小 型 微 型 计 算 机 系 统 2020 年月 第期
Journal of Chinese Computer Systems Vol. 41 No. 2020

# NO TEARS 算法在 XSS 攻击检测中的应用研究

孙宝丹[1],王培超[2],周 鋆[1]

[1](国防科技大学 信息系统工程重点实验室,长沙 410072)
[2](中国人民解放军 31104 部队)
E-mail:zhouyun@ nudt. edu. cn

**摘 要:** 近年来,利用机器学习技术对跨站脚本攻击(XSS 攻击)进行检测成为网络安全研究的热点. 由于检测特征多,样本标注有限,机器学习模型的精准训练问题一直是一个难题. 贝叶斯网络可以较好的适应小样本环境,最近提出的 NO TEARS 结构学习算法利用平滑约束优化方法,可以较好地对模型进行训练. 本文针对 XSS 攻击检测问题,利用 NO TEARS 算法训练贝叶斯网络模型进行 XSS 攻击载荷(Payload)的判断. 在实验中,本文使用了较为丰富的真实数据,并与传统的结构学习方法及其他分类算法进行了比较,实验结果表明,本文中使用的新的结构学习方法能够明显提升分类准确率,是一种检测 XSS 攻击的有效方法.

**关 键 词:** 贝叶斯网络;结构学习;NOTEARS 算法;XSS 攻击检测实验
**中图分类号:** TP311 **文献标识码:** A **文 章 编 号:** 1000-1220(2020)--

## Case Study of Using NO TEARS in XSS Attack Detection

SUN Bao-dan[1], WANG Pei-chao[2], ZHOU Yun[1]

[1](Science and Technology on Information Systems Engineering Laboratory, National University of Defense Technology, Changsha 410072, China)
[2](No. 31104 Unit of PLA, China)

**Abstract:** In recent years, machine learning is widelyused to detect cross-site scripting attacks (XSS attack) in cyber security. However, due to the large number of detection features and limited labeledsamples, trainingan effective machine learning classifier is alwayschallenging. Bayesian networks can achieve good performance even trainedwithsmall trainingsamples. The recently proposed NO TEARS structure learning algorithm uses smooth constrained optimization method to train Bayesian networksand achieves good performance. Therefore, in this paper, NO TEARS algorithm is used to train the Bayesian network todetect theXSSattack. This paper uses real XSSpayloaddata intheexperiments, and comparesNOTEARSwith traditional BNstructure learning methods and other classification algorithms. The experimental results show that the new structure learning algorithm used in this paper can significantly improve the classification accuracy. Thus, it is an effective way todetect XSS attack.

**Key words:** Bayesian networks; structure learning; NO TEARS algorithm; XSS attack detection

## 1 引 言

XSS(Cross-Site Scripting)全称跨站脚本,是一种常见的 Web 应用漏洞. XSS 攻击属于用于客户端的被动式攻击方式,所以危害性容易被忽视. 攻击者在 Web 页面里插入恶意脚本代码,当用户浏览该页时,嵌入 Web 页面里的恶意脚本代码就会被执行,从而达到恶意攻击用户的目的[13]. XSS 漏洞可以分为三类:Stored XSS 漏洞、Non-persistent XSS 漏洞以及 DOM-Based XSS 漏洞[13]. XSS 漏洞会给企业带来巨大的经济损失,利用 XSS 攻击,攻击者可以获取用户隐私、盗取用户身份 Cookie、劫持用户的浏览器等,会给用户带来严重的生活困扰. 目前虽然已经有一些检测 XSS 攻击的方法,但是这些方法的效果有限. 因此,如何高效检测 XSS 攻击仍然是一个需要深入研究的问题,本文将机器学习方法与 XSS 攻击检测相结合,实现了对 XSS 攻击的有效检测.

利用机器学习方法进行 XSS 检测目前已有一定的应用,其中包括:Gupta MK[1]等人将 XSS 漏洞检测转换为基于预测模型的分类问题,并提出了一种基于文本挖掘和模式匹配的新方法;Khan Nayeem[2]等提出了一种将一组有监督和无监督分类器作为在客户端使用的拦截器来检测恶意脚本的方法;Sunder NS[3]等提出了一种先进的 XSS 预测方法,引入新的评分系统对浏览器中的内容确定特权级别和漏洞级别,同时使用机器学习算法存储,分类和分析在浏览器中运行的 Java 脚本.

GuoXiaobing[4]等利用机器学习算法构建了优化模型,减小了攻击媒体库的大小,提高了 XSS 漏洞检测的效率;RathoreShailendra[5]等人用多种分类器区分网页是否受到 XSS 攻击;Angelo Eduardo Nunan[6]提出了从 Web 文档内容和 URL 中提取特征,并使用机器学习技术在网页上进行 XSS 自动分类;Xi Xiao[7]等介绍了一种对基于编码的注入攻击进行检测的方法,该攻击方式比一般注入攻击更加隐蔽,其中的

收稿日期:2019-06-17 收修改稿日期:2019-08-15 基金项目:国家自然科学基金项目(61703416)资助;湖南省自然科学基金项目(2018JJ3614)资助;湖南省研究生科研创新项目(CX2018B023)资助. 作者简介:**孙宝丹**,女,1993 年生,博士研究生,研究方向为概率图模型的结构学习;**王培超**,男,1993 年生,硕士,研究方向为网络安全技术;**周 鋆**,男,1987 年生,博士,研究方向为机器学习,贝叶斯网络模型.

JavaScript 代码以人类不可读的形式编码,文中使用机器学习的分类算法来确定应用程序是否遭受代码注入攻击. 贝叶斯网络作为一种解释性很强的机器学习模型,也可以很好应用到 XSS 检测中,目前有 Zhou Yun[8] 等使用集成贝叶斯网络的方法进行 XSS 攻击检测,但在模型结构获取时采用的是传统的贝叶斯网络结构学习算法.

本文中使用的 NO TEARS 算法[9] 区别于以往的贝叶斯网络学习算法,不需要深入了解图论的相关知识,将本来复杂的结构学习算法转化为较为容易求解的数值优化问题. 与基于局部启发式的结构学习算法不同,NO TEARS 能够找到全局最优的有向无环图结构,利用更优的模型对 XSS 攻击进行检测,从而可以在检测中达到更高的准确率. 算法中主要通过定义一个新的无环性的描述方法,将非凸组合约束项转化为容易求解梯度值的平滑函数,只涉及一些基本的矩阵运算,求解容易,工程化难度较低.

本文利用 NO TEARS 算法获取的贝叶斯网络作为分类器,对 XSS 攻击载荷(Payload)进行检测,其主要贡献有:1. 将NO TEARS 算法应用到 XSS 攻击检测领域,验证了 NO TEARS 算法在实际应用过程中的有效性;2. 使用机器学习方法实现了对 XSS 攻击进行自动检测;3. 本文中设计算法模型与其他模型相比取得了较高的准确率.

本文的创新点主要如下:1. 本文使用的结构学习算法能够寻找全局最优的贝叶斯网络结构;2. 首次将这种算法应用到网络安全领域关注的重要问题—XSS 攻击检测,并取得很好的实验结果,具有一定的参考及应用价值.

## 2 XSS 检测问题描述

要将 NO TEARS 算法应用到 XSS 检测中,首先要获取 XSS 攻击的特征,这里涉及对 XSS 攻击载荷的特征提取[14]. 根据 XSS 攻击的特点,本文从以下几个方面选取特征:1. 输入长度;2. XSS 攻击载荷常见的敏感关键词和敏感字符;3. 跳转链接对应的协议(protocol)出现的次数. 经过筛选,本文将一条记录用 30 个特征进行表示,这些特征从 1 开始编号到 30,同时节点 31 代表标签,表示当前记录是否为 XSS 攻击,具体特征如表 1 所示.

表 1 XSS 攻击特征

Table 1 Features of XSS attack

| 索引 | 特征名称 | 索引 | 特征名称 | 索引 | 特征名称 |
|---|---|---|---|---|---|
| 1 | 输入长度 | 11 | href | 21 | iframe |
| 2 | alert | 12 | javascript | 22 | onclick |
| 3 | script | 13 | window | 23 | 单引号数量 |
| 4 | onerror | 14 | fromcharcode | 24 | 双引号数量 |
| 5 | confirm | 15 | document | 25 | 左尖括号数量 |
| 6 | img | 16 | onmouseover | 26 | 右尖括号数量 |
| 7 | onload | 17 | cookie | 27 | 反斜杠数量 |
| 8 | eval | 18 | domain | 28 | 逗号数量 |
| 9 | prompt | 19 | onfocus | 29 | 加号数量 |
| 10 | src | 20 | expression | 30 | http://,https://,file:// |

攻击特征获取之后,便可以建模对 XSS 攻击进行检测,如图 1 所示. 这里在将数据输入到分类器之前,首先要对数据进行预处理. 攻击者对用户发动 XSS 攻击时,会将 XSS payload 进行隐藏,诸如使用大小写变换或编码转换等,因此需要对数据进行相关解码,解码依照如下顺序:变小写、URL 解码、HTML 解码、JavaScript 解码、Unicode 解码、URL 二次解码. 数据完成解码之后,对于每一条记录,可以获取相应特征的值,特征已经在上一节列出. 最后把处理后的数据输入到贝叶斯网络结构学习算法中,通过结构学习获取更优的贝叶斯网络模型,并基于此对样本进行检测,输出相应的分类标签.

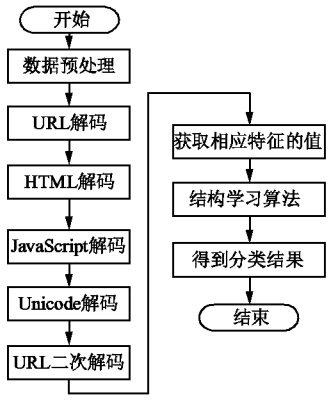


图 1 XSS 检测过程

Fig. 1 Process of XSS attack detection

## 3 贝叶斯网络结构学习

前文提到过,有向无环图的结构学习是一个 NP 难的问题,现有的结构学习算法都不能有效实现无环约束. 这是由于无环约束是组合约束,同时它的计算规模随节点数呈超指数增加. 另外,即便能够得到相对满足约束条件的有向无环图,它也不一定适合一般目的的优化. 目前的结构学习算法依赖于不同的局部启发式算法,这种方法虽然能够降低计算规模,但是不能得到全局最优的结构. 现有的算法大致有分支-切割法、动态规划法、A * 搜索法、贪心算法、坐标下降法等[10]. 与这些算法不同,本文应用的算法采用完全不同的求解方法,将原本的结构优化问题,转化成数学优化问题进行求解. 值得注意的是,这里得到的解是针对当前数据得到的全局最优的贝叶斯网络结构,相比传统启发式算法有了很大的提升. 同时这里使用的算法不要求研究人员具有很深的图论基础,从而具有广泛的研究和应用价值.

### 3.1 贝叶斯网络结构的数学表示

本文中使用的算法是一种新的描述贝叶斯网络的方法,通过求解一个带有平滑约束的优化问题,从而找到最优的有向无环图. 具体地,对于任意给定数据集 $W=(w_{ij})\in\mathbb{R}^{d\times d}$,令 $A(W)\in\{0,1\}^{d\times d}$是一个表示有向图的二元邻接矩阵,那么有如下描述:$[A(W)]_{ij}=1\Leftrightarrow w_{ij}\neq 0$,反之则相反. 同时 $D\subset\{0,1\}^{d\times d}$表示二元矩阵 $B$ 的子集,其中 $B$ 是无环图的邻接矩阵,那么贝叶斯结构优化问题转换成如下的非凸形式:

$$\min_{W\in\mathbb{R}^{d\times d}} Q(W;\mathbf{X}) \text{ subject to } h(W)=0 \tag{1}$$

其中 $Q$ 是与数据有关的损失函数,$\mathbf{X}\in\mathbb{R}^{n\times d}$是数据矩阵,$h$ 是一个平滑函数,$h:\mathbb{R}^{d\times d}\to\mathbb{R}$ 只有当 $A(W)\in D$ 时,$h(W)=0$. 那么上述基于图论表示的贝叶斯网络的结构,就转化成这样一个非凸优化的问题,可以根据数学优化的工具进行求解. 但是在正式求解前,需要将上式中的无环约束进行进一步的刻画,用数学方法表示出来,才能便于后续优化问题的求解.

### 3.2 无环约束的表示方法

这一部分主要介绍一种新的无环约束的表示方法,这里使用了矩阵指数的概念,便于后续优化问题的求解. 矩阵指数是

所有方块阵都能定义的一类函数,类似于指数函数.在表示方法上将指数函数的变量用方块矩阵代替,具体定义方式如下:

$$e^B=\sum_{k=0}^{\infty}\frac{1}{k!}B^k \tag{2}$$

值得注意的是这里,$B$ 为 $n\times n$ 的实数或复数矩阵,那么就有这样的定理:

**定义 1**. 当且仅当 $tr\exp(B)=d$ 时,$B\in\{0,1\}^{d\times d}$ 是有向无环图的邻接矩阵.

**证明**:当且仅当 $(B^k)_{ii}=0$ 对所有的 $k\geqslant 1$ 和所有 $i$ 都成立时,$B$ 表示在有向图中不存在环路,那么就有:

$$\begin{aligned}tr\exp(B)&=tr\sum_{k=0}^{\infty}\frac{B^k}{k!}=tr\sum_{k=1}^{\infty}\frac{B^k}{k!}+d\\&=tr\sum_{k=1}^{\infty}\sum_{i=1}^{d}\frac{(B^k)_{ii}}{k!}+d=d\end{aligned} \tag{3}$$

鉴于上述定理中使用的方块矩阵 $B$,且 $B$ 同时也是个二元矩阵,不能普遍适用于一般数据,因此接下来应该找到一种可以将 $B$ 替换成任意权重矩阵 $W$ 的方法,这里使用的是矩阵的 Hadamard 乘积,定义为:

$$\begin{aligned}A\circ B&=\begin{bmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&\ddots&\vdots\\a_{m1}&a_{m2}&\cdots&a_{mn}\end{bmatrix}\circ\begin{bmatrix}b_{11}&b_{12}&\cdots&b_{1n}\\b_{21}&b_{22}&\cdots&b_{2n}\\\vdots&\vdots&\ddots&\vdots\\b_{m1}&b_{m2}&\cdots&b_{mn}\end{bmatrix}\\&=\begin{bmatrix}a_{11}b_{11}&a_{12}b_{11}&\cdots&a_{1n}b_{1n}\\a_{21}b_{21}&a_{22}b_{22}&\cdots&a_{2n}b_{2n}\\\vdots&\vdots&\ddots&\vdots\\a_{m1}b_{m1}&a_{m2}b_{m2}&\cdots&a_{mn}b_{mn}\end{bmatrix}\end{aligned} \tag{4}$$

其中 $A,B\in\mathbb{C}^{m\times n}$ 且 $A=\{a_{ij}\}$,$B=\{b_{ij}\}$,均为 $m\times n$ 的矩阵.经过如上的变换,对于给定任意权重矩阵 $W\in\mathbb{R}^{d\times d}$,无环约束就可以表示为:

$$h(W)=tr\exp(W\circ W)-d=0 \tag{5}$$

$h(W)$ 的梯度值为:

$$\nabla h(W)=[\exp(W\circ W)]^T\circ 2W \tag{6}$$

这里需要说明,为什么这种替换能够成立.在上述的公式中有这样的表述 $tr(B+B^2+\cdots)$ 表示的是 $B$ 中环数目,经过矩阵指数的变换后只是简单重新给这些数目一个权重,使用 $W\circ W$ 代替 $B$ 后重新计算了这些有权重的环,每条边的权重是 $w_{ij}^2$.

## 4 NO TEARS 算法

### 4.1 无环约束优化问题

之前已经给出过贝叶斯网络的数学表达方式,并对其中的无环约束进行了数学变换,得到最终需要进行优化的数学表达式:

$$\min_{W\in\mathbb{R}^{d\times d}}Q(W;\mathbf{X})+\frac{\rho}{2}|h(W)|^2,\text{满足约束 }h(W)=0 \tag{7}$$

这里引入了一个二次惩罚项 $\rho>0$ 表示惩罚违反约束 $h(W)=0$,那么上式就可以使用增广拉格朗日法进行求解,带有对偶变量 $\alpha$ 的增广拉格朗日方法可以写作:

$$L^{\alpha}(W,\alpha)=Q(W;\mathbf{X})+\frac{\rho}{2}|h(W)|^2+\alpha h(W) \tag{8}$$

它的对偶形式为:

$$\max_{\alpha\in\mathbb{R}}D(\alpha),D(\alpha):=\min_{W\in\mathbb{R}^{d\times d}}L^{\rho}(W,\alpha) \tag{9}$$

那么一个难以求解的有约束的优化问题就变成上式那样无约束的增广问题,现在假设 $W_{\alpha}^{*}$ 是对于固定 $\alpha$ 的增广问题的局部解,那么有:

$$W_{\alpha}^{*}=\arg\min_{W\in\mathbb{R}^{d\times d}}L^{\rho}(W,\alpha) \tag{10}$$

这个问题可以由任何求解无约束平滑最小化问题的数值方法有效解决.现在已经获得了初始解 $W_{\alpha}^{*}$,由于对偶目标函数 $D(\alpha)$ 与 $\alpha$ 满足线性关系,它的梯度值可以写成 $\nabla D(\alpha)=h(W_{\alpha}^{*})$,那么求解上述优化问题最直接的方法是梯度上升法:

$$\alpha\leftarrow\alpha+\rho h(W_{\alpha}^{*}) \tag{11}$$

这里的步长 $\rho$ 的大小是比较增广问题和初始约束问题得来的,这两个表达式的梯度分别如下所示:

$$\nabla Q(W;\mathbf{X})+[\alpha+\rho h(W)]\nabla h(W)=0 \tag{12}$$

$$\nabla Q(W;\mathbf{X})+\alpha\nabla h(W)=0 \tag{13}$$

### 4.2 算法流程及后处理过程

根据上述无约束优化问题的求解过程,最终可以得到本文中使用的新的贝叶斯网络结构学习算法的总体流程如表 2 所示.需要注意的是在上文指出了对于无环约束的表示方法为 $h(W)=0$,但在算法中设置的优化准确率 $\varepsilon>0$,且是一个非常接近于 0 的值.这样带来一个问题,虽然最终的结果是一个非常接近有向无环图的网络,但仍然无法保证得到的是满足约束条件的有向无环图.因此这里引入一个后处理的过程:定义 $B(\omega)=\mathbf{I}(|W|>\omega)$,且找到满足定义的最小阈值 $\omega^{*}>0$,就能够得到有向无环图,这里 $\mathbf{I}(\cdot)$ 是指示函数.

表 2 增广拉格朗日方法

Table 2 Augmented lagrangian algorithm

**算法 1**. 使用增广拉格朗日方法求解约束优化问题

1. 输入:最小化速度 $c\in(0,1)$,惩罚增长率 $r>1$,初始解 $(W_0,\alpha_0)$,优化准确率 $\varepsilon>0$
2. 对于 $t=0,\cdots,\infty$:
   1) 求解初始问题 $W_{t+1}\leftarrow\text{argmin}_W L^{\rho}(W,\alpha_t)$;
   2) 如果 $h(W_{t+1})\geqslant c\cdot h(W_t)$,令 $\rho\leftarrow r\rho$ 并返回 1);
   3) 如果 $h(W_{t+1})<\varepsilon$ 则返回;
   4) 否则,使用对偶梯度上升法 $\alpha_{t+1}\leftarrow\alpha+\rho h(W_{t+1})$ 重复上述过程,直至满足提前设置的优化准确率;

## 5 实验结果与分析

### 5.1 实验设置

XSS Payload 的训练集从 GitHub 上获取而来,其具有 151658 条记录,包含 16151 条黑样本(XSS Payload)和 135507 条正常 URL[8].测试集包含了从 GitHub 和各大安全博客论坛上收集的 Payload,共有 10000 条记录,包含 6503 条正常样本和 3497 条黑样本.实验中使用 Python 集成环境 Anaconda3,Python 版本为 3.6,同时应用 NO TEARS 相应的 Python 算法包.为了验证本文中使用的结构学习算法的效果,这里设置对比实验,即将本文中使用的算法与目前效果较好的基于局部搜索和评分函数的结构学习算法(Tabu Search)[11]、Greedy Hill Climbing[12]算法使用相同的训练集和测试集进行实验,并比较它们分类的准确性.本文设置的另一组对比实验为:将本文使用的 NO TEARS 算法与现有的其他分类算法—朴素贝叶斯分类器(Naïve Bayes,NB)、逻辑回归(Logistics Regression,LR)、决策树(Decision Tree,DT)和随机森林

(Random Forest,RF)算法——进行比较. 两组实验均设定训练样本数取训练集中数据的 55%、60%、65%、70%,并取上述不同分类算法的准确率.

### 5.2 实验结果及分析

从表 3 中可以看出,本文中使用的 NO TEARS 算法的准确率普遍在 98.35% 以上,比 Tabu Search 和 Greedy Hill Climbing 算法都要高,这是因为 NO TEARS 算法求解出来的是贝叶斯网络的全局最优结构,因此分类的结果更加准确. 随着表格中训练样本数的增加,算法的分类准确率也在不断增大,当样本数达到训练集的 70% 时,即使用 105461 条数据进行训练时,准确率可以达到 98.56%,远超传统的结构学习算法,显示出了优越的性能.

表 3 不同贝叶斯结构学习算法的准确率比较

Table 3 Accuracy of different BN structure learning algorithms

| 样本数 | NO TEARS | Tabu Search | Greedy Hill Climbing |
|---|---|---|---|
| 55% | **98.35%** | 96.91% | 97.38% |
| 60% | **98.45%** | 97.38% | 97.42% |
| 65% | **98.53%** | 97.45% | 97.55% |
| 70% | **98.56%** | 97.57% | 97.63% |

本文中采用的 NO TEARS 算法与传统的基于评分和局部搜索的算法不同,是一个能够找到全局最优解的算法. 基于评分和局部搜索的贝叶斯网络结构学习算法,虽然能够有效减少解空间的规模,但是并不能保证找到全局最优的网络结构. 而 NO TEARS 算法能够找到全局最优的网络结构,构建的贝叶斯网络分类器结构更优,其准确率故而要高于一般的结构学习算法.

表 4 不同分类器算法的准确率比较

Table 4 Accuracy of different classifier algorithms

| 样本数 | NO TEARS | NB | LR | DT | RF |
|---|---|---|---|---|---|
| 55% | **98.35%** | 97.27% | 70.12% | 95.88% | 96.42% |
| 60% | **98.45%** | 97.32% | 72.04% | 95.91% | 97.85% |
| 65% | **98.53%** | 97.36% | 72.09% | 97.58% | 98.08% |
| 70% | **98.56%** | 97.45% | 72.27% | 97.96% | 98.22% |

从表 4 中可以看出,本文中使用的 NO TEARS 算法的效果均优于表中其他算法. 同时,逻辑回归在这些算法中分类准确率最低,在 70% 左右,而其余算法的准确率均在 95% 以上,分类效果相对其他算法较差.

## 6 结 论

网络空间安全如今日益受到关注,Web 安全是其中的重要方面,本文选择应用层常见漏洞 XSS,引入了机器学习中的贝叶斯网络的结构学习算法,用于检测 XSS 攻击载荷是否存在. 贝叶斯网络目前在多领域均具有广泛应用,其结构学习算法较为复杂,是一个 NP 难的问题. 尽管目前在贝叶斯网络的结构学习方面取得了进步,其仍然受到多方面条件的制约. 本文中使用的 NO TEARS 算法,不同于一般的结构学习算法,能够找到全局最优的结构,因此大大增加了分类准确率. 本文首先介绍了对 XSS 攻击及其类别,然后介绍了机器学习和贝叶斯网络在 XSS 检测领域的相关研究以及文中使用的 NO TEARS 算法. 接着,本文给出了 XSS 检测问题的描述,在将原始数据输入到分类器之前,首先要对数据进行预处理,文中对数据共进行 5 种预处理方式,将处理之后的数据依据特征进行相应值的提取并将提取值输入算法,经过算法学习之后就可以得到用于判断的分类器. 然后本文具体描述了使用的全局优化算法,给出了其原理、公式以及算法流程. 最后本文对使用的算法进行了实验,实验结果表明利用传统贝叶斯结构学习算法得到的网络进行分类最高可达 97.63% 的准确率,而 NO TEARS 算法能够达到 98.56% 的准确率,优于传统的结构学习算法和其他经典分类算法,更加有效地实现了对于 XSS 攻击载荷的检测.

**References:**


[1] Gupta M K, Govil M C, Singh G. Text-mining and pattern-matching based prediction models for detecing vulnerable files in web applications[J]. Journal of Web Engineering(JWE),2018,17:28-44.

[2] Khan Nayeem, Abdullah Johari, Khan Adnan Shahid. A dynamic method of detecting malicious scripts using classifiers[J]. Advanced Science Letters(ADV SCI LETT),2017,23(6):5352-5355.

[3] Sunder N S, Gireeshkumar T. Privilege-based scoring system against cross-site scripting using machine learning[J]. Advances in Intelligent Systems and Computing(AISC),2016,394:591-598.

[4] Guo Xiao-bing, Jin Shu-yuan, Zhang Ya-xing. XSS vulnerability detection using optimized attack vector repertory[C]//2015:29-36.

[5] Rathore Shailendra, Sharma Pradip Kumar. XSS classifier: an efficient XSS attack detection approach based on machine learning classifier on SNSs[J]. Journal of Information Processing Systems(JIPS),2017,13(4):1014-1028.

[6] Angelo Eduardo Nunan, Eduardo Souto, Eulanda M. dos Santos, et al. Automatic classification of cross-site scripting in web pages using document-based and URL-based features[C]//Computers & Communications, IEEE,2012:702-707.

[7] Xiao Xi, Yan Rui-bo, Ye Run-guo, et al. Detection and prevention of code injection attacks on HTML5-based apps[C]//2015:254-261.

[8] Zhou Yun, Wang Pei-chao. An ensemble learning approach for XSS attack detection with domain knowledge and threat intelligence[J]. Computers & Security(COMPUT SECUR),2019,(82):261-269.

[9] Zheng Xun, Aragam, Bryon Ravikumar, et al. DAGs with NO TEARS: smooth optimization for structure learning[J]. Advances in Neural Information Processing Systems(NIPS),2018.

[10] Barber David. Bayesian reasoning and machine learning[M]. Cambridge University Press,2012.

[11] Dorigo M, Maniezzo V, Colorni A. Ant system: optimization by a colony of cooperating agents[J]. IEEE Transactions on Systems Man & Cybernetics Part B Cybernetics A Publication of the IEEE Systems Man & Cybernetics Society(IEEE T SYST MAN CY B),1996,26(1):29-41.

[12] Tsamardinos I. The max-min hill-climbing Bayesian network structure learning algorithm[J]. Machine Learning(MACH LEARN),2006,65(1):31-78.

[13] Huang Bo, Sun Yu-zhuang. Research on principle and investigation method of XSS cross-site attack[J]. Network Security Technology and Application(NSTA),2017,(6):50-52.

[14] Wang Pei-chao, Zhou Yun, Zhu Cheng, et al. XSS attack detection based on Bayesian network[J]. Journal of University of Science and Technology of China(JUSTA),2019.


**附中文参考文献:**


[13] 黄 波,孙羽壮. XSS 跨站攻击原理与调查方法研究[J]. 网络安全技术与应用,2017,6:50-52.

[14] 王培超,周 鋆,朱 承,等. 基于贝叶斯网络的 XSS 攻击检测方法[J]. 中国科学技术大学学报,2019.