引用格式:施凡,开少锋,钟瑶. 面向实网环境的漏洞指标体系构建和应用研究[J]. 信息对抗技术,2023, 2(2):39-53. [SHI Fan, KAI Shaofeng, ZHONG Yao. Construction and application of the vulnerability metric system for the realistic network environment[J]. Information Countermeasure Technology, 2023, 2(2):39-53.(in Chinese)]

面向实网环境的漏洞指标体系构建和应用研究

施 凡[1*],开少锋[1,2],钟 瑶[1]

(1. 国防科技大学电子对抗学院,安徽合肥 230037; 2. 31121 部队,江苏南京 210042)

摘 要 互联网上的网络资产数量庞大,环境复杂多变。然而,现有的评估指标无法全面地评估这些因素对漏洞产生的影响,从而影响评估结果的准确性。为了解决上述问题,构建了一种面向实网环境的漏洞指标体系,并将其应用到实际评估中。采用通用漏洞评分系统的基本指标作为静态指标,并利用预训练模型对漏洞描述文本进行静态分数的自动评估。同时,使用资产和环境因素作为动态指标,基于层次分析法计算各指标的权重,构建评估方程。在基于网络空间资源测绘平台数据计算动态分数的基础上,将其与静态分数结合,计算漏洞危害评分。所提出的面向实网环境的漏洞评估指标体系和基于网络空间资源测绘平台数据的漏洞评估方法,能够对漏洞的真实危害性进行评估,具有较高的评估准确性和较快的评估速度,因而具有良好的应用价值。

关键词 漏洞评估;层次分析法;通用漏洞评分系统;预训练模型

中图分类号 TP 393 **文章编号** 2097-163X(2023)02-0039-15

文献标志码 A **DOI** 10.12399/j.issn.2097-163x.2023.02.004

Construction and application of the vulnerability metric system for the realistic network environment

SHI Fan[1*], KAI Shaofeng[1,2], ZHONG Yao[1]

(1. College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China; 2. Unit 31121 of PLA, Nanjing 210042, China)

Abstract Currently, there is a vast number of network assets on the Internet, and the environment is complex and constantly changing. However, the existing evaluation metrics cannot comprehensively assess the impact of these factors on vulnerabilities, which will affect the accuracy of assessment results. To solve this problem, a vulnerability metric system was constructed for realistic network environment and applied to practical assessments. Specifically, the basic metrics of the common vulnerability scoring system were used as static metrics and pre-trained models were applied to automatically evaluate the static scores of vulnerability description texts. Meanwhile, asset and environmental factors were used as dynamic metrics and the method of analytic hierarchy process was used to calculate the weight of each metric and construct an evaluation equation. Based on the data calculated by the network space resource mapping platform for dynamic scoring and static scores, the vulnerability hazard score

收稿日期:2022-11-30 **修回日期**:2023-01-13

通信作者:施凡,E-mail:shifan17@nudt.edu.cn

基金项目:国家重点研发计划项目(2021YFB3100500)

was obtained . The proposed vulnerability assessment metric system for realistic network environments and the vulnerability assessment method based on network space resource mapping platform data can accurately assess the true hazard of vulnerabilities and have high accuracy, high speed and good application value as well.

Keywords vulnerability assessment; analytic hierarchy process; common vulnerability scoring system; pre-trained model

0 引言

近年来,通用漏洞评分系统(common vulnerability scoring system, CVSS)已成为评估漏洞危害性的主要方法。然而,CVSS 评估的漏洞危害性仅基于漏洞固有危害性,难以全面评估漏洞的真实危害性,这主要是由于指标体系不完善所致。当前使用的 CVSS 指标体系是一套理论性指标体系,构建过程中没有充分考虑指标值的获取等问题,导致机密性、完整性、可用性等指标难以评估,评估结果存在主观性等问题。同时,随着网络环境的不断复杂化和网络资产的增加,现有指标体系的适用范围有限,只能评估漏洞的理论危害性,无法真实评估漏洞的危害程度。因此,本文提出了漏洞"实际危害性"的概念,强调漏洞能否发挥危害性,不仅与其本身有关,也与漏洞的外部环境有关。CVSS 评分仅基于漏洞本身的特性,无法评估环境因素和网络资产因素的叠加影响。在实际应用过程中,一些漏洞虽然评分接近,但是其实际危害性却可能差异巨大。例如,Log4j 远程代码执行漏洞(CVE-2021-44228)和 CSZ CMS SQL 注入漏洞(CVE-2022-27165)的 CVSS 评分分别为 10 分和 9.8 分,但是 Log4j 在应用场景中的普及率高,全网使用量众多,受影响的资产数量多,因此其实际危害性远高于 CSZ CMS SQL 漏洞。这说明传统 CVSS 模型的科学性和合理性在此方面值得商榷。此外,CVSS 的基本指标组主观性强,部分指标值无法准确获取,人工判定指标值时存在不确定性。因此,研究如何准确评估漏洞的实际危害性,并以客观便捷的方式获取指标值,是当前网络安全领域亟待解决的问题。

针对上述问题,本文提出了一种面向实网环境的指标体系,通过引入资产维度和环境维度指标作为实网环境指标,以 CVSS 基本指标作为静态指标;同时,改进评估方法,使用 DistilBERT 模型进行静态评估分数预测,以自研的网络空间资源测绘平台为支撑,实现自动化获取数据,解决了指标值获取难的问题。基于以上 2 种手段,有效获取了漏洞的静态评分和动态评分,从而实现了漏洞真实危害性的评估。

1 相关介绍

1.1 相关研究

网络安全领域的漏洞危害等级评估方法主要包括基于指标、基于模型和基于关联关系的评估方法。目前,基于指标的评估方法是主要研究方向,其研究主要集中于改进现有指标体系[1-6]和权重计算方式[7-16]。然而,基于指标的方法存在过于依赖领域知识的问题,从而限制了其自身的发展。相比之下,基于机器学习的漏洞评估方法则可以在大量数据中发现漏洞共有的特征,形成基于机器学习的模型,具有扩展性和易用性的优势。目前,针对漏洞评估的机器学习研究既有基于传统机器学习的方法,如 K-means、决策树、SVM 等[17-18],也有基于深度学习的方法[19-21],或使用自然语言处理相关技术进行漏洞描述信息的分析[22-26]。

然而,漏洞不是孤立存在的,它和存在的环境密切关联,同时漏洞和依赖环境上的其他漏洞也具有关联性。当前针对漏洞关联性的研究主要是在增加关联性指标或考虑漏洞前序、后序节点的关联关系的基础上进行关联评估[27-28]。漏洞的前后关联关系主要有链式结构、树形结构、图式结构,相应的便有基于攻击链、攻击树和攻击图的漏洞评估研究,其中以攻击图研究居多。

分析上述研究可以发现,当前针对网络资产、网络环境等因素对漏洞危害等级影响的研究还不多,从资产关联性视角开展的研究也不多。因此,本文旨在从资产、环境等动态视角出发,结合静态视角对漏洞危害等级进行评估。具体而言,将分别从漏洞基本属性、资产属性和环境属

性 3 个方面入手，构建适合网络安全实际需求的漏洞危害等级评估模型，为网络安全保障提供技术支持。

1.2　通用漏洞评分系统

通用漏洞评分系统[29-30]是由事件响应和安全团队论坛(forum of incident response and security teams，FIRST)开发并维护的一个开放式框架，旨在通过一套量化指标来描述软件漏洞的特征和严重程度，并帮助确定漏洞修复或缓解的优先级。CVSS 由 3 个指标组组成：基本指标组、时间指标组和环境指标组。其中，基本指标组表示随时间和跨用户环境而保持不变的漏洞固有属性，并生成 0～10 分之间的分数来反映漏洞危害程度。本文主要关注基本指标组，将在下文对其进行详细阐述。CVSS 3.1 版本是目前最新发布并被广泛采用的版本，其基本指标组包含 8 个指标，每个指标有若干取值选项，并对每个选项赋予一个数值权重。表 1 列出了 CVSS 3.1 基本指标组各指标及其取值范围以及矢量字符串表示法。以下是对各指标含义的简要说明：

1) 攻击向量。攻击向量指标描述了成功利用漏洞所使用的攻击发起方式，主要包含网络、相邻、本地和物理 4 种方式。一般来说，通过网络访问进行漏洞利用最容易，而通过物理访问路径利用漏洞最困难。

2) 攻击复杂度。攻击复杂度指标描述了为了利用此漏洞而必须存在的某些前提条件，这些条件可能需要攻击者收集目标的更多信息。需要注意的是，对此指标的评估并不包括为了利用漏洞而进行的任何用户交互的需求。如果攻击成功需要特定的配置，则应将此配置作为攻击复杂度指标并进行评分，攻击复杂度越低，则此项的基本得分越高。

3) 权限要求。权限要求指标描述了在成功利用漏洞之前必须拥有的权限级别。权限需求级别越低，漏洞越容易被利用。

4) 用户交互。用户交互指标描述了除攻击者外，想要成功攻击易受攻击组件所需的其他用户参与攻击活动的要求。此指标决定了攻击者利用此漏洞是否需要一个单独的用户(或用户启动的进程)以某种方式参与。

5) 范围。范围指标描述了漏洞对系统安全范围的影响。当漏洞的影响超出安全/信任边界并影响易受攻击组件所在的安全范围之外的组件时，就会发生范围更改。范围指标可以衡量漏洞对系统安全的整体影响。

6) 机密性。机密性指标衡量了漏洞利用对系统中管理的信息资源的机密性影响。机密性是指将信息访问和披露仅限于授权用户，以防止未经授权的用户访问或披露信息。机密性指标可以衡量漏洞对信息保密性的影响。

7) 完整性。完整性指标衡量了漏洞利用对信息的可信度和准确性的影响。完整性是指信息的完整性和准确性。当漏洞影响信息的完整性时，此项指标的分数会相应增加。完整性指标可以衡量漏洞对信息准确性和完整性的影响。

8) 可用性。可用性指标衡量了漏洞利用对系统受影响组件的可用性的影响。当漏洞导致组件无法访问或使用时，此项指标的分数会相应增加。可用性指标可以衡量漏洞对系统可用性的影响。

表 1　CVSS 3.1 基本指标及其字符含义

Tab.1　Basic metric group and character meaning in CVSS 3.1

指标	指标值
攻击向量	physical(P)/local(L)/network(N)/adjacent(A)
攻击复杂度	low(L)/high(H)
权限要求	none(N)/low(L)/high(H)
用户交互	required(R)/none(N)
范围	unchanged(U)/changed(C)
机密性	none(N)/low(L)/high(H)
完整性	none(N)/low(L)/high(H)
可用性	none(N)/low(L)/high(H)

2　面向实网环境的漏洞评估方法构建

2.1　指标体系构建流程

为建立一个全面的漏洞评估指标体系，本文进行了多方面的调研和专家评估。在研究过程中，参考了多个标准和规范，包括《CNNVD 漏洞分级规范》《NVD 漏洞评级规范》《STIX 2.1 威胁情报规范》以及《网络安全漏洞分类分级指南》(GB/T 30279—2020)。基于这些标准和规范，结合专家评估，筛选出了 57 个漏洞评估影响因素，涉及 10 个维度。指标选取的过程如图 1 所示。

为了确保选取的指标能够较好地解决现有

问题并具有较低的冗余性，在进行多轮专家调研、厂家走访和语义降维等工作的基础上，最终确定了一个包含 13 个指标的指标体系，涉及 3 个维度。

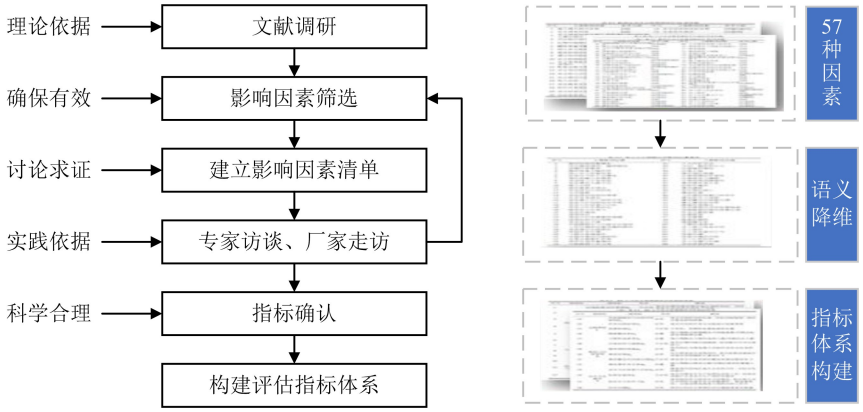


图 1 指标选取流程

Fig. 1 Metric selection process

2.2 静态指标体系构建

CVSS 是一种被广泛用于评估漏洞固有危害性的方法，为了利用 CVSS 的优势，选取了 CVSS 基本指标组作为静态指标。CVSS 基本指标组包含了 8 个指标，分别为攻击向量、攻击复杂度、权限要求、用户交互、范围、机密性、完整性、可用性，可以较为全面地描述漏洞的危害性，从而帮助安全专家和研究人员进行漏洞评估和风险管理。选取 CVSS 基本指标组作为静态指标，旨在提高漏洞评估的准确性和全面性，为网络安全领域的研究和实践提供更为可靠的指导和支持。

2.3 动态指标体系构建

当前互联网环境处于不断变化之中，传统静态指标评估方法已无法准确反映漏洞的动态危害性，因此提出一种面向实网环境的漏洞评估方法。该方法在 CVSS 基本指标的基础上，从资产和环境 2 个视角出发，结合静态指标，构建面向实网环境的指标体系，以反映漏洞危害性的时效性和准确性。

随着互联网的发展，网络资产的类型越来越多，除了传统意义上连接到互联网的主机、服务器、路由器、交换机、防火墙等硬件设备外，还包括域名、社交账号等虚拟资产[31-32]。这些资产一旦被攻击者控制，将带来严重的安全风险和损失。因此，本文将网络资产定义为连接到互联网的硬件设备以及以这些设备为载体的数据资源的合集。

2.3.1 资产维度

采用自研的网络空间资源测绘平台以及现有数据，用以下 3 个指标来分析漏洞对资产所造成的影响，从而评估其危害性。这 3 个指标分别是：受影响资产总量、受影响重要资产总量以及受影响关联资产总量。其中，受影响资产总量反映了漏洞攻击面的大小，受影响重要资产总量反映了漏洞攻击的目标价值，受影响关联资产总量反映了漏洞攻击的影响范围。通过综合分析这 3 个指标，可以较为准确地评估漏洞的危害性。

与传统指标评估方法相比，该方法更具有时效性和准确性，能够快速反映漏洞对网络资产的危害，为网络安全防御提供有力支撑。

2.3.1.1 受影响资产总量

受影响资产总量是一个重要的漏洞影响度量指标，它反映了漏洞对重点保护区域互联网资产的影响。使用自研的网络空间资源测绘平台，对漏洞影响的资产总量进行统计分析，结果显示，受漏洞影响资产数量在 2 000 以下的占总数的 30.76%，2 000 ～ 15 000 之间的占总数的 34.62%，15 000 以上的占总数的 34.62%。图 2 给出了相关统计结果。基于这些结果，本文将受影响资产数量划分为 3 个等级，即“少”“中等”和“多”。具体而言，受影响资产数量在 2 000 以下的定义为“少”，2 000～15 000 之间的定义为“中等”，15 000 以上的定义为“多”。这个指标可以用来评估漏洞的危害程度，如果漏洞影响的资产数量越多，则漏洞危害等级越高。值得注意的是，出于安全考虑，这里没有公开漏洞的具体信息，只展示了漏洞编号和受影响资产数量的统计数据。

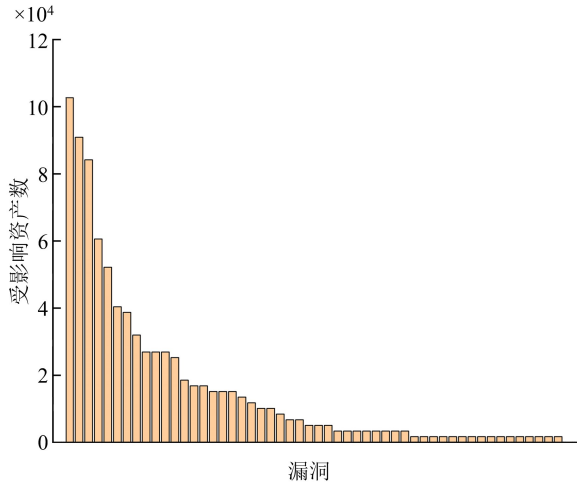


图 2　网络空间资源测绘平台受漏洞影响的资产分布情况

Fig. 2　Distribution of assets affected by vulnerabilities in the cyberspace resource mapping platform

2.3.1.2　受影响重要资产总量

受影响重要资产总量是指在重要区域内，受漏洞影响的重要资产总数量。该指标反映了漏洞影响的广度和深度。重要资产总量数据来源于自研的网络空间资源测绘平台，该平台定义了 4 类重要资产。首先是重点行业的资产，如政务、能源、交通、金融等，因为这些行业涉及国家经济发展命脉，需要重点保护；其次是重点区域的资产，如北京、上海等大城市，这些城市分别承担国家政治和经济中心的功能，需要重点保护，因此也属于重要资产；第三是需要重点保护目标的资产，例如举办冬奥会期间各类场馆及其网站等保护目标；第四是高价值资产，例如 Alexa 综合排名靠前的网站，由于此类网站价值度高，一旦被控制，也将带来很强的危害性，因此也属于重要资产。以上资产不重复计算，例如某资产既是重点行业的资产，又是重要区域的资产，则只按单条资产计算。对平台现有数据进行统计，结果如图 3 所示。根据统计数据，不受漏洞影响的重要资产达到了 90%。受漏洞影响的重要资产数量在 5 000 以下占 3.33%，受漏洞影响资产数量在 5 000～15 000 的占 3.33%，受漏洞影响资产数量在 15 000 以上的占 3.33%。根据上述统计结果，将资产总量分为 4 个量级，其中，未受影响的重要资产定义为“无”，受影响重要资产数量在 5 000 以下的定义为“少”，受影响重要资产数量在 5 000～15 000 的定义为“中等”，受影响重要资产数量在 15 000 以上的定义为“多”。根据实际评估任务的需要，可以给出不同行业、区域、保护目标的重要资产情况。

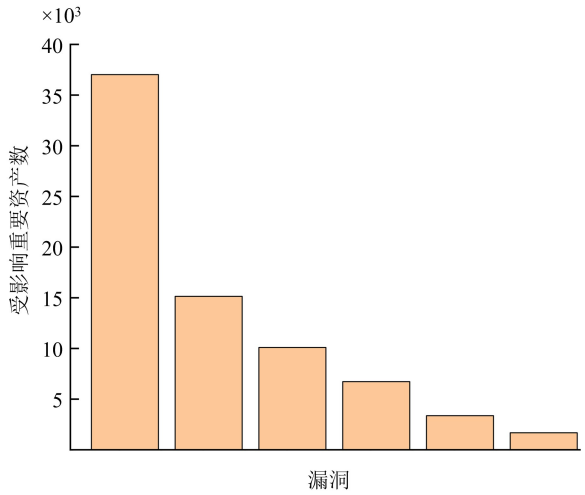


图 3　网络空间资源测绘平台受漏洞影响的重要资产分布情况

Fig. 3　Distribution of important assets affected by vulnerabilities in the cyberspace resource mapping platform

2.3.1.3　受影响关联资产总量

漏洞关联资产总量反映了漏洞可能对资产造成的潜在影响。漏洞不仅会直接影响到其所处资产，还会通过横向攻击间接影响到与之关联的其他资产。将这种关联关系分为 3 类：外链资产、同 C 段资产以及同域名或 IP 的不同服务或网站。这些资产不包括重复计算。通过对平台现有数据的统计，发现受影响的资产中，无关联资产的情况占据 58.33%。同时，受漏洞影响的关联资产数量在 5 000 以下的情况占据总数的 16.67%，在 5 000～20 000 的情况占据总数的 13.33%，在 20 000 以上的情况占据总数的 11.67%，受漏洞影响的关联资产分布情况如图 4 所示。基于这些统计结果，可以将资产总量分为 4 个量级。其中，没有关联资产的定义为“无”，受影响关联资产数量 5 000 以下的定义为“少”，5 000～20 000 的定义为“中等”，20 000 以上的定义为“多”。

值得注意的是，漏洞关联资产总量是一个重要的指标，它可以帮助企业评估漏洞的影响和优先级。在漏洞评估过程中，评估人员应该考虑资产之间的关联性，以确定漏洞可能会对哪些资产造成影响。同时，企业也应该采取相应的措施来减少漏洞带来的风险，例如加强网络隔离、限制权限、以及及时修补漏洞等。

2.3.2　环境维度

网络环境分为内网和外网 2 种类型，内网包

括软件、硬件和连接关系等基本组成部分。网络环境通常具有高度复杂性。然而，在没有权限的情况下，网络空间资源测绘平台无法准确地测绘内网环境。因此，本文从攻防角度出发，提出了利用代码成熟度和漏洞补丁成熟度这 2 个指标来评估网络环境的安全性。

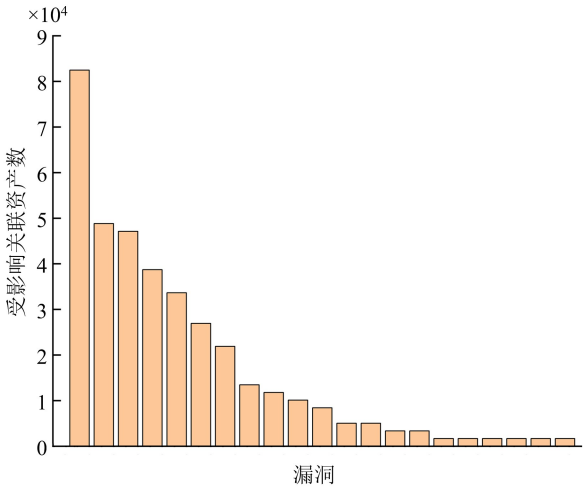


图 4 网络空间资源测绘平台受漏洞影响的关联资产分布情况

Fig. 4 Distribution of related assets affected by vulnerabilities in the cyberspace resource mapping platform

当漏洞被披露后，如果攻击利用代码出现，则漏洞所处的网络环境将不再安全，相应漏洞的危害性也会提高。然而，漏洞补丁的出现可以为漏洞所处的环境带来保障，相应漏洞的危害性也会降低。本文将漏洞补丁成熟度和利用代码成熟度作为环境维度指标使用，认为它们是漏洞可利用性的体现，影响漏洞所处的环境因素。这 2 个指标的含义与 CVSS 3.1 的 Remediation Level、Exploit Code Maturity 等指标类似，但 CVSS 3.1 将这 2 个指标作为时间指标。本文中，这 2 个指标的值来自网络空间资源测绘系统，数据来源方便，加快了评估速度，可以为网络环境的安全性评估提供重要参考，并且适用于内网环境。这些指标的使用可以帮助网络拥有者更好地评估网络环境，进一步提高网络的安全性。

2.3.2.1 利用代码成熟度

漏洞的利用程度决定了其危害的程度。当漏洞具备被利用的条件时，例如，当漏洞出现 POC 时，说明漏洞已经可以被利用；当漏洞出现 EXP 时，说明漏洞可以被利用且成熟度更高；当漏洞出现自动化利用工具时，说明漏洞已经可以被大规模利用，其危害性最大。基于此，将利用代码成熟度指标分为 4 类：无利用代码、存在 POC、存在 EXP 以及存在利用工具。

2.3.2.2 漏洞补丁成熟度

漏洞补丁成熟度也是评估漏洞危害的重要指标。不同类型的漏洞需要不同的修复措施，官方正式补丁和临时补丁是 2 种常见的补丁类型。一些漏洞由于危害级别高、修复难度大，在厂商发布官方正式补丁之前可能会出现临时补丁或第三方补丁。但对于一些危害性低或修复难度大的漏洞，可能会存在较长时间没有补丁的情况。因此，将漏洞补丁成熟度指标分为 3 类：官方补丁、临时补丁和无补丁。

这些动态指标的取值来源于网络空间资源测绘系统，该系统服务器可以对重要区域资产进行实时测绘，并且及时更新数据。此外，还可以根据评估任务重要性，实时抓取数据进行分析。

2.4 评估方法构建

基于前文构建的指标体系，结合预训练模型和层次分析法，对漏洞进行指标预测和评级。由于人工评估的时效性不高，利用预训练模型对漏洞描述文本进行自动化预测，提高了漏洞评估的效率和准确性。同时，为了更好地研究网络资产和实际环境因素对漏洞危害等级评估的影响，构建了面向实网环境的指标体系，并利用层次分析法确定了各指标的权重，从而使评估结果更加科学准确。最终，使用加权公式计算漏洞的最终评分，提供了一种快速有效的漏洞评估方法。

2.4.1 基于预训练模型的静态分数计算

作为当前广泛的漏洞评估方法，CVSS 的科学性已得到实践检验。为了与 CVSS 兼容，静态指标采用了 CVSS 基本指标组的指标。然而，基本指标组的某些指标存在主观性强、难以人工评估等问题，从而导致评估不及时。为此，使用预训练模型，基于漏洞描述文本预测漏洞危害等级，并将此预测作为静态评分，以提高评估速度。该模型能够在不损失太多准确率的情况下提高评估速度，并且为预测漏洞危害等级的静态分数提供了一种新的评估模型。

在选择机器学习模型时，考虑到多种因素，包括性能、速度、资源消耗以及可部署性。对比

多个预训练模型，发现 DistilBERT 在预测精度相近的情况下，可以在保持较高性能的同时具有较低的资源消耗和较快的速度，因此参数更少、预测更快。事实上，DistilBERT 的参数只有 BERT 的 40%，但速度却快了 60%，性能仍可达到原模型的 97%。因此，在漏洞危害等级预测中，DistilBERT 是一个较优的选择。

2.4.1.1　模型结构概述

基于 DistilBERT 模型构造漏洞危害等级预测模型，预测任务主要由迁移学习和预测应用 2 个阶段组成，模型结构如图 5 所示。预测过程包括 3 个步骤，即词元化、词元嵌入和数值预测。图 5 显示了这些步骤的顺序关系。在词元化步骤中，通过词元化算法将漏洞描述文本拆分为多个词元；在词元嵌入步骤，将词元化的词元放入微调后的预训练模型中；微调后的预训练模型在第 $l(l=1,2,\cdots,L)$ 层的输出是本层的词元嵌入，其中，L 是 DistilBERT 中传输层的总数。最后，将单个全连接层用于预测漏洞危害等级的可能性。

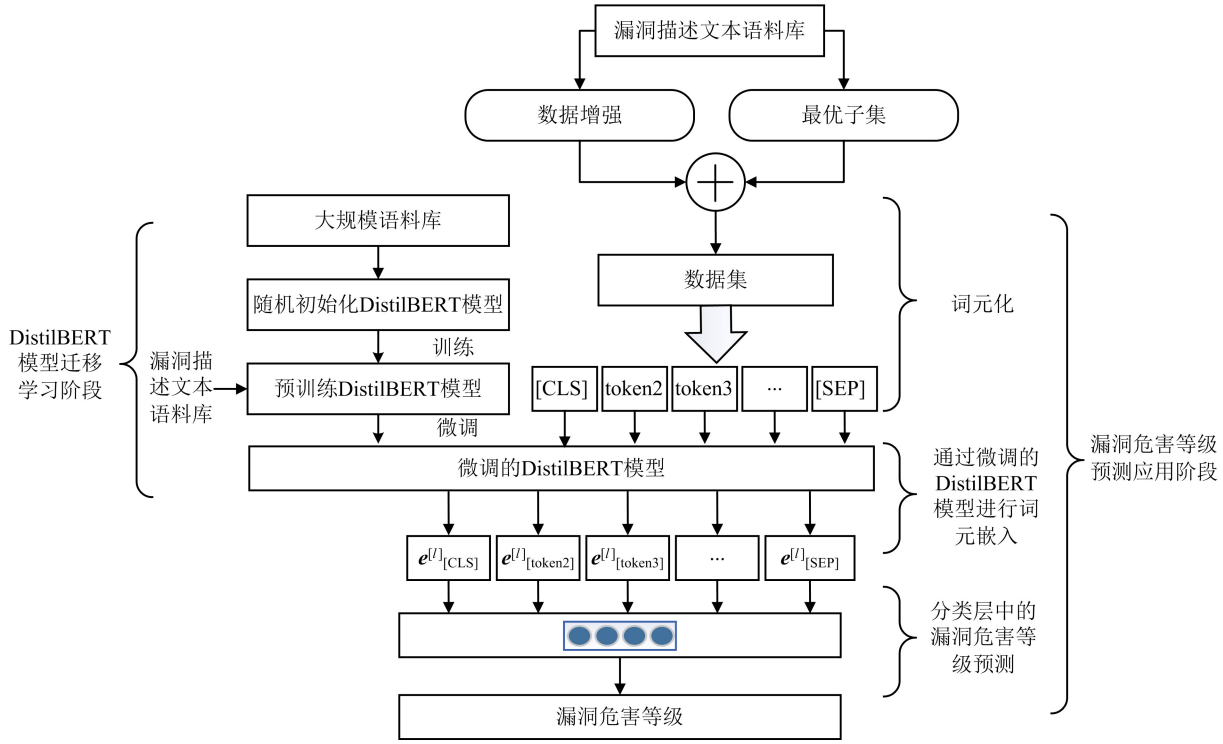


图 5　漏洞危害等级预测模型框架

Fig. 5　Model framework of vulnerability hazard level prediction

2.4.1.2　输入层设计

模型的输入为漏洞描述文本，在此过程中设定描述文本 $\boldsymbol{X}=[V_1,V_2,\cdots,V_n]$ 被表征为词元序列 $\boldsymbol{T}=[\boldsymbol{t}^{(1)},\boldsymbol{t}^{(2)},\cdots,\boldsymbol{t}^{(n)}]$，其中，$\boldsymbol{t}^{(i)}=[t_1,t_2,\cdots,t_k]$ 是从描述 V_i 中表征得到的词元序列；k 是预先设置的词元的最大序列长度。符号 t_j 表示从描述文本 V_i 表征得到的第 j 个词元，其中，$i\in\{1,2,\cdots,n\}$，$j\in\{1,2,\cdots,k\}$。又因为漏洞描述文本存在数据不平衡现象，直接用于训练任务会导致模型鲁棒性不强，为此，用于漏洞危害等级预测的数据经过了最优子集融入和数据增强，从而提高了数据的信息量，解决了漏洞危害等级标签存在不平衡的问题。

2.4.1.3　特征提取层设计

词元化的输出是词元嵌入的输入，当输入一个词元序列 $\boldsymbol{t}$ 时，微调后的预训练模型将通过不同的传输层输出不同级别的词元嵌入。例如，从微调的预训练模型中提取的第 l 层的词元嵌入表示为：

$$\boldsymbol{e}^{[l]}=f_{\text{fine-tuned model}}(\Theta_{\text{fine-tuned model}},\boldsymbol{t}) \tag{1}$$

$\boldsymbol{t}=[t_1,t_2,\cdots,t_k]$ 是一个有 k 个词元的词元序列，$\boldsymbol{e}^{[l]}=[e_1^{[l]},e_2^{[l]},\cdots,e_n^{[l]}]$ 是从微调的预训练模型中提取的相应第 l 层的词元嵌入。$e_i^{[l]}$ 是第 i 个词元 t_i 的第 l 层词元嵌入，$e_i^{[l]}\in\mathbb{R}^{H^{[l]}_{\text{pre-trained model}}}$，其中，$H^{[l]}_{\text{pre-trained model}}$ 是预训练模型的第 l 层隐层大小[33]。

2.4.1.4 输出层设计

针对漏洞危害等级预测任务，将单个全连接层用于预测最终的漏洞危害等级，输出包含 4 个神经元，分别对应 4 个漏洞危害等级，使用 Softmax 函数计算 4 个神经元的概率，其概率之和为 1，将最大的概率作为输出。输出层的结构如图 6 所示。

模型的计算公式表示为：

$$y=\mathrm{Softmax}(\boldsymbol{W}^k\boldsymbol{e}^{[L]}+\boldsymbol{b}^k) \tag{2}$$

式中，y 为分类概率，$\boldsymbol{W}^k$ 为分类器的权重矩阵，$\boldsymbol{e}^{[L]}$ 为词元嵌入的输入数据，$\boldsymbol{b}^k$ 为分类器的偏置向量，Softmax 函数是常用的归一化函数。

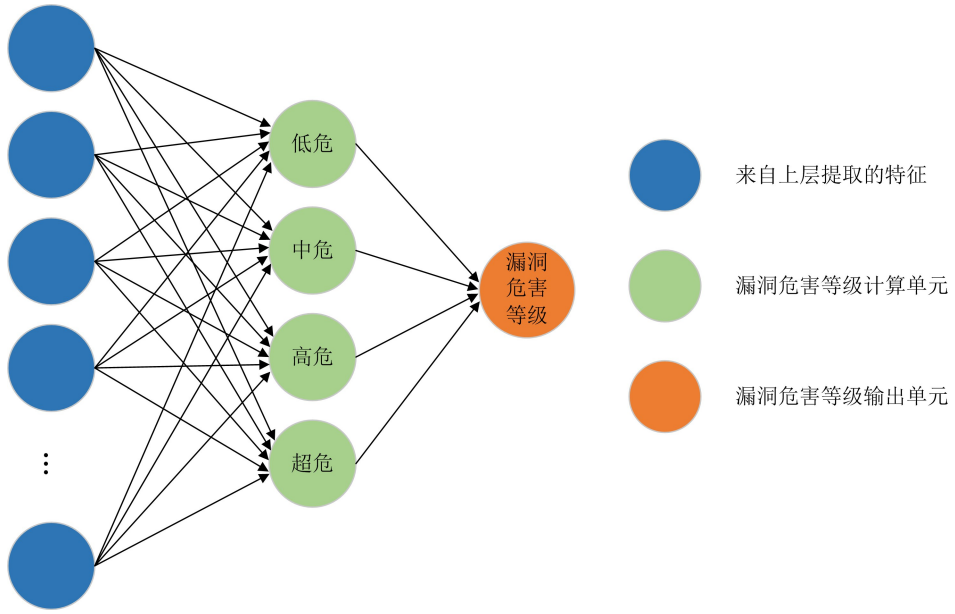


图 6 漏洞危害等级预测模型输出层结构

Fig. 6 Prediction model of the output layer structure of vulnerability hazard level

2.4.1.5 模型效果分析

使用美国国家漏洞库(national vulnerability database，NVD)的相关数据，包含了 1999—2022 年 9 月间发布的所有安全漏洞。漏洞描述信息被用作数据集的文本项，漏洞的危害等级被处理为标签项。数据集中有 4 种类型的标签，分别对应漏洞的 4 种严重程度，即超危、高危、中危、低危。数据集包含 105 984 个漏洞样本，按 85%∶15% 的比例分为训练集和测试集。

从 Accuracy(A_{Acc})、Precision(P_{Pre})、Recall(R_{Rec})、F_1 4 个方面将本文模型效果与其他相似工作的结果[21,23,34-37]进行了比较。其他工作的结果均来自原始论文。对比结果如表 2 所列，可以看出，预测模型在 Accuracy、Precision、Recall、F_1 方面提高了漏洞危害等级预测的性能。

2.4.2 基于层次分析法的动态分数计算

本文采用层次分析法构建了一种面向实网环境的漏洞评估方法。层次分析法兼具定量评估和定性评估的优点。该方法首先将评估目标逐层分解，然后根据各因素的影响和关联建立层次模型，并比较各层因素的重要性，从而较好地量化评估目标[38]。

2.4.2.1 层次分析模型构建

提出的漏洞评估方法采用层次分析法构建层次模型，将目标层、维度层和指标层 3 个层次分别划分，从而逐步深入分析可能影响漏洞危害等级的因素。其中，最上层为目标层，即最终漏洞危害等级的决策因素；中间层为维度层，包括 3 个维度，即基本维度、资产维度和环境维度；最下层为指标层，每个维度包含若干指标，每个指标又包含若干指标值。所提模型能够很好地结合定量评估和定性评估的优势，通过逐层分解目标，建立层次模型，比较各层因素的两两重要性，从而较好地量化需要评估的目标。值得注意的是，漏洞评估往往受到评估专家的主观经验的影响，为了减少这种偶然因素对评估结果的影响，采用群决策的方法进行漏洞评估，共邀请了 5 位专家参与权重评估工作。漏洞评估方法的相关层次结构及指标如表 3 所列。

表 2　与相似研究的结果比较

Tab. 2　Comparison of results with similar studies

方法	特征提取方法	分类器	A_{Acc}(%)	P_{Pre}(%)	R_{Rec}(%)	F_1(%)
文献[34]	词频-逆文档频率	Fuzzy system	88.37	/	/	/
		Decision Tree	79.12	75.54	71.26	73.02
文献[23]	文档-词项矩阵	Neural Network	78.26	73.59	70.24	71.68
		SVM	79.53	78.49	68.21	71.50
文献[35]	独热编码	CNN	72.50	/	/	/
文献[36]	特征向量	PCA+XGBOOST	92.38	/	/	/
文献[21]	词嵌入	1-layer CNN	81.60	81.80	81.50	81.60
文献[37]	文本挖掘	XGBoost	87.30	/	/	/
		CNN	92.04	/	/	/
		LSTM	93.73	/	/	/
		TextRCNN	93.95	/	/	/
本文模型	进行数据增强的微调模型	Linear	90.64	91.92	91.92	91.83
	融合最优子集的微调模型	Linear	92.80	88.32	87.26	87.07
	结合最优子集和数据增强的微调模型	Linear	96.62	97.11	97.06	97.05

表 3　层次分析模型包含的要素

Tab. 3　The elements included in the AHP model

决策层	维度层	指标层	指标值
漏洞危害等级(A)	基本维度(B_1)	C_{11} 攻击向量	网络(N)/相邻网络(A)/本地(L)/物理(P)
		C_{12} 攻击复杂度	低(L)/高(H)
		C_{13} 所需特权	无(N)/低(L)/高(H)
		C_{14} 用户交互	无(N)/必须(R)
		C_{15} 范围	未更改(U)/已更改(C)
		C_{16} 保密性	无(N)/低(L)/高(H)
		C_{17} 完整性	无(N)/低(L)/高(H)
		C_{18} 可用性	无(N)/低(L)/高(H)
	资产维度(B_2)	C_{21} 受影响资产总量	少(L)/中等(M)/多(G)
		C_{22} 受影响重要资产总量	无(N)/少(L)/中等(M)/多(G)
		C_{23} 受影响关联资产总量	无(N)/少(L)/中等(M)/多(G)
	环境维度(B_3)	C_{31} 利用代码成熟度	无(N)/存在 POC(P)/存在 EXP(E)/存在利用工具(T)
		C_{32} 漏洞补丁成熟度	无(N)/临时补丁(T)/官方补丁(O)

2.4.2.2　构造判断矩阵

采用问卷调查的方式,以收集专家对各层级指标的评估结果。针对专家的判断矩阵,进行一致性检查,调整不符合逻辑的判断,最后使用加权方式生成了最终的判断矩阵。其中,一致性检查是评估专家意见一致性的过程,可以有效减少

评估误差，提高评估结果的可信度。判断矩阵加权方式是指在确定各层级指标的权重时，根据专家的评估结果以及其对应的重要性，对不同专家的意见进行加权处理，以确保各位专家的意见得到充分的体现。通过问卷调查的形式和一致性检查的过程，结合加权方式生成最终的判断矩阵。

2.4.2.3 权重计算

使用和积法对相关的判断矩阵进行最终求和，设维度层的指标集合为 $B_i(i=1,2,3)$，其权重为 $\boldsymbol{W}=[w_1,w_2,w_3]^{\mathrm{T}}$，指标层资产维度和环境维度的指标集合为 $C_{ij}(i=2,j=1,2,3;i=3,j=1,2)$，其权重分别是 $\boldsymbol{W}_1=[w_{21},w_{22},w_{23}]^{\mathrm{T}}$，$\boldsymbol{W}_2=[w_{31},w_{32}]^{\mathrm{T}}$。虽然每个指标值从定性角度分析，其重要度是显而易见的，但具体应该给每个指标值赋多少分值却不容易确定，这里采用层次分析法对每个指标下属的指标值进行两两重要性比较以确定各个指标值的权重，设指标值层各指标值的集合为 $C_{ijk}(i=2,j=1,k=1,2,3;i=2,j=2,k=1,2,3,4;i=2,j=3,k=1,2,3,4;i=3,j=1,k=1,2,3,4;i=3,j=2,k=1,2,3)$，其权重表示为：

$$\boldsymbol{W}_{11}=[w_{211},w_{212},w_{213}]^{\mathrm{T}}$$

$$\boldsymbol{W}_{12}=[w_{221},w_{222},w_{223},w_{224}]^{\mathrm{T}}$$

$$\boldsymbol{W}_{13}=[w_{231},w_{232},w_{233},w_{234}]^{\mathrm{T}}$$

$$\boldsymbol{W}_{21}=[w_{311},w_{312},w_{313},w_{314}]^{\mathrm{T}}$$

$$\boldsymbol{W}_{22}=[w_{321},w_{322},w_{323}]^{\mathrm{T}}$$

同时，将每个指标值赋值 100 分，并将各个指标值单排序的权重乘以 100 作为每个指标值的最终赋分，将每个维度下的指标的层次单排序的权重作为每个指标的权重，将每个维度的权重作为维度重要度参与最终的漏洞危害等级计算。对各个专家的判断矩阵进行计算后，再进行算数平均，得到 $\boldsymbol{W}$、$\boldsymbol{W}_1$、$\boldsymbol{W}_2$、$\boldsymbol{W}_{11}$、$\boldsymbol{W}_{12}$、$\boldsymbol{W}_{13}$、$\boldsymbol{W}_{21}$、$\boldsymbol{W}_{22}$ 的权值，分别是：

$$\boldsymbol{W}=[0.108\ 8,0.458\ 5,0.432\ 8]^{\mathrm{T}}$$

$$\boldsymbol{W}_1=[0.213\ 7,0.148\ 0,0.638\ 3]^{\mathrm{T}}$$

$$\boldsymbol{W}_2=[0.500\ 02,0.499\ 98]^{\mathrm{T}}$$

$$\boldsymbol{W}_{11}=[0.113\ 3,0.301\ 5,0.585\ 2]^{\mathrm{T}}$$

$$\boldsymbol{W}_{12}=[0.057\ 6,0.154\ 5,0.236\ 5,0.551\ 4]^{\mathrm{T}}$$

$$\boldsymbol{W}_{13}=[0.057\ 6,0.154\ 5,0.236\ 5,0.551\ 4]^{\mathrm{T}}$$

$$\boldsymbol{W}_{21}=[0.054\ 1,0.147\ 6,0.220\ 8,0.577\ 5]^{\mathrm{T}}$$

$$\boldsymbol{W}_{22}=[0.684\ 4,0.235\ 5,0.080\ 1]^{\mathrm{T}}$$

2.4.2.4 动态分数计算

动态评分的计算主要基于 3 个权重，分别是指标值权重、指标权重和维度权重，其中资产维度分数和环境维度分数之和为评分总分数，指标初始值为 100，最终维度分数是指标分数和 3 个权重的乘积。

为方便表述，将资产维度评分和环境维度评分分别表示为 S_2、S_3。漏洞危害等级的动态评分可以使用以下公式进行计算：

$$S_2=100\Big(\Big(\sum_{i=1}^{3}w_{21}w_{21i}+\sum_{j=1}^{4}w_{22}w_{22j}+\sum_{k=1}^{4}w_{23}w_{23k}\Big)w_2\Big) \tag{3}$$

$$S_3=100\Big(\Big(\sum_{m=1}^{4}w_{31}w_{31m}+\sum_{n=1}^{3}w_{32}w_{32n}\Big)w_3\Big) \tag{4}$$

通过式(3)～(4)可以计算出漏洞危害等级的动态评分。这些公式使用权重来考虑各个指标的重要性，其中指标值权重和指标权重反映了不同指标之间的重要性差异，而维度权重则反映了资产和环境维度的重要性差异。这种计算方法可以提高漏洞评估的准确性和可靠性，帮助网络安全人员更好地识别和管理安全风险。

2.4.3 漏洞危害等级计算

漏洞危害等级评分由静态指标部分和动态指标部分之和构成。其中，静态指标部分的评分依赖于基本维度分数，基本维度分数依托于 CVSS 分数进行评估，如果漏洞库中没有 CVSS 分数，可以利用预训练模型对漏洞危害等级进行预测，并将预测结果作为静态评分。动态指标部分的评分是资产维度分数和环境维度分数之和，并且主要依托于三重权重进行计算。这三重权重分别是指标值权重、指标权重和维度权重。为了构建评估方程进行计算，需要将所有指标值初始赋值为 100，并将其与三重权重相乘得到最终维度分数，这一过程基于层次分析法实现。

将 S、S_1 分别表示为漏洞危害等级评分、基本维度评分，漏洞危害等级计算公式为：

$$S=S_1+S_2+S_3 \tag{5}$$

$$S_1=10\cdot\text{CVSS 分数}\cdot w_1 \tag{6}$$

利用漏洞评估指标体系，对漏洞危害等级进行评分。根据此方法，共计算出 2 304 种组合结果，通过归一化处理后，漏洞危害等级分数分布

情况如图 7 所示。由图 7 可以看出，分数高峰位于图像的中部，两侧大致对称，结果大致符合正态分布的趋势。即高危漏洞和低危漏洞数量较少，而中危漏洞数量较多。

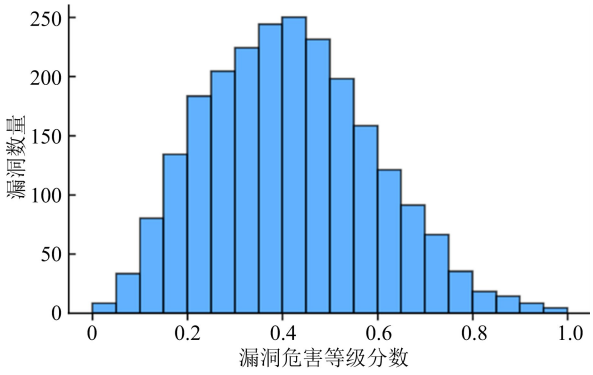


图 7　归一化后的漏洞危害等级分数分布情况

Fig. 7　Normalized vulnerability damage rating distribution

在数据计算方面，主要涉及 2 部分：静态指标和动态指标。静态指标通过美国国家漏洞库官网或 DistilBERT 模型预测得出。动态指标来源于网络空间资源测绘系统，但在无法获取数据的情况下，本文对指标值进行分类，以覆盖所有可能的情况，包括指标值为 0 的情况，并为其指定相应的指标值。因此，本文提出的方法具有较高的鲁棒性，可以得到可靠的漏洞危害等级评估结果。

根据漏洞危害等级分布情况，将最终的漏洞危害等级与计算分数对应关系定义如表 4 所列。

表 4　漏洞危害等级对应表

Tab. 4　Vulnerability hazard level table

漏洞危害等级分数	漏洞危害等级	占比情况(%)
0～0.25	低危	19.02
0.25～0.45	中危	40.03
0.45～0.60	高危	25.49
0.60～1.00	超危	15.46

3　实例分析

3.1　数据获取

数据的获取基于自研的网络空间资源测绘平台，该平台收集了大量的网络资产，截至 2022 年 10 月 16 日，已有网络资产 1 239 202 060 条。通过对这些资产进行检索，发现当前网络空间的安全状况并不乐观，其中有 841 781 条资产存在已披露的漏洞，而且这些资产中还有一部分属于重要行业资产。出于安全性考虑，这里对具体资产的 IP、域名、行业等信息进行了隐去，只呈现了部分统计信息。在这 841 781 条存在漏洞的资产中，本文选取了 10 个漏洞进行实例分析，这些漏洞涉及不同的漏洞类型和危害程度。表 5 列出了这些漏洞的相关数据信息，包括漏洞类型、CVSS 评分、攻击复杂度等指标。通过对这些漏洞进行深入的研究，可以更好地了解漏洞的危害和影响，进而有针对性地制定漏洞防范策略和安全措施。

表 5　真实漏洞数据信息

Tab. 5　Real vulnerability data information

CVE ID	CVSS 3.1 分数	C_{21}	C_{22}	C_{23}	C_{31}	C_{32}
CVE-2021-26723	6.1	52 173	37 026	47 124	存在 POC	无补丁
CVE-2021-26855	9.8	102 663	15 147	82 467	存在 EXP	官方补丁
CVE-2020-3452	7.5	84 150	6 732	0	存在 EXP	官方补丁
CVE-2021-26084	9.8	26 928	3 366	21 879	存在 EXP	官方补丁
CVE-2021-21972	9.8	38 709	1 683	33 660	存在 EXP	官方补丁
CVE-2019-9670	9.8	40 392	0	38 527	存在 POC	官方补丁
CVE-2021-43798	7.5	11 781	0	11 781	存在 EXP	官方补丁
CVE-2020-13942	9.8	5 049	0	5 049	存在 EXP	官方补丁
CVE-2021-22986	9.8	3 366	0	3 366	存在 EXP	官方补丁
CVE-2020-10148	9.8	1 683	0	1 683	存在 EXP	官方补丁

3.2 实例评估

对近 3 年曝出的 10 个真实漏洞进行实例分析，结果见表 6，其中包括漏洞指标值和使用本研究方法计算的漏洞危害等级。表 7 列出了本文计算的漏洞评级与 CVSS 评分和 NVD 评级的对比情况。其中，表 7 中漏洞相关评价指标的指标值来源于表 5，并经过定性转换得到现有指标值（转换方式详见 2.3.1 节）。

表 6 真实漏洞指标值选取情况

Tab. 6 Selection of real vulnerability metric values

CVE ID	CVSS 分数	C_{21}	C_{22}	C_{23}	C_{31}	C_{32}	评级
CVE-2021-26723	6.1	多	多	多	存在 POC	无	超危
CVE-2021-26855	9.8	多	多	多	存在 EXP	官方补丁	超危
CVE-2020-3452	7.5	多	中等	无	存在 EXP	官方补丁	中危
CVE-2021-26084	9.8	多	中等	多	存在 EXP	官方补丁	高危
CVE-2021-21972	9.8	多	少	多	存在 EXP	官方补丁	中危
CVE-2019-9670	9.8	多	无	多	存在 POC	官方补丁	中危
CVE-2021-43798	7.5	中等	无	中等	存在 EXP	官方补丁	低危
CVE-2020-13942	9.8	中等	无	中等	存在 EXP	官方补丁	中危
CVE-2021-22986	9.8	中等	无	少	存在 EXP	官方补丁	中危
CVE-2020-10148	9.8	少	无	少	存在 EXP	官方补丁	低危

表 7 本文评级与 CVSS 评级对比情况

Tab. 7 Comparison between the rating of this study and the rating of CVSS

CVE 编号	CVSS 评分	NVD 评级	本文评级
CVE-2021-26723	6.1	中危	超危
CVE-2021-26855	9.8	超危	超危
CVE-2020-3452	7.5	高危	中危
CVE-2021-26084	9.8	超危	高危
CVE-2021-21972	9.8	超危	中危
CVE-2019-9670	9.8	超危	中危
CVE-2021-43798	7.5	高危	低危
CVE-2020-13942	9.8	超危	中危
CVE-2021-22986	9.8	超危	中危
CVE-2020-10148	9.8	超危	低危

从表中数据可以看出，有些 NVD 高危、超危漏洞，由于受到影响的资产数量较少且相应漏洞存在补丁，漏洞评级相应进行了调低。而一些中危、低危漏洞，影响资产数量多，但受重视度不够，部分漏洞没有对应补丁，相应漏洞危害等级得到了提高。例如，CVE-2021-26723 影响 Linkedin Oncall 建站系统，其 1.4.0 版本存在跨站脚本漏洞，截至 2022 年 10 月 5 日，平台中可以搜到的受影响资产有 52 173 个，受影响重要资产有 37 026 个，受影响关联资产有 47 124 个。虽然此漏洞对单个资产造成影响较小，但当漏洞影响全网资产数量达到一定程度时，对全网造成的影响就不容小觑。该建站系统也会被用来搭建一些重要行业的网站，如政务、教育行业等网站，资产的价值也会相应提高。

一些 CVSS 评分较高的漏洞，因为影响全网资产数量较少，获得了较低的评级。例如，CVE-2020-13942 影响 Apache Unomi 客户数据平台，Apache Unomi 1.5.2 之前版本存在注入漏洞。截至 2022 年 10 月 5 日，平台可以搜到的受影响资产有 5 049 个，且不涉及重要行业，资产价值较低，同时 Apache 官方还发布了针对此漏洞的补丁。虽然此漏洞对单个资产危害等级较高，但因为影响的全网资产数量较少且资产价值低，所以获得了较低的漏洞评级。

这也证实了本文所提方法可以较好地结合漏洞影响资产和所处环境对漏洞进行实际危害性评估，而现有的评估方法并没有较好地结合资产和环境对漏洞进行评估，评估的结果更倾向于漏洞本身的危害性，而不是漏洞实际的危害性，使用本文提出的方法对漏洞进行评估可以较好地避免高危、超危漏洞危害性评估不足，低危、中危漏洞重视程度不够的情况。

4　结束语

为解决现有漏洞评估手段无法准确评估漏洞实际危害性的问题，本文提出了一种面向实网环境的漏洞危害等级评估方法。该方法在原有指标体系的基础上增加了资产和环境维度的指标，构建了一套面向实网环境的新指标体系。基于这个指标体系，构建了基于网络空间资源测绘平台数据的漏洞自动化评估方法，使用微调后的 DistilBERT 模型和层次分析法分别预测漏洞的静态和动态分数，从而对漏洞的真实危害性进行客观准确地评估。相较于 CVSS 等评估方式，本方法减少了人为主观判断的引入，使用网络空间资源测绘平台数据进行客观评估，在评估速度和准确度上均得到一定提升，具有良好的应用前景。

参 考 文 献

[1] 王秋艳，张玉清. 一种通用漏洞评级方法[J]. 计算机工程，2008，34(19)：133-136.
WANG Qiuyan，ZHANG Yuqing. Common vulnerability rating method [J]. Computer Engineering，2008，34(19)：133-136.(in Chinese)

[2] 温涛. 安全漏洞危害评估研究暨标准漏洞库的设计与实现[D]. 西安：西安电子科技大学，2016.
WEN Tao. The design and implementation of the standard vulnerability database and the research of security vulnerability severity assessment[D]. Xi'an：Xidian University，2016.(in Chinese)

[3] 雷柯楠，张玉清，吴晨思，等. 基于漏洞类型的漏洞可利用性量化评估系统[J]. 计算机研究与发展，2017，54(10)：2296-2309.
LEI Kenan，ZHANG Yuqing，WU Chensi，et al. A system for scoring the exploitability of vulnerability based types[J]. Journal of Computer Research and Development，2017，54(10)：2296-2309.(in Chinese)

[4] LUO J，LO K，QU H R. A software vulnerability rating approach based on the vulnerability database [J]. Journal of Applied Mathematics，2014，2014：1-9.

[5] GHANI H，LUNA J，SURI N. Quantitative assessment of software vulnerabilities based on economic-driven security metrics[C]//Proceedings of 2013 International Conference on Risks and Security of Internet and Systems (CRiSIS).[S.l.]：IEEE，2013：1-8.

[6] LIU Q，ZHANG Y Q. VRSS：a new system for rating and scoring vulnerabilities[J]. Computer Communications，2011，34(3)：264-273.

[7] 马驰，高岭，孙骞，等. 基于模糊理论的漏洞危害等级评估[J]. 计算机应用研究，2014，31(3)：815-818.
MA Chi，GAO Ling，SUN Qian，et al. Assessment of vulnerability threat based on fuzzy theory[J]. Application Research of Computers，2014，31(3)：815-818.(in Chinese)

[8] 陈秀真，郑庆华，管晓宏，等. 基于模糊信息融合的漏洞评估方法[J]. 小型微型计算机系统，2004，25(8)：1424-1427.
CHEN Xiuzhen，ZHENG Qinghua，GUAN Xiaohong，et al. Method of vulnerability evaluation based on fuzzy data fusion[J]. Mini-micro Systems，2004，25(8)：1424-1427.(in Chinese)

[9] 付志耀，高岭，孙骞，等. 基于粗糙集的漏洞属性约简及严重性评估[J]. 计算机研究与发展，2016，53(5)：1009-1017.
FU Zhiyao，GAO Ling，SUN Qian，et al. Evaluation of vulnerability severity based on rough sets and attributes reduction[J]. Journal of Computer Research and Development，2016，53(5)：1009-1017.(in Chinese)

[10] 周峥伟，陈秀真，林梦泉，等. 基于攻击路径的漏洞风险评估模型[J]. 信息安全与通信保密，2007(5)：165-167.
ZHOU Zhengwei，CHEN Xiuzhen，LIN Mengquan，et al. Research on attack-graph based model of vulnerability risk evaluation[J]. Information Security and Communications Privacy，2007(5)：165-167.(in Chinese)

[11] 宋舜宏，陆余良，杨国正，等. 一种应用主机访问图的网络漏洞评估模型[J]. 小型微型计算机系统，2011，32(3)：483-488.
SONG Shunhong，LU Yuliang，YANG Guozheng，et al. Network vulnerability assessment model applying host-based access graphs[J]. Journal of Chinese Computer Systems，2011，32(3)：483-488.(in Chinese)

[12] 朱禹铭. 基于贝叶斯的动态网络攻击行为预测方法研究[D]. 秦皇岛：燕山大学，2019.
ZHU Yuming. Research on dynamic network attack behavior prediction method based on Bayesian[D].

Qinhuangdao: Yanshan University, 2019. (in Chinese)

[13] FRIGAULT M, WANG L, JAJODIA S, et al. Measuring the overall network security by combining CVSS scores based on attack graphs and bayesian networks [M]. [S. l.]: Springer, 2017: 1-23.

[14] LIU Y, MAN H. Network vulnerability assessment using Bayesian networks[C]//Proceedings of 2005 Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security. [S. l.: s. n.], 2005: 61-71.

[15] JOHNSON P, LAGERSTRÖM R, EKSTEDT M, et al. Can the common vulnerability scoring system be trusted? A Bayesian analysis[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(6): 1002-1015.

[16] 杨宏宇, 谢丽霞, 朱丹. 漏洞严重性的灰色层次分析评估模型[J]. 电子科技大学学报, 2010, 39(5): 778-782.
YANG Hongyu, XIE Lixia, ZHU Dan. A vulnerability severity grey hierarchy analytic evaluation model [J]. Journal of University of Electronic Science and Technology of China, 2010, 39(5): 778-782. (in Chinese)

[17] LIU P, TIAN Z, WU X, et al. An improved common vulnerability scoring system based on K-means[C]//Proceedings of 2013 International Conference on Trustworthy Computing and Services. [S. l.]: Springer, 2013: 62-69.

[18] SAULAIMAN M, TAKÁCS M, KOZLOVSZKY M, et al. Fuzzy model for common vulnerability scoring system [C]//Proceedings of the 15th International Symposium on Applied Computational Intelligence and Informatics (SACI). [S. l.]: IEEE, 2021: 419-424.

[19] 赵培超. 基于报警关联的漏洞威胁评估方法研究[D]. 桂林: 桂林电子科技大学, 2020.
ZHAO Peichao. Research on vulnerability threat assessment method based on alarm correlation[D]. Guilin: Guilin Universities of Electronic Technology, 2020. (in Chinese)

[20] 廖丹, 周明, 刘丹, 等. 一种自动优化 CVSS v2.0 漏洞指标的评估方法[J]. 计算机工程与应用, 2015, 51(2): 103-107.
LIAO Dan, ZHOU Ming, LIU Dan, et al. Assessment method of automatic optimizing CVSS v2.0 vulnerability indicators [J]. Computer Engineering and Applications, 2015, 51(2): 103-107. (in Chinese)

[21] HAN Z, LI X, XING Z, et al. Learning to predict severity of software vulnerability using only vulnerability description[C]//Proceedings of 2017 IEEE International Conference on Software Maintenance and Evolution (ICSME). [S. l.]: IEEE, 2017: 125-136.

[22] YAMAMOTO Y, MIYAMOTO D, NAKAYAMA M. Text-mining approach for estimating vulnerability score[C]//Proceedings of the 4th International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS). [S. l.]: IEEE, 2015: 67-73.

[23] SPANOS G, ANGELIS L, TOLOUDIS D. Assessment of vulnerability severity using text mining[C]//Proceedings of the 21st Pan-Hellenic Conference on Informatics. [S. l.: s. n.], 2017: 1-6.

[24] SHAHID M, DEBAR H. CVSS-BERT: explainable natural language processing to determine the severity of a computer security vulnerability from its description[C]//Proceedings of the 20th IEEE International Conference on Machine Learning and Applications (ICMLA). [S. l.]: IEEE, 2021: 1600-1607.

[25] GONG X, XING Z, LI X, et al. Joint prediction of multiple vulnerability characteristics through multi-task learning[C]//Proceedings of the 24th International Conference on Engineering of Complex Computer Systems(ICECCS). [S. l.]: IEEE, 2019: 31-40.

[26] COSTA J C, ROXO T, SEQUEIROS J B F, et al. Predicting CVSS metric via description interpretation [J]. IEEE Access, 2022, 10: 59125-59134.

[27] 张玺, 黄曙光, 夏阳, 等. 一种基于攻击图的漏洞风险评估方法[J]. 计算机应用研究, 2010(1): 278-280.
ZHANG Xi, HUANG Shuguang, XIA Yang, et al. Attack graph-based method for vulnerability risk evaluation[J]. Application Research of Computers, 2010 (1): 278-280. (in Chinese)

[28] 谢丽霞, 江典盛, 张利, 等. 漏洞威胁的关联评估方法[J]. 计算机应用, 2012, 32(3): 679-682.
XIE Lixia, JIANG Diansheng, ZHANG Li, et al. Vulnerability threat correlation assessment method [J]. Journal of Computer Applications, 2012, 32(3): 679-682. (in Chinese)

[29] MELL P, SCARFONE K, ROMANOSKY S. Common vulnerability scoring system[J]. IEEE Security & Privacy, 2006, 4: 85-89.

[30] MELL P, SCARFONE K, ROMANOSKY S. A complete guide to the common vulnerability scoring system version 2.0[C]//Proceedings of Forum of Incident Response and Security Teams. [S. l.: s. n.], 2007: 1-23.

[31] 郭莉, 曹亚男, 苏马婧, 等. 网络空间资源测绘: 概念与技术[J]. 信息安全学报, 2018, 3(4): 1-14.
GUO Li, CAO Yanan, SU Majing, et al. Cyberspace

resources surveying and mapping: the concepts and technologies[J]. Journal of Cyber Security, 2018, 3(4): 1-14. (in Chinese)

[32] 周杨，徐青，罗向阳，等. 网络空间测绘的概念及其技术体系的研究[J]. 计算机科学，2018，45(5)：1-7. ZHOU Yang, XU Qing, LUO Xiangyang, et al. Research on definition and technological system of cyberspace surveying and mapping[J]. Computer Science, 2018, 45(5): 1-7. (in Chinese)

[33] YIN J, TANG M, CAO J, et al. Apply transfer learning to cybersecurity: predicting exploitability of vulnerabilities by description[J]. Knowledge-Based Systems, 2020, 210: 106529.

[34] KHAZAEI A, GHASEMZADEH M, DERHAMI V. An automatic method for CVSS score prediction using vulnerabilities description[J]. Journal of Intelligent & Fuzzy Systems, 2016, 30(1): 89-96.

[35] NAKAGAWA S, NAGAI T, KANEHARA H, et al. Character-level convolutional neural network for predicting severity of software vulnerability from vulnerability description[J]. IEICE Transactions on Information and Systems, 2019, 102(9): 1679-1682.

[36] WANG P, ZHOU Y, SUN B, et al. Intelligent prediction of vulnerability severity level based on text mining and XGBboost[C]//Proceedings of 2019 Eleventh International Conference on Advanced Computational Intelligence (ICACI). [S. l.]: IEEE, 2019: 72-77.

[37] LIU K, ZHOU Y, WANG Q, et al. Vulnerability severity prediction with deep neural network[C]//Proceedings of the 5th International Conference on Big Data and Information Analytics (BigDIA). [S. l.]: IEEE, 2019: 114-119.

[38] SAATYTL. What is the analytic hierarchy process? [M]. [S. l.]: Springer, 1988.

作 者 简 介

施　凡

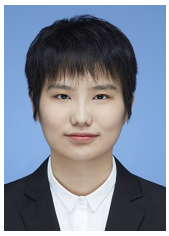
男，1983 年生，副教授，国家漏洞库(CNNVD)特聘专家，军队青年科技英才培养对象，研究方向为网络空间测绘、网络安全态势感知、网络自动化渗透测试

E-mail：shifan17@nudt.edu.cn

开少锋

男，1993 年生，助理工程师，研究方向为网络安全态势感知

E-mail：kaishaofeng@nudt.edu.cn



钟　瑶

女，1998 年生，硕士研究生，研究方向为网络空间测绘

E-mail：zhongyao@nudt.edu.cn

责任编辑　董　莉