自动化移动应用安全测试作为 2022 年的优先事项

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	A 2022 priority: Automated mobile application security testing		
原文作者	瑞安·劳埃德（Ryan Lloyd）	**原文发布日期**	2022 年 1 月 24 日
作者简介	瑞安·劳埃德是 Guardsquare 公司的首席产品官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2022/01/24/mobile-application-security-testing/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	在 2022 年，移动应用安全测试会成为应用开发团队的职责，他们将使用自动化的工具来实现这一点。这样一来，安全测试就会具有成本效益和可管理性，开发团队可以定期收到有关应用安全性的反馈。此外，自动化测试工具使开发人员能够按照他们想要（或需要）的频率进行测试，为高效、成功的外部评估或渗透测试做好准备。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

自动化移动应用安全测试作为 2022 年的优先事项

瑞安·劳埃德

2022 年 1 月 24 日

在过去的两年中，移动设备的数量激增，移动应用市场也随之飙升。预计到 2023 年，移动应用的收入将超过 9350 亿美元。

不幸的是，具有增长潜力的领域往往会引起攻击者的注意，他们试图利用移动应用的漏洞来获取经济利益。因此，移动应用安全已成为各行业（尤其是拥有高价值知识产权[IP]或敏感数据的企业）关注的重要领域。

企业应在整个应用程序开发过程中实施安全措施，并在应用程序发布后继续对其进行监控，这是确保移动应用安全和业务安全的根本方法。

如今，移动应用面临很多安全威胁，这些威胁会对企业产生严重的影响。因此，企业应将移动应用安全测试作为其 2022 年的优先事项。

移动应用的安全威胁

移动应用面临独特的威胁。

我们以 MATE（终端人）攻击向量为例。攻击者可以在其本地设备上加载移动应用，然后使用专门的工具和资源来检查应用，并对其进行逆向工程。这样一来，他们就可以了解该应用的运行方式了。

此外，移动应用还面临不安全的数据存储、错误配置和不安全的通信等威胁，详情可参考 OWASP TOP 10 移动风险列表。如果企业未部署多层保护措施，其应用程序就很容易遭到攻击。

尽管这些威胁的严重程度和复杂程度各不相同，但它们造成的结果通常是相同的：数据泄露、IP 被盗、收入损失，以及失去客户信任等。因此，企业应将移动应用安全作为其应用开发周期各个阶段的重点。

移动应用安全测试

如果能够对移动应用进行频繁的安全测试并获得真实的反馈，移动应用开发人员就可以更好地识别和缓解移动应用威胁和漏洞。

移动应用安全测试是指，扫描移动应用程序以识别可能影响这些应用的潜在安全问题。尽管应用扫描的具体需求（无论是出于合规性还是响应安全事件）会有所不同，但其目标都是有效地强化应用程序并降低风险。

企业可以使用两种方法进行安全测试：静态分析和动态分析。这两者都非常有效。当它们结合使用时，更是可以大大提高移动应用程序的安全性。

渗透测试并不总是有效

传统上，移动团队倾向于将渗透测试作为移动应用测试的首选方法。渗透测试是一种有效的安全评估方法，可以发现代码强化和防篡改保护的缺失问题。但是在快节奏的移动应用开发领域，渗透测试并不总是有效的。

渗透测试既昂贵又缓慢，通常要在软件开发过程之后（有时是几个月后）才能给出结果。因此，企业需要做出艰难的决定：按时发布应用程序还是先处理已识别的风险？

如果风险很严重，开发团队需要放弃一切来进行修复，这会对新功能的开发和发布带来严重的影响。因此，安全团队和移动应用开发团队不怎么喜欢使用渗透测试。

因此，识别和选择专为移动应用设计，为开发人员构建的安全测试工具非常重要。对开发人员友好的移动安全工具能够提供可操作的反馈，从而更好地协调开发和安全团队。

自动化应用安全测试受到青睐

如今，企业的任务是“不断创新以满足客户快速变化的需求”，他们不能冒险使用不安全的应用程序。

我们预计，在 2022 年，移动应用安全测试会成为应用开发团队的职责，他们将使用自动化的工具来实现这一点。这样一来，安全测试就会具有成本效益和可管理性，开发团队可以定期收到有关应用安全性的反馈。此外，自动化测试工具使开发人员能够按照他们想要（或需要）的频率进行测试，为高效、成功的外部评估或渗透测试做好准备。

移动应用已逐渐成为用户与企业交互的主要方式。在 2022 年，企业应将应用安全测试作为优先事项，采取主动的措施来防止数据泄露、IP 盗窃、收入损失和声誉损失。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com