Web 应用扫描器评估标准的研究

倪评福[1],吴作顺[2]
(1. 西安通信学院,陕西 西安 710106;
2. 中国电子设备系统工程研究所,北京 100141)

摘 要:为了评估现有 Web 应用程序扫描器功能的完整性和优缺点,研究 Web 应用扫描器的整体框架,对框架的重要组成部分提出了其评估指标。针对国内缺乏统一 Web 应用程序扫描器评估标准,研究了国外 Web 应用程序扫描器厂商联合提出的 Web 应用程序扫描器评估标准,指出了该标准的优势和劣势。使用提出的评估指标对选取的三款商业 Web 应用程序扫描器进行评估,评估结果能够在功能上有效区分这三款 Web 应用程序扫描器,证明了提出的评估指标能够较好评估 Web 应用程序扫描器的功能性。

关键词:网络应用程序扫描器;评估标准;评估指标
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2013)03-0139-04
doi:10.3969/j.issn.1673-629X.2013.03.035

Study of Web Application Scanners Evaluation Criteria

NI Ping-fu[1], WU Zuo-shun[2]
(1. Xi'an Communication Institute, Xi'an 710106, China;
2. China Electronic Installation Systems Engineering Institute, Beijing 100141, China)

Abstract: In order to assess integrity and advantages and disadvantages of Web application scanners function, study the Web application scanner overall framework, put forward the evaluation indicators for the important parts of the framework. Aiming to the domestic lack of unified Web application scanner evaluation criteria, Web application scanner assessment standards are researched proposed by the foreign Web application scanner manufacturers combination, pointing out the advantages and disadvantages of this standard. Using the proposed evaluation indicators to evaluate the selected three paragraphs commercial Web application scanner, the evaluation results can effectively distinguish between the three paragraphs Web application scanner on the function, proved that the proposed evaluation indicators can better evaluate Web application scanner function.

Key words: Web application program scanner; evaluation criteria; assessment indicators

0 引 言

随着互联网的发展,金融网上交易、电子商务、社区论坛等等 Web 应用越来越深入到人们的生活中,Web 应用面临着前所未有的挑战,Web 应用程序扫描器(Web Application Security Scanner, WASS)产品越来越多。

目前国外的 WASS 有 IBM Appscan、HP WebInspect、Acunetix Web Security Scanner[1]等;国内的 WASS 有 JSky、Matrixay、WebRavor 等。如何对 WASS 进行评估,保证 WASS 功能的完整性,研究 Web 应用程序安全扫描评估标准(Web Application Security Scanner Nation Evaluation Criteria, WASSEC)[2]显得十分必要。

收稿日期:2012-05-28;**修回日期**:2012-08-29
基金项目:国防 973 项目(6131180401)
作者简介:倪评福(1988-),男,硕士研究生,主研方向为网络安全。

1 WASSEC 的研究

WASSEC 是由国外 WASS 厂商在 Web Application Security Consortium 组织下讨论形成[3]。WASSEC 对 WASS 的功能模块进行了分类,包含了 WASS 的全部基本功能,保证了 WASS 功能的完整性。WASSEC 的组成部分如图 1 所示。

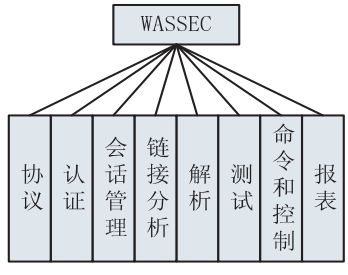

图 1 WASSEC 组成部分

1.1 协 议

为了扫描测试 Web 应用程序,扫描器应该支持

Web 应用程序和中介网络设备所使用的协议。

Web 应用程序使用的协议:

HTTP1.1、HTTP1.0、安全套接层(Secure Sockets Layer,SSL)/安全传输层协议(Transport Layer Security,TLS)、HTTP Keep-Alive、HTTP 压缩、HTTP 用户代理配置[4]。

通常情况下 Web 应用程序扫描器通过代理服务访问网站,因此应支持以下代理协议:

HTTP 1.0 、HTTP 1.1、Socks 4 、Socks 5、支持自动配置代理文件[5]。

1.2 认 证

Web 应用程序一般都部署着广泛的验证机制,为了有效扫描测试 Web 应用程序,Web 应用程序扫描器需要通过相应的认证[6]。例如:Basic 认证、Digest 认证、HTTP 协商认证、Kerberos 第三方认证协议、自动化认证、脚本认证、基于 HTML 表单认证、单点登陆认证、SSL 客户端认证、在扩展的 HTTP 身份验证框架内的定制认证。

1.3 会话管理

Web 应用程序扫描器对 Web 应用程序进行扫描测试时,需要保持与应用程序有效会话,扫描器需要应对所有的会话管理机制[7]。

1.3.1 会话管理功能

Web 扫描器应该具备以下功能:

1. 创建会话;

2. 执行令牌刷新;

3. 删除无效会话;

4. 会话过期时,启动新的会话并重新获得会话令牌。

1.3.2 会话管理令牌类型

Web 应用程序扫描器应该支持以下常用的会话管理令牌:

1. HTTP 令牌(RFC 2965);

2. HTTP 参数:Web 应用程序有时会使用 HTTP 参数来跟踪 Web 会话,例如将 HTTP 参数嵌入到随后的 HTML 连接中或者隐藏 HTML 表格参数;

3. HTTP URL 路径:将会话令牌嵌入到 URL 部分路径中,例如:http://example.co/app/{SESSION_TOKEN}/dir/file.aspx[8]。

1.3.3 会话令牌检测配置

Web 应用程序扫描器会话令牌配置选项:

1. 自动检测和刷新会话令牌:扫描器自动检测 Web 应用程序拥有的会话令牌并在扫描的过程中自动跟踪和刷新;

2. 手动会话令牌配置:使用者手动设置会话令牌,例如 HTTP 参数、令牌或者其他配置类型。

1.3.4 会话令牌刷新策略

Web 应用程序在扫描会话过程中有时要求对会话令牌进行刷新[9],因此扫描器应该提供以下的配置选项:

1. 固定的会话令牌值:当使用固定值作为会话令牌时,在扫描过程中会话令牌将不会改变;

2. 登录时提供令牌值:当用程序扫描器登录应用程序时将会提取登录程序发行的令牌值,使用令牌直到会话无效;

3. 动态令牌值:扫描器在任何时候始终使用应用程序提供的最新的会话令牌,在爬行和扫描测试阶段时刻检测刷新新的令牌值。

1.4 链接分析

首先访问起始 URL,解析爬行链接,直到达到用户设置的标准或者链接全部爬行。链接分析是 Web 应用程序扫描器必不可少的组成部分,体现了扫描器的扫描能力。

1.4.1 网站爬行配置

Web 应用扫描器应提供以下几个配置选项:

1. 定义一个起始 URL;

2. 使用一个列表或者范围定义一个额外的主机名(IP 地址);

3. 排除特定的主机名(IP 地址)、特定 URL 或者 URL 模式、特定文件扩展名、具体参数;

4. 限制重复请求的能力;

5. 支持并发会话;

6. 支持用户设置请求延迟时间;7:支持用户设置最大的爬行深度;8:设置爬行策略。

1.4.2 网站爬行的功能

1. 判定新发现的主机名,网站通常都包含其他网站的链接,识别链接能够帮助用户在必要的情况下可以增加抓取的范围;

2. 支持自动提交表单,通常附加网页中存在新的链接,扫描器应该具有访问附加网页的能力;

3. 检测错误页面和自定义的 404 错误响应;

4. 支持 HTTP 重定向、刷新重定向、Java 脚本重定向;

5. 检测和接受令牌:在访问网站的时候,令牌可能重新设置,扫描器应该能够识别并存储,在扫描的过程中将令牌传递给 Web 服务器;

6. 支持 AJAX 应用程序。

1.5 解 析

为了扫描 Web 应用程序的安全问题,Web 应用扫描器必须首先映射 Web 应用程序的结构和功能。映射过程是通过解析器从网页中提取的不同类型信息。这些信息可能包括网址、HTML 表单、HTML 表单参

数、HTML 注释等等[10]。

1.5.1　网站内容类型

扫描器应该能够解析常见的 Web 内容类型,提取应用程序的结构和功能信息,例如:HTML,JavaScript,VBScript,XML,明文,Active 对象,Java 程序,Flash,CSS。

1.5.2　支持字符编码

Web 应用程序扫描器应该支持以下常见的 Web 应用程序编码:ASCII,ISO-8859-1,UTF-7,UTF-8,UTF-16。

1.5.3　解析器容差

网站内容可能不符合标准,在出错的情况下,解析器应该仍然能够提取有关应用程序的资料。

1.5.4　定制解析器

由于网络技术和标准的发展,Web 应用程序可能使用自定义的链接和其他类型信息,Web 应用程序扫描器应该提供选项来支持解析自定义链接和内容。

1.5.5　提取动态内容

由于客户端脚本语言的动态性,Web 应用程序扫描器不能静态解析脚本语言,如:JavaScript、VBScript 和 Flash 应用程序,为了检测链接和其他相关信息,扫描器应该能够模拟客户端用户交互来动态提取信息。

1.6　测　试

Web 应用程序漏洞测试是 Web 应用程序扫描器的核心功能,以下列出 Web 应用程序扫描器应该提供的配置测试、能力测试和自定义测试。

1.6.1　配置测试

配置测试在扫描器测试 Web 应用程序之前是很重要的,减少基于不同标准的网络应用的可视化水平。配置测试主要有:主机名或者主机 IP,URL 模式,文件扩展名,参数,令牌,HTTP 头。

1.6.2　能力测试

以下测试选项主要从网络应用安全联盟(Web Application Security Consortium,WASC)威胁分类 2.0 版提取出来的:

1. 认证测试包括:蛮力、不足认证、弱口令恢复验证、缺乏对 SSL 的登录页面、未禁止自动完成密码参数;

2. 授权测试包括:会话令牌预测、不足授权、会话到期、固定会话、会话弱点;

3. 客户端攻击测试包括:内容欺骗、跨站点脚本、跨框架脚本、HTML 注入、伪造跨站点请求、Flash 攻击等;

4. 命令执行测试包括:格式化字符串攻击、LDAP 注入、操作系统命令注入、SQL 注入、SSI 注入、XPath 注入、HTTP 头注入/响应拆分、远程文件包含、本地文件包含、潜在的恶意文件上传;

5. 信息披露测试包括:目录索引、信息泄漏、路径遍历、可预测的资源位置、不安全的 HTTP 方法启用、启用 WebDAV、默认的 Web 服务器上的文件、测试和诊断页、前页扩展启用、内部的 IP 地址信息披露。

1.6.3　自定义测试

Web 应用程序扫描器应该支持用户修改现有的测试和创建新的自定义测试。

1.6.4　测试策略

大多数 Web 应用程序扫描器有大量内置的测试,但在许多情况下,只有需要这些测试的子集,Web 应用程序扫描器应该允许用户创建个性化的测试集合。

1.7　命令和控制

Web 应用程序扫描器的命令和控制功能影响其可用性,是扫描器评估的一个重要考察方面。

1.7.1　扫描控制功能

Web 应用程序扫描器评估应该评估以下扫描控制功能:开始扫描;暂停和恢复扫描;实时查看扫描运行状态;重复使用扫描配置模块;同时运行多个扫描;支持多个用户;支持远程、分布式扫描。

1.7.2　提供控制接口

Web 应用程序扫描器应该提供各种控制扫描器的用户界面,例如:GUI 客户端应用程序,命令行界面,基于 Web 界面。

1.7.3　可扩展性和互操作性

Web 应用程序扫描器的扩展功能以及和漏洞跟踪系统的互操作功能是一些用户考虑的重要因素,可以通过 API 接口实现扩展功能,与漏洞跟踪系统的互操作功能可以通过网络提供解决方案。API 接口:Web 应用程序扫描器高级用户通过 API 接口写自己的代码,用于控制扫描器,执行自定义测试,提取自定义报表等资料;与漏洞跟踪系统的整合:使用漏洞跟踪系统来跟踪 Web 应用程序漏洞的状态,Web 应用程序扫描器提供漏洞信息发送到漏洞跟踪系统能力。

1.8　报　告

为了更加直观方便查看扫描结果,Web 应用程序扫描器应该将扫描结果生成扫描报告。

1.8.1　报告类型

虽然具体的报告选项会有所不同,但是扫描器应该提供以下类型的报告:内容摘要,技术细节报告,差异报告,报告符合的安全标准。

1.8.2　漏洞类型报告

扫描器应提供详细漏洞情况报告,漏洞情况包括以下信息:漏洞的描述,漏洞 ID,严重等级,通用弱点评价体系(CVSS)第二版本的评分,修订建议,修订的代码示例。

1.8.3 定制报表

扫描器应该在报告中提供给用户定制的功能,例如:添加自定义的笔记;标记、删除误报漏洞;调整漏洞的风险水平;识别和报告漏洞的位置;添加自定义的内容。

1.8.4 报告格式

扫描器应该提供可读的报告格式,包括:PDF,HTML,XML。

1.8.5 供应商反馈

扫描器应该提供能够自动将扫描器误报或其他类型的反馈报告提供给供应商,以帮助提高产品的未来版本质量。

2 WASSEC 的扩展

WASSEC 将 WASS 分为八个组成部分:协议、认证、会话管理、链接分析、解析、测试、命令和控制、报表,形成 WASS 整体功能框架,包含 WASS 全部的基本功能。

随着科技的发展,大部分成熟的 WASS 都符合 WASSEC,如何评估 WASS 的优劣就摆在我们的面前。

表 1 评估标准和评估结果

		IBM AppScan	AWVS	Web Ravor
协议	复杂应用(ERP)	NO	NO	YES
	HTTPS	YES	YES	YES
	SSL 转发	NO	NO	NO
	代理服务器	单个	NO	支持多个
链接分析	FORM 检测	YES	YES	YES
	重复页面过滤	手工	NO	自动、手工
	Javascript 页面爬行	YES	YES	YES
	目录访问	YES	YES	YES
测试	交互性测试	YES	YES	YES
	网页木马检测	NO	NO	YES
	隐藏目录扫描	YES	YES	YES
	XSS	YES	YES	YES
	数据库基线审计	NO	NO	YES
	渗透测试框架	NO	NO	YES
	Cookie 注入检测	NO	NO	YES
	SQL 注入	YES	YES	YES
	数据库结构和内容的获取	NO	NO	YES
	数据库类型的识别	NO	NO	YES
命令和控制	支持多任务	NO	NO	YES
	批量扫描	NO	YES	YES
	被动扫描(对访问的网站进行扫描)	YES	NO	YES
	全域扫描	NO	NO	YES
	混合扫描	NO	NO	YES
	线程控制	NO	NO	YES
报表	扩展性	YES	NO	YES
	数据导出	XML	XML,AVDL	CSV,XML
	报告格式	PDF、HTML	TEXT、PDF、WORD、HTML	PDF、XML、HTML、MHT、DOC
	支持语言	英文/中文	英文	英文/中文
	报告模块自定义	YES	YES	YES

在对 WASSEC 研究的基础上,对 WASSEC 的八个组成部分提出评估指标,用来对现有 WASS 进行评估,为了显示所提出评估指标的有效性,选取市场上占有率较高的三款商业 Web 应用程序扫描器:IBM Rational AppScan、Acunetix Web Vulnerability Scanner 和 SecDomain WebRavor 进行评估。商业 Web 应用程序扫描器都具有应对所有的会话管理机制,且都还不能应对 Web 应用程序的验证机制,只能在扫描前或者扫描过程中输入正确的用户名和密码,所以这两项没有提出新的评估指标。其它的评估指标和评估结果如表 1 所示。

从表 1 可以得出:

1. WebRavor 支持复杂的 ERP 系统且支持多个代理服务器,而 AppScan 和 AWVS 无法支持 ERP 系统,AppScan 支持单个代理服务器,AWVS 不支持代理服务器[11]。

2. 网页木马检测、Cookie 注入检测、渗透测试框架和数据库方面的扫描都是 WebRavor 独有的功能。

3. WebRavor 具有良好的扩展性和多样的扫描方式,AWVS 只允许自动扫描,不允许手动测试和策略扩展,扩展性差,扫描方式单一[12]。

综上所述,从软件的功能上来讲,在面对复杂的应用系统的检测能力上,WebRavor 最强,AWVS 最差。

3 结束语

Web 应用程序安全扫描评估标准,分析 Web 应用扫描器的整体框架,对框架的重要组成部分提出了其评估指标,有助于评估 Web 应用程序扫描器功能的完整性和优缺点。

参考文献:

[1] Acunetix Ltd. Acunetix Web Vulnerability Scanner[EB/OL]. 2005. http://www.acunetix.com/2005.

[2] Web Application Security Scanner Evaluation Criteria-Web Application Security Consortium[EB/OL]. 2005. http://projects.webappsec.org/f/Web+Application+Security+Scanner+uation+Criteria+-+Version+1.0.pdf.

[3] Krsul I V. Software Vulnerability Analysis[D]. Purdue: Purdue University,1998.

[4] Feng D G,Zhang Y,Zhang Y Q. Survey of information security risk assessmemt[J]. Journal of China Institute of Communications,2004,25(7):10-18.

[5] 苏 彬,杨 寅. 网络应用程序漏洞扫描器的局限性[J]. 计算机安全,2011(5):77-79.

[6] 顾韵华,王 兴,丁 妮. Web 应用安全扫描系统及关键技术研究[J]. 计算机工程与设计,2008(18):4715-4717.

[7] 戴祖锋,张玉清,胡予濮. 安全扫描器综述[J]. 计算机工程,2004,30(2):5-7.

(下转第 146 页)

层驱动,这时 I/O 管理器会发送对应的 IOCTL 代码的 IRP 到底层驱动,底层驱动对 IRP 堆栈信息域指针的读写就可以实现用户模式和内核模式的信息交换。实现代码如下:

```
pInfoNode = (PINFO_NODE) Irp->UserBuffer;
if( pInfoNode->flag = = 1) { //添加进程白名单
pInfoNodeNew = ( PINFO _ NODE ) ExAllocatePoolWithTag ( NonPagedPool,sizeof( INFO_NODE),SFLT_POOL_TAG );
RtlCopyMemory( ( char * ) pInfoNodeNew, ( char * ) pInfoNode,sizeof( INFO_NODE));
KeEnterCriticalRegion( );
pInfoNodeNew->pNext = pInfoListHead->pNext;
//在进程白名单链表中插入节点
pInfoListHead->pNext = pInfoNodeNew;
KeLeaveCriticalRegion( );
}
```

以上从对文件的打开、写入以及关闭分别对整个方法的实现作了一个介绍,该方法的实现更加底层,能够从细粒度上实时监控病毒的恶意行为。

根据以上实现原理,功能结构如图 2 所示。

通过实验验证,该方法能够检测到病毒的传播行为并能加以阻止,达到主动防御病毒的目的。

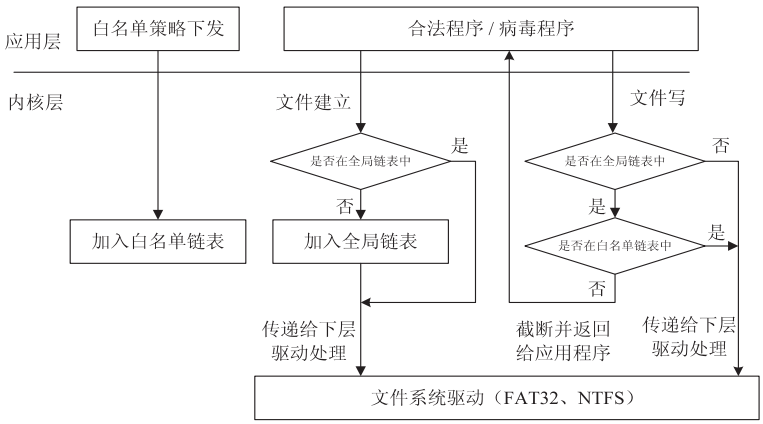

图 2 功能结构图

3 结束语

基于文件过滤驱动,通过在文件驱动上层附加一层过滤驱动,从而在操作系统内核截获文件的读写操作,通过判断是不是对 PE 可执行文件进行写操作,来判断是否是病毒行为。实验结果表明,该方法能够有效地检测病毒程序对可执行文件的写操作,由于直接截获文件读写 IRP,因此该方法比其它方法在实现上更加底层,截获恶意行为更加有效。

参考文献:

[1] Pietrek M. Peer Inside the PE:A Tour of the Win32 Portable Executable File Format[EB/OL]. 2002 - 11 - 01. http://www. microsoft. com.

[2] 樊 震,杨秋翔. 基于 PE 文件结构异常的未知病毒检测[J]. 计算机技术与发展,2009,19(10):160-163.

[3] Skoudis E,Zeltser L. Malware:Fighting Malicious Code[EB/OL]. 2005. http://dl. acm. org/citation. cfm? id = 1212670&coll = DL&dl = GUIDE&CFID = 146756038&CFTOKEN = 30644509.

[4] Conklin W A,White G B,Cothren C,et al. 计算机安全原理[M]. 王 昭,译. 北京:高等教育出版社,2006.

[5] 杨阿辉,陈鑫昕. 基于 SSDT 的病毒主动防御技术研究[J]. 计算机应用与软件,2010,27(10):288-290.

[6] Microsoft Corporation. Installable File System Development Kit[EB/OL]. 2004-12. www. microsoft. com/whdc/devtools/ifskit/default. mspx.

[7] Nagar R. Windows NT file system internals:developer's guid[M]. Cambridge: O`Reilly & Associates, 1997:615-667.

[8] 刘 亮,周安民,沈 东. 基于文件过滤驱动的文件保护技术研究[J]. 四川大学学报(自然科学版),2009,46(3):589-593.

[9] 李 凡,刘学照,卢 安,等. WindowsNT 内核下文件系统过滤驱动程序开发[J]. 华中科技大学学报(自然科学版),2003,31(1):19-21.

[10] 王全民,周 清,刘宗明,等. 文件透明加密技术研究[J]. 计算机技术与发展,2010,20(3):147-150.

[11] 曹成龙,傅德胜,曹凤艳. 基于文件过滤驱动的移动存储控制方法[J]. 计算机应用,2011,31(6):1498-1501.

[12] Russionvich M E,Solomon D A. 深入解析 Windows 操作系统[M]. 潘爱民,译. 第 4 版. 北京:电子工业出版社,2007:539-541.

[13] 谭 文,杨 潇,邵坚磊,等. 寒江独钓:Windows 内核安全编程[M]. 北京:电子工业出版社,2009:252-255.

(上接第 142 页)

[8] 杨新英. 基于网络爬虫的 Web 应用程序漏洞扫描器的研究和实现[D]. 成都:电子科技大学,2007.

[9] 陶亚平. Web 应用安全漏洞扫描工具的设计与实现[D]. 成都:电子科技大学,2007.

[10] 陈秀真,郑庆宏,管晓宏,等. 网络化系统安全态势评估的研究[J]. 西安交通大学学报,2004,38(4):404-408.

[11] 王廷博,徐世超. 基于层次分析法的网络安全态势评估方法研究[J]. 电脑知识与技术,2008,5(4):56-58.

[12] 朱振国,鄢 羽,张 闽,等. 一种量化的网络安全态势评估方法[J]. 微计算机信息,2007,23(3):62-65.

Web应用扫描器评估标准的研究

作者： 倪评福， 吴作顺
作者单位： 倪评福(西安通信学院,陕西 西安710106)， 吴作顺(中国电子设备系统工程研究所,北京100141)

刊名： 计算机技术与发展
英文刊名： Computer Technology and Development
年，卷(期)： 2013(3)