计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200600010

基于信息携带的SQL注入攻击检测方法

程 希 曹晓梅
南京邮电大学计算机学院 南京 210023
(2531183128@qq.com)

摘 要 目前,基于传统机器学习的SQL注入攻击检测的准确度仍有待提高,产生这一问题的主要原因是:在提取特征向量时,若选择的特征向量过多,则会导致模型过拟合,并影响算法的效率;若选择的特征向量过少,则会产生大量的误报数和漏报数。针对这一问题,文中提出了一种基于信息携带的SQL注入攻击检测方法SQLIA-IC。SQLIA-IC在机器学习的检测基础上加入了标记器和内容匹配模块,标记器用于检测样本中的敏感信息,内容匹配模块用于对样本进行特征项匹配,以达到二次判断的目的。为了提高SQL注入攻击检测的效率,利用信息值简化机器学习和标记器的检测结果,在内容匹配模块中根据样本携带的信息值进行动态匹配。仿真实验结果表明,相比传统的机器学习方法,所提方法的准确率平均高出2.62%,精确率平均高出4.35%,召回率平均高出0.96%,而时间损耗仅增加了5ms左右,便能够快速、有效地检测出SQL注入攻击。

关键词:机器学习;特征项匹配;信息携带;SQL注入攻击;入侵检测
中图法分类号 TP181

SQL Injection Attack Detection Method Based on Information Carrying

CHENG Xi and CAO Xiao-mei
School of Computer Science,Nanjing University of Posts and Telecommunications,Nanjing 210023,China

Abstract At present,the accuracy of SQL injection attack detection based on traditional machine learning still needs to be improved. The main reason behind this phenomenon is that if too many features are selected when extracting feature vectors,it will cause the overfitting of the model and negatively affect the efficiency of the algorithm,whereas a large number of false and missed number will be generated if too little features are selected. To solve this problem,the paper proposes SQLIA-IC,a SQL injection attack detection method based on information carrying. The SQLIA-IC adds a marker and content matching module on the basis of machine learning detection. The marker is used to detect sensitive information in the sample,and the content matching module is used to match the feature items of the sample to achieve the purpose of secondary judgment. In order to improve the efficiency of SQL injection attack detection,the information value is used to simplify the detection results of machine learning and markers. In the content matching module,the dynamic matching is performed according to the information value carried by the sample. The simulation experiment results show that compared with the traditional machine learning methods,the accuracy rate of the method proposed in this paper is 2.62% higher on average,the precision ratio is 4.35% higher on average,the recall rate is 0.96% higher on average while the time loss has only increased by about 5ms,which reveals that the method proposed can detect SQL injection attacks efficiently and effectively.

Keywords Machine learning,Feature matching,Information carrying,SQL injection attack,Intrusion detection

1 引言

近年来,基于Web技术的互联网应用日益增多,引起了黑客的广泛关注,从而给Web的安全带来了巨大的挑战[1]。Web攻击手段多种多样,主要包括注入攻击、失效的身份认证、会话管理、跨站脚本攻击、失效的访问控制和安全配置错误等。在OWASP发布的2013年和2017年的Web安全漏洞Top10[2]中,注入漏洞(以SQL注入攻击为主体)一直稳居第一。

SQL注入攻击产生的主要原因是未对用户输入的内容进行适当的验证和过滤,黑客常常使用构建后的语句与数据库产生交互,从而造成服务器中存储的敏感信息泄露或主机中毒。由于其操作简单、危害巨大,如何准确而又高效地检测出SQL注入攻击一直备受学术界和企业界的关注。目前,国内外学者针对注入攻击提出了大量的检测和防御方法。Mitropoulos等[3]对最新的研究成果进行了总结,并将它们分为基于病因的检测方法、基于病症的检测方法和混合检测方法。Su等[4]提出的SQLcheck方法和Buehrer等[5]提出的SQLGuard方法均是基于推理树来进行验证的理论。推理树验证法是使用一定的语法将SQL语句抽象为树结构,比较当

到稿日期:2020-05-31 返修日期:2020-09-19
通信作者:曹晓梅(caoxm@njupt.edu.cn)

前执行的 SQL 语句的树结构与正常 SQL 语句的树结构的差异，推理树验证法能够有效地检测 SQL 注入攻击，但对每一种查询语句都需要建立相应的树结构。Kemalis 等[6]基于规则约束的理论实现了 SQL-IDS 系统，在 Web 与数据库交互时增加了动作监听模块，用户在查询数据库前都要将输入的语句与之前建立完成的规则库中的规则集进行验证比对。通过建立规则集能够对入侵访问进行拦截，但硬规则很容易被绕过，且很难管理。Nanda 等[7]使用污点追踪技术检测 SQL 注入攻击，污点追踪通常是将用户输入的数据标记为不信任数据（污点），然后跟踪这些数据在程序中的传播路径，污点跟踪技术的难处在于如何保证污点数据的准确性。Hedin 等[8]基于信息流控制机制提出了 JSFlow 方法，信息流控制机制结合污点追踪技术和规则约束法，允许开发者使用 JavaScript 语言描述信息流规则，最后可被 JavaScript 编译器编译并进行动态检测。信息流机制不仅适用于脚本检测，还适用于安全应用中，如 Giffin 等[9]提出的 Hails 的方法就能够成功防御 SQL 注入攻击。

随着大数据技术的发展，机器学习在面对海量数据时以其强大的自适应性、自学习能力为安全领域提供了一系列有效的分析决策工具，使用机器学习检测 SQL 攻击也成为一种较为新颖的方法[10]。机器学习主要分为监督学习[11]、无监督学习[12]、半监督学习[13]和强化学习[14]四种，其中监督学习常常被用于 Web 攻击检测场景中。监督学习是从一些事先标记过的样例中获取规律并为此建立模型，进而预测下一组未被标记的样本。模型预测的值可以是连续的（称为回归分析），亦可是多个离散值（称为分类），常见的监督学习算法有 K-近邻[15]、决策树[16]、随机森林[17]、SVM[18]等。文献[19-24]均基于机器学习方法来检测 SQL 注入攻击，大多通过研究特征向量来提高机器学习预测结果的准确度，若选择的特征过多，则会造成模型效率低或过拟合的情况出现，若选择的特征过少，则会导致原样本内容失真，降低模型预测的准确性。为了提高机器学习模型预测的准确性，本文提出了基于信息携带的 SQL 注入攻击检测方法（SQL Injection Attack Detection Based on Information Carrying，SQLIA-IC）。本文首先介绍了 SQL 注入攻击的特征和语法规则，并据此提出了一种基于特征项的内容匹配方法；随后具体介绍了 SQLIA-IC，它的核心思想是利用信息值来简化机器学习和标记器的检测结果，信息值跟随样本进入内容匹配模块中，根据信息值进行动态的内容匹配，并根据内容匹配的结果判断是否为 SQL 注入攻击语句，以达到二次检测的目的。在进行内容匹配时，使用了两种不同模式的特征项匹配方法，以提高内容匹配的效率。仿真实验结果表明，SQLIA-IC 方案能够快速且有效地检测出 SQL 注入攻击。

2　相关工作

Kamtuo 等[19]提出了一种提取数据集重要元素并将其标记为输入属性的方法，该方法共提取出 20 个属性值，将这些输入属性发送到机器学习模型，并报告 SQL 注入攻击的预测。该方案选择了多种机器学习模型进行测试，最终结果表明，决策树（Decision Tree，DT）的时间开销最小，检测准确度最高。决策树能够根据一系列的属性值做出决策，但它必须要定期建立，一旦攻击特征库发生改变，所有的树结构就必须重新建立，因此使用决策树检测攻击手段时可能会出现不稳定的现象。Sun 等[20]提出了基于执行路径控制流的轻量级在线模型和特定于应用程序的离线模型，离线模型使用了随机森林（Random Forest，RF）算法对 SQL 注入攻击检测进行测试，随机森林由多个决策树组成。相比决策树，随机森林不仅更加稳定，还能提高检测精度，但会增加时间开销。Wu 等[21]提出了基于支持向量机（Support Vector Machine，SVM）的 Web 攻击异常检测方法，该方法利用人工挑选和数据统计的方式概括出 6 个特征，将原始样本集转化成固定维数的特征向量。这种方法能够有效检测出 SQL 注入攻击，但未对 SQL 注入攻击的多样性进行深入研究，且未明确给出该方法的漏报率。Uwagbole 等[22]使用 N-grams 的特征提取方法，将提取出的特征进行哈希处理，从而得到一个二进制矩阵。二进制矩阵能更快地计算特征向量的权值，但 N-grams 方法对数据集的多样性要求较高，会直接影响机器学习的学习效果。Hu 等[23]提出基于朴素贝叶斯算法（Naive Bayesian Model，NBM）的 SQL 注入攻击检测方法，将提取出的特征加入词法分析过程中，根据词法分析的结果设计一个阈值进行去噪，从而提高检测 SQL 注入攻击的准确率。然而在提取特征时，若特征项设置得过多，则会影响机器学习算法的学习效率。Komiya 等[24]使用 TF-IDF 方法计算每个特征向量的权重，将处理好的特征向量放入支持向量机、朴素贝叶斯及 k 近邻（k-NearestNeighbor，KNN）3 种机器学习模型中进行训练和测试，并对结果进行分析。实验结果表明，3 种机器学习模型对 SQL 注入攻击检测的效果均表现较好，但测试时使用的数据集规模较小。

与同类工作相比，本文的主要贡献和创新点如下：1）设计了两种不同模式的特征项内容匹配方法，提高了内容匹配的效率；2）在机器学习检测的基础上加入内容匹配模块，使得部分特征项无须出现在机器学习算法的特征向量中，既提高了机器学习的运行效率，也保证了检测的效果；3）引入了信息值和信息携带的概念，根据样本携带的信息值设计了一种动态内容匹配方式，提高了 SQL 注入攻击的检测效率；4）实验结果表明，本文方法能够有效检测出 SQL 注入攻击，与 3 种经典的机器学习算法（RF，KNN 和 SVM）相比，大大减少了误报数，并在一定程度上降低了漏报数。

3　特征项匹配方法

3.1　SQL 注入攻击特征描述及一般语法

SQL 注入攻击具有数量大、变种多的特性，根据不同的情景，攻击者使用的攻击语句也有所差异，但是值得庆幸的是，变种后的 SQL 注入攻击语句的原理万变不离其宗。本文分析了大量数据集并参考文献[25-26]，对 SQL 注入攻击的常见特征进行了总结，最终提取出 10 个常见特征项（见表 1），这些特征项经过组合可以构造出成千上万的 SQL 注入攻击语句。因此，在识别这些 SQL 注入攻击语句时，亦可通过识别某个或某几个特征的方式来达到检测目的。与匹配整个用户输入的语句相比，本文方法将大大缩短检测消耗的时间。

表 1 SQL 注入攻击中常见的特征和实例

Table 1 Common features and examples of SQL injection attacks

Feature Number	Feature Description	Example
1	Select keywords	select, union select
2	Comparison operators(tautology or contradictory)	1=1, 'a'='a', 2=3, 'c'>'d'
3	Comparison operators(conditional categories)	=, >, <, !=, >=, <=, in, like, between, exists, rlike
4	Special function	load_file(), into outfile, xp_cmdshell
5	Time function	sleep(), benchmark(), waitfor delay,
6	Conditional function	if()
7	Logical conjunctions	and, or, xor, &&, ||
8	Error keywords	floor, extractvalue, updatexml, exp,
9	Return database information function	version(), user(), datebase(), @@version
10	SQL command verb keywords	create, insert, update, delete, drop, exec

一个 SQL 注入攻击语句若想被成功执行，除了含有 SQL 注入攻击特征之外，还必须符合 SQL 注入的语法规则。本文根据文献[27]提出的分类方法，对每种类型下的 SQL 注入攻击语法进行描述。

(1)基于布尔的盲注，攻击语句的构造方式为逻辑连接词+重言式/矛盾式，如 and 1=1。

(2)基于时间的盲注，攻击语句的构造方式为 if(判断条件，1 或其他，时间函数)，如 if(ascii(substr(database(),1,1))=115,1,sleep(5))。

(3)报错注入，攻击语句往往有两种构造方式，其中一种为报错函数中含执行语句，如 extractvalue(1,concat(0x7e,(select user()),0x7e))。另一种是报错函数中含有条件判断或比较判断，如 substring(@@version,1,1)=5。

(4)Union 查询注入的构造方式为 union select 1,2,3,…, from 表名，在攻击时常将数字换成能查询数据库信息的函数，数字的个数取决于表的字段数，攻击语句如 union select version(),datebase(),3,4,5,6,7,8 from admin。

(5)执行 SQL 命令的攻击语句也有两种构造方式，其中一种为与 union 查询注入的构造方式相同，但将数字换成特定的函数，如 select 1,load_file('/etc/passwd'),3,4,5,6,7,8,9 from admin；另一种则含有能更改数据库信息类的关键字，执行语法与关键字有关，如 drop table UserTable 和 update users set password=1，在判断这类语句时看关键字即可。

3.2 特征项匹配方法

为了提高 SQL 注入攻击语句的识别效率，基于上述描述与分析，本文设计了两种模式的内容匹配方法，分别为基于特征项的内容匹配方法(Feature Matching，FM)和基于 SQL 语法规则的特征项内容匹配方法(Feature Matching based on SQL Rules，r-FM)。

(1)FM 方法

FM 方法的设计思想是通过匹配样本中含有的特征关键字，根据关键字的组合方式判断 SQL 注入攻击的类型，进而判断其是否为 SQL 注入攻击，详细的设计思路如下：用一个比特表示一个特征项，0 代表含有此特征项，1 表示不含此特征项。对于不同类型的 SQL 注入攻击，从序号 1 到序号 10(参照表 1)依次考虑每个特征，经判断后标记为 0 或 1。若某项特征为关键特征，即必须含有或不含有，将这些特征位加粗并加下划线，对其他非关键特征不做任何处理，最后能形成一个由 0 和 1 组成的表达式。经处理后，每种类型的攻击都有一种或多种由 0 和 1 组成的表达式，如表 2 所列。对于任何一条用户输入的语句，若它满足表达式，则代表这是一条 SQL 注入攻击语句，FM 方法不考虑特征项之间的前后顺序或是否出现其他字符。

表 2 FM 和 r-FM 的具体实现

Table 2 Implementation of FM and r-FM

Feature number										Types of SQL injection attacks	FM method	r-FM method
1	2	3	4	5	6	7	8	9	10			
1	1	1	**0**	**1**	**1**	1	**0**	1	**0**	Time based blind	不考虑各特征项对应的特征号之间的组合顺序及中间是否出现其他字符	6 在 5 前，中间任意匹配
0	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	Boolean blind		7 在 2 前，中间不出现任何字符
1	1	**1**	**0**	0	1	1	**0**	**1**	0	Error injection		9 在 3 前，中间任意匹配
1	1	1	**0**	0	1	1	**1**	1	**0**			仅匹配 8
1	1	1	**0**	1	**0**	1	**0**	**1**	**0**	Joint query		1 在 9 前，在 1 的前面或 9 的后面或两者之间匹配数字或“,”
1	1	1	**1**	**0**	**0**	1	**0**	1	1			1 在 4 前，在 1 的前面或 4 的后面或两者之间匹配数字或“,”
0	**0**	1	**0**	1	1	1	**0**	1	**1**	Execute SQL		仅匹配 10

(2)r-FM 方法

根据上文的描述，r-FM 方法中一个被成功执行的 SQL 注入攻击语句除了含有 SQL 注入攻击的特征项，还必须符合相应的语法规则。FM 方法仅提取了每种 SQL 注入攻击类型的特征项，不关心特征项之间的组合顺序，这会导致组合后的语句不具有实际意义。为减小此类情况出现的概率，需在 FM 方法的基础上考虑各特征项之间是否按照 SQL 注入攻击的语法规则进行组合。表 2 列出了每种 SQL 注入攻击类型中必须含有的特征项间的前后位置关系，这种融入了 SQL 注入攻击语法规则的方法被称为 r-FM 方法。

4　SQLIA-IC 方案

4.1　设计思路

传统的基于机器学习的 SQL 注入攻击检测方法，会因算法本身产生误报数和漏报数。为了提高机器学习的识别率，本文设计并实现了 SQLIA-IC 方案。SQLIA-IC 方案在机器学习检测的基础上增加了标记器和内容匹配模块，标记器用于筛选含有 SQL 注入攻击特征却被机器学习检测为非 SQL 注入攻击的样本，内容匹配模块用于对检测结果进行二次判断。为了提高识别 SQL 注入攻击的效率，本文引入了信息值和信息携带的概念，检测时根据样本携带的信息值进行强、弱两种模式的内容匹配，最终形成了基于信息携带的 SQL 注入攻击检测方法。

SQLIA-IC 方案的流程图如图 1 所示，主要包含信息值产生模块和内容匹配模块。信息值产生模块负责将机器学习算法和标记器的检测结果简化为信息值，信息值跟随样本一同进入内容匹配模块。在内容匹配模块中，根据样本携带的信息值判断样本类型，挑选出既不含 SQL 注入攻击特征也未被机器学习检测为 SQL 注入攻击的样本。对于其他类型的样本，将根据信息值选择相应的内容匹配模式。

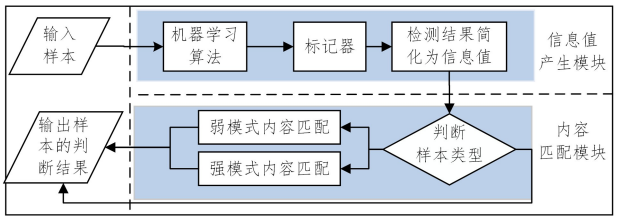

图 1　SQLIA-IC 方案流程图

Fig. 1　Flow chart of SQLIA-IC

4.2　信息值产生模块

信息值产生模块的主要作用是记录并整理机器学习算法和标记器的检测结果，并将它们简化为信息值，这是后续决定内容匹配模式的判断条件。使用机器学习检测样本是否为 SQL 注入攻击语句时，采用人工挑选和数据统计相结合的方式，概括出 7 个特征，分别为特殊关键字的使用次数、特殊字符的使用次数、字符总长度、大写字母的数量、数字使用次数、空格使用次数以及是否含有注释符。实验时，每组实验的各项指标均达到 92%以上，说明这 7 个特征具有良好的可区分性和稳定性。当使用标记器检测样本是否包含敏感信息时，主要判断样本是否含有 SQL 注入关键字、特殊字符及注释符，若有则认定含有敏感信息，敏感信息及相关实例如表 3 所列。信息值产生的流程图如图 2 所示，具体步骤如下：

1）通过机器学习算法检测样本是否为 SQL 注入攻击语句，若是则进入步骤 2），若不是则进入步骤 3）。

2）判断样本中是否含有 SQL 注入敏感词，若含有则标记为 YY，否则标记为 Yy。

3）同样判断样本中是否含有敏感词，若是则标记为 yY，否则标记为 yy。

经过上述步骤后，原始样本被标记为 4 种类型：YY，Yy，yY 及 yy，本文将这些能反映检测结果的标记值定义为信息值，并将其分为 3 类：

（1）强阳性样本，携带信息值 YY 或 Yy；

（2）弱阳性样本，携带信息值 yY；

（3）阴性样本，携带信息值 yy。

表 3　敏感信息及相关实例

Table 3　Sensitive information and related examples

Sensitive information	Example
comment	#，－－，%，/＊　＊/，;and etc
Special characters	!，@，$，＊，&，<，>，=，/，+，-，非闭合字符 etc
Special code	十六进制编码，ascii 编码，url 编码
SQL keywords	select，order，add，declare，delete，update，insert，group，limit，exec，open，and，or，exists and etc

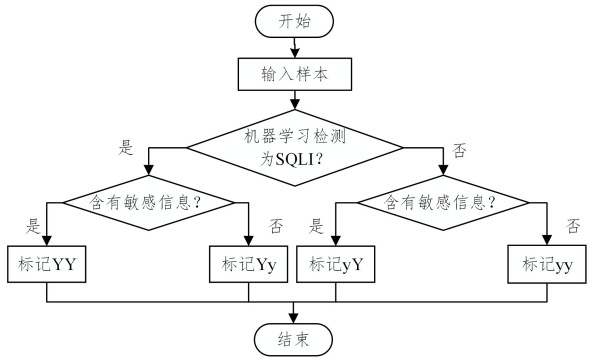

图 2　信息值产生过程

Fig. 2　Information value generation process

4.3　内容匹配模块

内容匹配模块是检测样本是否为 SQL 注入攻击较为关键的一步，其主要作用是分析样本类型，筛选出阴性样本，并对阳性样本进行内容匹配，若符合内容匹配条件则认定为 SQL 注入攻击，否则判断为非 SQL 注入攻击。为了提高 SQL 注入攻击识别的效率和准确率，内容匹配模块需根据样本类型动态选择是否进行匹配以及匹配的方式，同时内容匹配的方式有强、弱两种模式。其中，弱模式内容匹配中使用 FM 方法，仅对特征项进行匹配；强模式内容匹配中使用 r-FM 方法，除了匹配特征项之外还考虑是否符合 SQL 注入攻击的语法规则，内容匹配流程图如图 3 所示。

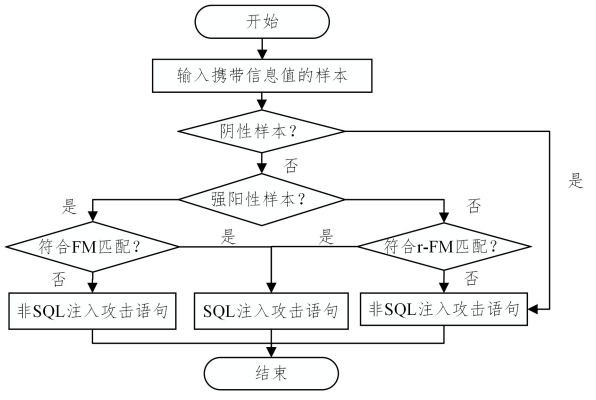

图 3　内容匹配流程图

Fig. 3　Flow chat of content matching

将机器学习检测为非 SQL 注入攻击且标记器判断不含有敏感信息（阴性）的样本，直接判断为非 SQL 注入语句；对于机器学习检测为 SQL 注入攻击（强阳性）的样本，进行匹配度较低的工作，即弱模式内容匹配，以判断其是否符合 FM 匹配；对标记器标记为敏感信息但机器学习检测为非 SQL 注入

攻击(弱阳性)的样本,进行匹配度较强的工作,即强模式内容匹配,判断其是否符合 r-FM 匹配。

5 系统仿真实验

5.1 数据集来源

实验中的数据集主要来自 3 方面,一部分来自 libinjection[1] 项目,一部分来自漏洞提交网站(Exploit-db 和 Wooyun)中最新的 SQL 注入攻击样本,还有一部分是 SQLmap 中的样本。本文精心挑选了 2000 个样本,正常样本与攻击样本的比例为1:1,正常样本中还包含了 300 个易产生误报的数据。

5.2 模型评价

本节将通过实验对基于信息携带的 SQL 注入攻击检测模型进行深入评价,评价的方向主要为 SQL 注入攻击检测的性能评估和时间损耗两方面。性能评估的指标有 4 个:准确率(accuracy)、召回率(recall)、精确率(precision)和 F1-score。准确率表示预测正确的样本占总样本的百分率;召回率代表检测为 SQL 注入攻击的样本占所有 SQL 注入攻击样本的比例,用于反映检测方法的误报问题;精确率代表所有检测为 SQL 注入攻击的样本占实际为 SQL 注入攻击样本的比例,用于反映检测方法的漏报问题;F1-score 是召回率和精确率的调和均值,是召回率和精确率的综合评价指标。

5.2.1 性能评估

本文方法是对机器学习算法的改进,为了证明提出的改进方法对机器学习方法具有普遍适用性,本文对随机森林、支持向量机和 k 近邻 3 种算法均进行了改进。在实验中,先将数据集按照 7:3 的比例划分成训练集和测试集,训练集用于对机器学习模型进行训练,测试集用于验证模型的性能,然后分别使用随机森林、支持向量机和 k 近邻 3 种算法来检测 SQL 注入攻击。

在随机森林算法中,理论上树的最深深度 max_depth 越大,训练集的准确率就越高,但这会造成过拟合的情况,会降低测试集的准确率。在支持向量机中,本文选择了高斯径向核函数,其他的核函数的效果都很差。在高斯径向核函数的支持向量机中有两个重要参数,分别是 gamma 和惩罚系数 C。gamma 值用于调整支持向量的个数,因为支持向量的个数会影响训练和检测的速度;惩罚系数 C 越高,就越容易过拟合。在 k 近邻算法中,参数 k 对算法的性能有一定的影响,k 值较小意味着模型变得复杂,泛化误差大,容易过拟合;k 值较大模型简单,近拟误差大,容易欠拟合。根据实验的具体情况,本文对上述参数进行了调整,最后使用的参数值如表 4 所列。

表 4 不同机器学习算法的参数最优值

Table 4 Optimal values of parameters for different machine learning algorithms

Machine learning algorithm	Parameter	Value	Accuracy/%
Random Forest	*max_depth*	16	95
Support Vector Machine	*gamma*	1.9307	92
	C	1.8	
k-NearestNeighbor	*k*	2	94

在此基础上,在每个机器学习算法中都加入了标记器并进行了内容匹配,整个实验反复进行 10 次,取测试集上的平均值作为实验结果,具体如图 4 所示。

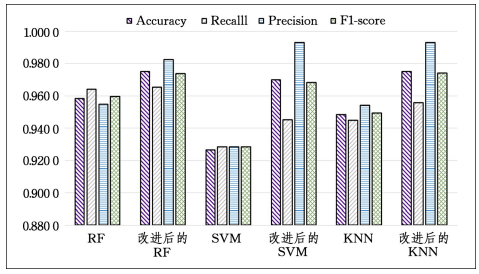

图 4 不同算法及其改进算法下的检测效果

Fig. 4 Different algorithms and their improved detection effects

图 4 所示的结果表明,相比传统机器学习算法,本文提出的改进方法在准确率、精确率和 F1-score 3 个评价指标上均有明显提升,但召回率提高效果并不明显。经过分析,这里认为产生这种情况的主要原因是在减少检测漏报数的同时增加了一些误报数,虽然本文方法能有效地减少机器学习产生的误报数,但在内容匹配时也会产生新的误报。如何有效减少内容匹配时产生的误报数量是提高召回率的关键所在,也是后期研究的关注点。

5.2.2 时间损耗

本文方法是在原有的机器学习算法的基础上增加了标记器和内容匹配模块,为了检测此方法的时间损耗,在实验时分别记录样本进入模型前和退出模型时的系统时间,得到的时间差值,即为此方案从完成训练到检测 SQL 注入攻击的时间损耗。作为对比,本文在实验过程中还记录了传统机器学习模型从建立到进行 SQL 注入攻击检测的时间损耗。整个实验进行 200 次,每次训练集和测试集均发生改变,最终的实验结果如图 5 所示。

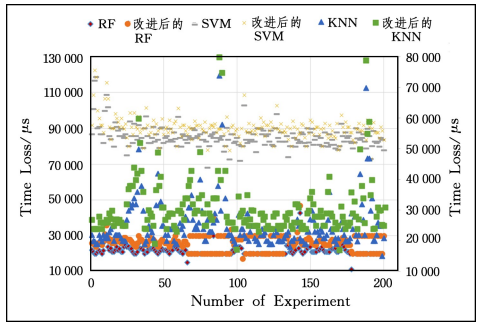

图 5 不同算法及其改进算法下的时间损耗

Fig. 5 Time loss under different algorithms and improved algorithms

图 5 中,k 近邻及改进的 k 近邻算法产生的时间损耗参照右纵轴坐标,其他均参照左纵轴坐标,从散点图可以看出,本文提出的改进方法所产生的时间损耗点都集中出现在原始机器学习算法的上方。为了对时间损耗进行定性、定量的分析,这里对每个模型产生的时间损耗做了趋势线,具体如图 6 所示。从图中可以明显看出,每个模型产生的时间损耗都很稳定,且改进后的方法产生的时间损耗相比传统机器学习模

[1] http://github.com/client9//libinjection

型大约增加了 5 ms。由于方案中增加了标记器和内容匹配方法，这样的时间损耗可被接受。

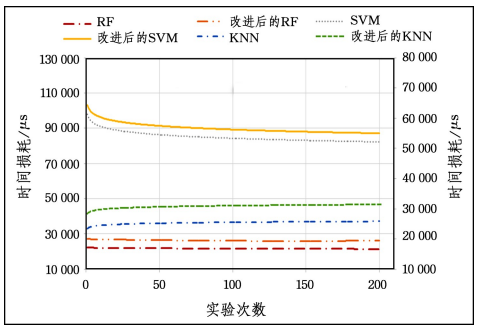

图 6　不同算法及其改进算法下的时间损耗趋势图

Fig. 6　Trend graph of time loss under different algorithms and their improved algorithm

结束语　本文以机器学习算法为基础，融入标记器和内容匹配模块，提出了一种基于信息携带的 SQL 注入攻击检测方法。本文的创新点主要在于对机器学习的检测结果进行了二次判断，提高了机器学习算法的识别率，并在此基础上引入了信息值和信息携带的概念，提出了一种根据信息值进行动态内容匹配的方法。为了提高内容匹配的效率，本文通过分析 SQL 注入攻击的特点和语法规则，提出了一种基于特征值的内容匹配方法。实验结果表明，本文方法能够快速、有效地检测 SQL 注入攻击，相比 3 种经典机器学习算法均有一定的改进。然而，不足之处在于，在内容匹配时依然存在一些误报问题，在未来工作中，我们将继续改善内容匹配方法，尤其是 r-FM 方法，目前仍存在未能充分考虑 SQL 注入攻击语法规则的问题。

参 考 文 献

[1] JIA Z P, FANG B X, CUI X. ArkHoney: AWeb honeypot based on collaborative mechanism [J]. Chinese Journal of Computers, 2018, 41(2): 413-425.

[2] OWASP T T. Category: OWASP_TopTen_Projec[EB/OL]. [2017]. http://owasp.org/index.php/Top10.

[3] MITROPOULOS D, LOURIDAS P, POLYCHRONAKIS M, et al. Defending against web application attacks: approaches, challenges and implications [J]. IEEE Transactions, 2019, 16(2): 188-203.

[4] SU Z, WASSERMANN G. The essence of command injection attacks in web applications[C]// The 33rd ACM Symposium on Principles of Programming Languages. ACM, 2006: 372-382.

[5] BUEHRER G, WEIDE B W, SIVILOTTI P A G. Using parse tree validation to prevent SQL injection attacks[C]// The 5th International Workshop on Software Engineering and Middleware. ACM, 2005: 106-113.

[6] KEMALIS K, TZOURAMANIS T. SQL-IDS: a specification-based approach for SQL-injection detection [C] // The 2008 ACM Symposium on Applied Computing. ACM, 2008: 2153-2158.

[7] NANDA S, LAM L C, CHIUEH T. Dynamic multiprocess information flow tracking for web application security [C] // The 2007 International Conference on Middleware Companion. ACM, 2007: 1-20.

[8] HEDIN D, BIRGISSON A, BELLO L, et al. JSFlow: Tracking information flow in javascript and its APIs[C]// The 29th Annual ACM Symposium on Applied Computing. ACM, 2014: 1663-1671.

[9] GIFFIN D B, LEVY A, STEFAN D, et al. Hails: protecting data privacy in untrusted web applications[C]// The 10th USENIX Conference on Operating Systems Design and Implementation. USENIX Association, 2012: 47-60.

[10] ZHANG L, CUI Y, LIU J. Application of machine learning in cyberspace security research[J]. Chinese Journal of Computers, 2018, 41(9): 1943-1975.

[11] LIANG L M, LIU B W, YANG H L, et al. Supervised retinal vessel extraction based on multi-feature fusion [J]. Chinese Journal of Computers, 2018, 41(11): 2566-2580.

[12] HE G C, LIU X B. Unsupervised visual representation learning based on image triples mining[J]. Chinese Journal of Computers, 2018, 41(12): 2787-2803.

[13] QIN Y, DING S F. A review of semi-supervised clustering[J]. Computer Science, 2019, 46(9): 15-21.

[14] HUANG J H, DING Y Z, XIAO L, et al. A Cache Scheduling Scheme for Embedded System Resistance Against Denial of Service Attacks Based on Reinforcement Learning[J]. Computer Science, 2020, 47(7): 282-286.

[15] HABIBI G, SURANTHA N. XSS attack detection with machine learning and n-Gram methods[C]// 2020 International Conference on Information Management and Technology (ICIMTech). IEEE, 2020: 516-520.

[16] WEI M, LIU Y, CHEN X, et al. Decision tree applied in web-based intrusion detection system[C]// 2010 Second International Conference on Future Networks. IEEE, 2010: 110-113.

[17] DENG X B, YE Y M, LI H B, et al. An improved random forest approach for detection of hidden web search interfaces[C]// 2008 International Conference on Machine Learning and Cybernetics. Kunming, IEEE, 2008: 1586-1591.

[18] PATIL R C, PATIL D R. Web spam detection using SVM classifier[C]// 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO). IEEE, 2015: 1-4.

[19] KAMTUO K, SOOMLEK C. Machine learning for SQL injection prevention on server-side scripting[C]// 2016 International Computer Science and Engineering Conference (ICSEC). IEEE, 2016: 1-6.

[20] SUN F Z, ZHANG P, WHITE J, et al. A feasibility study of autonomically detecting in-process cyber-attacks [C] // The 3rd IEEE International Conference on Cybernetics. IEEE, 2017: 1-8.

[21] WU S H, CHENG S B, HU Y. Web attack detection technology based on SVM [J]. Computer Science, 2015, 42(S1): 362-364.

[22] UWAGBOLE S O, BUCHANAN W J, FAN L. Numerical encoding to tame SQL injection attacks [C] // NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium. 2016: 1253-1256.

[23] HU F S, LI C, WANG M, et al. SQL injection detection scheme based on machine learning[J]. Computer Engineering and Design, 2019, 40(6): 1554-1558.

[24] KOMIYA R, PAIK I, HISADA M. Classification of malicious

web code by machine learning[C]// 2011 3rd International Conference on Awareness Science and Technology(iCAST). IEEE, 2012. 406-411.

[25] LI Q, LI W, WANG J, et al. A SQL injection detection method based on adaptive deep forest[J]. IEE EAccess, 2019, 7(7): 145385-145394.

[26] LI Q, WANG F, WANG J F, et al. LSTM-Based SQL injection detection method for intelligent transportation system[J]. IEEE Transactions on Vehicular Technology, 2019, 68(5): 4182-4191.

[27] DAS D, SHARMA U, BHATTACHARYYA D K. Defeating SQL injection attack in authentication security: an experimental study[J]. International Journal of Information Security, 2019, 18(1): 1-22.

CHENG Xi, born in 1996, postgraduate. Her main research interests include Web security, machine learning.

CAO Xiao-mei, born in 1974, Ph.D. Her main research interests include wireless network security, mobile computing technology and security.