Penetration Testing Software with Acunetix

Acunetix 渗透测试软件

The modern cybersecurity threat landscape continuously changing. One of the most popular ways for organizations to keep up with the onslaught of security vulnerabilities is through Penetration Testing (pen testing).

Penetration testing, also known as “Pen-Testing” or “Ethical hacking” is a process in which a skilled penetration tester conducts a series of tests using penetration testing software which is then likely combined into a report and sent to development teams to fix vulnerabilities found by a pen tester.

现代网络安全威胁形势不断变化。渗透测试（PEN 测试）是组织容易受到安全漏洞攻击的最普遍方法之一。

渗透测试，也称为笔测试”或“黑客道德 ”（“Pen-Testing”or“Ethical hacking”）。一个熟练的渗透测试人员使用渗透测试软件进行一系列测试的渗透的过程，合并成一个报告，发送给开发团队，然后由笔测试仪进行修复。

While manual security testing provides organizations with thorough point in time security assessment, unfortunately, manual penetration tests are time consuming, expensive, only provide point-in-time security assessment (not continuous), and does not provide a scaleable approach when organizations have several hundreds or even thousands of web applications to test.

虽然手动安全测试能为组织提供全面彻底的时间点安全性评估，但遗憾的是，手动渗透测试耗时、成本高昂，仅提供时间点安全性评估（不连续），并且在组织有数百甚至数千个网站应用程序要测试时，不提供可扩展的方法。

Fortunately, automated penetration testing tools like Acunetix web vulnerability scanner allow organizations to scan anywhere from a handful to thousands of web applications quickly, cost effectively and, most importantly, continuously. Pen Testers are able to leverage the pros of automation for their web penetration testing freeing up their time for more important manual tests.

幸运的是，自动化渗透测试工具（如 Acunitix 网站漏洞扫描程序）可以让组织快速、经济高效地扫描从一到数千个网站应用程序，最重要的是，自动化渗透测试工具具有持续扫描的功能。Pen 测试人员能够利用自动化的优点进行“网站渗透测试”，从而腾出时间进行更重要的手动测试。

Industry leading technology coverage

行业领先的技术覆盖范围

With Acunetix, security teams can setup scheduled automated scans, to test for thousands of web application vulnerabilities (including SQL Injection, XSS) as well as misconfigurations.

While most penetration testing tools supports legacy technologies, Acunetix takes technology support to the next level with the best-of-breed JavaScript support. Unlike most software, Acunetix has full support for modern Single Page Applications (SPAs) and can understand and fully test applications which rely on JavaScript frameworks like React, Angular, Ember and Vue. This means that unlike most penetration testing software, Acunetix can scan everything from legacy web applications developed on traditional stacks, as well as modern web apps taking advantage of all the latest and greatest technologies.

通过使用 Acunetix，安全团队可以设置有计划性的自动扫描，来测试数千个网站应用程序漏洞（包括 SQL 注入、XSS）以及错误配置。

虽然大多数渗透测试工具提供了传统技术的支持，但 Acunetix 通过最佳的 JavaScript 支持将技术支持提升到了一个新的层面。与大多数软件不同，Acunetix 完全支持现代单页应用程序（SPAs），能够读懂并全方面测试依赖于 JavaScript 框架的应用程序如 React、Angular、Ember 和 Vue 等。这意味着，与大多数渗透测试软件不同的是，Acunetix 不仅可以扫描传统技术基础上开发的传统网站应用程序，还可以扫描运用了所有最新和最好的技术的现代网站应用程序。

Speed without sacrificing flexibility

速度不影响灵活性

Additionally, unlike many other web and network penetration software, Acunetix is lightning fast. With a re-engineered core, and a highly optimized crawler, every inch of Acunetix is tuned for speed and efficiency, allowing it to scan hundreds of thousands of pages without breaking a sweat.

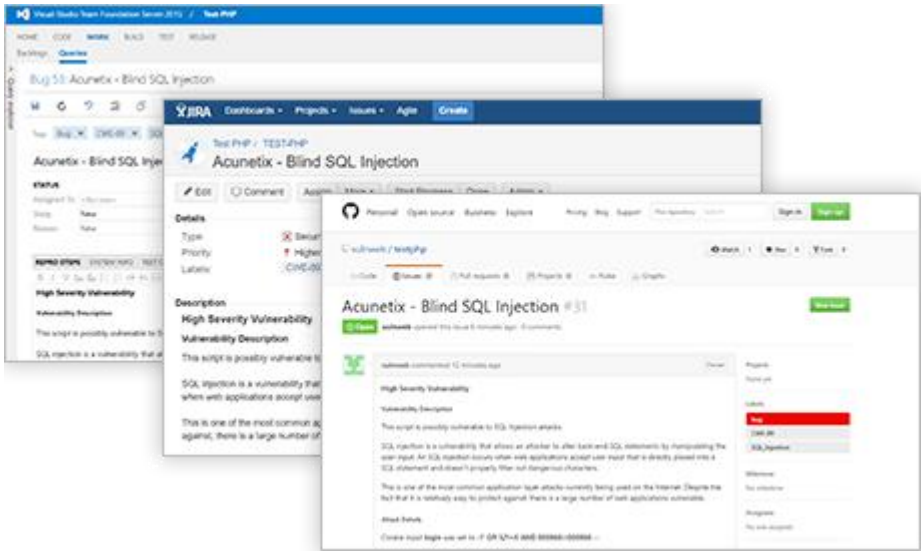
此外，与许多其他网站和网络渗透软件不同，Acunetix 的速度极快。Acunetix 拥有重新设计的核心以及高度优化的爬虫，Acunetix 一切服务于速度和效率，使得它扫描几十万页面而不会负载。

What's more, Acunetix can save the progress of a scan mid way, pause it, and resume it later on from where it left off entirely automatically. This is a crucial for time boxed pen testing or when scanning enormous web applications with time restrictions.

另外，Acunetix 还可以在扫描过程中保存扫描进度，暂停扫描，稍后从停止的位置恢复自动扫描。这对于具有时间限制的 Pen 测试，或具有时间限制的大型网站应用程序扫描，都是至关重要。

Integrations with third-party penetration testing software make it easy to move between automatic and manual testing for advanced users who need it. Moreover, vulnerabilities Acunetix discovers may be exported to a wide variety of industry leading Web Application Firewalls (WAFs) such as Imperva SecureSphere and F5 Big-IP ASM.

与第三方渗透测试软件的集成使得 Acunetix 可以轻松按照高级客户的需求进行自动测试和手动测试之间的调整。除此之外，Acunetix 发现的漏洞可能会被导出到各种行业领先的网站应用程序防火墙（WAFs）中，例如数据库安全网关（Imperva SecureSphere）和 F5 BIG-IP ASM 应用安全管理器产品。



Easy reporting and Issue Tracker integration 轻松报告和问题跟踪器集成

Another issue that Acunetix solves over other web application security software is the ability to instantly generate a wide variety of technical and regulatory and compliance reports such as PCI DSS, HIPAA, OWASP Top 10 and many others. Additionally, Acunetix allows users to export discovered vulnerabilities to Issue Trackers such as:

Acunetix 解决的另一个问题是，能够立即生成各种技术，法规和合规性报告，如 PCI DSS，HIPAA，OWASP Top 10 等等。此外，Acunetix 允许用户将已发现的漏洞导出到问题跟踪器，例如：

- Atlassian JIRA,
- GitHub
- Microsoft Team Foundation Server (TFS).

亚特兰西 JIRA
Github 公司
微软 Team Foundation Server（TFS）。