

基于熵权的 Web 应用安全模糊综合评估模型

顾韵华¹ 李丹¹

摘要

针对 Web 应用安全评估问题,提出一种基于熵权和模糊综合评价方法的 Web 应用安全评估模型.该模型将熵权与模糊理论相结合,利用熵权系数法确定 Web 应用安全评价因素集中的权重向量,采用最大隶属度原则确定安全漏洞风险等级.实例分析结果表明该方法简单、实用,能有效进行 Web 应用安全漏洞风险等级的评估.

关键词

Web 应用安全;熵权;评估

中图分类号 TP393.08

文献标志码 A

0 引言

Introduction

Web 应用是目前互联网上最广泛的应用,据 CNCERT/CC 网络安全监测系统对流量数据进行的抽样统计显示,在 TCP 协议中,占网络带宽前 3 名的网络应用分别是 Web 浏览、电子邮件和 P2P 软件,其中 Web 应用流量占整个 TCP 流量的 33.1%^[1].但 Web 的开放性、易用性和 Web 应用的易于开发性使 Web 应用的安全问题日益突出,跨站脚本攻击(XSS,Cross Site Scripting)、注入式攻击(Injection Flaws)、恶意文件执行(Malicious File Execution)等各种 Web 安全漏洞不断出现,Web 安全问题已成为人们关注的核心问题.如何对 Web 应用系统进行安全评估已成为信息安全领域中一项重要的研究课题.

目前国内外在 Web 应用安全方面的研究主要集中在漏洞发现、漏洞描述标准以及漏洞扫描系统的研制方面^[2].已有一些研究组织(如 OASIS、OWASP、Sanctum 等)致力于这些问题的探讨和研究.目前受到广泛认可的研究成果是 OWASP 对 Web 应用安全缺陷的分类^[3]及 OASIS 发布的应用漏洞描述语言 AVDL^[4](Application Vulnerability Description Language).近年来,已有一些著名安全厂商或开源项目推出了 Web 应用安全扫描系统,如:Nikto、Paros proxy、Acunetix Web Vulnerability Scanner、X-Scan^[5]等.它们各有千秋,在业界的影响度也有差异.不同的扫描系统所遵循的漏洞分类标准不同,所产生的安全报告也没有统一的格式与标准.而在漏洞风险评估方面,这些扫描系统大多依据本系统的结果进行评价,因此存在一定的局限性.

为了综合利用已有系统的安全报告,在其基础上形成更为客观可靠的评估结果,本文提出一种基于熵权和模糊综合评价方法的 Web 应用安全评估模型,该模型引入信息熵^[6],利用熵权系数法确定 Web 应用安全评价因素集中的权重向量,并结合模糊理论进行综合评价^[7].

1 评估模型

Evaluation model

模糊综合评价是以模糊数学为基础,应用关系合成原理,将一些边界不清,不易量化的因素定量化,进行综合评价的一种方法^[8-9].运用模糊综合评价方法^[7]对 Web 应用安全进行评估,可分以下几个步

收稿日期 2009-04-25

基金项目 国家自然科学基金资助项目(60874110)

作者简介

顾韵华,女,副教授,主要研究方向为网络与信息安全. yhgu@nuist.edu.cn

¹ 南京信息工程大学 计算机与软件学院,南京,210044

骤:1)确定 Web 应用安全评估的因素集和评判集;
2)确定模糊评价矩阵,建立模糊关系;3)确定因素集
权重向量;4)计算模糊综合评价向量,进行综合评判
处理. 其中,因素集权重的确定在综合评判处理中起
着重要作用,比较常用的方法是采用统计法或专家
打分法,带有明显的主观性. 本模型将采用熵权系
数法确定权重向量,可增强评判结果的客观性.

1.1 因素集和评判集的构造

Web 应用安全评估的因素集

$$U = \{u_1, u_2, \cdots, u_m\}$$

是由评估 Web 应用安全风险 m 个因素(指标)组
成. 有关 Web 应用的安全漏洞的研究,可参考的成
果主要有 CVE (Common Vulnerabilities and Expo-
sures)漏洞数据库^[10]以及 OASIS(Organization for the
Advancement of Structured Information Standards,结构
化信息标准促进组织)所提出的基于 XML 的 Web
安全漏洞描述语言 AVDL (Application Vulnerability
Description Language,应用漏洞描述语言),OWASP
(Open Web Application Security Project,开放 Web 应
用安全项目)所提出的 10 类 Web 安全漏洞分类
方法^[3].

在借鉴上述相关安全漏洞分类或描述语言的基
础上,本文选择与系统安全紧密相关的 5 个因素来
构成模型的因素集,分别是潜在危害、重复利用的可
能性、利用的困难程度、受影响用户范围和发现的难
易程度,即:

$$U = \left\{ \begin{array}{l} \text{潜在危害 } u_1, \text{重复利用的可能性 } u_2, \\ \text{利用的困难程度 } u_3, \text{受影响用户范围 } u_4, \\ \text{发现的难易程度 } u_5. \end{array} \right\}$$

评判集

$$V = \{v_1, v_2, \cdots, v_k\}$$

是由对 Web 应用安全的各因素的 k 种评价所构成
的集合. 考虑到评价安全漏洞的风险等级特点以及评
判集元素数为基数的原则,本模型的评判集 V 选择
3 个等级,分别是高、中、低,即

$$V = \{\text{高 } v_1, \text{中 } v_2, \text{低 } v_3\}.$$

由上述所确定的因素集和评判集,借鉴 CVE 等
标准漏洞库描述,可给出评价因素和风险等级评价
描述标准,如表 1 所示.

1.2 模糊评价矩阵的建立

建立模糊评价矩阵需对 Web 应用安全评估的
因素集 U 中的每个因素 u_i 作评价,即根据模糊映射

$$f: U \rightarrow V,$$

表 1 评价因素和风险等级评价描述表

Table 1 Evaluation factors and risk rate description			
因素	高(v_1)	中(v_2)	低(v_3)
潜在危害(u_1)	获取完全验证权限;执行管理员操作;非法上传文件	泄露敏感信息	泄露其他信息
重复利用的可能性(u_2)	攻击者可以随意再次攻击	攻击者可以重复攻击,但有时限制	攻击者很难重复攻击过程
利用的困难程度(u_3)	初学者在短时间能掌握攻击方法	熟练的攻击者才能完成攻击	漏洞利用条件非常苛刻
受影响用户的范围(u_4)	所有用户,缺省配置,关键用户	部分用户,非缺省配置	极少数用户,匿名用户
发现的难易程度(u_5)	漏洞很明显,攻击条件很容易获得	在私有区域,部分人能看到,需要深入挖掘漏洞	发现该漏洞极为困难

确定因素 u_i 对评价集 V 的值.

首先对各因素 u_i 分别按评判集 V 中各 v_j 进行评
分;然后计算各因素 u_i 对评价集 V 中的第 j 个元素 v_j
的值 r_{ij} ,计算公式为

$$r_{ij} = d_{ij}/d,$$

其中 d_{ij} 为对因素集中的第 i 个因素 u_i 做出第 j 个评
价等级的软件个数, d 为用来扫描的软件总数. 由此
可得出因素 u_i 的模糊评价向量

$$\mathbf{r}_i = \{r_{i1}, r_{i2}, \cdots, r_{ik}\},$$

于是 m 个因素有 m 个评价向量

$$\mathbf{r}_1, \mathbf{r}_2, \cdots, \mathbf{r}_m,$$

这样即可确定一个模糊关系

$$\mathbf{R} = (\mathbf{r}_1, \mathbf{r}_2, \cdots, \mathbf{r}_m),$$

称为模糊评价矩阵:

$$\mathbf{R} = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \\ \vdots \\ \mathbf{r}_m \end{pmatrix} = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1k} \\ r_{21} & r_{22} & \cdots & r_{2k} \\ \vdots & \vdots & & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mk} \end{pmatrix}. \tag{1}$$

1.3 因素集权重向量的确定

1.3.1 信息熵理论

信息熵 (Entropy) 概念是香农 (Shannon) 提出
的,它是对信息量进行度量的一个概念. 自提出以
来,信息熵理论已经在工程科学和社会科学的诸多
领域得到应用.

设系统 S 的可能状态集为

$$\{s_1, s_2, \cdots, s_n\},$$

每种状态出现的概率为

$$\{p_1, p_2, \dots, p_n\},$$

为了度量系统的不确定性, 香农引入如下函数:

$$H_n(S) = H(p_1, p_2, \dots, p_n) = -\sum_{i=1}^n p_i \ln p_i. \quad (2)$$

其中 H_n 称为信息熵, 也称 Shannon 熵^[6,11].

在系统 S 中, 若某状态的概率 p_i 为 1, 则 H_n 恒为零, 该系统不存在不确定性; 若各状态出现概率相等, 则 H_n 达最大值, 此时系统具有最大不确定性.

1.3.2 基于熵权的因素集权重向量

利用 Web 应用安全评估因素集的因素 u_i 的熵权作为其权重, 由此确定因素集权重向量 w . 根据信息熵概念, 评估因素 u_i 的重要程度可由其熵值来表示. 对于有 m 个评估因素, n 个评估对象的评估问题, 设第 j 个评估对象为第 i 个评估因素的评分值为 a'_{ij} , 则该评估问题的评分矩阵为

$$A' = \begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1n} \\ a'_{21} & a'_{22} & \cdots & a'_{2n} \\ \vdots & \vdots & & \vdots \\ a'_{m1} & a'_{m2} & \cdots & a'_{mn} \end{pmatrix}.$$

对 A' 作标准化处理得到

$$A = (a_{ij})_{m \times n},$$

其中

$$a_{ij} = \frac{a'_{ij}}{\sum_{j=1}^n a'_{ij}}.$$

由香农信息熵定义, 第 i 个评估因素 u_i 对评估结果重要度的不确定性可由 u_i 的熵值来度量. 根据公式(2)可得 u_i 的熵值为

$$e_i = -\sum_{j=1}^n a_{ij} \ln a_{ij}. \quad (3)$$

当各 a_{ij} 相等时, e_i 达到最大值 $\ln n$. 用其对公式(3)进行归一化处理, 得到衡量因素 u_i 相对重要性的熵值为

$$H_i = -\frac{1}{\ln n} \sum_{j=1}^n a_{ij} \ln a_{ij}, i = 1, 2, \dots, m. \quad (4)$$

在本模型中, 评估对象为所采用的各扫描系统. 由公式(4)可知, 因素 u_i 的熵值越大, 其对评估的重要程度越低. 因此, 其重要程度可表示为 $1 - H_i$, 从而可得因素 u_i 的熵权 ω_i 为

$$\omega_i = \frac{1 - H_i}{m - \sum_{i=1}^m H_i}. \quad (5)$$

故因素集权重向量

$$w = (\omega_1, \omega_2, \dots, \omega_m).$$

1.4 综合评价处理

所谓综合评价处理是经过模糊变换, 求出决策向量模糊综合评价向量 b , 确定评判结果的过程. 由于因素集中各个因素 u_i 对于安全风险评估的重要程度是有差异的, 因此应综合考虑各因素对 Web 安全的影响, 得出更为合理的评判结果.

设因素集权重向量

$$w = (\omega_1, \omega_2, \dots, \omega_m),$$

由 w 和模糊评价矩阵 R 即可计算出模糊综合评价向量

$$b = w \circ R = (b_1, b_2, \dots, b_k), \quad (6)$$

其中: “ $\circ$ ” 为模糊变换的合成算子, b_j 表示 Web 应用安全漏洞风险被评为 v_j 的模糊隶属度. “ $\circ$ ” 合成算子有 4 种选择: $M(\vee, \wedge)$ 型、 $M(\cdot, \vee)$ 型、 $M(\cdot, \oplus)$ 型和 $M(\cdot, +)$ 型, 其中后 2 种类型合成算子可兼顾各种因素, 并保留各因素评价的全部信息. 考虑到本评估模型既要兼顾各因素、保留全部因素评价信息, 又要计算简便, 故选择 $M(\cdot, +)$ 型合成算子.

对模糊综合评价向量 b , 本模型采用最大隶属度原则进行处理, 即以隶属度最高的等级, 作为所评判 Web 应用安全漏洞的风险等级.

2 应用实例

Application

2.1 评估流程

评估流程如图 1 所示. 首先选择 n 个 Web 安全扫描软件对所要评估的 Web 应用系统进行扫描, 得出 n 份安全报告; 然后将各报告中所提出的安全漏洞进行分类; 接着对每类漏洞, 利用所提出的“基于熵权的 Web 应用安全模糊评估模型”进行模糊综合评价, 给出各类漏洞的风险等级评估报告.

本应用实例中将选择 5 种目前较为流行和具有代表性的 Web 应用安全扫描软件来对 Web 应用系统进行扫描, 它们分别是 Nikto、Paros proxy、Acunetix Web Vulnerability Scanner、X-Scan 和 N-stalker.

由于每种扫描软件对漏洞的分类并没有统一的标准, 这样会造成扫描报告中对某一类漏洞出现不同分类的情况, 因此需要对漏洞制定统一的分类标准, 本文中采用 OWASP 组织于 2007 年提出的分类方法, 将漏洞分为 10 大类. 有了明确分类之后, 就可以先将扫描报告的漏洞进行类别确定, 然后利用评估模型对该类漏洞进行风险等级评估, 最终可得出某 Web 应用系统具有哪些类漏洞, 并且得到这些漏

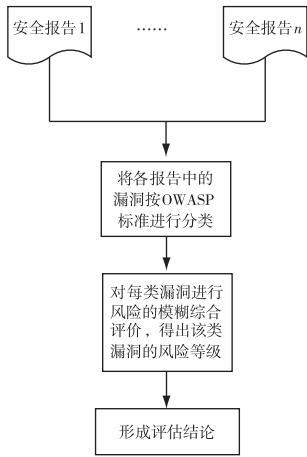


图1 评估流程
Fig.1 Evaluation flow chart

洞的风险程度的高低.

2.2 Web 应用安全漏洞分类

如何对 Web 应用中存在的安全漏洞进行分类, 目前受到广泛认可的是 OWASP 的分类方法^[3]. OWASP 在研究了很多漏洞分类机制的基础上, 将 Web 应用中的主要安全漏洞分成了 10 大类别, 分别是: 跨站脚本、注入式攻击、恶意文件执行、不安全的直接对象引用(Insecure Direct Object Reference)、跨站请求伪造(CSRF, Cross Site Request Forgery)、信息泄漏和不适当的错误处理(Information Leakage and Improper Error Handling)、不完整的认证和会话管理(Broken Authentication and Session Management)、不安全的加密存储(Insecure Cryptographic Storage)、不安全的通信(Insecure Communications)、未限制的 URL 访问(Failure to Restrict URL Access).

2.3 Web 应用安全漏洞风险评估

2.3.1 对 Web 应用系统进行安全扫描并分析

选定一个 B2B 电子商务网站应用系统作为应用实例进行测试. 采用上述的 5 种扫描软件分别对该系统进行漏洞扫描, 得出 5 份扫描报告, 报告显示该网站存在一些漏洞信息. 根据上述 Web 安全漏洞分类标准, 可分析出该网站存在的漏洞包括跨站点脚本攻击、注入式攻击、跨站请求伪造. 根据评估流程, 接下来就要利用本文所构建的评估模型, 分别对这三类漏洞进行风险等级评估. 由于每类漏洞的评估计算方法是一样的, 因此下面以对跨站脚本攻击漏洞风险等级评估为例来说明.

2.3.2 跨站脚本攻击漏洞风险等级评估

按以下步骤进行跨站脚本攻击漏洞风险等级

评估.

- 1) 由表 1 确定模型中的因素集和评价集.
- 2) 建立模糊评价矩阵. 根据 5 种扫描软件对 XSS 漏洞的报告建立模糊评价矩阵. 首先根据表 1, 对 5 份报告中关于 XSS 漏洞的评价确定等级, 然后按照(高, 中, 低)分别对应(5, 3, 1), 对等级进行量化. 所得结果如表 2 所示.

表 2 应用实例的漏洞等级量化表
Table 2 Quantification of vulnerability level in the test example

因素	R1	R2	R3	R4	R5
u_1	1	3	5	3	3
u_2	3	5	5	3	5
u_3	3	5	5	1	5
u_4	5	1	3	1	5
u_5	5	3	5	5	5

注: R1: Nikto; R2: Paros proxy; R3: Acunetix Web vulnerability scanner; R4: X-scan; R5: N-stalker

再根据式(1)所述方法, 建立如下模糊评价矩阵:

$$R = \begin{pmatrix} 0.2 & 0.6 & 0.2 \\ 0.6 & 0.4 & 0.0 \\ 0.6 & 0.2 & 0.2 \\ 0.4 & 0.2 & 0.2 \\ 0.8 & 0.2 & 0.0 \end{pmatrix}.$$

- 3) 确定因素集权重向量. 本应用实例中评估对象为所采用的 5 个扫描系统, 采用熵权系数法, 对表 2 所示的评分矩阵作标准化处理后, 根据公式(4)计算各因素 u_i 的熵值向量为 $H = (H_1, H_2, H_3, H_4, H_5) = (0.943\ 0, 0.980\ 4, 0.939\ 9, 0.886\ 0, 0.986\ 0)$.

然后根据公式(5)计算出因素集权重向量为 $w = (\omega_1, \omega_2, \omega_3, \omega_4, \omega_5) = (0.200\ 2, 0.068\ 8, 0.211\ 1, 0.470\ 9, 0.049)$.

- 4) 计算模糊综合评价向量, 进行综合评价处理. 根据公式(5)计算出模糊综合评价向量为 $b = w \circ R = (0.435\ 6, 0.293\ 8, 0.270\ 6)$.

由模糊综合评价向量 b , 根据最大隶属度原则, 可以得出该 Web 应用系统跨站点脚本攻击的风险等级为高.

按照上述模型对每个漏洞, 分析所有的扫描报告, 最终可以得出该 Web 应用系统存在着跨站点脚本攻击、注入攻击、跨站请求伪造这 3 类漏洞, 风险等级分别为高、中、高.

3 结束语

Concluding remarks

Web 应用安全已引起人们的高度重视,对 Web 应用进行安全评估将成为信息安全工程的重要工作. 本文将应用熵学和模糊理论应用于 Web 应用安全评估领域,提出了基于熵权和模糊综合评价方法的 Web 应用安全评估模型,采用熵权系数法确定安全评价因素集中的权重向量,避免了直接赋值的主观性,从而实现了对 Web 应用安全漏洞风险较为客观的评估. 进一步的研究工作将对评价因素集和评价集进行完善,扩大选用的评测系统范围并对其报告作更详细的分析.

参考文献

References

[1] CNCERT/CC. 中国互联网安全报告 (2008 年上半年) [R/OL]. [2008-11-23]. <http://www.cert.org.cn/articles/docs/common/2008112124134.shtml>
CNCERT/CC. Internet security report of China (The first half of 2008) [R/OL]. [2008-11-23]. <http://www.cert.org.cn/articles/docs/common/2008112124134.shtml>

[2] Chau J. Application security; it all starts from here [J]. Computer Fraud & Security, 2006 (6) : 7-9

[3] OWASP. The ten most critical web application security vulnerability, 2007 Update [EB/OL]. [2007-01-18]. http://www.owasp.org/index.php/Top_10_2007

[4] Jan B, Kevin H. Application vulnerability description language [EB/OL]. [2004-05-07] <http://www.oasis-open.org/specs/index.php#avdl>

[5] 吴海燕, 苗春雨, 刘启新, 等. Web 应用系统安全评测研究 [J]. 计算机安全, 2008, 4 : 44-46
WU Haiyan, MIAO Chunyu, LIU Qixin, et al. The research on Web application security assessment and testing [J]. Computer Security, 2008, 4 : 44-46

[6] 邱苑华. 管理决策与应用熵学 [M]. 北京: 机械工业出版社, 2002 : 193-253
QIU Wanhua. Management decision-making and application entropy [M]. Beijing: Machinery Industry Press, 2002 : 193-253

[7] 曹炳元. 应用模糊数学与系统 [M]. 北京: 科学出版社, 2005 : 66-69
CAO Bingyuan. Applied fuzzy mathematics and its system [M]. Beijing: Science Press, 2005 : 66-69

[8] 谢季坚, 刘承平. 模糊数学方法及其应用 [M]. 武汉: 华中科技大学出版社, 2003 : 100-118
XIE Jijian, LIU Chengping. Fuzzy mathematics and its applications [M]. Wuhai: Huazhong University of Science and Technology Press, 2003 : 100-118

[9] 汪培庄. 模糊集合论及其应用 [M]. 上海: 上海科学技术出版社, 2002 : 35-49
WANG Peizhuang. Fuzzy sets and its applications [M]. Shanghai: Shanghai Science and Technology Press, 2002 : 35-49

[10] Steve Christey, Robert A Martin. Vulnerability type distributions in CVE [EB/OL]. [2007-05-22]. <http://www.cve.mitre.org/docs/vuln-trends/index.html>

[11] 周荣喜, 刘善存, 邱苑华. 熵在决策分析中的应用综述 [J]. 控制与决策, 2008, 23 (4) : 262-266
ZHOU Rongxi, LIU Shancun, QIU Wanhua. Survey of applications of entropy in decision analysis [J]. Control and Decision, 2008, 23 (4) : 262-266

Fuzzy comprehensive evaluation model for Web application security based on entropy weight

GU Yunhua¹ LI Dan¹

1 School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044

Abstract Aimed at evaluating Web application security, a fuzzy comprehensive evaluation model based on entropy weight is proposed. The model combines entropy weight with fuzzy theory. The weight in the model is determined by using the entropy weight coefficient method, and the principle of maximum degree of membership is used to determine the risk level of vulnerabilities. The results of the example analysis indicate that the method is simple and practical, and the model presented may realize an effective risk assessment of security loopholes present in Web application.

Key words Web application security; entropy weight; evaluation