

刘梓乐, 吴晓鸽, 冯永晋, 等. 面向Web安全扫描器的网络入侵检测研究[J]. 广东工业大学学报, 2025, 42(6): 52–61. doi: 10.12052/gdutxb.240151.
Liu Zile, Wu Xiaoling, Feng Yongjin, et al. Network intrusion detection for Web security scanner[J]. Journal of Guangdong University of Technology, 2025, 42(6): 52–61. doi: 10.12052/gdutxb.240151.

面向Web安全扫描器的网络入侵检测研究

刘梓乐¹, 吴晓鸽¹, 冯永晋¹, Hoon Heo²

(1. 广东工业大学 计算机学院, 广东 广州 510006; 2. 三星电机有限公司, 韩国 京畿道水原市 16674)

摘要: 在网络攻击中, 使用Web安全扫描器的扫描探测是Web攻击前期侦察的主要手段。现有的Web入侵检测方法侧重于对已知攻击数据和正常数据进行分类, 存在容易被绕过、无法检测未知攻击等问题。为了弥补现有的缺陷, 本文提出从Web安全扫描器探测扫描的角度检测Web攻击。首先, 通过实验采集了多种Web安全扫描器的扫描数据, 并分析、验证了扫描数据间存在的相似性。然后, 提出了一种基于扫描数据的Web入侵检测方案(CharEmbedding-CGRU($M \times N$)), 其中包括特征提取方法及卷积门控循环网络模型。最后, 在收集的扫描数据集上进行对比实验, 结果表明, 本文提出的Web入侵检测方案具有更好的攻击检测效果, 对已知Web安全扫描器的检测精确率是99.87%、 F_1 值为98.99%, 对未知Web安全扫描器的检测精确率为92.98%、 F_1 值为95.71%。

关键词: 网络入侵检测; Web安全扫描器; 卷积神经网络; 门控循环单元

中图分类号: TP391

文献标志码: A

文章编号: 1007-7162(2025)06-0052-10

Network Intrusion Detection for Web Security Scanner

Liu Zile¹, Wu Xiaoling¹, Feng Yongjin¹, Hoon Heo²

(1. School of Computer Science and Technology, Guangdong University of Technology, Guangzhou 510006, China;

2. Samsung Electro-mechanics Co., Ltd., Suwon City, 16674, Korea)

Abstract: The use of Web security scanners for scanning and probing serves as a primary way of cyber reconnaissance in the early stages of Web attacks. Existing Web intrusion detection methods primarily focus on addressing the binary classification problem between known attack flows and normal flows, which have issues such as being easily bypassed and an inability to detect unknown attacks. To address these, this paper proposes a method for detecting Web intrusion attacks from the perspective of Web security scanner scanning. Firstly, this paper collects scanning data from various Web security scanners through experiments, and analyzes the similarity of the scanning data. Secondly, a Web intrusion detection scheme based on scanning data is proposed, which includes a feature extraction method and a convolutional gated recurrent network model. Finally, comparative experiments are conducted on the collected dataset, and the results show that the Web intrusion detection scheme proposed in this paper achieves superior attack detection performance. Specifically, it achieves a detection precision of 99.87% and an F_1 -score of 98.99% for known Web security scanners, and a detection precision of 92.98% and an F_1 -score of 95.71% for unknown Web security scanners.

Key words: network intrusion detection; Web security scanner; convolutional neural networks; gated recurrent unit

从Web安全扫描器探测扫描的角度检测Web攻击可以在网络攻击的早期阶段发现攻击行为。Web攻击是多阶段的, 其中两个主要的网络入侵阶段是信息探测阶段和漏洞利用阶段。在信息探测阶段, Web安全扫描器是攻击者主要使用的侦察工具。

攻击者通过使用Web安全扫描器对目标Web应用进行信息探测, 像侦察机掠过一样快速总览Web应用信息。在漏洞利用阶段, 攻击者再根据信息探测阶段收集的Web应用相关信息, 如Web应用类型信息、版本信息或相关漏洞信息等, 制定相对应的攻击方案,

收稿日期: 2024-12-05 录用日期: 2025-01-09 网络首发日期: 2025-06-17

基金项目: 广东省重点领域研发计划项目(2019B010139002); 广东省国际科技合作领域项目(2019A050513010)

作者简介: 刘梓乐(1997-), 男, 硕士研究生, 主要研究方向为入侵检测、欺骗防御, E-mail: lauzero21th@qq.com

通信作者: 吴晓鸽(1979-), 女, 副教授, 博士, 主要研究方向为信息安全、物联网, E-mail: xl.wu@gdut.edu.cn

最终实现攻击目的。

现有的Web入侵检测方法侧重于解决已知漏洞利用数据与正常数据的二分类问题,可以分为两类^[1]:漏洞利用特征检测及异常检测。前者侧重关注漏洞利用数据的特征,后者侧重关注正常数据的特征。

侧重关注漏洞利用特征的Web入侵检测方法是静态、可预测的^[2],存在无法检测未知漏洞利用特征、容易被绕过检测的问题。这类入侵检测方法常见通过字符匹配或正则表达式匹配的方式检测已知漏洞利用特征。随着神经网络技术逐步得到验证,研究开始探索通过神经网络模型挖掘单组数据内在的潜在联系。2021年,Gniewkowski等^[3]提出使用RoBERTa模型提取Web请求特征;Tekerek^[4]提出使用卷积神经网络进行Web攻击的检测分类;Zuech等^[5]提出使用随机欠采样的方法来提升Web入侵检测的性能。2022年,Toprak等^[6]提出使用基于多层长短期记忆(Long Short-Term Memory, LSTM)网络层的神经网络模型对漏洞利用数据和正常数据进行检测分类;范禹辰等^[7]提出使用BERT模型提取Web请求特征,并基于结合LSTM、Transformer层的神经网络模型实现Web入侵的分类检测。2023年,周桥等^[8]提出融合word2vec提取的词向量特征及统计特征,并采用GRU作为池化层的卷积神经网络模型对Web攻击进行检测与分类;Dawadi等^[9]提出对DDoS、SQL注入、XSS三种不同类型的攻击采取不同的特征提取方法,并使用LSTM神经网络模型对Web攻击进行检测分类。2024年,李道全等^[10]提出使用鸽群优化算法提取特征,并使用Transformer结合双向门控循环单元的模型对Web攻击进行检测分类;孙红哲等^[11]提出对流量数据经双向滑窗法生成双向序列,并使用注意力机制和双向时间卷积神经网络对攻击进行检测分类;张子迎等^[12]设计了基于XGBoost-DNN的工业控制系统入侵检测架构,通过权重焦点损失函数和特征选择机制增强了检测的鲁棒性,缩短了深度神经网络(Deep Neural Network, DNN)训练时间;金志刚等^[13]通过特征提取和时序相关性分析,提出了结合堆叠循环卷积和头部注意力机制的工业互联网入侵检测方法;陈虹等^[14]通过减少类间相似性和特征选择,提出了融合对比学习和特征选择的入侵检测模型CL-FS(Contrastive Learning and Feature Selection);龚星宇等^[15]通过自动阈值选择和特征融合,设计了基于多尺度融合和时空特征的ML-PFN(MSFE LSTM-parallel feature network)入侵检测模型;刘涛等^[16]通过对种群初始化和位置更新改进,

提出了改进麻雀搜索算法的入侵检测特征选择方法。

随着学者们对攻击过程的进一步研究,开始转向从多组数据中挖掘数据的潜在联系。Bao等^[17]提出将包含Payload的整个HTTP请求数据进行图嵌入,再使用图注意力网络(Graph Attention Network, GAT)模型对漏洞利用数据和正常数据进行分类检测;沈学利等^[18]提出基于图边缘特征注意力的入侵检测方法,通过图池化和边缘特征聚合,并使用多层感知器(Multi-Layer Perceptron, MLP)分类器对Web攻击进行检测分类。尽管现有的入侵检测方法已取得显著进展,但仍过于依赖公开的漏洞利用细节数据。因此,有必要进一步探索能够降低对公开漏洞数据依赖性的检测方法,以更有效地应对复杂的网络入侵威胁。

在持续更新的Web应用环境中,侧重关注正常数据特征的Web入侵检测方法容易将更新的正常数据误检测为攻击数据^[2]。这类入侵检测方法的本质是检测已知正常数据的离群数据,常见使用的算法有K-Means Clustering、Hidden Markov Model(HMM)等。2018年,Mac等^[19]提出使用AutoEncoder神经网络模型提取Web请求特征,再通过预设阈值的方式确定异常数据,从而实现异常数据的检测分类。2022年,Sevri等^[20]提出两段式深度神经网络模型,其中第一阶段基于深度神经网络模型进行异常数据的检测分类,第二阶段对异常流量进行不同攻击的分类。2024年,Benova等^[21]提出通过结合专家系统,使用隔离森林算法对Web日志中的正常数据进行聚类分析、界定异常数据,并使用DBSCAN算法对异常数据进行检测分类。尹兆良等^[22]提出一种注意力扩展期望最大化的无监督算法,通过注意力网络模型对流量数据进行结构化,并使用注意力扩展期望最大化算法(Attention Expand Expectation-maximization Algorithm, AE-EM)对结构化后的数据进行异常检测。

现有基于已知漏洞利用数据和正常数据分类的Web入侵检测方法,虽然使用机器学习模型提高了检测能力和泛化能力,但是仍存在容易被绕过、误报率高的问题。而这些问题存在的本质原因是对正常数据和攻击数据的界定是后验的,即需要根据已知的Web请求结果判断是否为攻击数据。本文提出从Web安全扫描器探测扫描的角度检测Web攻击,先验地将使用Web安全扫描器进行信息探测的行为定义为攻击行为,从不同的角度实现Web入侵检测,弥补现有Web入侵检测方法存在的缺陷。

在神经网络模型中,卷积神经网络(Convolutional

Neural Network, CNN)模型在特征提取上的出色性能已得到验证^[23], 门控循环单元(Gated Recurrent Unit, GRU)可以高效地提取并保留具有上下文关系的重要序列特征。因此, 本文构建了使用不同形状卷积核提取特征的卷积门控循环网络模型(CGRU($M \times N$)), 并将其用于检测Web安全扫描器发起的网络攻击。本文的主要贡献和创新点概括如下:

(1) 从Web安全扫描器探测扫描的角度提出检测Web攻击, 并分析、验证了Web安全扫描器扫描请求数据间的相似性。

(2) 提出一种面向Web安全扫描器的网络入侵检测方案(CharEmbedding-CGRU($M \times N$)), 并将其用于检测利用Web安全扫描器的发起攻击行为。该入侵检测方案包括基于字符嵌入的特征提取方法, 以及一种卷积门控循环网络模型。

(3) 通过对比实验表明, 本文提出的CharEmbedding-CGRU($M \times N$)入侵检测方案的检测效果表现更优, 对已知Web安全扫描器的检测精确率是99.87%、 F_1 值为98.99%, 对未知Web安全扫描器扫描数据的检测

精确率为92.98%、 F_1 值为95.71%。

1 扫描数据分析及入侵检测方案

1.1 扫描数据收集

本文针对Web安全扫描器通过模拟实验的方式开展网络入侵检测研究。首先选用了5个Web安全扫描器对两类Web应用进行了两次独立的扫描实验, 并收集了相应的Web请求日志。在Web安全扫描器的选择上, 选取了两个常见的Web安全扫描器(Nikto和ZAP)和3个企业级的Web安全扫描器(后续简称为扫描器A、扫描器B和扫描器C)。在Web应用的选择上, 选取了基于PHP环境的漏洞靶场应用DVWA (Damn Vulnerable Web Application)及基于Java环境的漏洞靶场应用Webgoat。

1.2 数据特征提取

从Web请求日志中提取的请求特征主要有以下3部分: 请求方法、请求路径和请求参数。本文对请求特征的各部分作了如下处理(如图1所示)。

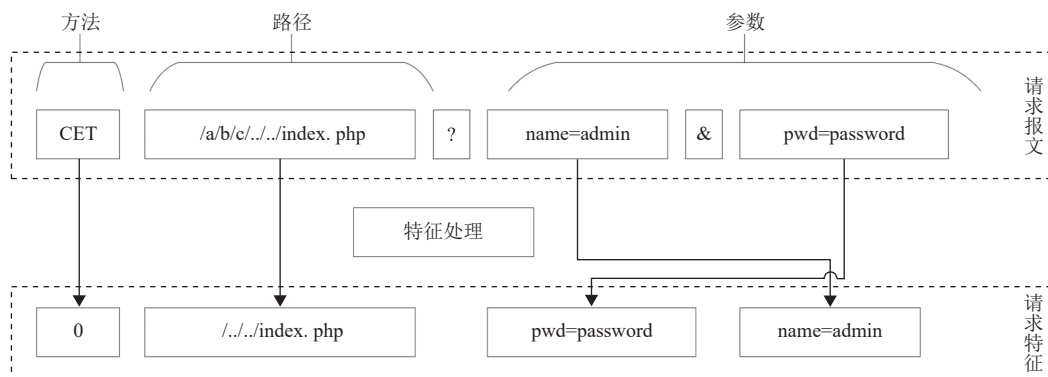


图1 请求特征处理流程

Fig.1 Processing flow of request feature extraction

(1) 请求方法: 用数字表示请求方法, 即用0表示GET方法、1表示POST方法, 以此类推。

(2) 请求路径: 通过“.”符号定位请求路径的资源位置, 仅保留请求路径的资源路径信息, 如: 请求路径“/dvwa/php.ini”仅保留“/php.ini”路径信息, 请求路径“/dvwa/../../php.ini”仅保留“/../../php.ini”路径信息。

(3) 请求参数: 对请求参数按其键长度进行了重新排序, 并使用0替换参数值中出现的数字。

使用上述方法对扫描数据进行特征提取后, 统计了所有数据的扫描请求特征的长度, 如图2所示。为了提高扫描请求特征分析的性能, 本文以150个字符作为最大长度对后续使用的扫描请求特征进行了截取。

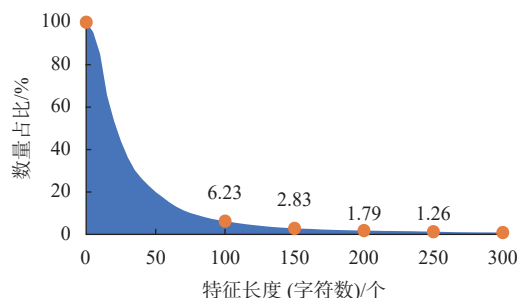


图2 请求特征长度统计

Fig.2 Statistics of request feature length

1.3 扫描数据相似性分析

Web安全扫描器在不同情形的扫描中发送的请求数据具有相似性, 因此Web安全扫描器的请求数

据适用于分类检测。不同Web安全扫描器在模块组成和运行模式上是相似的。Web安全扫描器主要由两个模块组成: 信息收集模块(包括资产信息收集和端口服务收集)和漏洞检测模块^[24-27]。其中, 信息收集模块收集Web应用的相关信息, 漏洞检测模块根据对应信息验证Web应用安全实情。Web安全扫描器通过两个主要模块进行配合、有序的运行(即相似的运行模式), 实现Web安全信息探测的目标。同一时期内, 已知的Web应用信息、安全信息集合是固定的, 因此本文假设Web安全扫描器需探测验证的Web应用信息、安全信息是相似的, 即在Web安全扫描器进行不同的扫描探测时发送的请求数据也是相似的。在本节中, 将使用收集的扫描数据对其相似性作进一步的分析和验证。

1.3.1 相似性衡量指标

本文选用相对差异百分比作为请求数据间差异程度的衡量指标, 设扫描数据集1的请求次数为 C_1 、扫描数据集2的请求次数为 C_2 , 则两个数据集间的请求次数相对差异百分比(Relative Percentage Difference, RPD)计算如式(1)所示。选用编辑距离作为不同请求特征间相似程度的衡量指标。编辑距离, 又称为Levenshtein距离, 它利用编辑操作步数的距离来衡量两个字符串相似度, 其中编辑操作包括插入一个字符、删除一个字符和替换一个字符。例如: 从字符串“index”变到字符串“Index”需要替换一个字符则编辑距离为1, 从字符串“index”到字符串“ndexl”需要删除并插入一个字符则编辑距离为2, 两个字符串相同则编辑距离为0。

$$RPD = \frac{|C_1 - C_2|}{(C_1 + C_2)/2} \times 100\%$$
 (1)

为了衡量两个扫描数据集间的相似程度, 统计了两个数据集请求特征最小编辑距离的数量分布, 并计算了相同请求特征的最大占比(简称相同最大占比)。扫描数据集1和扫描数据集2间存在相同请求特征数 S , 则相同最大占比 P 计算如式(2)所示。

$$P = \frac{S}{\min(C_1, C_2)}$$
 (2)

1.3.2 扫描请求数据的相似性

在本文的模拟实验中, 根据不同扫描间的对比差异, 给出如下概念定义。

定义1 连续扫描 同一种Web安全扫描器对同一类Web应用的多次扫描。

定义2 不同目标网站的扫描 同一种Web安全扫描器对不同类Web应用的扫描。

定义3 不同Web安全扫描器的扫描 不同种Web安全扫描器对同一类Web应用的扫描。

(1) 连续扫描的相似性。

表1、表2分别是不同Web安全扫描器对DVWA应用和Webgoat应用进行连续扫描的请求次数统计结果。由此可以观察到不同次的扫描数据间从请求次数上已显示其相似性, 综合表1、表2的平均相对差异百分比为5.81%, 即不同次扫描数据的请求次数差异小, 由此可以验证同一种Web安全扫描器对同一类Web应用进行多次扫描请求次数的相似性。

表 1 基于DVWA应用的连续扫描请求数据统计
Table 1 Statistical analysis of continuous scan request data based on DVWA

扫描器	第1次扫描请求次数	第2次扫描请求次数	相对差异百分比/%
Nikto	6 297	6 297	0.00
ZAP	4 161	4 162	0.02
扫描器A	34 914	36 505	4.46
扫描器B	10 555	9 337	12.25
扫描器C	12 752	12 721	0.24

表 2 基于Webgoat应用的连续扫描请求数据统计
Table 2 Statistical analysis of continuous scan request data based on Webgoat

扫描器	第1次扫描请求次数	第2次扫描请求次数	相对差异百分比/%
Nikto	6 295	6 295	0.00
ZAP	382	382	0.00
扫描器A	26 284	26 159	0.48
扫描器B	2 394	2 102	12.99
扫描器C	15 234	20 139	27.73

根据表3、图3所示的结果分析, 在连续扫描中, 平均有93.0%的请求特征是相同的, 而其他请求特征的编辑距离平均有80%集中在1~10之间。因此, 该对比分析说明在连续扫描中, 请求特征具有较高的重复性, 并且存在着较高的相似性。

(2) 不同目标网站扫描的相似性。

根据表4、图4所示的结果分析, 在相同Web安全扫描器对不同目标网站的非连续扫描中, 平均相同最大占比为32.2%, 而请求特征编辑距离的分布也主要集中在0~10之间。因此, 不同目标网站扫描的请求特征集合具有相似性, 且可预见基于已知扫描数据训练的Web检测模型, 迁移到不同类的Web网站中仍具有不错的攻击检测能力。

(3) 不同Web安全扫描器扫描的相似性。

据图5、图6与表5、表6所示的结果分析, 在同目

表 3 连续扫描,相同特征数统计
Table 3 Statistical analysis of identical feature counts in continuous scans

扫描器	Web应用	相同特征数/个	最大占比
Nikto	DVWA	6 078	0.965
ZAP	DVWA	4 138	0.994
扫描器A	DVWA	33 448	0.958
扫描器B	DVWA	7 498	0.803
扫描器C	DVWA	11 969	0.941
Nikto	Webgoat	6 076	0.965
ZAP	Webgoat	381	0.997
扫描器A	Webgoat	24 810	0.948
扫描器B	Webgoat	1 808	0.860
扫描器C	Webgoat	13 300	0.873
平均			0.930

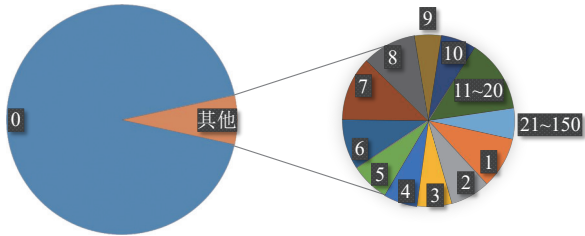


图 3 连续扫描数据编辑距离统计
Fig.3 Statistics of edit distance in continuous scanning

表 4 不同目标网站扫描,相同特征数统计
Table 4 Statistical analysis of identical feature counts in scans of different target websites

扫描器	相同特征数/个	最大占比
Nikto	12 152	0.965
ZAP	441	0.577
扫描器A	20 994	0.400
扫描器B	4 048	0.900
扫描器C	9 480	0.372
平均		0.322

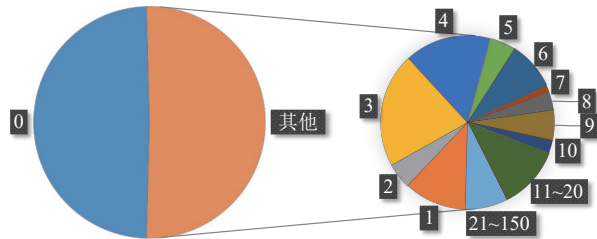


图 4 不同目标网站扫描数据编辑距离统计
Fig.4 Statistics of edit distance in scans of different target websites

标网站不同Web安全扫描器的非连续扫描中,对于DVWA目标网站的平均相同最大占比为35.0%,对于Webgoat目标网站平均有33.7%的请求特征是相同

的。而对于DVWA目标网站及Webgoat目标网站请求特征最小编辑距离的分布也主要分布在0~10之间。因此,不同Web安全扫描器扫描的请求特征集合具有相似性,且可预见基于已知Web安全扫描器训练得到的Web检测模型,用于未知Web安全扫描器的攻击检测仍具有良好的效果。

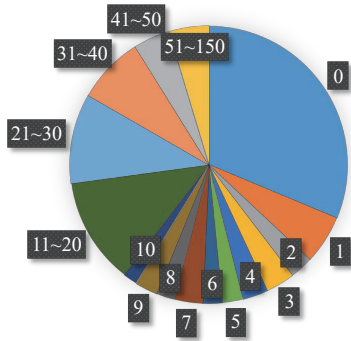


图 5 不同Web安全扫描器对DVWA应用扫描数据编辑距离统计
Fig.5 Statistics of edit distance in scans of the DVWA by different web security scanners

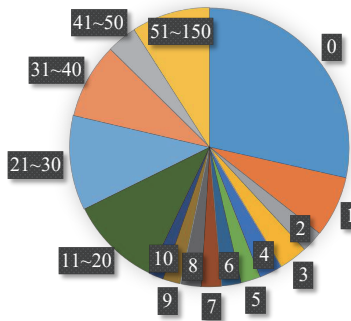


图 6 不同Web安全扫描器对Webgoat应用扫描数据编辑距离统计
Fig.6 Statistics of edit distance in scans of the Webgoat by different web security scanners

因此,Web安全扫描器在不同情形的扫描中,发送的请求数据具有相似性。Web安全扫描器的请求数据适合用于分类检测,且可预见基于已知扫描探测数据训练的攻击检测模型在同种扫描探测行为,及未知Web安全扫描器和不同的Web应用场景的扫描探测行为仍会有良好的攻击检测效果。

1.4 CharEmbedding-CGRU(M×N) 入侵检测方案

本文提出针对Web安全扫描器的网络入侵检测方案(CharEmbedding-CGRU(M×N)),包括基于字符嵌入的特征提取方法(CharEmbedding),以及一种卷积门控循环网络模型(CGRU(M×N))。其中,基于字符嵌入的特征提取方法分为3步,首先提取特征,然

表 5 不同Web安全扫描器对DVWA应用扫描, 相同特征数统计

Table 5 Statistical analysis of identical feature counts in scans of the DVWA by different web security scanners

扫描器	扫描器	相同特征数/个	最大占比
Nikto	ZAP	2 313	0.278
Nikto	扫描器A	626	0.050
Nikto	扫描器B	292	0.023
Nikto	扫描器C	370	0.029
ZAP	扫描器A	6 507	0.782
ZAP	扫描器B	4 942	0.594
ZAP	扫描器C	5 416	0.651
扫描器A	扫描器B	4 083	0.205
扫描器A	扫描器C	15 756	0.619
扫描器B	扫描器C	2 313	0.272
平均			0.350

表 6 不同Web安全扫描器对Webgoat应用扫描, 相同特征数统计

Table 6 Statistical analysis of identical feature counts in scans of the Webgoat by different web security scanners

扫描器	扫描器	相同特征数/个	最大占比
Nikto	ZAP	294	0.385
Nikto	扫描器A	492	0.039
Nikto	扫描器B	280	0.062
Nikto	扫描器C	354	0.028
ZAP	扫描器A	643	0.842
ZAP	扫描器B	239	0.313
ZAP	扫描器C	603	0.789
扫描器A	扫描器B	1 340	0.298
扫描器A	扫描器C	17 181	0.486
扫描器B	扫描器C	575	0.128
平均			0.337

后再对请求特征进行字符嵌入, 最后将3个连续的请求特征合并作为一个检测组合特征, 并将检测组合特征用于最后的分类检测。相比于词嵌入的特征提取方法(如word2vec等), 基于字符嵌入的请求特征提取方法无需对请求数据进行预训练, 降低了检测方案实际的应用难度。再者, 由于Web安全扫描器的运行是有序配合的, 基于多个请求合成的检测特征可以增强扫描请求数据的特征表现。

本文构建的不同形状卷积核的卷积门控循环网络模型(CGRU($M \times N$))结构如图7所示, 其中用 $M \times N$ 表示使用了不同形状的卷积核。CGRU模型由周桥等^[8]提出并用于Web攻击检测, 其探索了在卷积神经网络中使用GRU作为池化层在Web攻击检测中的优秀表现。为了进一步提升模型在Web安全扫描器的请求特征上进行分类检测的性能表现, 本文对

CGRU模型做了如下改进。首先, 使用5组不同形状的卷积核在组合检测特征上抽象提取特征, 同时采用GRU作为池化层, 实现在不改变请求特征序列关系的前提下保留重要特征。卷积神经网络中, 使用5组不同形状的卷积核可以从单个及多个请求的角度提取请求的重要特征。由于扫描检测特征是多组请求合并的融合特征, 相比于全部使用 $N \times N$ 的方形卷积核, 1×2 、 1×3 、 1×4 的长条形卷积核可以确保每个请求的特征被独立提取, 在特征提取时不改变单个请求的特征特点、不改变请求间的序列关系。

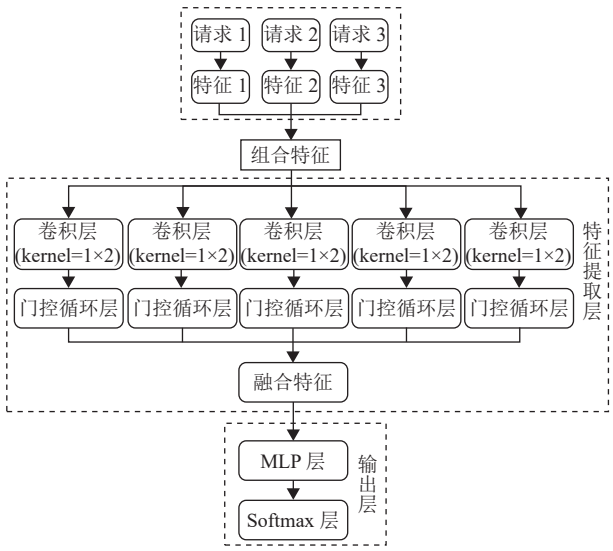


图 7 本文卷积门控循环网络模型结构
Fig.7 The CGRU($M \times N$) model structure

2 实验设计与结果分析

2.1 实验环境与数据集

本文入侵检测分类实验的开发环境为Intel Core i7-1255U CPU, 32 GiB RAM, NVIDIA GeForce MX570 GPU, Manjaro Linux 64位操作系统, 使用Pytorch深度学习库、Sklearn机器学习库等。实验采用上文中“扫描数据收集”章节描述的对DVWA Web应用的扫描探测数据作为恶意样本。经过实验对比, 模拟正常访问DVWA应用的请求数据较单一。为了模拟现实Web应用中业务请求的复杂程度、平衡实验中恶意样本与正常样本的数量, 从生产环境中的业务Web应用日志中提取了135 548条正常请求日志作为实验的正常样本。本文使用的数据样本数量如表7所示。

2.2 评估指标

在网络入侵检测的性能评估上, 常用的评价标

表 7 实验数据列表
Table 7 List of experimental data

数据类型	数据名称	请求数/条
恶意样本	开源扫描器数据集1	10 458
	开源扫描器数据集2	10 459
	商业扫描器数据集1	58 221
	商业扫描器数据集2	58 563
正常样本	业务请求数据集1	20 006
	业务请求数据集2	50 246
	业务请求数据集3	65 296

准有精确率(Precision)、召回率(Recall)和 F_1 值。然而,虚假的警报导致警报疲劳。在实际网络攻防过程中,检测模型即使 F_1 值性能再高,如果检测的误报数量过高,也会让防守方对检测结果失去信任。因此,本文新增使用万份误报数评价指标,旨在更灵敏、更直观地评价模型的准确性。本文最终使用的评价指标具体如下:

- (1) 精确率Precision: 用于表示模型的正确检出率,如式(3)所示。
- (2) 召回率Recall: 用于表示模型的检出率,如式(4)所示。
- (3) F_1 值: 用于表示模型的综合性能,如式(5)所示。
- (4) 万份误报数 $FP_{10\,000}$: 用于表示每检测1万份样本平均的误报数(False Positive),如式(6)所示。

$$Precision = \frac{TP}{TP + FP} \tag{3}$$

$$Recall = \frac{TP}{TP + FN} \tag{4}$$

$$F_1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{5}$$

$$FP_{10\,000} = \frac{FP}{TP + FP + TN + FN} \times 10\,000 \tag{6}$$

其中,TP表示恶意样本被正确预测为恶意样本的数目,FP表示正常样本被错误预测为恶意样本的数目,TN表示正常样本被正确预测为正常样本的数目,FN表示恶意样本被错误预测为正常样本的数目。

2.3 实验设计

为了验证面向Web安全扫描器的网络入侵检测方案的性能,本文通过设置不同的训练数据和测试数据分设两组实验,如表8所示。

其中,实验1旨在验证面向Web安全扫描器的入侵检测在连续扫描中的检测性能,以Web安全扫描

表 8 实验数据设置
Table 8 Experimental data setup

实验序号	训练数据集	测试数据集
实验1	开源扫描器数据集1	开源扫描器数据集2
	商业扫描器数据集1	商业扫描器数据集2
	业务请求数据集1	业务请求数据集3
	业务请求数据集2	
实验2	开源扫描器数据集1	商业扫描器数据集1
	开源扫描器数据集2	商业扫描器数据集2
	业务请求数据集1	业务请求数据集2
		业务请求数据集3

器第1次扫描的请求数据作为训练的恶意样本,以第2次扫描的请求数据作为测试的恶意样本。实验2旨在验证面向Web安全扫描器的入侵检测在未知Web安全扫描器扫描中的检测性能,以开源Web安全扫描器扫描的请求数据作为训练的恶意样本,商业Web安全扫描器扫描的请求数据作为测试样本。

为了验证所提出的CharEmbedding-CGRU($M \times N$)入侵检测方案的网络入侵检测效果,本文选择了多种机器学习模型及入侵检测方案进行了对比实验。作为不同模型的对照实验,基于提出的CharEmbedding特征提取方法,本文选取了传统机器学习方法的k近邻(k-Nearest Neighbors, KNN)、逻辑回归(Logistic Regression, LR)、支持向量机(Support Vector Machine, SVM)作为对比。针对 1×2 、 1×3 、 1×4 的长条形卷积核提升模型分类检测效果开展消融实验,使用 1×1 、 2×2 、 3×3 的方形卷积核替代本文卷积门控循环网络模型中 1×2 、 1×3 、 1×4 的长条形卷积核,构成对比模型CGRU($N \times N$)。针对门控循环单元作为池化层提升模型分类检测效果开展消融实验,使用去除池化层的网络模型CNN($M \times N$)作为对比模型,及使用MaxPooling作为池化层的网络模型CNN($M \times N$)-MaxPooling作为对比模型。作为已有基于漏洞利用特征的入侵检测对照组实验,选取了郭志民等^[28]提出的Transformer网络模型及周桥等^[8]提出的WordEmbedding-CGRU入侵检测方案作为对比。实验参数的设置对实验结果具有很大的影响,经过实验对比,深度学习模型训练参数设计如下:损失函数为交叉熵函数,训练epoch设置为30, batch size设置为128,优化器为Adam,学习率为0.001。

2.4 实验结果对比与分析

为了验证针对Web安全扫描器扫描数据进行网络入侵检测的有效性,在相同的实验环境下,将本文提出的CharEmbedding-CGRU($M \times N$)入侵检测方案

与其他入侵检测方案在设计的实验1、实验2中进行对比,最后在测试集上的预测结果如表9、表10所示。

表 9 实验1结果对比
Table 9 Comparative results of the experiment 1

入侵检测方案	精确率/%	召回率/%	F_1 值/%	万份误报数	误报总数(FP)/个
CharEmbedding-SVM	97.75	93.50	95.58	110.49	1 484
CharEmbedding-LR	99.18	94.31	96.68	40.13	539
CharEmbedding-Transformer ^[28]	99.50	97.03	98.25	24.80	333
WordEmbedding-CGRU ^[8]	99.51	96.88	98.18	21.67	291
CharEmbedding-CGRU($N \times N$)	99.61	97.10	98.34	19.29	259
CharEmbedding-KNN	99.74	93.34	96.43	12.73	171
CharEmbedding-CNN($M \times N$) -MaxPooling	99.84	96.63	98.21	8.04	108
CharEmbedding-CNN($M \times N$)	99.84	97.44	98.63	7.82	105
CharEmbedding-CGRU($M \times N$) (Ours)	99.87	98.12	98.99	6.55	88

表 10 实验2结果对比
Table 10 Comparative results of the experiment 2

入侵检测方案	精确率/%	召回率/%	F_1 值/%	万份误报数	误报总数(FP)/个
CharEmbedding-SVM	91.53	98.05	94.68	456.20	10 598
CharEmbedding-Transformer ^[28]	91.95	97.64	94.71	429.60	9 975
CharEmbedding-CGRU($N \times N$)	92.36	99.20	95.66	412.55	9 579
CharEmbedding-KNN	91.57	87.35	89.41	404.24	9 391
CharEmbedding-CNN($M \times N$)	92.52	98.98	95.64	402.21	9 339
CharEmbedding-CNN($M \times N$) -MaxPooling	92.50	97.03	94.71	395.62	9 186
CharEmbedding-LR	92.71	97.83	95.20	386.81	8 986
WordEmbedding-CGRU ^[8]	92.42	91.59	92.00	377.84	8 778
CharEmbedding-CGRU($M \times N$) (Ours)	92.98	98.60	95.71	374.09	8 686

Web安全扫描器在连续扫描中的请求数据具有相似性。为了验证针对Web安全扫描器扫描数据进行网络入侵检测对连续扫描的检测性能,本文开展了实验1。由表9可知,各检测方案在Web安全扫描器在连续扫描中都具有很好的指标,即针对Web安全扫描器的扫描请求数据进行入侵检测可以很好地发现已知的Web安全扫描器探测行为。对比方案CharEmbedding-SVM、CharEmbedding-LR、CharEmbedding-KNN,是为了说明本文提出的CharEmbedding特征提取方法具有很好的检测分类性能。本文提出的CharEmbedding-CGRU($M \times N$)入侵检测方案比已有研究文献[8]、[28]具有更好的分类检测效果。为了验证GRU池化层提取特征关联信息后的分类检测效果,与方案CharEmbedding-CNN($M \times N$)、CharEmbedding-CNN($M \times N$) -MaxPooling进行了对比。对比方案CharEmbedding-CGRU($N \times N$),是为了对比多种形状卷积核的卷积神经网络与 $N \times N$ 正方形卷积核的卷积神经网络的入侵检测效果。从表9中得知,本文CharEmbedding-CGRU($M \times N$)

入侵检测方案在Web安全扫描器连续扫描的入侵检测上具有更好的效果,检测精确率为99.87%、 F_1 值为98.99%、万份误报数为6.55。

Web安全扫描器在非连续扫描中的请求数据具有相似性。为了进一步验证基于Web安全扫描器扫描数据进行网络入侵检测对于未知Web安全扫描器的检测性能,本文开展了实验2。由表10可知,本文提出的CharEmbedding-CGRU($M \times N$)入侵检测方案相较于其他方案仍具有更好的检测效果,检测精确率为92.98%、 F_1 值为95.71%、万份误报数为374.09。

综上所述,在面向Web安全扫描器的网络入侵检测中,本文提出的CharEmbedding-CGRU($M \times N$)入侵检测方案相较于其他入侵检测方案具有更好的检测分类效果。

3 结束语

在网络攻击中,Web安全扫描器是攻击者重要的侦察工具,本文提出从Web安全扫描器扫描探测的角度检测Web攻击。首先,分析并验证了Web安全

扫描器扫描数据间的相似性。其次,提出了一种基于扫描数据的Web入侵检测方案,其中包括基于字符嵌入的特征提取方法以及一种卷积门控循环网络模型。该入侵检测方案利用所提出的特征提取方法提取请求特征,并将3个连续请求特征合成一个检测特征,再利用卷积门控循环网络模型进行Web入侵检测。在不同训练、测试集中的实验结果均表明,本文提出的Web入侵检测方案在各个指标上对Web安全扫描器攻击行为的检测都达到了预期效果,对已知Web安全扫描器的检测精确率是99.87%、 F_1 值为98.99%,对未知Web安全扫描器扫描数据的检测精确率为92.98%、 F_1 值为95.71%。

参考文献:

- [1] 邓淼磊, 阚雨培, 孙川川, 等. 基于深度学习的网络入侵检测系统综述[J]. 计算机应用, 2025, 45(2): 453-466.
DENG M L, KAN Y P, SUN C C, *et al.* Summary of network intrusion detection systems based on deep learning[J]. Journal of Computer Applications, 2025, 45(2): 453-466.
- [2] SEPCZUK M. Dynamic Web application firewall detection supported by cyber mimic defense approach[J]. Journal of Network and Computer Applications, 2023, 213: 103596.
- [3] GNIEWKOWSKI M, MACIEJEWSKI H, SURMACZ T R, *et al.* HTTP2vec: embedding of HTTP requests for detection of anomalous traffic[EB/OL]. arXiv: 2108.01763(2021-08-03) [2024-09-02]. <https://arxiv.org/abs/2108.01763>.
- [4] TEKEREK A. A novel architecture for Web-based attack detection using convolutional neural network[J]. Computers & Security, 2021, 100: 102096.
- [5] ZUECH R, HANCOCK J, KHOSHGOFTAAR T M. Detecting Web attacks using random undersampling and ensemble learners[J]. Journal of Big Data, 2021, 8(1): 1-20.
- [6] TOPRAK S, YAVUZ A G. Web application firewall based on anomaly detection using deep learning[J]. Acta Infologica, 2022, 6(2): 219-244.
- [7] 范禹辰, 刘相坤, 朱建生, 等. 基于BERT的服务网站Web攻击检测研究[J]. 计算机技术与发展, 2022, 32(8): 168-173.
FAN Y C, LIU X K, ZHU J S, *et al.* Research on Web attack detection of service website based on BERT[J]. Computer Technology and Development, 2022, 32(8): 168-173.
- [8] 周桥, 翟江涛, 龚东升, 等. 基于卷积门控循环神经网络的Web攻击检测方法[J]. 广西师范大学学报(自然科学版), 2023, 41(6): 51-61.
ZHOU Q, ZHAI J T, JIA D S, *et al.* A Web attack detection method based on convolutional gated recurrent neural network[J]. Journal of Guangxi Normal University (Natural Science Edition), 2023, 41(6): 51-61.
- [9] DAWADI B R, ADHIKARI B, SRIVASTAVA D K. Deep learning technique-enabled Web application firewall for the detection of Web attacks[J]. Sensors, 2023, 23(4): 2073.
- [10] 李道全, 刘旭寅, 刘嘉宇, 等. 结合Transformer的双向GRU入侵检测研究[J/OL]. 计算机工程与应用. <http://kns.cnki.net/kcms/detail/11.2127.TP.20240819.1043.010.html>.
LI D Q, LIU X Y, LIU J Y, *et al.* Intrusion detection research combining transformer and bidirectional GRU [J/OL]. Computer Engineering and Applications. <http://kns.cnki.net/kcms/detail/11.2127.TP.20240819.1043.010.html>.
- [11] 孙红哲, 王坚, 王鹏, 等. 基于Attention-BiTCN的网络入侵检测方法[J]. 信息安全, 2024, 24(2): 309-318.
SUN H Z, WANG J, WANG P, *et al.* Network intrusion detection method based on Attention-BiTCN[J]. Netinfo Security, 2024, 24(2): 309-318.
- [12] 张子迎, 陈玉炜, 王宇华. 基于XGBoost-DNN的工业控制系统入侵检测架构[J]. 哈尔滨工程大学学报, 2024, 45(11): 2243-2249.
ZHANG Z Y, CHEN Y W, WANG Y H. Intrusion detection architecture for ICS based on XGBoost-DNN[J]. Journal of Harbin Engineering University, 2024, 45(11): 2243-2249.
- [13] 金志刚, 刘凯, 武晓栋. 堆叠循环卷积和头部注意力的工业互联网入侵检测[J/OL]. 哈尔滨工业大学学报. <http://kns.cnki.net/kcms/detail/23.1235.t.20240622.1013.002.html>.
JIN Z G, LIU K, WU X D. Industrial internet intrusion detection integrating circular convolutional and head attention mechanism [J/OL]. Journal of Harbin Institute of Technology. <http://kns.cnki.net/kcms/detail/23.1235.t.20240622.1013.002.html>.
- [14] 陈虹, 程明佳, 金海波, 等. 融合对比学习和特征选择的入侵检测模型[J]. 信息安全研究, 2024, 10(5): 453-461.
CHEN H, CHENG M J, JIN H B, *et al.* Intrusion detection model incorporating contrastive learning and feature selection[J]. Journal of Information Security Research, 2024, 10(5): 453-461.
- [15] 龚星宇, 来源, 李娜, 等. 基于多尺度融合和时空特征的网络入侵检测模型[J]. 计算机工程与设计, 2024, 45(6): 1640-1646.
GONG X Y, LAI Y, LI N, *et al.* Network intrusion detection model based on multiscale fusion and spatial-temporal feature[J]. Computer Engineering and Design, 2024, 45(6): 1640-1646.
- [16] 刘涛, 蒙学强. 改进麻雀搜索算法的入侵检测特征选择[J]. 计算机工程与设计, 2024, 45(4): 989-996.
LIU T, MENG X Q. Feature selection of intrusion detection based on improved sparrow search algorithm[J]. Computer Engineering and Design, 2024, 45(4): 989-996.

- [17] BAO H F, LI W H, WANG X Y, *et al.* Payload level graph attention network for web attack traffic detection[C]//International Conference on Computational Science. Cham: Springer Nature Switzerland, 2023: 394-407.
- [18] 沈学利, 刘士枫. 基于图边缘特征注意力的入侵检测模型[J]. 计算机工程, 2024, 50(11): 236-245.
SHEN X L, LIU S F. Intrusion detection model based on graph edge feature attention[J]. Computer Engineering, 2024, 50(11): 236-245.
- [19] MAC H, TRUONG D, NGUYEN L, *et al.* Detecting attacks on Web applications using autoencoder[C]//Proceedings of the 9th International Symposium on Information and Communication Technology. New York: ACM, 2018: 416-421.
- [20] SEVRI M, KARACAN H. Two stage deep learning based stacked ensemble model for Web application security[J]. KSII Transactions on Internet and Information Systems (TIIS), 2022, 16(2): 632-657.
- [21] BENOVA L, HUDEC L. Comprehensive analysis and evaluation of anomalous user activity in Web server logs[J]. *Sensors*, 2024, 24(3): 746.
- [22] 尹兆良, 黄于欣, 余正涛. AE-EM: 一种期望最大化Web入侵检测算法[J]. 计算机工程与应用, 2025, 61(3): 315-325.
YIN Z L, HUANG Y X, YU Z T. AE-EM: a Web intrusion detection algorithm based on expectation maximization[J]. *Computer Engineering and Applications*, 2025, 61(3): 315-325.
- [23] JEMAL I, HADDAR M A, CHEIKHROUHOU O, *et al.* Performance evaluation of convolutional neural network for Web security[J]. *Computer Communications*, 2021, 175: 58-67.
- [24] CHEN H, CHEN J, CHEN J, *et al.* An automatic vulnerability scanner for Web applications[C]//2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Guangzhou: IEEE, 2020: 1519-1524.
- [25] 段鹏飞. 基于Web应用安全扫描器的设计与实现[D]. 兰州: 西北师范大学, 2021.
- [26] 郝子希. 基于渗透技术的Web应用漏洞扫描器设计与实现[D]. 上海: 东华大学, 2018.
- [27] 龙华秋, 周皓健, 燕紫君. Web漏洞扫描系统的设计与实现[J]. 现代信息科技, 2024, 8(12): 32-35.
LONG H Q, ZHOU H J, YAN Z J. Design and implementation of Web vulnerability scanning system[J]. *Modern Information Technology*, 2024, 8(12): 32-35.
- [28] 郭志民, 周劼英, 王丹, 等. 基于Transformer神经网络模型的网络入侵检测方法[J]. 重庆大学学报, 2021, 44(11): 81-88.
GUO Z M, ZHOU J Y, WANG D, *et al.* Network intrusion detection method based on Transformer neural network model[J]. *Journal of Chongqing University*, 2021, 44(11): 81-88.
- (责任编辑: 杨耀辉 英文审核: 费伦科)