Fine penetration tests for fine websites

2017 年 6 月沃通 CA 安全审计报告总结

由沃通根据英文报告翻译，仅供参考，以英文版为准

一、测试总结

该总结报告记录了对沃通证书系统的广泛渗透测试和源代码审查的结果。该项目由德国 Cure53 于 2017 年 6 月完成，共发现了 20 个与安全有关的问题。Cure53 八位高级渗透测试工程师组成的团队用了 40 天/人的时间完成了该任务。

有关该安全审计的基本原理及范围，应强调的是安全测试是针对由沃通团队开发的新的证书系统代码和新的基础设施。对代码的彻底检修并且建立一个新的基础设施的原因是由于浏览器厂商对沃通证书系统的不信任。浏览器厂商提出的主要问题反映了证书签发系统的安全性未达到相关标准。为了使产品能重新获得主要浏览器厂家的信任，需完成一系列的步骤和程序，而此次 Cure53 安全测试是推动重获信任的必要措施之一。

本次安全测试范围所涵盖的具体项目包括 4 个主要系统：登录系统、Buy 系统、证书管理系统(CMS)和相关基础设施。测试方式主要利用 VPN 远程访问测试，此方法容许 Cure53 测试工程师对测试范围内的系统的相关部分进行全权限访问。测试的时间选择经过谨慎的挑选，这是因为测试版本就是即将切换到真实系统的版本。这意味着被 Cure53 测试的系统将成为核心真实系统。为了全面细致的审查，沃通提供了所有系统的源代码压缩包供 Cure53 下载，包括 Buy 网站、CMS 和一些后台系统(如 CA 代理、CT 代理、验证系统和 OCSP 系统)。

测试过程中一旦发现问题，则通过 S/MIME 加密邮件的方式进行实时报告。这样沃通就可以马上解决问题并且对可能产生的任何疑惑与测试团队讨论。在整个测试过程中，对于我们发现的所有问题，沃通开发团队收到后马上修改代码及时修复问题，这样就可以让 Cure53 团队可以马上进行重新测试并核实问题是否已经解决，确保了在最终安全审计报告出台之前就都修复了所有问题。这反映了沃通开发团队的令人钦佩的敬业精神，许多问题都是快速找到问题点，并修改源代码和修改服务器配置等。例如，处理上传的文件的问题有一个很大的漏洞，但都已经得到了正确的解决。

二、测试范围和测试参数

- WoSign CMS/Buy 系统、相关服务器和基础设施(约 9 万 1 千行代码)
- WoSign CA 代理系统、相关服务器和基础设施(约 8 千行代码)
- WoSign CT 代理系统、相关服务器和基础设施(约 3 千行代码)
- WoSign 验证系统(约 1 万 1 千行代码)
- WoSign OCSP 系统(约 2 万 7 千行代码)

//沃通备注：CA 系统没有纳入审计，因为我们使用的是开源 EJBCA 系统。

三、审计结论

沃通证书系统的安全是第一重要要务，2017 年 6 月的渗透测试和源代码审计由 Cure53 团队的八名高级测试工程师费时 40 天/人完成。引入外部审计师对源代码和相关基础设施进行了全面检查，是沃通下一步发展的重要战略举措。我们认为：沃通一定是投入了很多开发资源和内部测试资源才达到了目前的系统安全水平，必须强调的是，**新系统的安全是值得肯定的**。

虽然在测试过程中发现了 22 个问题，考虑到测试范围的广度和深度(代码量大)，这些问题并不算多。并且必须强调的是，大多数问题并不构成实际的安全威胁。

沃通平台通过安全测试采用了一些新技术来增强加固而受益，我们鼓励沃通团队学习并熟悉这些安全技术包括 CSP 标头、SameSite Cookie、缓存控制头和其他基于浏览器的技术来使得应用程序更加安全。

回到测试流程，值得称赞的是，沃通团队能快速和适当的对发现的问题做出相应处理。更具体地说，沃通团队在大多数情况下都能快速成功地修复所有被报告的问题，只有几个小问题的修复需要多次交流才完成，这使得 Cure53 团队能及时完成修复验证工作。由于与远在中国的服务器的 VPN 连接比较慢，使得某些针对基础设施的安全测试难以执行，若不提及这些则报告缺乏完整性。尽管如此，必须重复强调的是，沃通团队已经尽其所能，为测试团队提供了尽可能高效率和高产出的测试体验。

总之，系统安全性显然是沃通必须优先考虑的事情。Cure53 团队确信沃通已经向创建安全的 Web 应用程序和后端系统迈出了正确的第一步，而按照这个正确的方向走下去是必须坚持的。这就要求系统开发人员能将系统安全的理解提升到一个非常重要的高度，而不是一种喊口号声称的安全，需要真正采用各种安全防御机制。

更重要的是，应该强调的，新的安全技术在没有被正确地集成到日常的开发过程中是不会带来利益的。当然，某些方面还有待进一步优化，但是总的安全基准还是达到了一个 CA 系统的应有的安全水平。

沃通开发团队现在可以开始下一个阶段的针对所有 Web 功能和后台进程的更高级别的安全加固工作。 作为一个 CA，将安全性和数据私密性置于项目的最根本的目标对于沃通来说是至关重要的。

Cure53 要感谢沃通 Richard Wang 和他的团队在这次任务开始之前和期间的出色的项目协调、支持和协助。