Hans Journal of Data Mining 数据挖掘, 2024, 14(2), 94-101
Published Online April 2024 in Hans. https://www.hanspub.org/journal/hjdm
https://doi.org/10.12677/hjdm.2024.142008

Hans汉斯

基于区块链的网络安全漏洞扫描的研究

王　宇，康晓凤，范鸿铭，何培延，顾晓敏

徐州工程学院信息工程学院(大数据学院)，江苏　徐州

收稿日期：2024年3月10日；录用日期：2024年4月10日；发布日期：2024年4月22日

摘　要

随着信息技术的迅猛发展，网络安全漏洞成为互联网应用的一项重要挑战，本文提出了一种基于区块链的漏洞扫描系统，利用分布式账本技术、区块结构、加密算法以及智能合约等核心技术，解决了传统漏洞扫描中存在的安全性、透明度和可信度等问题。首先采用分布式账本技术，实现了增强的安全性，确保了漏洞扫描过程的透明度和可信度，再利用区块链的不可篡改性，实现了漏洞检测历史记录的可追溯和不可篡改。最后利用区块链技术的去中心化特性有效降低了单点故障风险。使用基于区块链的漏洞扫描可以在线扫描漏洞、检测目录和端口，查看所有的历史记录、可追溯性和可靠性，提高企业网络的安全性和可靠性，为企业网络提供安全、全面的解决方案。

关键词

区块链，Python，网络安全，漏洞扫描

Research on Blockchain Based Network Security Vulnerability Scanning

Yu Wang, Xiaofeng Kang, Hongming Fan, Peiyan He, Xiaomin Gu

College of Information Engineering (Big Data College), Xuzhou University of Technology, Xuzhou Jiangsu

Received: Mar. 10th, 2024; accepted: Apr. 10th, 2024; published: Apr. 22nd, 2024

Abstract

With the rapid development of information technology, network security vulnerabilities have become a significant challenge for Internet applications. This paper proposes a blockchain-based vulnerability scanning system, utilizing core technologies such as distributed ledger technology, block structure, encryption algorithms, and smart contracts. It addresses the security, transparency, and trust issues present in traditional vulnerability scanning methods. Firstly, distributed ledger technology is employed to enhance security, ensuring the transparency and trustworthi-

文章引用: 王宇, 康晓凤, 范鸿铭, 何培延, 顾晓敏. 基于区块链的网络安全漏洞扫描的研究[J]. 数据挖掘, 2024, 14(2): 94-101. DOI: 10.12677/hjdm.2024.142008

ness of the vulnerability scanning process. Secondly, the immutability of blockchain is utilized to achieve traceability and tamper-proofing of vulnerability detection history records. Finally, the decentralized nature of blockchain technology effectively reduces the risk of single point failures. Utilizing blockchain-based vulnerability scanning enables online detection of vulnerabilities, directory and port scanning, viewing of all historical records, traceability, and reliability. This enhances the security and reliability of enterprise networks, providing a secure and comprehensive solution for enterprise network security.

Keywords

Blockchain, Python, Network Security, Vulnerability Scanning

1. 引言

随着数字化时代的不断演进，网络安全已成为制约数字经济发展的关键问题。互联网的广泛应用为我们带来了便捷和创新，同时也引发了一系列新的安全隐患和威胁。传统的漏洞扫描系统虽然能够检测并报告系统和应用程序中的安全漏洞，但是在面对日益复杂和高级的网络攻击时显得力不从心。因此，研究人员纷纷探寻新的技术手段以提高漏洞扫描系统的效能和可靠性。随着区块链技术的发展，通过深入研究区块链技术在网络安全中的应用，并把此技术应用到网络安全扫描领域，寻求构建一个能够有效应对新型网络威胁的系统，从而更好地保护用户隐私和企业关键信息[1]。

首先，中心化的漏洞扫描平台往往面临信任缺失和单点故障的风险，使得攻击者有机可乘。其次，传统漏洞扫描难以应对数据篡改的挑战，导致扫描结果的可靠性受到质疑。此外，随着攻击手段的不断演进，传统扫描技术往往难以跟上日新月异的网络威胁，使得网络安全防护愈发形同虚设。

为解决这些问题，基于区块链的网络安全漏洞扫描技术崭露头角。区块链作为一种去中心化、分布式的记账技术，为漏洞扫描提供了全新的解决思路。通过区块链的不可篡改性和分布式记账的特点，我们能够有效解决传统漏洞扫描中的信任和数据完整性问题。本研究将深入探讨基于区块链的漏洞扫描技术如何应对当前网络安全面临的诸多挑战，为构建更加安全可信的网络防护体系提供新的视角和解决方案。

2. 基于区块链的漏洞扫描

伴随着网络应用的普及，大量的网络漏洞也随之出现，这些漏洞会对网络用户的行为和数据产生一定的威胁，因此及时地进行漏洞检测，成为当前网络安全领域关注的主要问题，相关企业也结合实际的漏洞检测需求，设计了漏洞检测系统，例如传统 C/S 型网络漏洞检测系统，都采用中心化管理的方式，通过服务器集中存储漏洞数据库、管理扫描引擎和分配扫描任务，提供用户界面，使用户能够配置扫描任务、查看扫描结果和进行必要的操作。而基于区块链技术的漏洞扫描具有去中心化、不可篡改性、智能合约的自动化响应、信任度提升、较高的网络抗攻击能力等优点，并且可以结合网页的实际运转逻辑进行专项编码，综合缓和区数据库分析数据的溢出条件，这样能够快速地定位网络环境中具体的安全数据值，以便来完成漏洞检测[2]。总之在安全研究人员或黑客的工作中，首先需要发现潜在的漏洞。这可能涉及到代码审计、渗透测试或其他安全研究方法。在确认漏洞存在后，研究人员会尝试复现漏洞，以

确保其可被利用。这可能包括构建恶意载荷、制作特定的网络请求或模拟攻击条件。而本系统通过 POC 验证来检测漏洞的存在，POC (Proof of Concept)验证是指通过演示、实验或原型来验证某个概念、理念或想法的可行性。在网络安全领域，POC 通常用于验证漏洞的存在和危害性[3]。

而基于区块链技术的漏洞扫描具有去中心化、不可篡改性、智能合约的自动化响应、信任度提升、较高的网络抗攻击能力等优点。

去中心化和分布式：传统的 C/S 和 B/S 漏洞检测系统通常依赖于中心化架构，容易成为攻击目标，而区块链技术检测体系采用去中心化和分布式的方式，将信息存储在多个节点上，减轻了单点故障和攻击的威胁。

不可篡改性：区块链技术的不可篡改性确保了检测结果的完整性，防止结果被篡改或删除。这是因为一旦信息被写入区块链，几乎不可能在所有节点上修改或删除。

信任度提升：区块链技术的透明性和不可篡改性提高了系统的整体信任度。用户和管理员可以追溯所有的操作和检测活动，确保检测过程的透明和可验证性。

智能合约的自动化响应：区块链技术引入了智能合约的概念，可以实现自动化的响应机制。一旦检测到威胁，智能合约可以自动触发预定义的操作，提高响应速度和效率。

提高网络抗攻击能力：通过分布式存储和共识机制，区块链技术检测体系能够提高系统的鲁棒性，降低遭受攻击的风险，增强整体的网络安全。

当扫描出漏洞时将漏洞的所有信息写入用户的个人区块，并且加入哈希值，如果要修改一个区块，必须重写整个链。由于哈希值无法反向计算且为了防止重写区块，必须以一定数量的零开头，也就是在加密货币所应用的技术。

这个系统的核心技术包括分布式账本技术(DLT)、区块结构、加密算法以及智能合约。首先，分布式账本技术通过在网络中的多个节点上维护相同的完整账本，实现了信息的去中心化存储。这种分散式的账本架构通过共识机制确保了数据的一致性和安全性，消除了传统中心化数据库可能存在的单点故障。

其次，系统采用区块结构，将数据以块的形式存储，并通过哈希算法将这些块链接在一起，形成不可篡改的链条。每个区块包含了一定数量的交易信息以及前一个区块的哈希值，确保了数据的安全性和完整性。

加密算法在系统中发挥着关键作用，通过哈希函数生成区块的哈希值，数字签名用于验证交易的真实性，非对称加密则保护了数据的机密性。这些加密技术为系统提供了强大的安全性基础，有效防范各种潜在的威胁和攻击。

最后，智能合约作为一组编程代码，定义了在满足特定条件时应执行的操作。通过智能合约，系统能够实现自动化的、无需信任第三方的交易和业务逻辑。这使得系统具备更高的灵活性和效率，同时减少了对中介机构的依赖。

这些核心技术共同构建了一个基于区块链的系统，使其成为一种具有去中心化、安全、透明和可靠特性的分布式数据库系统。这些技术的综合应用为系统提供了强大的基础，满足了在网络安全漏洞扫描等方面的复杂需求。

较为全面的漏洞检测方法是基于贝叶斯网络的检查方法、模式预测、机器学习等技术，而不加入区块链技术始终对于大规模的、实时性要求高的网络安全扫描可能有一定局限。对实时共享信息能力相对较弱，需要更多历史数据的积累。引入区块链技术的分布式账本技术(DLT)，区块结构，加密算法以及智能合约技术可以为这些挑战提供一些潜在的解决方案，综合考虑，将区块链技术与先进的漏洞检测方法结合，可以为大规模、实时性要求高的网络安全扫描提供更为全面和创新的解决方案[4]。

3. 系统设计与实现

本系统的核心模块包括区块链模块和漏洞检测模块以及 Web 端。Web 端分前后两个部分，Web 前端采用广泛使用的 JavaScript 库和 HTML 构成前端界面，后端是使用 Python 的 flask 库结合构建后端，并采用区块链缓存数据。区块链部分通过接受漏洞扫描模块的数据储存在公共链中，任何用户可以访问，并且发送数据到 Web 段生成漏洞报告，如图 1。

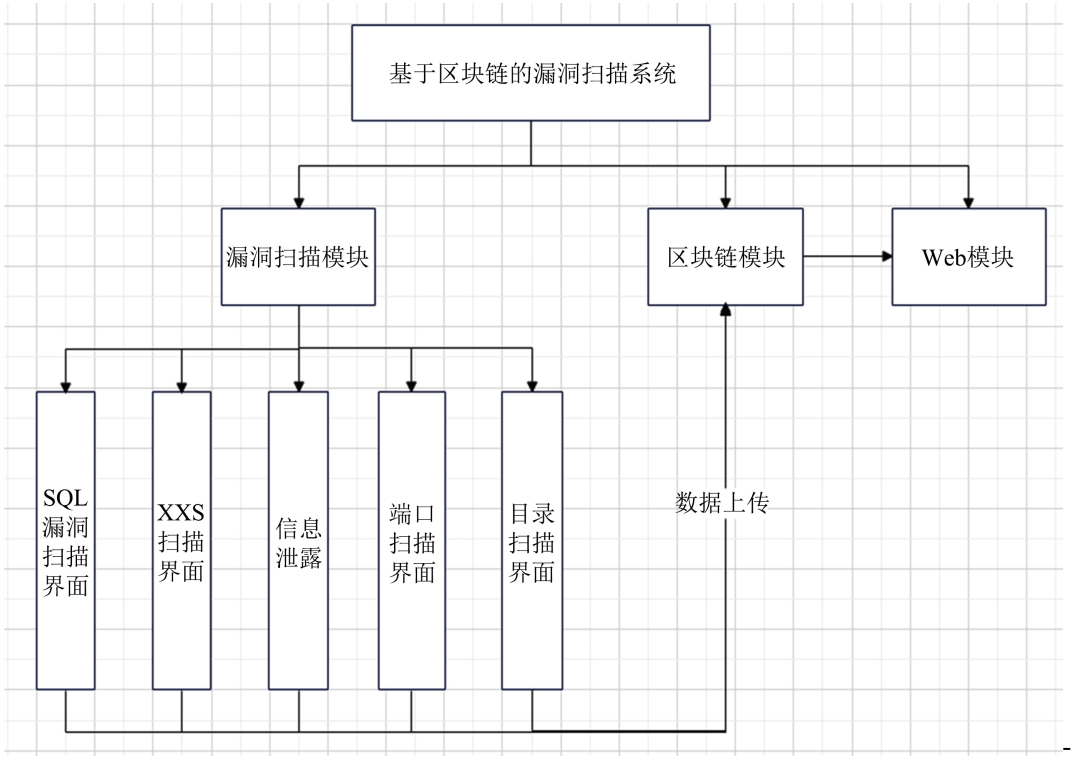

Figure 1. System module
图 1. 系统模块

3.1. 用户登录以及注册模块

用户登录界面可以登录以及注册进而使用漏洞扫描模块，用户不区分等级，任何用户可以使用漏洞模块的扫描漏洞功能并且将发现漏洞的用户以及漏洞上传到区块链，注册的用户会直接写入本地。不可以留空和输入错误账户和密码。用户登录的意义在于区分每个人的扫描出的漏洞。用户密码以哈希形式存储在数据库中，而不是以明文形式存储，以增加安全性。

3.2. 漏洞扫描模块

漏洞扫描模块分为目录扫描、端口扫描、XSS 扫描、SQL 注入扫描和信息泄露扫描五个小模块。漏洞检测模块主要的职能是实现漏洞的精准定位以及快速的抓取，当前较为常见的漏洞检测模块以 XSS 漏洞检测还有端口检测、目录检测等，其主要优势在于可以直接从数据库中检测和安全漏洞相关的字符串，通过对这些参数进行读取，能够形成一个新的检测队列，可以将其中的部分查询字符进行更换[5]。智能合约的自动化响应操作漏洞检测模块，主要的职能是实现漏洞的精准定位以及快速的抓取，当前较为常见的漏洞检测模块以 XSS 漏洞检测还有端口检测、目录检测等，其主要优势在于一旦检测漏洞便自动触

发预定义的上传操作，可以提高数据发送效率[6]。漏洞检测模块通常与爬虫模块相互配合。如果爬虫模块提取的目标未经修改，那么漏洞检测模块中的相关数值和表单也将保持不变。这种协同工作使得系统能够有效截取当前网络上绝大部分漏洞形式，并能够自动转换在 GET 或 POST 等源码编译行为中。在实际应用中，一旦经过检测后，如果最终的响应状态编码为 2XX 形式，表明当前网络体系中尚无漏洞存在。此时，服务器会自动生成 HTML 文档，并结合可能存在的漏洞类型和实际位置进行标注。这种协同模式的优势在于全面性地覆盖了潜在的漏洞形式，并通过实时的响应状态编码来迅速判断漏洞的存在与否。同时，通过生成详细的 HTML 文档，系统管理员或安全团队能够清晰地了解可能存在的漏洞类型和位置，有利于更加迅速、精准地进行修复工作。这种集成式的漏洞检测方法在保障系统安全性的同时，也提高了安全团队的工作效率。该 XSS 扫描能够直接从本地的文档中读取与网络爬虫相关的安全漏洞检测的 POC 代码。用于构造新的待检测 URL 队列形式[2]。

图 2 是 XSS 扫描的界面，通过静态代码分析判断漏洞的存在，这种方法必须有较多的数据匹配。确定要测试的 Web 应用程序和其相关页面，明确测试的范围和目标。

XSS 扫描的流程如下：

1) 创建包含恶意负载的输入，这些输入可能会导致 XSS 漏洞。模糊测试用例应包括各种情况，例如：

基本的 XSS 攻击向量，如<script>alert('XSS');</script>；

使用编码绕过过滤机制的攻击向量，如<script>alert('XSS');</script>。

尝试不同的事件处理器和 HTML 标签，以便绕过特定的过滤规则。

2) 将模糊测试用例发送到目标 Web 应用程序的输入端点，例如表单字段、URL 参数或 Cookie。这可以通过手动发送 HTTP 请求，使用专门的工具(例如 OWASP ZAP、Burp Suite 等)或自动化脚本完成。

3) 检查 Web 应用程序的响应，特别是观察是否存在潜在的 XSS 漏洞迹象。关注以下方面：

a) 页面是否执行了未经过滤的 JavaScript 代码。

b) 是否有弹出警告框或其他异常行为。

c) 检查页面源代码，查看是否出现恶意注入的 HTML、JavaScript 等代码。

扫描出 XSS 漏洞时会于区块链中的个人的初始区块创建链，将漏洞的所有信息写入区块，并且加入哈希值。如果发现潜在的 XSS 漏洞，进一步验证其可利用性。这可能包括执行更高级的攻击向量，获取敏感信息，或尝试与服务器进行交互。

Figure 2. XSS interface
图 2. XSS 界面

目录扫描的基本原理是尝试访问 Web 服务器上的不同路径，以确定哪些路径是有效的。这通常涉及到发送 HTTP 请求，观察服务器的响应状态码和内容，以判断路径是否存在，实现页面如图 3 所示。

Figure 3. Port scan interface
图 3. 端口扫描界面

信息泄露扫描的基本原理是尝试访问常见泄露的路径和链接，Web 服务器上的不同路径，以确定哪些路径是有效的。这通常也涉及到发送 HTTP 请求，观察服务器的响应状态码和内容，以判断路径是否存在，实现页面如图 4 所示。

Figure 4. Information leak scan interface
图 4. 信息泄露扫描界面

SQL 注入扫描模块

在网络爬虫模块与整体系统的协同工作中，若提升 CPU 自身的承载能力，将直接影响系统中其他相关节点，导致最终表现形式的一定差异。这种变化对于网络漏洞检测系统而言具有潜在的好处，尤其是对于满足系统主机的实际检测需求。

在利用这样的系统进行网络漏洞检测时，进一步引入 SQL 注入漏洞检测模块是至关重要的。该模块建立在计算机系统的基础上运行，其中“nd1”代表了系统中网络安全漏洞输入的实际节点，而“nd2”主要代表了区块链组织摄入的节点。与 XSS 漏洞检测模块不同的是，SQL 注入漏洞检测模块能够同时针对多个网络安全漏洞的数据进行检测，并发起攻击。它可以在网络爬虫模块的基础上分析系统的运行状态变化，有效地调整区块链信息之间的控制体系[5]。

简而言之，该模块具有较大的灵活性和主动性，能够结合实际的检测情况进行有针对性的调控。其智能化程度较高，使得系统更具适应性和响应性。这种设计不仅增强了系统整体的性能，也提高了漏洞检测的准确性和效率。

SQL 注入扫描的大体流程：

1) 确定要测试的 Web 应用程序，特别是那些涉及数据库查询的功能，如登录表单、搜索框、用户输入的过滤等。

创建包含 SQL 注入攻击向量的输入，以测试是否存在潜在的 SQL 注入漏洞。模糊测试用例应包括：

基本的 SQL 注入攻击向量，如' OR '1'='1'; --；

尝试绕过输入过滤的攻击向量，如 UNION SELECT * FROM users--；

使用编码和转义绕过输入过滤的攻击向量，如%27%20UNION%20SELECT%20*%20FROM%20users--。

2) 将模糊测试用例发送到目标 Web 应用程序的输入端点，如用户登录表单、搜索框等。这可以通过手动发送 HTTP 请求、使用专门的工具(例如 OWASP ZAP、Burp Suite 等)或自动化脚本完成。

3) 检查 Web 应用程序的响应，以观察是否存在潜在的 SQL 注入漏洞迹象。关注以下方面：

a) 否返回了与预期不同的结果，如错误消息、异常页面或非正常的行为。

b) 是否有 SQL 错误的提示或堆栈跟踪信息。

c) 检查页面源代码，查看是否存在注入的 SQL 代码。

如果发现潜在的 SQL 注入漏洞，进一步验证其可利用性。这可能包括执行更高级的攻击向量，获取敏感信息，或尝试与数据库进行交互。如图 5 为查询结果。

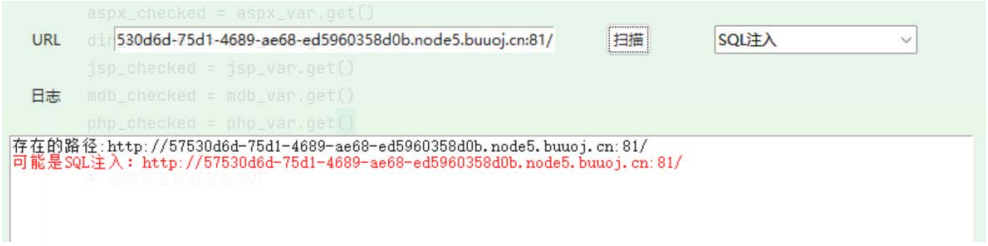

Figure 5. SQL vulnerability scanning
图 5. SQL 漏洞扫描界面

4. 访问历史模块

访问检测历史模块，前端会请求访问区块链的访问接口，区块链接口会调用存储在区块链中的链表，调用之后以 json 的格式返回并在前端表单中填充。如图 6 所示。

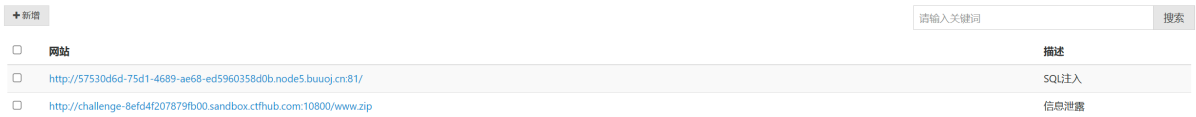

Figure 6. Access the history module interface
图 6. 访问历史模块界面

5. 结论

基于区块链的网络安全漏洞扫描系统具备分布式、不可篡改和透明的特性，提高了系统的安全性和可信度，同时系统具备可扩展性，可以根据需求灵活扩展，适应不同规模和复杂度的网络环境。然而系统的进一步研究和改进仍需解决区块链技术在性能、扩展性和标准化方面的挑战，以更好地满足未来网络安全的需求，为构建更为安全可靠的数字社会奠定基础。

基金项目

2023 年江苏省大学生创新训练计划项目(xcx2023189)；2023 年大学生创新训练计划项目(xcx2023204)。

参考文献

[1] 朱小栋, 魏紫钰, 颜礼蓉, 等. MOOC 背景下信息安全原理课程的教学方法[J]. 电子商务, 2020(11): 82-84.

[2] 熊琭. 基于区块链技术的网络安全漏洞检测系统设计[J]. 计算机测量与控制, 2021, 29(5): 59-63.

[3] 李婷. 面向区块链智能合约的实时漏洞检测技术研究[D]: [硕士学位论文]. 成都: 电子科技大学, 2021.

[4] 蒋建春, 马恒太, 任党恩, 等. 网络安全入侵检测: 研究综述[J]. 软件学报, 2000(11): 1460-1466.

[5] 张磊, 周泓雨. 基于区块链技术的网络安全漏洞检测方法设计[J]. 现代信息科技, 2022, 6(18): 96-98+102.

[6] 邓土亮. 基于区块链技术的网络安全漏洞检测系统设计[J]. 电脑编程技巧与维护, 2022(3): 170-173.