绿盟 WEB 应用漏洞扫描系统

产品白皮书

目录

一. 概述

近年来，Web 应用系统随着互联网技术的不断发展呈现出爆炸式的增长。据中国互联网络信息中心(CNNIC)发布的《第 30 次中国互联网络发展状况统计报告》①显示，截至 2012 年 6 月底，中国网民数量达到 5.38 亿，网站域名总数为 873 万个，而据瑞典互联网市场研究公司 Royal Pingdom 在 2012 年初的一份研究报告指出，全球网民总量已经达到 22.7 亿②人，也就是说每 3 个人里面就有 1 个网民。同一时期，互联网监测机构 NetCraft 在 2012 年 1 月的报告指出，全球共有各类网站 5.8 亿③个，也就是说每 11 个人就拥有一个网站。

Web 应用系统已广泛应用于各个公共领域（政治、经济、文化、国防等）以及个人领域（娱乐、咨询、交流、沟通等），其中蕴含了越来越多的经济价值，而 Web 应用系统在被广泛应用的同时，因其互联、开放等特性，更容易遭受黑客的攻击。从 2005 年到 2006 年跳跃式增加至今，每年发现的 Web 漏洞数量一直居高不下，这也是导致 Web 应用频繁遭受攻击的重要原因。从最新的 IBM 2012 年风险报告可看到，2012 年上半年发现的漏洞已达到 4,400 个，预计今年全年漏洞数将超过 2010 年创下历史新高（逼近 9,000 个），而其中 Web 漏洞占了 47%之多。

① http://download.sina.com.cn/2012/PDF/30.pdf
② http://www.cnbeta.com/articles/183656.htm
③ http://software.it168.com/a2012/0104/1297/000001297648.shtml

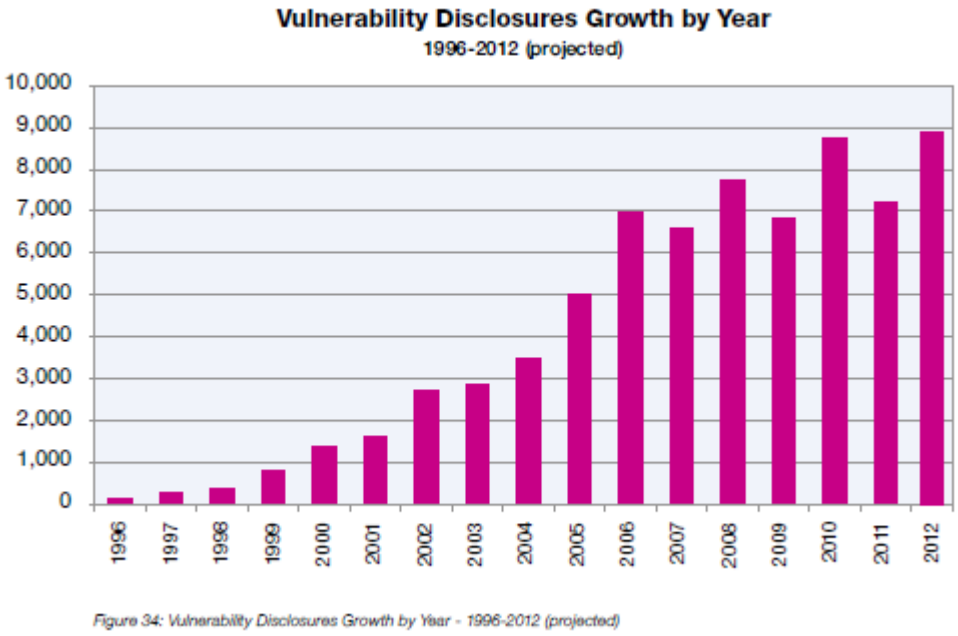

Figure 34: Vulnerability Disclosures Growth by Year - 1996-2012 (projected)

图 1.1　1996-2012 年上半年漏洞数量增长趋势图[①]

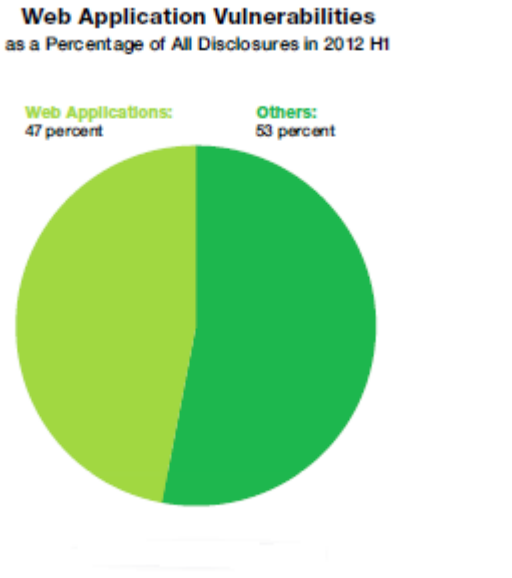

Figure 35: Web Application Vulnerabilities as a Percentage of All Disclosures in 2012 H1

图 1.2　2012 年上半年 Web 应用漏洞百分比[①]

因 Web 漏洞引起的安全事件极大困扰着网站维护部门，影响了用户体验，甚至对信息网络等核心业务造成严重的破坏，导致了机构门户的经济受损和公信力的下降：

[①] http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03014usen/WGL03014USEN.PDF

1) 网站数据库被拖库——导致注册用户身份信息、银行卡信息、密码等被盗取；

2) 网站被挂马、被篡改——导致网站信誉受损、网站资源被滥用，以及给访问该网站的用户带来被入侵甚至成为僵尸主机的风险。

从 CNCERT 发布的中国互联网网络安全报告可看到，至 11 月的第 3 周，2012 年被篡改的网站数一直居高不下已达 31,663 个，其中政府网站高达 3,069 个，而被植入网站后门的境内网站也有 22,854 个，其中包括政府网站 2,762 个①。

如何应对频频发生的 Web 应用安全事件，给网站维护部门及其安全监管部门带来新的挑战。

二. Web 应用安全面临的挑战

■ “源代码”带来的挑战

Web 应用系统通常是供应商针对不同业务目标进行定制化开发，并以“源代码”的形式交付，依靠各种应用环境进行动态解析以实现特定功能。因此，对于 Web 漏洞而言，供应商往往也很难提供类似于 Windows 漏洞补丁的通用补丁，这给 Web 应用系统的维护带来了新的挑战——不能仅依靠被动的“打补丁”方式，而需要采用更主动的方式——使用专业 Web 漏洞扫描器进行评估，提前发现 Web 应用系统中隐藏的漏洞，根据评估工具给出详尽的漏洞描述和修补方案，指导维护人员进行安全加固，防患于未然。

■ 繁重的检查任务带来的挑战

安全检查任务往往时间紧、任务重，尤其现在的网站规模日趋庞大，单个站点动辄上千甚至上万个页面，而检查时往往需要面对的还不止一个的网站，同时，随着 Web 新技术的不断涌现，网站的构成也越来越复杂，因此，如何快速、稳定的完成扫描任务，成为亟待解决的问题。

① http://www.cert.org.cn/publish/main/upload/File/2011-4%281%29.pdf

三. 绿盟 WEB 应用漏洞扫描系统

若能够主动的发现网站的风险隐患，并及时采取修补措施，则可以降低风险、减少损失。绿盟科技针对该需求，推出了绿盟 WEB 应用漏洞扫描系统（NSFOCUS Web Vulnerability Scanning System，简称：NSFOCUS WVSS），该系统可自动获取网站包含的所有资源，并全面模拟网站访问的各种行为，比如按钮点击、鼠标移动、表单复杂填充等，通过内建的“安全模型”检测 Web 应用系统潜在的各种漏洞，同时为用户构建了从急到缓的修补流程，能够有效解决 Web 应用维护面临的挑战，也能较好满足安全检查工作中所需要的高效性和准确性。

◆ 采用高效稳定的扫描引擎，基于嵌入式系统平台，通过内核级优化，实现了对大规模网站的快速、稳定的扫描。

◆ 全面的 Web 应用安全检测，检测范围覆盖了各企事业单位的门户网站、电子政务的互动平台和政务信息公开服务系统等，覆盖了论坛、内容管理系统（CMS）和电子商务应用系统等平台。

◆ 采用多视角风险评估模型，同时提供了安全评估和风险自评两种模式，既可以周期性的进行全面安全检测，还可以结合实际业务系统进行深入的安全评估。

◆ 专家级统计分析报告，融入漏洞修补流程和漏洞精确定位技术，既可以展示各站点的整体风险等级和对比风险情况，还可以直观、便捷的查看每个漏洞的详细信息及修补建议，很好的帮助用户分步骤的修补漏洞以及验证修补效果。

3.1 产品体系结构

NSFOCUS WVSS 是基于 Web 的管理方式，用户使用浏览器通过 SSL 加密通道和系统进行交互，方便用户管理。NSFOCUS WVSS 采用模块化设计，整个系统可分为：UI、web 应用服务、扫描引擎、状态引擎、调度引擎、升级系统、证书系统、报表系统和基础系统。

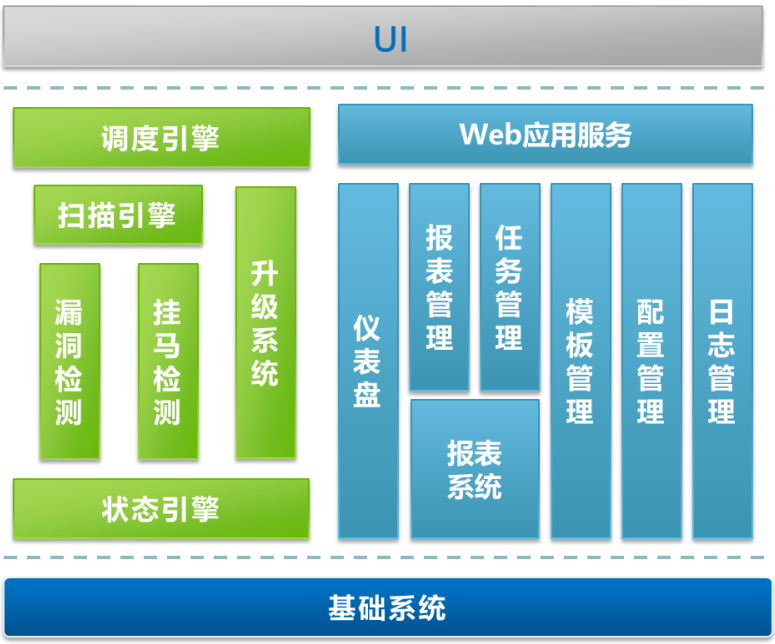

图 3.1 NSFOCUS WVSS 系统架构

主要模块说明：

a) 调度引擎模块

该模块采用内置的算法实时监控系统任务的运行情况，并依据结果对各任务进行优化和调整，以达到系统资源的充分利用和任务的高效运行。

b) 扫描引擎模块

该模块根据配置的策略，对被扫描站点进行全面准确的 web 漏洞和网页挂马检测。

c) Web 应用模块

该模块通过友好的 UI 设计为用户提供了便捷的操作，同时还负责对扫描结果的数据分析和呈现。

d) 基础系统

该模块采用嵌入式操作系统平台，通过内核级优化，为系统的高性能、高稳定性和安全性提供了基础。

3.2 产品特性

3.2.1 高效稳定的扫描引擎

NSFOCUS WVSS 基于绿盟科技多年技术积累自主研发的统一基础平台，采用嵌入式系统，通过内核级修改实现了多任务、多线程、数据存储、数据访问等多方面的优化，使系统相比使用第三方平台产品拥有更好的性能、稳定性和安全性，实现了对包括运营商等各种大规模网站的快速、稳定扫描。

3.2.2 全面 Web 应用安全检测

NSFOCUS WVSS 可对包括门户网站、电子商务、网上营业厅等各种 Web 应用系统进行安全检测，同时其全面性还体现在检测技术上。NSFOCUS WVSS 检测的漏洞覆盖了 OWASP Top10 和 WASC 分类，系统支持挂马检测，支持 IPv6、Web2.0、AJAX、各种脚本语言、PHP、ASP、.NET 和 Java 等环境，支持 Flash 攻击检测、复杂字符编码、会话令牌管理、多种认证方式（Basic、NTLM、Cookie、SSL 等），支持代理扫描，HTTPS 扫描等。同时，通过绿盟科技规则组对最新 Web 漏洞的持续跟踪和分析，进一步保障了产品检测能力的及时性和全面性。

3.2.3 多视角风险评估

NSFOCUS WVSS 在绿盟科技多年的安全评估服务基础上，构建了不同级别的风险评估模型，保证了风险评估结果的有效性；同时结合用户实际使用场景，围绕“评估任务”形成了细粒度的管理模式，不仅可对任务进行实时跟踪、定时周期启动、复制、断点续扫等，还可以对每一个任务的设置进行详细的配置，包括爬虫的优先顺序、限制文件个数、目录深度、Flash 检测开关、页面消重策略、表单填充和黑白名单等，以及 Web 访问、Web 认证、Web 检测等保障 Web 安全检测全面性的各种配置。这些功能支撑了系统既可以周期性的对 Web 应用进行安全检测，还可以结合实际业务系统进行更深入的安全评估，同时通过对历史任务的跟踪和对比分析实现了对风险趋势的评估，也实现了漏洞修补效果的跟踪和验证。

3.2.4 专家级统计分析报告

NSFOCUS WVSS 从汇总、单站点、趋势、危险级别、关注程度等多个方面直观展示了被检查站点的风险情况，同时提供了针对不同角色的、不同内容和不同格式的报表。在报表生成过程中不仅提供了便捷的配置流程，还对报表生成进度进行实时跟踪和展示，同时报表生成后可自动发送到指定的邮箱或者 FTP 服务器。用户可根据网站的不同危险级别，和精确定位到“站点资源树”上的每一个漏洞信息，进行有步骤的漏洞修补，再结合周期评估任务，可直观展现出网站维护工作的效果，为网站安全状况的评定和未来站点的安全建设提供了强有力的决策支持。

3.2.5 支持多路扫描的快速检测机制

NSFOCUS WVSS 支持的多路扫描功能不仅使得 WVSS 设备具有负载均衡的特性，同时还可满足生产和应用环境不同的检测要求。尤其对于门户网站，网站的频繁更新使得需要在上线检查和实际应用的检查之间来回切换，以确保两种环境的一致性，而使用多路扫描技术，既可以只针对上线前的更新内容进行安全检查，还可以同时对已上线的 Web 应用进行周期的风险评估，这种方式既提高了检测的性能，又简便了使用流程，也为跨部门使用该系统提供了方便。

3.2.6 大容量多任务多用户管理模式

安全检查是一项持续的任务，众多检查任务的统一管理、历史数据的追溯和复制，以及不同用户的分权使用，均是工作中必不可少的。NSFOCUS WVSS 能较好满足这些需求，可支持多用户和多任务，同时数据采用加密压缩的方式，既保证了数据的安全性，又加大了存储容量。

3.3 典型应用方式

NSFOCUS WVSS 适用于各种网站，部署灵活简单，只需要对目标站点“网络可达”即可进行 Web 漏洞、挂马等检测。同时系统支持多路扫描技术，可对不同应用环境的网站进行统一检测，获得汇总、对比、负载均衡等由单路扫描无法获得的特性。

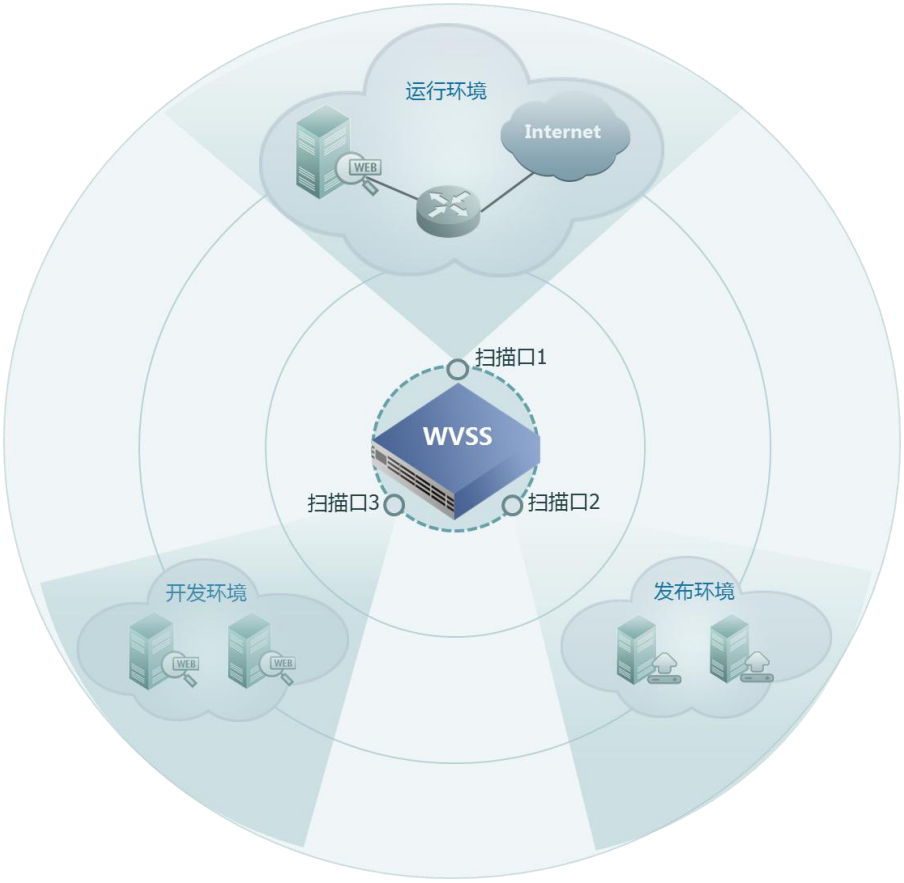

图 3.2 NSFOCUS WVSS 典型应用

四. 结语

随着互联网的高速发展，越来越多的行业通过互联网为公众提供信息以及数字服务，而随着应用的深入，越来越多的经济价值融入其中。在这个生态链中，安全保障业已成为重要的一环，如何保障数据的安全、如何保障业务安全、如何保障可用性安全均成为新的挑战，同时每一个网站也担负着保护访问者安全的责任。

安全评估是保障网站安全的重要手段，通过扫描评估发现目标网站是否存在挂马，以及是否存在能被黑客利用的各种漏洞，进而促进网站漏洞修补工作，这是从根本上解决安全问题的有效途径。

NSFOCUS WVSS 以其便捷的配置、全面快速的检测能力和多环境适应性成为 Web 应用安全评估的利器。广泛适用于政府、等级保护测评机构、公安、运营商、金融、能源、教育、医疗、互联网等行业，适应于针对 Web 应用的安全检查和风险自评。