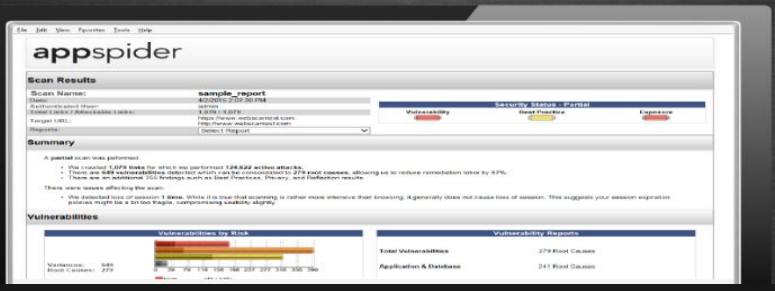
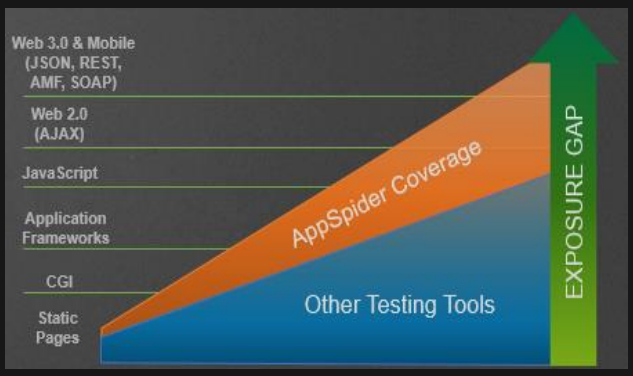
AppSpide

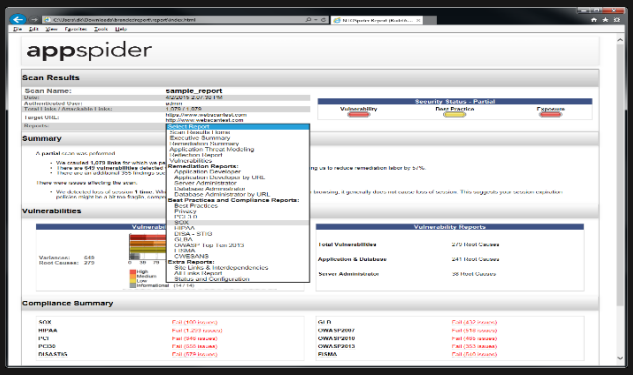
现代环境下的应用评估利器





最大化的扫描深度和广度

- 利用通用转换器消除扫描范围的盲点
- 智能化模拟实际攻击
- 持续监控您的应用
- 加强验证以进行深入评估

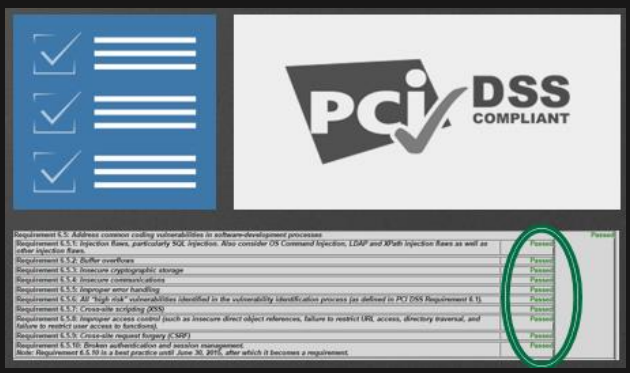


交互式报告，风险可视化

- 利用交互式可操作型报告执行更便捷的分析
- 针对漏洞进行风险分析与排序
- 深入分析漏洞，一键重现攻击
- 提高开发人员沟通效率，减少修复漏洞成本

可与应用防火墙形成联动

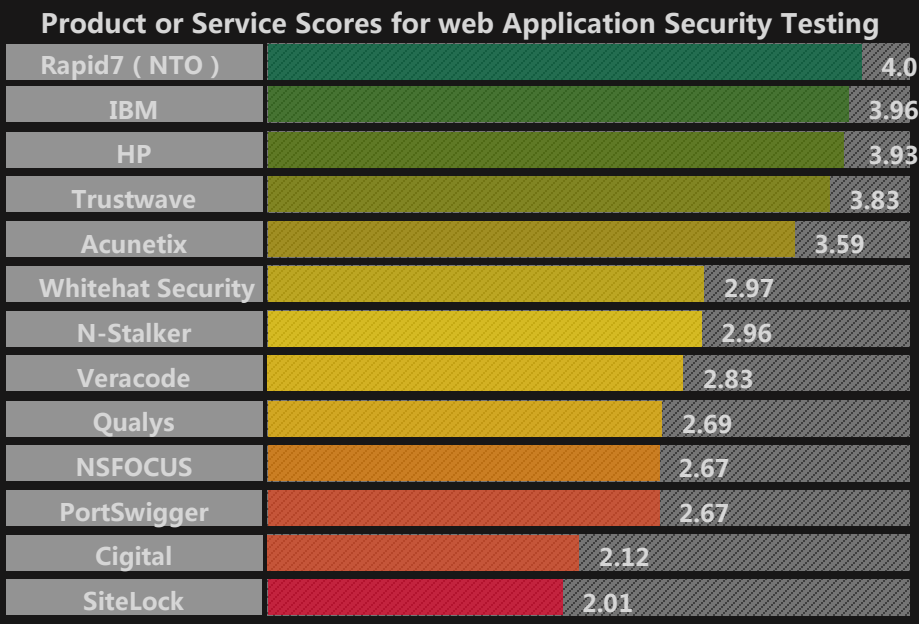
- 管理和控制应用安全程序
- 自动定位虚拟补丁，与WAF及IPS完美联动
- 将评估整合到开发流程，降低修复成本



帮助企业更好地达到合规性要求

始终追随行业最佳实践，并符合相关法律、法规的要求绝非易事。AppSpider可帮助您的团队快速发现合规问题以及与如下熟知的最佳时间不符的情况，包括：**PCI**、**FISMA**、**SOX**、**HIPMA**、**GLBA**、**OWASP**等。

gartner魔力象限排名第一

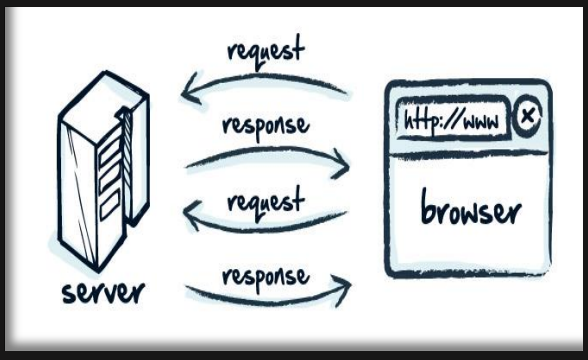


[AppSpider] 正是企业所寻求的简单易用且功能全面的 DAST 技术，它在价格上极具竞争力，在众多 DAST 技术提供商之外，为您提供一个更佳选择。

----Gartner，Critical Capabilities Report，2014， 2014 年 9 月 22 日，Neil MacDonald， Joseph Feiman

虽然当今的恶意攻击者追求的目标多种多样，但是他们首选的攻击方式却如出一辙，即攻击各个公司为了服务客户所部署的数以百万计的定制网络、移动应用和云应用。

AppSpider 利用多种现代技术对这些应用漏洞进行动态评估，并提供加速修复以及监控应用变化的工具，确保应用安全可靠并且正常运行。



Why AppSpider？

覆盖范围广	AppSpider简单地扫描更多。 AppSpider能够测试当今现代网络中部署的所有高级格式，包括AJAX，JSON和RESTful API。
准确度更高	AppSpider广泛的覆盖面与复杂、专有的自动化技术相结合，使AppSpider提供较少的误报和漏报，并最终获得更高的准确度。
创新和自动化	在大多数情况下，AppSpider提供真正的点和射击功能 - 没有训练，没有手持，没有崩溃。
交互式报表及与提高开发者协作	AppSpider的“一键式漏洞验证”可帮助开发人员加快修复速度，并提供交互式HTML报告（PDF和XML可用性），以便于使用和有效性。
广泛的结合	AppSpider与持续集成，QA自动化，错误跟踪和WAF的集成使开发人员能够快速方便地解决现有工具集中的安全缺陷。

AppSpider企业安全价值

了解薄弱环节

AppSpider 能够自动检测多种应用（从相对简单的应用到最复杂的应用）中的漏洞，包括一些独特的功能，帮助项目团队在从开发到生产的整个软件开发生命周期内，实现更多安全测试程序的自动执行。扫描程序的扫描范围是保证精准性的首要因素。扫描程序最初都采用抓取和攻击架构，但是抓取方式并不适用于网络服务及其他动态技术。 AppSpider 不但能抓取传统的名称/值配对格式（如 HTML），同时还配备通用转换器，能对当今网络和移动应用（ AJAX、 GWT、REST、 JSON 等）使用的新技术进行解析。

提高安全定位

为了提高应用程序的整体安全性，您需要拥有对应用安全程序的高层次视野，从而帮助您掌握全局。AppSpider 可在企业网络应用安全程序的各个方面实现集中控制、自动化和互操作性，包括连续扫描配置、用户许可、计划和监控。另外， AppSpider 还提供有助于利益相关者之间紧密合作的趋势和分析数据，从而确保不断改善应用程序的安全性。

修复漏洞的时间十分关键。 AppSpider 采用创新的自动化规则生成技术，其防御功能有助于信息安全专家随时对网络应用漏洞进行修复，整个过程只需几分钟而无需几天或几周的时间。无需为网络应用防火墙（WAF）或入侵防御系统（IPS）建立自定义规则，也无需提供源代码补丁，我们的软件即可帮助您快速识别问题的根源并在代码中进行修复。

- 管理和控制应用安全程序
- 自动定位虚拟补丁
- 符合合规要求
- 整合到您的开发工作流程中

符合合规要求

始终追随行业最佳实践，并符合相关法律、法规的要求绝非易事。 AppSpider 可帮助您的团队快速发现合规问题以及与如下熟知的最佳实践不符的情况，包括： PCI、 FISMA、 SOX、 HIPAA、GLBA、OWASP 等。

优先处理紧急事项

AppSpider 包含交互式的可操作型报告，该报告对漏洞危险性进行了从高到低的优先级排序，并简化了修复措施，使用户能够快速获取并分析最重要的数据。只需单击一下，您就可以深入了解漏洞，及时获取详细信息并重现攻击。

从 PDF 报告的众多页面中筛选出漏洞信息需要花费很长时间。 AppSpider 提供的交互式可操作型报告以网页形式显示，结构清晰，并包含可供深入分析的链接。由于报告的结果已按照攻击类型（ XSS、 XSS 等）进行分类和合并，因此进行分析十分简单，只需单击即可深入了解各个漏洞并获取详细信息。 AppSpider 的精密报告减少了修复时间并简化了开发人员之间的沟通方式。

- 利用交互式报告执行更深入的分析
- 快速重现网络攻击
- 对应用进行分类，更易于提出报告

强大的支持

当前支持的 WAF 产品：

Imperva SecureSphere　　F5 ASM
Barracuda WAF　　ModSecurity
Citrix NetScaler　　DenyAll rWeb
Fortinet*

支持的 IPS 产品：

Cisco SourceFire　　CheckPoint*
Fortinet*　　Nitro Security
其他基于SNORT技术的IPS

与 WAF/IPS 集成带来的好处：

为 WAF 和 IPS 生成规则和过滤器
提高 WAF 和 IPS 的效果
从 AppSpider 中导入规则可以节省时间提高效率

闭环漏洞管理解决方案

1.深度集成的卓越漏洞验证漏洞扫描器可以评估您网络系统中安装的软件系统和其可能存在的漏洞，但并不能确定这些漏 洞是否会给贵组织造成风险。这不仅仅是效率不高的问题,而且可能会在IT安全部门花大量时间修复那些并不会造成真正风险的安全问题的同时使您的组织处于容易被攻击的危险之中。

漏洞验证可以通过确认一个漏洞在您组织中的特定IT环境下是否可被渗透来帮助您识别致命的 风险。通过专注于存在已知的公开的可渗透方式(甚至是并不具有丰富经验的攻击者都可以使用的简单方法)的漏洞，您可以轻松的进行行动优先级划分，从而可以快速处理那些真正会带来风险的安全问题。

目前世界上只有Rapid7通过Metasploit提供闭环漏洞验证， 世界上最被广泛使用的渗透测试软件和企业版的漏洞管理系统Nexpose就是我们的漏洞管理解决方案。这两者的深度集成使漏洞管理的工作流变的简单， 并给用户带来更高效的风险优先级划分， 使您可以有更多的时间来定位真正的威胁。

2. 不象其它的解决方案需要的手工的XML导入导出， 漏洞扫描结果通过API自动的从Nexpose导入到Metasploit。 通过Metasploit的简单漏洞验证向导可以安全地在您的网络中模拟攻击， 从而识别哪些漏洞是可以真正被攻击的。 验证结果自动的推回到Nexpose进行管理和生成报表。 使用Nexpose轻松地对被证明可被攻击的IT资产进行分组和进行补救优先级划分， 自动地把那些不可被攻击的漏洞设置成为例外。

3.AppSpider提供针对最新WEB应用的安全评估，并支持分布式部署，可以大大提高大型分布式WEB应用的评估效率。 并且扫描结果可以导入到Nexpose时行管理。

企业攻防演练解决方案

战略合作伙伴

关于 Rapid7

Rapid7 的安全解决方案可提供您需要的可见性和洞察力， 以帮助您制定明智的决策、制定可靠的行动计划和监控进展。这些解决方案独辟蹊径地将环境威胁分析与跨用户、资产、服务和网络（ 无论是否基于实体、移动或云） 的快速综合数据收集相结合， 简化了您的风险管理步骤。 Rapid7 简单且创新的解决方案已在超过 65 个国家或地区的2,500 多家企业和政府机构中使用， 公司的免费产品每年还在其开放资源安全社区内通过二十多万会员下载超过一百万次。Rapid7 被《公司杂志》 (Inc. Magazine) 认为是发展最迅速的安全公司之一，还获得了《波士顿环球报》 (Boston Globe) 的“最佳工作场所”称号。公司的产品得到了Gartner® 和《 SC 杂志》的最高评价。关于Rapid7 的更多信息， 请访问http://www.rapid7.com。