Web Application Security with Acunetix

Acunetix 的网站应用程序的安全性

Unlike traditional thick-client applications, which are locked away behind corporate firewalls, web applications are typically accessible from outside corporate networks and potentially open to dangers such as SQL Injection and application-layer denial of service attacks. This makes web application security and web service security a different beast altogether. Moreover, in case of attacks such as Cross-site Scripting, client-side JavaScript source code is right there in the browser for any malicious user to tinker with. With so many threats to sensitive data, it's no surprise many organizations are seeking tools to help them secure their software development life cycle.

与被锁定在企业防火墙之外的传统的胖客户端应用程序不同，Acunetix 的网站应用程序通常可以从企业外部网络访问，可以发现诸如 SQLi 和应用层拒绝服务攻击等危险。这就使得网站应用程序安全性和网站服务安全性截然不同。此外，在发生跨站点脚本攻击时，客户端的 Java 脚本（javascript）源代码就在浏览器中，任何恶意用户都可以随意修改。面对如此多的对敏感数据的威胁，许多组织都在情理之中地寻找能够帮助他们确保软件开发生命周期安全的工具。

Defend Against Known Application Vulnerabilities

防范已知的程序漏洞

The first step to kick starting your web application security program is to look for known application vulnerabilities. Keeping known vulnerabilities out of your code base prevents attackers from easily exploiting them and running malicious code. Attacks such as SQL injection and Cross-site Scripting are usually much easier to fix than to find them, so educating developers about best practices, defining a security policy and enforcing development security standards are all important approaches when defending against web security vulnerabilities.

启动 Acunetix 网站应用程序安全程序的第一步是查找已知的应用程序漏洞。将已知的漏洞移除出代码库可以防止攻击者轻易地利用漏洞并运行恶意代码。结构查询语言注入(SQLi)和跨站点脚本等攻击的修复通常比查找容易，因此向开发人员介绍最佳实践、定义安全策略和实施开发安全标准都是防御网站安全漏洞的重要方法。

Acunetix is a software product for web application security testing which helps you quickly and easily identify known vulnerabilities, as well as vulnerabilities in any website or web application, including sites built with hard-to-scan HTML5 and JavaScript Single Page Applications (SPAs). With Acunetix you can:

Acunetix 是一款用于网站应用程序安全测试的软件产品，可帮助您快速轻松地识别已知的漏洞，以及任何网站或网站应用程序中的漏洞，包括使用难以扫描的 HTML5 和 Java 脚本（JavaScript）单页应用程序（SPA）构建的网站。

使用 Acuteix，您可以：

- Discover in excess of more than 4,500 security vulnerabilities
- Detect SQL Injection and Cross-site Scripting and all of their variants
- Automatically scan all website files with custom form authentication or other custom access controls and session management
- 发现超过 4500 个安全漏洞
- 检测结构查询语言注入(SQLi)和跨站点脚本及其所有变体
- 通过定制的表单认证或其他定制的访问控制和会话管理进行自动扫描，扫描所有网站文件

Defend Your Entire Attack Surface 保护您的整个可攻击范围

Web applications have a large attack surface and security threats can come from anywhere, including third-party code. Vulnerabilities can exist in several layers of an application, be it in the frontend, the backend or even within web server configurations.

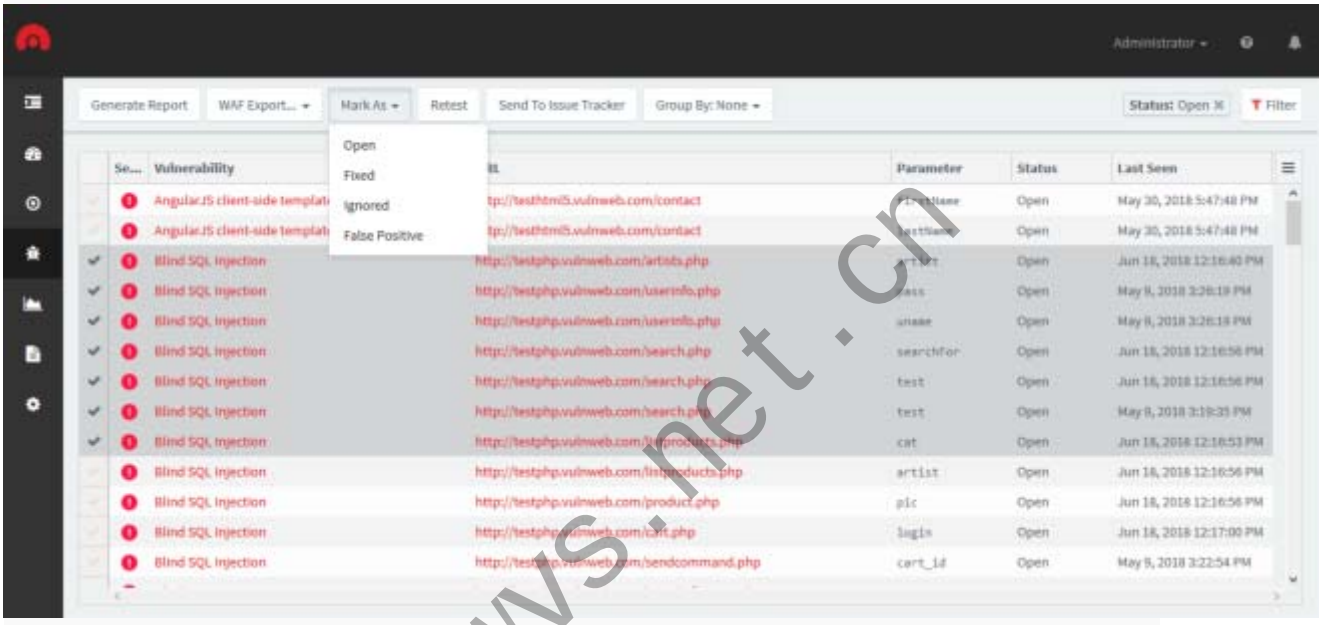
网站应用程序具有很大的攻击范围，安全威胁可能来自任何地方，包括第三方代码。漏洞可能存在于应用程序的多个层中，无论是在前端，还是后端，甚至可能是在网站服务器配置中。

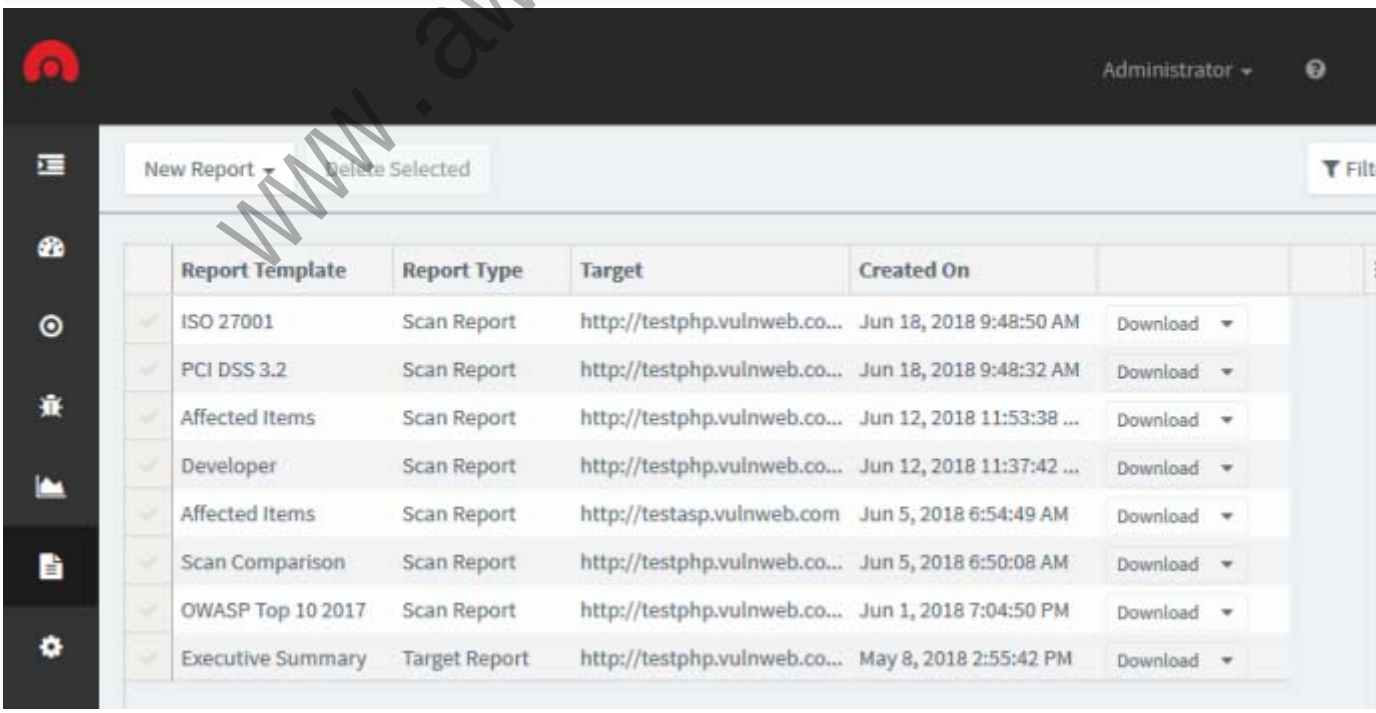
With built-in support for exporting discovered vulnerabilities to the most popular security tools such as web application firewalls, you can take automated testing even further. Virtually patching the vulnerabilities in production will give you enough breathing room to fully and carefully undergo remediation.

将发现的漏洞导出到最常用的安全工具（如 Web 应用程序防火墙）的内置支持之下，您可以进一步进行自动化测试。实际上，修补生产中的漏洞将为您提供足够的运行空间，以便全面、仔细地进行修复。

Additionally, Acunetix can find security issues beyond the typical black-box scanning approach thanks to its AcuSensor gray-box scanning technology. With AcuSensor, Acunetix can automatically examine Java, ASP.NET and PHP server-side code that is being executed. This allows Acunetix to pinpoint the exact line of code where vulnerabilities lie, as well as dramatically reduce an already low false positive rate.

此外，Acunetix 凭借其 AcuSensor 灰盒扫描技术，可以发现典型的黑盒扫描之外的安全问题。使用 AcuSensor，Acunetix 可以自动检查正在执行的 Java、ASP.NET 和 PHP 服务器端代码。这使得 Acuteix 能够精确定位漏洞所在的代码行，并显著降低已经很低的假阳性率。





Get Actionable Insights into Your Web Application Vulnerabilities

深入了解网站应用程序漏洞

By using tools to help you simulate web application attacks, you'll be in a position to find and fix security vulnerabilities before an attacker has the chance to exploit them. A vulnerability scanner like Acunetix also recommends actions that you can take to correct the vulnerabilities it identifies, as well as the ability to retest fixes.

通过使用工具帮助您模拟网站应用程序攻击，您将能够在攻击者有可乘之机之前找到并修复安全漏洞。漏洞扫描器（如 Acunetix）还能为您提供建议和措施来纠正其识别的漏洞，以及重新测试修复程序的能力。

Acunetix also allows you to produce dozens of technical and compliance reports with actionable information web application developers, security professionals, and regulators can use to assess and reduce security risks:

Acunetix 还可以让您在可操作的信息网站应用程序开发人员、安全专业人员和监管机构的协助下制作数十份技术和合规报告，以评估和降低安全风险：

- Out-of-the-box vulnerability management tools including historic trends, and prioritization
- Integration with popular Issue Trackers such as Atlassian JIRA, GitHub and Microsoft Team Foundation Server
- Easy to generate compliance reports for PCI DSS, OWASP Top 10, ISO 27001 and HIPAA
- 现成的漏洞管理工具，包括历史趋势和优先等级
- 与大众的跟踪器集成，如亚特兰西斯 JIRA、GitHub 和微软 Team 基金会服务器
- 易于生成数据安全标准(PCI DSS)、OWASP 前 10、ISO 27001 标准和医疗保险可携性和责任法案（HIPAA）的合规报告