| 密级 | 公开 |
| --- | --- |

# Websaber 网站应用安全评估系统

# 技术白皮书

北京知道创宇信息技术有限公司

2011-5-21

# 版本说明

| 修订人 | 修订内容 | 修订时间 | 版本号 | 审阅人 |
|---|---|---|---|---|
| 周冉 | 创建文档 | 2011.07.28 | V1.0 | |
| 潘少华 | 修订 | 2011.08.20 | V1.0 | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# 文档信息

| 文档名称 | | 文档编号 | |
|---|---|---|---|
| 文档版本号 | | 保密级别 | |
| 扩散范围 | | | |
| 扩散批准人 | | | |

# 文档说明

此文档作为北京知道创宇信息技术有限公司的正式文档编写规范，用于公司对外发布的各种系统说明书、系统白皮书、技术手册等文档。

# 版权声明

# 目录

# 1. 网站安全发展趋势

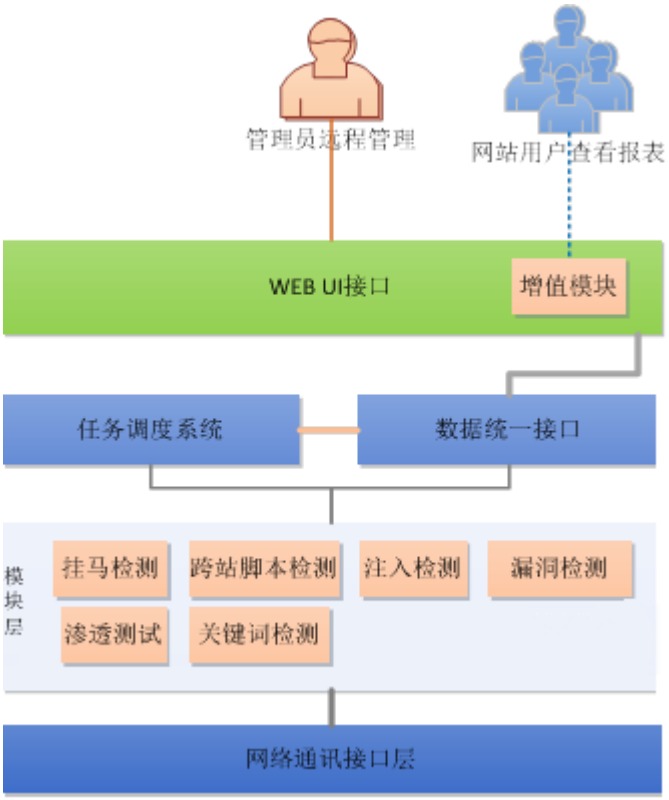
从互联网兴起至今，利用漏洞攻击的网络安全事件不断，并且呈日趋严重的态势。每年全球因漏洞导致的经济损失巨大并且在逐年增加，漏洞已经成为危害互联网的罪魁祸首之一，也成了万众瞩目的焦点。人们也在一次次的蠕虫爆发之后在不断地寻求着漏洞的解决之道，不断尝试将由漏洞带来的风险降到最低，虽然也取得了一定成效，但是利用漏洞的攻击也在逐渐表现为多种不同的危害形式并且出现了新的攻击趋势。

随着互联网的发展及经济利益的驱动，黑客正逐渐将攻击重点转在 web 应用服务器上，如利用网站漏洞获取网站数据，通过网页挂马等，由此危害了服务器安全及客户端安全。

而同时，网站在内容安全上新出现的一些趋势，已成为当今网络安全课题的重点关注内容。

# 2. 产品体系结构

## 2.1. 产品体系结构




# 3. 需求配置列表

## 3.1. 需求配置列表

| 硬件名称 | 硬件参数 |
|---|---|
| 操作系统 | Windows2000/20003/2008、WindowsXP、Windows7 |
| CPU | 主频大于 2G |
| 硬盘 | 使用空间大于 5G |
| 内存 | 大于 512M |

# 4. 主要功能列表

| 检测功能名称 | 描述 |
|---|---|
| 网站安全监测 | 提供对网站的 SQL 注入漏洞、XSS 跨站脚本漏洞、Web 漏洞 |

| | | |
|---|---|---|
| | | 和后门等进行检测。 |
| 挂马监测 | | 智能爬虫、静态解析技术和“云特征库”结合，对网站进行挂马检测，准确率>95%。 |
| 页面关键字监测 | | 采用先进的中文分词及中文语义识别技术，对网站页面中的内容进行敏感、低俗关键字检测。 |
| 其他信息 | 调试信息检测 | 包括：<br>1. Web 开发框架的调试信息，如 Django 等框架<br>2. .NET 调试信息<br>3. Java 调试信息<br>4. PHP, |
| | 出错信息检测 | 包括：<br>1. 数据库出错信息识别<br>2. Web 容器错误信息识别<br>3. 常见 Web 开发框架出错信息识别<br>4. 常见服务端语言出错信息识别 |
| | 目录浏览检测 | 覆盖 IIS, Apache, Tomcat, Jboss 等 Web 容器的目录浏览识别 |
| | 敏感文件检测 | 包括：<br>1. 备份文件<br>2. 数据库文件<br>3. Phpinfo<br>4. 服务器探针<br>5. Webshell<br>6. svn 等版本控制器的隐藏文件<br>7. vim 等编辑器留下的中间临时交换文件 |
| | 源码泄露检测 | 覆盖 PHP, .NET, ASP, JSP 等服务端语言的源码泄露识别 |
| | phpinfo 文件 | 识别 PHP 的环境探针文件 |
| | 内网地址检测 | 智能识别内网地址泄露，如：192.168.123.10 这样的内网地址 |
| | Email 地址检测 | 识别网页中的 Email 地址信息 |
| | 隐藏表单项检测 | 识别网页中隐藏的表单项 |

| | |
|---|---|
| SQL 注入验证工具 | |

# 5. 产品功能亮点

## 5.1. 漏洞检测功能

漏洞检测模块采用插件体系结构，能够快速的通过插件扩展来实现漏洞检测功能的升级。

目前系统支持以下检测模块：

### 5.1.1. 基本信息安全分析

本系统对网站基本信息进行扫描评估，判断目标网站使用的应用系统是否存在已公开的安全漏洞，是否有调试信息泄露等安全隐患等。

### 5.1.2. SQL 注入漏洞检测

本系统对多个字段进行注入测试，除了对传统的 get 参数字段进行检测，还对 COOKIE，REFERER 等 HTTP 头部字段进行检测。

同时，通过使用网页动态参数判定、网页结构分析等技术，有效过滤非动态参数，大大提高了检测效率，降低了误报的可能性。

本系统采用多种业内领先的识别技术进行漏洞判定，如关键字匹配、返回信息智能识别等技术。

### 5.1.3. XSS 跨站脚本漏洞检测

本系统通过使用网页动态参数判定、网页结构分析等技术，有效过滤非动态参数，大大提高了检测效率，降低了误报的可能性。

本系统采用多种业内领先的识别技术进行漏洞判定，如关键字匹配、返回信息智能识别等技术。

针对 XSS 跨站漏洞的特殊性和检测环境的复杂性，本系统储备了大量的 XSS 检测代码，从而保证了漏洞检出的成功率。

### 5.1.4. 其他信息检测功能

该功能用于检测网站的信息泄露、不恰当配置等导致的潜在安全风险。

其他信息检测功能列表

| 功能 | 具体内容 |
| --- | --- |
| 调试信息检测 | 包括：<br>5. Web 开发框架的调试信息，如 Django 等框架<br>6. .NET 调试信息<br>7. Java 调试信息<br>8. PHP, |
| 出错信息检测 | 包括：<br>5. 数据库出错信息识别<br>6. Web 容器错误信息识别<br>7. 常见 Web 开发框架出错信息识别<br>8. 常见服务端语言出错信息识别 |
| 目录浏览检测 | 覆盖 IIS, Apache, Tomcat, Jboss 等 Web 容器的目录浏览识别 |
| 敏感文件检测 | 包括：<br>8. 备份文件<br>9. 数据库文件<br>10. Phpinfo<br>11. 服务器探针<br>12. Webshell<br>13. svn 等版本控制器的隐藏文件<br>14. vim 等编辑器留下的中间临时交换文件 |
| 源码泄露检测 | 覆盖 PHP, .NET, ASP, JSP 等服务端语言的源码泄露识别 |
| phpinfo 文件 | 识别 PHP 的环境探针文件 |
| 内网地址检测 | 智能识别内网地址泄露，如：192.168.123.10 这样的内网地址 |
| Email 地址检测 | 识别网页中的 Email 地址信息 |
| 隐藏表单项检测 | 识别网页中隐藏的表单项 |

## 5.2. 网站挂马检测功能

挂马攻击是指攻击者在已经获得控制权的网站的网页中嵌入恶意代码 （通常是通过 IFrame、Script 引用来实现），当用户访问该网页时， 嵌入的恶意代码利用浏览器本身的漏洞、第三方 ActiveX 漏洞或者其它插件（如 Flash、PDF 插件等）漏洞， 在用户不知情的情况下下载并执行恶意木马。

网站被挂马不仅严重影响到了网站的公众信誉度，还可能对访问该网站的用户计算机造成很大的破坏。

一般情况下，攻击者挂马的目的只有一个：利益。 如果用户访问被挂网站时，用户计算机就有可能被植入病毒，这些病毒会偷盗各类账号密码，如网银账户、游戏账号、邮箱账号、QQ 及 MSN 账号等。 植入的病毒还可能破坏用户的本地数据，从而给用户带来巨大的损失，甚至让用户计算机沦为僵尸网络中的一员。

## 5.3. 关键词检测功能

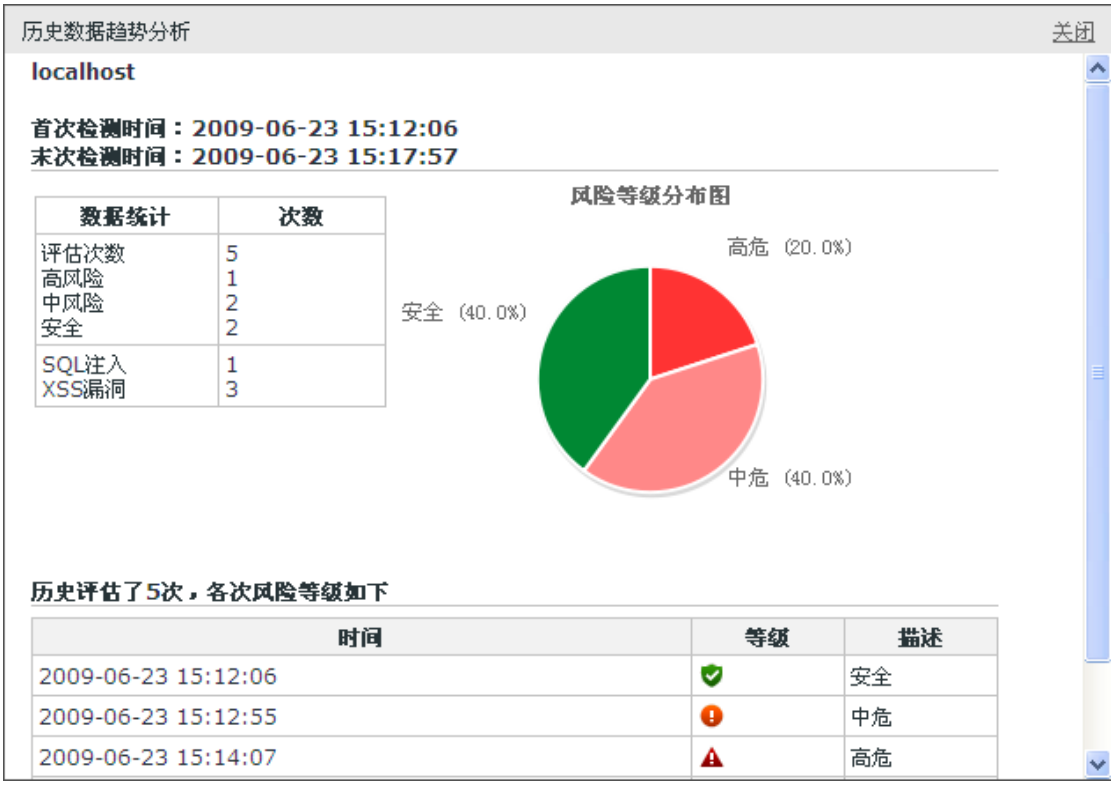
通过先进、高效的中文分词技术，能准确定位目标网页存在的低俗或政治敏感关键词。此外还允许用户自定义或批量导入关键词。

## 5.4. 报表功能

系统扫描报表可以直接导出为 CSV 或 OFFICE 格式。

报表视图分为历史任务、单次任务分析。

如图：




# 6. 核心技术优势

## 6.1. 网页抓取分析技术

系统使用了基于正则匹配、动态文档结构、动态脚本解析、flash 解析等技术来访问 web 应用系统，从而在目标信息收集中不会出现网页地址及参数遗漏、解析错误等问题，确保了信息收集时数据的完整性。

独有的基于智能网页指纹识匹配法的网页相似度算法，能够准确识别网站自定义 404 页面等，避免其他 Web 应用程序出现的误报现象。

## 6.2. 网页漏洞判别技术

系统使用网页动态参数判定、网页结构分析等技术，有效过滤非动态参数，大大提高了检测效率，降低了误报的可能性。

采用多种业内领先的识别技术进行漏洞判定，如关键字匹配、返回信息智能识别等技术。

## 6.3. 中文分词技术及语义分析技术

通过先进的中文语义分词系统及系统词表，准备拆分中文词组。系统更是附带了大量精心挑选的关键词，从而快速定位目标网站存在负面影响的关键词页面。

## 6.4. 插件扩展功能

针对 web 平台新的漏洞攻击技术发展越来越快的现象，系统采用插件系统，增强了系统漏洞检测的可扩展性，能够方便的增加新漏洞检测功能。

# 7. 产品生命周期支持

## 7.1. 产品升级周期

正常情况下,产品每季度提供一个功能性更新包；如有临时的功能更新，随时发布功能性更新包。

当产品有非功能性更新,如数据库及规则库更新时,随时发布非功能性更新包。

对产品提供不低于授权周期的升级支持服务。在产品授权周期内保证升级功能的正常。

## 7.2. 产品更新方式

用户可选择在线更新或本地手动导入更新包。

用户在产品的关于页面，可以查看当前是否有新的升级包，并可以选择下载。

对于用户提供的本地更新包，用户可进行本地导入更新包。

用户选择本地导入更新包后，系统自动进行升级操作，并提示用户是否升级成功。

## 7.3. 产品版本号说明

产品版本分为三个字段：主版本号，功能性更新版本号，非功能性更新版本号。格式为 xx.yy.zz，具体内容如下：

xx：大版本号

yy：小版本号

zz：日常升级包号

如：1.2.13，表示主版本号 1，功能性更新版本号 2，非功能性更新版本号 13。

升级网站提供的每个升级包也有 6 位数字的版本编号：xxyyzz，当升级包安装成功后系统版本将变为最新安装的升级包的版本。

## 7.4. 产品升级策略

- 进入关于页面，用户可以查看当前是否有版本更新，并决定是否进行在线升级
- 系统自动在线升级时自动读取证书文件，不需要用户干预。
- 测试版本无法进行在线升级。
- 授权证书过期后系统无法进行在线升级。
- 用户可选择在线升级或手动导入升级包的方式进行升级。
- 系统启动时自动进行规则库更新。