OWASP) Top 10和常见弱点枚举 (CWE) Top 25提供了最常见和最危险的安全漏洞清单。这两个清单都基于多种来源的数据，包括安全研究人员、漏洞数据库和安全事件报告。

OWASP Top 10清单代表了大量开发人员和 Web 应用程序安全团队对 Web 应用程序最关键的安全风险的共识。CWE Top 25清单由MITRE与SANS研究所合作创建，对25个最危险的软件漏洞进行了排名。虽然这两个清单的本意都是提高安全意识，但许多组织也将其作为安全标准来检验内部安全控制措施的效果。

OWASP Top 10清单专注于Web应用特有的安全风险，CWE Top 25清单则专注于软件缺陷和相关CWE。

如图2所示，虽然这两个清单使用的术语有所不同，但它们之间是有重叠的。例如，OWASP的“A05:2021—安全配置错误”与CWE Top 25中列出的多个弱点有关，包括CWE-798（使用了硬编码凭据）和CWE-276（默认权限不正确）。

“指纹”（探测Web应用以获取信息）可以合理地归入OWASP Top 10中的“安全日志和监控失败”或“访问控制失败”类别（我们将其归入前者），但这两个类别中都没有直接提到它。同样，指纹可能与CWE中的“向未经授权的行为者暴露敏感信息” (CWE-200) 关系最密切。如图2的第1、4、6和9行所示，在许多测试中都发现了各方面的信息泄露/泄漏问题。

公共应用商店中85%的移动应用包含一个或多个高风险漏洞。

新思科技2022年十大漏洞类别	2021年排名	2020年排名	相关的OWASP Top 10/ Mobile Top 10类别	相关的CWE(s)
1. 信息披露:信息泄露	1	1	A01:2021—访问控制失效	向未经授权的行为者暴露敏感信息 (CWE-200)。其他访问控制管理问题,包括授权缺失/错误 (CWE-863) 以及客户端/服务器端请求伪造漏洞 (CWE-918)。
2. 服务器配置错误	2	2	A05:2021—安全配置错误	安全配置错误,如 CWE-798 和 CWE-276.
3. 传输层保护不足	3	3	A05:2021—安全配置错误 M3: 传输层保护不足	安全配置错误,如 CWE-798 和 CWE-276.
4. 授权不足	4	4	A01:2021—访问控制失效 M6: 授权不足	向未经授权的行为者暴露敏感信息 (CWE-200)。其他访问控制管理问题,包括授权缺失/错误 (CWE-863) 以及客户端/服务器端请求伪造漏洞 (CWE-918)。
5. 应用配置错误	9	9	A05:2021—安全配置错误	安全配置错误,如 CWE-798 和 CWE-276.
6. 应用隐私失败	5	5	A02:2021—加密失败	向未经授权的行为者暴露敏感信息 (CWE-200)。不可信数据的反序列化 (CWE-502)。
7. 身份验证:身份验证不足	8	8	A07:2021—身份验证和认证失败	认证不正确或缺失,如 CWE-287 或 CWE-306.
8. 内容欺骗/内容注入	6	6	A03:2021—注入	SQL注入 (CWE-89),命令注入 (CWE-78和CWE-77),代码注入(CWE-94),跨站脚本 (CWE-79)。
9. 指纹敏感性	7	7	A09:2021—安全日志和监控失败	向未经授权的行为者暴露敏感信息 (CWE 200).
10. 暴露于客户端/跨站脚本攻击	不在十大漏洞范围内	10	A03:2021—注入	跨站脚本 CWE-79, 跨站请求伪造 (CWE-352).

图2. 新思科技十大漏洞类别

安全问题详解

如图2所示，漏洞类别的排名多年来基本保持不变。有趣的是，“应用配置错误”成为唯一的例外。该类别在2022年从第9位跃升到第5位，之前两年一直排在第9位。

配置错误可能发生在应用、浏览器、网络、操作系统和服务器中。例如，澳大利亚电信巨头Optus在2022年经历了一起严重的数据泄露事件，泄露了970万名客户的个人数据。造成这起事件的原因是公司的防火墙配置错误，使得第三方承包商能够访问敏感的客户数据。

人为错误通常是配置错误的最常见原因。例如，组织机构没有充分检查其应用和部署脚本，使自己容易受到攻击；测试人员在测试过程中修改了配置，但没有恢复到更安全的设置；组织机构未对新的硬件和软件进行适当的测试，无法保证其能够满足他们的安全要求。

“应用配置错误”排名上升，说明了组织机构需要使用多种安全测试工具，而不是只依赖一种测试工具。如果只使用一种测试工具，虽然在减少编码漏洞总数方面可能很有效，但并不是好的实践，尤其涉及到运行时环境时。组织机构需要使用多种测试工具来发现运行中的应用问题，如配置错误。

2022年测试中发现的十大漏洞类别如下：

1. **信息披露，又称信息泄露。**当敏感信息暴露给未授权方时，就会出现这种安全问题。例如，网站可能会因为安全配置错误而泄露用户名或财务信息等用户数据。在三年来开展的所有测试中，平均有19%的漏洞与信息泄露问题直接相关。

   OWASP团队将信息泄露归入“A01:2021-访问控制失效”类别，并指出与其他类别相比，这个类别中的漏洞最多。“向未经授权的行为者暴露敏感信息”、“通过发送的数据暴露敏感信息”以及“跨站请求伪造”等，都是该类别中最常见的漏洞。

在三年来开展的所有测试中，平均有19%的漏洞与信息泄露问题直接相关。

2. **服务器（安全）配置错误。**服务器配置错误属于OWASP的“A05:2021-安全配置错误”类别，在三年来开展的所有测试中，这一类别平均占到漏洞总数的18%。虽然我们的研究结果集中在服务器配置错误上，但安全配置错误可以发生在应用程序堆栈的任何层级，包括网络服务、平台、Web服务器、应用服务器、数据库、框架、自定义代码和预安装的虚拟机、容器或存储器（见第5类）。这类缺陷经常允许攻击者未经授权访问系统数据或功能，有时甚至会导致整个系统被攻陷。

在三年来开展的所有测试中，平均有11%的漏洞与传输层保护不足有关。

3. **传输层保护不足。**这些安全缺陷是由于应用没有采取适当措施来保护网络流量而导致的。在身份验证期间，应用可能会使用SSL/ TLS来保护数据安全，但通常不对其他操作使用这些技术，从而使数据和会话ID暴露给第三方。

   许多移动应用都存在与传输层安全性不足相关的特定问题，以至于OWASP在其OWASP Mobile Top list中专门为其设立了一个类别。正如OWASP所指出的那样，“移动应用通常不会保护网络流量。它们可能会在身份验证期间使用SSL/TLS，但不会在其他地方使用这些技术。这种不一致性导致数据和会话ID容易被拦截。”在三年来开展的所有测试中，平均有11%的漏洞与传输层保护不足有关。

4. **授权不足。**这些漏洞可能允许用户访问他们无权访问的数据、内容或功能。当应用或系统没有正确验证用户身份或未能实施适当的访问控制时，就可能发生这种情况。

   例如，移动应用根据请求将用户角色或权限信息未经加密传输到后端系统，就属于不安全的授权。OWASP指出，IDOR漏洞的存在通常表明代码没有执行有效的授权检查。在三年来开展的所有测试中，平均有9%的漏洞与授权不足问题有关。

在三年来开展的所有测试中，平均有18%的漏洞与服务器配置错误有关。

5. **应用配置错误。**这也是一种安全配置错误，也是在OWASP十大漏洞列表中排名第五的危险漏洞。

   许多应用都有一些开发者功能，这些功能如果在部署时没有关闭，就会非常危险，比如调试和QA功能。未被适当锁定的配置文件可能以明文显示（即任何人都可以读取的未加密文本），并且配置文件中的默认设置可能并没有考虑到安全因素。在三年来开展的所有测试中，平均有5%的漏洞与应用配置错误有关。

6. **应用隐私失败。**应用隐私失败与信息泄露/披露相关，是指应用在设计、实施或修补方面存在缺陷，导致未授权的用户可以访问数据或内容，发生隐私泄露。组织机构在构建应用时，应考虑到一些隐私问题，例如：

   - 我们的开发人员是否接受过Web应用隐私方面的培训？
   - 是否编制了安全编码指南？
   - 我们的软件（包括服务器、数据库和库代码）能否及时更新？
   - 是否定期安装补丁？
   - 为确保软件中使用的第三方和开源代码是安全且最新的，我们采取了哪些措施？
   - 个人数据在完成指定任务后是否会被删除？

   在三年来开展的所有测试中，平均有5%的漏洞与隐私问题有关。

7. **身份验证不足。**以前称为“身份验证失败”，属于OWASP“A07:2021—身份验证和认证失败”类别，现在涵盖与身份验证失败相关的漏洞，例如我们列表中的第4类和第7类漏洞。在三年来开展的所有测试中，平均有5%的漏洞与身份验证不足有关。

   身份验证和授权不足是指因应用或系统没有正确验证用户身份或未能实施适当的访问控制而导致的安全漏洞。未经授权的用户可能会访问敏感信息或执行他们无权执行的操作，从而引发数据泄露和数据丢失等安全问题。

8. **内容欺骗/内容注入。**内容欺骗也称为内容注入，是一种针对用户的攻击，可能是由于Web应用中存在漏洞，无法正确处理用户提供的数据而造成的。

   当Web应用将攻击者提供的内容呈现给毫无戒心的用户时，就会发生这种情况，其发生的形式通常是可信域名下修改过的页面。OWASP指出，这类攻击经常被误解为常见的Web漏洞，几乎或根本没有业务影响。但实际上，内容欺骗攻击频繁出现在各种欺诈中，攻击者冒充合法实体诱骗用户提供登录凭证。

许多应用都有一些开发者功能，这些功能如果在部署时没有关闭，就会非常危险，比如调试和QA功能。

更令人担忧的是，内容欺骗有可能发起危险的攻击，包括代码注入和跨站脚本。三年来开展的所有测试中，平均有4%的漏洞与内容欺骗或内容注入有关。

9. **指纹敏感性。**指纹（探测Web应用以获取信息）可以给攻击者提供有价值的信息，如操作系统类型、操作系统版本、SNMP信息、域名、网络区域和VPN连接点等。三年来开展的所有测试中，平均有3%的漏洞与指纹有关。

测试中发现的许多具体的指纹类安全问题都属于微风险、低风险或中风险问题。也就是说，攻击者不能直接利用这些漏洞来访问系统或敏感数据。然而，揭示这些漏洞并不是一件徒劳无功的事情，因为即使是低风险的漏洞，也可能被用来促进攻击。

例如，在三分之一的渗透测试和近一半的DAST扫描中，持续发现了与指纹相关的一个安全问题，即冗长的服务器标识（图5）。虽然这是一个中风险漏洞，但却能够给攻击者发动攻击提供足够的信息，如服务器名称、类型和版本号等。//右图下面的文字没有翻译

在2022年测试发现的所有高风险漏洞中，有19%与跨站脚本攻击有关。

	测试发现的高危漏洞的百分比	2021年排名	2020年排名
1. 跨站脚本	19%	2	1
2. 授权不足	16%	1	2
3. 身份验证不足	6%	3	3
4. 应用配置错误	4%	6	9
5. 传输层保护不足	4%	4	5
6. 信息披露/信息泄露	3%	7	6
7. 服务器配置错误	2%	9	8
8. SQL注入	2%	8	10
9. 意外数据泄漏	1%	*	*
10. 程序验证不足	1%	*	*

* 不在十大漏洞范围内

图3. 2022年测试发现的十大高危漏洞（不包括重新测试）

	测试发现的超高危漏洞的百分比	2021年排名	2020年排名

1. SQL注入	30%	1	1
2. 授权不足	9%	2	2
3. 跨站脚本	7%	9	9
4. 身份验证不足	7%	3	3
5. 信息披露/信息泄露	6%	4	4
6. 程序验证不足	5%	8	5
7. OS命令	3%	7	7
8. 服务器配置错误	2%	*	*
9. 应用程序配置错误	2%	6	9
10. SQL注入	1%	*	*

* 不在十大漏洞范围内

图4. 2022年测试发现的十大超高危漏洞(不包括重新测试)

SQL命令注入是测试中发现的排名第一的超高危漏洞。

10. 遭遇客户端/跨站脚本攻击。跨站脚本 (XSS) 攻击是一类客户端代码注入攻击,是在新思科技三年测试中排名第一或第二的高危漏洞。攻击者试图通过在合法的网页或Web应用中注入恶意代码而在受害者的Web浏览器中执行恶意脚本。在2022年测试发现的所有高风险漏洞中,有19%与跨站脚本攻击有关(见图3)。

实施或加强诸如内容安全策略 (CSP) 之类的保护措施可以提供额外的安全层,帮助检测和缓解某些类型的攻击,包括跨站脚本和数据注入攻击(测试中发现的头号超高危漏洞,见图4)。攻击者可以使用不安全的用户数据传输(如cookie和表单),将命令注入到Web服务器上的系统Shell中,然后利用特权来破坏服务器。

许多组织都认为,CSP不安全或缺失只是低风险漏洞。然而,跨站脚本、点击劫持和跨站泄漏等攻击的频繁发生,凸显出应用CSP的必要性,尤其是可以防止恶意脚本在客户端执行的CSP — 作为第二层防线来抵御各种类型的攻击,包括跨站脚本和数据注入攻击。

脆弱的第三方库的危险

如图6所示，在新思科技开展的2022年测试中，25%的测试发现了使用易受攻击的第三方库，这与OWASP Top 10中的“A06:2021—易受攻击或过时的组件”漏洞有关。OWASP指出，无论是在客户端还是服务器端，您都必须清楚所有组件的版本，包括软件中使用的第三方和开源组件，否则，您的软件很可能会受到攻击。

	占2022年测试目标总数的百分比	2021年排名	2020年排名
1. 弱SSL/TLS配置	70%	1	4
2. 缺失Content-Security-Policy标头	43%	2	1
3. 冗长的服务器标识	37%	3	2
4. 可缓存HTTPS内容	34%	5	5
5. 未实施HTTP严格传输安全 (HSTS) 机制	34%	4	3
6. 不安全的Content-Security-Policy标头	31%	6	8
7. 弱密码策略	28%	7	7
8. 未屏蔽非公开信息数据	25%	*	*
9. 使用了易受攻击的第三方库	25%	*	*
10. 会话超时时间过长	24%	*	*

* 不在十大漏洞范围内

图5. 2022年测试发现的十大安全问题

开源代码可以显著提升软件构建的速度和效率，这已成为现代软件的重要组成部分，深受开发者欢迎。作为经过验证的代码，开源代码便于开发者访问和使用，无需浪费时间和资源做重复工作。

然而，新思科技的年度《开源安全与风险分析报告》，显示，开源代码并非没有风险。事实上，2023年的报告显示，开源安全风险已经达到了前所未有的水平，并且大多数企业并不十分清楚自己的代码组成。

报告指出，高风险的开源漏洞在过去五年增速惊人（仅在零售和电子商务领域就增长了557%）。最重要的是，令人不安的是缺乏安全补丁和项目依赖维护（91%的项目包含了过时的开源组件）。

大多数企业都不十分清楚自己的代码组成。

从BSIMM报告中可以看出，“为软件创建物料清单”这项安全活动呈现增长趋势，证明了各组织机构都在朝着SBOM进行转变。BSIMM报告还显示，由于针对脆弱的开源项目的攻击越来越猖獗，导致“识别开源代码”和“控制开源风险”这两项活动显著增加。

由于许多公司都在同时使用数百个应用或软件系统，每个应用或软件系统本身又可能依赖成百上千个不同的第三方和开源组件，因此，他们迫切需要借助准确、最新的SBOM来有效跟踪这些组件。

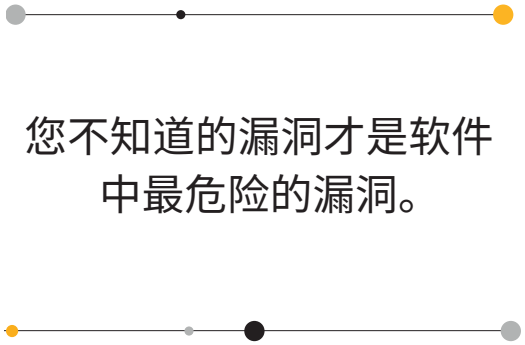
启发和建议

- **实施多层安全方法。**仅依赖单一的安全测试解决方案，如静态应用安全测试 (SAST)，已经不足以满足安全需求。组织机构应实施多层安全方法，通过SAST来识别编码缺陷，通过DAST来检查运行中的应用，通过软件组成分析 (SCA) 来识别由第三方组件引入的漏洞，通过渗透测试来发现错误配置等问题以及其他测试可能遗漏的漏洞。

  新思科技《2023年全球 DevSecOps现状调查》报告显示，44%的受访者将外部渗透测试视为安全测试的重要组成部分，也是对其他测试的有效补充。外部渗透测试的好处在于，它能从客观的第三方角度评估您的安全状况，并能准确模拟其他测试可能无法发现的潜在威胁和漏洞，以防它们被攻击者利用。

- **自动和手动安全测试相结合。**自动测试能够保证一致性和可扩展性，并节省时间和成本，而手动测试则能够增加一层洞察力和适应性，这对识别复杂和微妙的安全问题至关重要。例如，DAST作为黑盒测试（即不了解应用的内部结构）就需要开发者和安全专家验证和分析所发现的问题。

- **重视补丁管理。**保持警惕，及时修补漏洞，尤其是对第三方和开源组件。建立清晰的流程来识别、评估和快速应用补丁，有效防止漏洞利用。



- **实施严格的访问控制。**对应用和网络实施严格的访问控制策略。遵循最小权限原则，确保用户只拥有执行任务所需的最低访问权限。定期检查和更新应用的访问权限，防止未授权的访问。
- **将SBOM生成纳入软件开发生命周期。**您不知道的漏洞才是软件中最危险的漏洞。通过使用完整的清单来识别组件，您可以更好地了解安全状况，并且及时有效地应对漏洞问题。
- **确定是否需要补充安全测试。**您的安全团队是否具备足够的应用安全技能和资源来测试安全缺陷？是否有时间按照监管机构和客户的要求来测试软件？
- **选择能够随时随地提供专业安全测试服务的供应商。**新思科技安全测试服务部专业技能过硬、工具丰富、纪律严明，能够随时随地为您提供经济高效的支持，对任何应用开展任何深度的分析。

新思科技提供全方位的测试服务，包括渗透测试、动态应用安全测试、静态应用安全测试、移动应用安全测试、网络渗透测试、红队测试、物联网和嵌入式软件测试、以及胖客户端测试。

我们的按需测试服务可以帮助贵组织的安全测试团队提升实力。
立即联系新思科技，预约免费咨询。

SYNOPSYS®

新思科技与众不同

新思科技提供的集成解决方案，可以改变您构建和交付软件的方式，在应对业务风险的同时加速创新。与新思科技同行，您的开发人员可以在编写代码的时候快速兼顾安全。您的开发和DevSecOps团队可以在不影响速度的情况下在开发管道中自动进行安全测试。您的安全团队可以主动管理风险，并将补救工作聚焦在对贵组织最重要的事情上。我们无与伦比的专业知识可以帮助您规划和执行所需的安全计划。只有新思科技能够满足您构建可信软件的一切需求。

如需了解更多信息，请访问：www.synopsys.com/software.