01

Web应用漏洞扫描工具

Web Application Vulnerability Tool

Secuguard WSE WebSCAN

获得国情院国际共同评价标准CC(Common Criteria)认证

WSE 的介绍

Web Application Security Explorer I Web Application Vulnerability Tool

随着因特网的日益普及和网络的扩张，黑客事故也随之增加。作为管理员必须周期性扫描系统漏洞并采取相应的措施，以便防御各种外部入侵。但这需要系统管理员对于安全的专业知识和新型黑客技术的长时间研究和努力。

Secuguard WSE(Web Application Security Explorer)可以对网络环境中暴露的多种蠕虫、DOS、黑客攻击、web设置漏洞进行诊断并提供相应的解决方法、以此预防黑客攻击和计算机犯罪。

WSE必要性

Web Application Security Explorer I Web Application Vulnerability Tool

Web应用脆弱的理由

- 由于各种服务都集中到web上，所以风险相对提高
- 很容易暴露在蠕虫及DOS攻击状态中
- 可迂回或突破当前安全系统(防火墙、入侵检测等)的攻击的存在
- Web应用的编程失误及设置错误
- 通过新漏洞的攻击方法持续公开
- 通过清除接入痕迹反复入侵

Web应用漏洞扫描器

Secuguard WSE

WebSCAN

Web应用扫描必要性

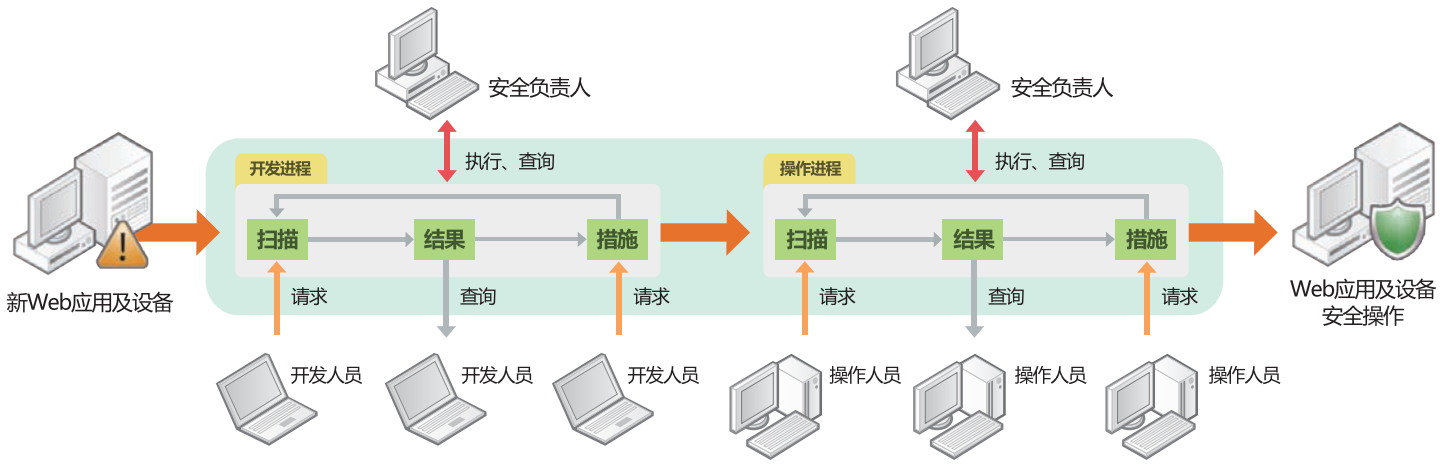
- 通过web应用漏洞进行的黑客攻击的增加
- 有必要搭建维持最佳安全状态的安全的web站点
- Web应用需要持续的开发、修改、完善等的过程
- 往往需要多个web服务器而web服务器中运行很多URL及应用程序
- 程序编码及设置失误引起的漏洞
- 要应对各种强化了的合规条款及审计

Web应用的脆弱现状

- 随着因特网的普及很多企业及公共机关的业务都以web应用的形式开发并提供服务。但据Gartner Group的统计全部攻击的75%的都属于web应用攻击。而Sim Group通报300个以上的web站点中有97%存在web应用程序漏洞。

WSE及扫描管理进程

Web Application Security Explorer I Web Application Vulnerability Tool



www.nilesoft.co.kr | 信息安全的大众化

首尔特别市九老区Digital 路 32街 30, Kolon Digital Tower Bilant 1期 1004号
TEL : +82-2-783-0961 FAX : +82-2-783-0963 E-mail : webmaster@nilesoft.co.kr

System, Security and NileSOFT
NileSOFT

ITSCC
获得国情院国际共同评价标准CC认证

GOOD Softward
获得软件品质认证

Web安全 第一步 用WSE 掃描

System, Security and NileSOFT | 信息安全的大众化

WSE 详细特点

Web Application Security Explorer I Web Application Vulnerability Tool

- 类似Windows资源管理器形状的熟悉的用户界面及基于Install Shield的简单的安装方式
- 包括XSS, SQL Injection等的多种模拟攻击进行检测
- 提供用于浏览漏洞结果及信息分析的专门的web浏览器
- 提供多种用于web测试 (模拟攻击) 及结果确认的测试工具
- 检测包括身份证号在内的个人信息及特定用语
- 基于多线程的快速而强大的同步多重的安全漏洞扫描
- 基于CVE (Common Vulnerabilities and Exposures) 的扫描模块及漏洞信息
- 支持韩国国家情报院TOP 8，OWASP TOP 10，SANS TOP 20，WASC TOP 24漏洞
- 对控制台/Agent之间的通信及结果资料的加密处理
- 对web服务器IP，主机名称、服务器应用信息的自动识别
- 使用内存队列和表的强大的web URL收集引擎
- 基于强大的URL 收集功能的网页结构分析
- 拥有多种搜索功能的基于用户的漏洞扫描策略的设置功能
- 通过电子邮件自动发送扫描结果等方便的预约 (预约设置) 功能
- 基于NVIS的迅速而便利的在线自动更新
- 漏洞列表报表，危险级别漏洞分布报表等多种报表
- 可以转换成DOC, RTF, PDF, XLS, XML等多种文件形式
- 与综合漏洞管理系统 (UVM) 互联

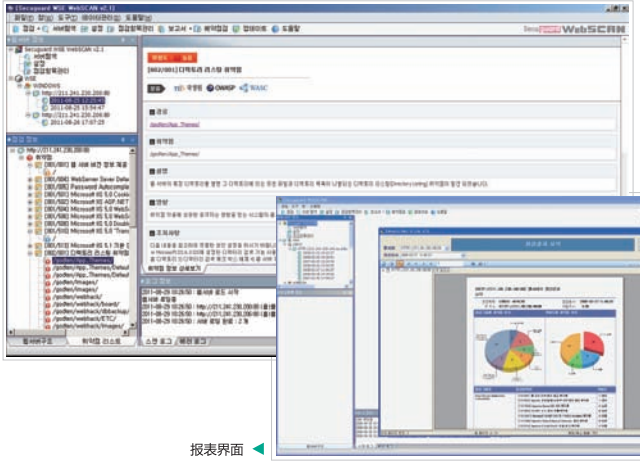
WSE 的主要功能

Web Application Security Explorer I Web Application Vulnerability Tool

主要功能	功能简要说明	主要功能	功能简要说明
服务器浏览	• Web服务器的IP，主机名的自动识别 • Web服务器的操作系统及服务器应用的自动识别	扫描项目	• Cross Site Scripting, SQL Injection, CRLF Injection, Code Execution, Directory Traversal, File Inclusion, Input Validation, Authentication 等 • JavaScript, AJAX, Flash File 分析等 • 输入登录信息 (账号及密码) • 提取web页或附件中包含的信用卡信息、身份证号、电子邮件地址 • 检测是否包含特定用语 (性, 谩骂, 诽谤, 暴力等)
页面分析	• 掌握扫描对象的web结构及URL自动收集功能 • 从JavaScript, AJAX, Flash中提取URL • 基于用户的URL过滤功能 • 环境设置 (Proxy 与否, URI 扫描深度, URI计数限制等) • 树状结构显示的URL收集器 (URL信息, HTML头信息, URL浏览器)	扫描策略	• 支持韩国国家情报院TOP 8, OWASP 10, SANS TOP 20, WASC TOP 24漏洞
执行扫描	• 多重扫描：对扫描对象同时扫描的方式 • 扫描历史记录：提供用户的扫描历史记录 • 基于多线程的快速而强大的同步多重安全漏洞的扫描 • 在一个控制台画面中对多个web服务器的漏洞同时进行扫描 • 同时扫描可以缩短扫描时间 • 可布置多重控制台 • 各个服务器管理员的扫描权限分离功能 • 通过一个Agent扫描多个web服务器的漏洞 • 提供针对组、全部、各个操作系统的扫描功能 • 针对发现的安全漏洞提供危险级别、内容、影响及弥补措施等内容	模拟攻击工具	• HTTP 登录Brute Force 工具 • HTTP接入测试工具 • HTTP 编码 / 解码工具 • HTTP Fuzzer 之外的多种工具
		预约设置	• 在指定事件执行扫描并把扫描结果通过电子邮件通报
		报表	• 漏洞列表报表，危险级别漏洞分布报表等多种报表 • 通过Crystal Report提供多种图表和表格形式的报表 • 提供DOC, RTF, PDF, XLS, XML等多种文件转换形式
		更新	• 接入更新服务器对新增漏洞扫描模块进行升级 • 在用于指定的时间自动更新扫描模块 • 针对不能接入更新服务器的用户提供离线更新功能 • 在封闭的网络中通过搭建更新服务器提供在线更新

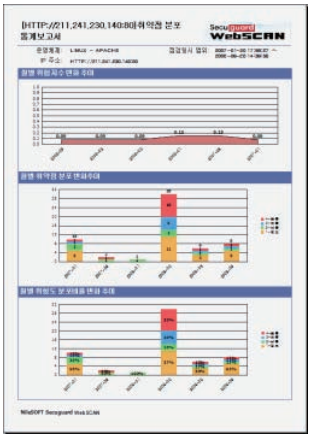
WSE 执行画面

Web Application Security Explorer I Web Application Vulnerability Tool



▶ Web服务器漏洞信息

报表界面 ◀



▲ 每个机关的统计报表

▲ 各个危险级别、漏洞项目的详细报表

www.nilesoft.co.kr | 信息安全的大众化

首尔特别市九老区Digital 路 32街 30, Kolon Digital Tower Bilant 1期 1004号
TEL : +82-2-783-0961 FAX : +82-2-783-0963 E-mail : webmaster@nilesoft.co.kr

System, Security and NileSOFT
NileSOFT