文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

基于渗透测试的医院信息系统网络安全检测

彭俊标　何国健
深圳市人民医院
DOI:10.12238/acair.v3i1.11879

[摘　要] 目的：主要是对某医院的RBRVS系统进行安全性检测,找出其中存在的网络安全漏洞和风险点,跟进整改,以保证系统安全和稳定运行,并为其他医院的信息系统网络安全检测提供一定的参考和借鉴。方法：采用渗透测试和漏洞扫描在2024年12月10日对某医院的RBRVS系统进行安全性检测,利用常见的攻击手段对其进行模拟测试,并收集测试结果和发现的问题。最后,针对测试结果制定了相应的检测报告和整改建议。结果：通过渗透测试和漏洞扫描发现了RBRVS系统中SQL注入、弱口令、越权访问等安全漏洞,并组织相关技术人员进行了漏洞修复。结论：通过渗透测试和漏洞扫描,可以有效地检测了信息系统安全性,发现各类应用层面的网络安全漏洞,及时修复收敛风险面。
[关键词] 渗透测试；医院；信息系统；网络安全
中图分类号：C37　文献标识码：A

Network security detection of hospital information system based on penetration testing

Junbiao Peng　Guojian He
Shenzhen Municipal People's Hospital

[Abstract] Objective: The primary purpose is to conduct a security assessment on the RBRVS system of a certain hospital, identify existing network security vulnerabilities and risk points, follow up with rectification measures, thereby ensuring the safe and stable operation of the system. Additionally, this study aims to provide a reference for the network security assessment of information systems in other hospitals. Methods: On December 10, 2024, penetration testing and vulnerability scanning were employed to conduct a security assessment on the RBRVS system of a certain hospital. Common attack methods were used to simulate tests, and test results and identified issues were collected. Finally, based on the test results, a corresponding test report and rectification suggestions were formulated. Results: Through penetration testing and vulnerability scanning, security vulnerabilities such as SQL injection, weak passwords, and unauthorized access were discovered within the RBRVS system, and relevant technical personnel were organized to carry out vulnerability repairs. Conclusion: Penetration testing and vulnerability scanning can effectively assess the security of information systems, identify various application-level network security vulnerabilities, and promptly repair and mitigate risk areas.
[Key words] Penetration Testing; Hospitals; Information Systems; Network Security

1 研究背景

随着互联网技术的迅速发展,医疗行业都在不断地推进数字化转型,对于网络的依赖程度越来越高。与此同时网络安全相关的攻击技术也在不断地发展,网络攻击的手段越来越多样,攻击的频次越来越高[1]。网络攻击造成的数据泄露会给医院、个人等带来不可挽回的损失。在此背景下,我国相继制定发布了《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《医疗卫生机构网络安全管理办法》等法律法规,对医院的网络安全管理进行规范、约束和指导。因此,加强对医院信息系统的网络安全检测,防范化解安全风险就显得尤为重要。

2 相关理论

2.1数字化。狭义的数字化是指利用信息系统、各类传感器、机器视觉等信息通讯技术,将物理世界中复杂多变的数据、信息、知识,转变为一系列二进制代码,引入计算机内部,形成可识别、可存储、可计算的数字、数据,再以这些数字、数据建立起相关的数据模型,进行统一处理、分析、应用,这就是数字化的基本过程。广义的数字化则是通过利用互联网、大数据、人工智能、区块链、人工智能等新一代信息技术,来对企业、政府等各类主体的战略、架构、运营、管理、 生产、营销等各个层面,

进行系统性的、全面的变革，强调的是数字技术对整个组织的重塑，数字技术能力不再只是单纯的解决降本增效问题，而成为赋能模式创新和业务突破的核心力量[2]。

2.2信息安全。信息安全是指为数据处理系统建立和采用的技术和管理上的安全保护措施，以防止计算机硬件、软件、数据因偶然或恶意原因遭到破坏、更改和泄露。根据国际标准化组织(ISO)的定义，信息安全的核心目标是确保信息的保密性、完整性、可用性和可靠性。

2.3数据安全。数据安全是指保护数据免受未经授权的访问、使用、泄露、破坏或篡改的一系列措施和技术。它确保数据的机密性、完整性和可用性，防止数据在存储、传输和处理过程中被非法获取或篡改。

2.4网络安全。网络安全(Cyber Security)是指通过采取技术、管理和法律等手段，确保网络系统的硬件、软件、数据和服务的安全性，防止未经授权的访问、破坏、泄露或篡改。网络安全包括两方面内容：一是网络系统的安全，二是网络的信息数据安全。具体来说，网络安全旨在保护个人和组织的系统、应用程序、计算设备、敏感数据和金融资产，使其免受计算机病毒、勒索软件攻击等各种威胁。

3 测试方法

3.1渗透测试。渗透测试是一种在计算机系统上进行的授权模拟攻击，旨在对其安全性进行评估。通过模拟恶意黑客的攻击方法，渗透测试能够独立地检查网络系统的安全策略，发现网站、应用系统中存在的安全漏洞和风险点[3]。

3.2漏洞扫描。漏洞扫描是一种安全检测工具，用于检查计算机系统、网络或应用程序中的漏洞和安全弱点。它通过扫描等手段对指定的远程或本地计算机系统的安全脆弱性进行检测，发现可利用漏洞。常见的漏洞扫描工具，包括Nmap、Metasploit、XRAY、OpenVAS等。

4 RBRVS系统渗透测试的过程

采用渗透测试和漏洞扫描在2024年12月10日对某医院的RBRVS系统进行安全性检测，利用常见的攻击手段对其进行模拟测试，并收集测试结果和发现的问题。

本次检测过程用时两天，分为六个阶段。

4.1信息收集阶段。此阶段中，笔者收集该系统的域名和IP地址，确定目标系统的操作系统类型。使用BurpSuite等工具，收集网站地图和敏感目录，发现隐藏的漏洞。通过抓包、日志分析等技术，收集目标系统中的敏感信息，包括登录凭证、数据库密码、用户数据等。

4.2渗透测试阶段。使用nmap等扫描工具对目标系统的端口进行扫描，识别出有哪些服务在运行。漏洞扫描：利用XRAY扫描工具等对目标系统进行漏洞扫描，探测目标系统存在的漏洞和弱点。根据第一阶段获得的信息对网络、系统进行渗透测试。

4.3缺陷利用阶段。尝试使用弱密码或字典攻击破解管理员账号密码，并获取对目标系统的完全控制。尝试由普通权限提升为管理员权限，获得对系统的完全控制权。在时间许可的情况下，必要时从第一阶段重新进行[4]。

4.4成果收集阶段。对前期收集的各类弱点、漏洞等问题进行分类整理，集中展示。

4.5威胁分析阶段。对发现的上述问题进行威胁分类和分析其影响。

4.6输出报告阶段。根据测试和分析的结果编写直观的渗透测试服务报告。

5 RBRVS系统渗透测试的结果

依据本次渗透测试结果，我们发现该系统的五个较大安全漏洞。

5.1弱口令。通过密码字典爆破，笔者得到账号1和密码1为可用的账号密码组合，然后成功登录该系统。

5.2 sql注入。笔者发现某接口处没有对相关参数过滤导致sql注入，注入参数为property。于是在property参数处输入1/user，可获取到数据库用户名dbo。

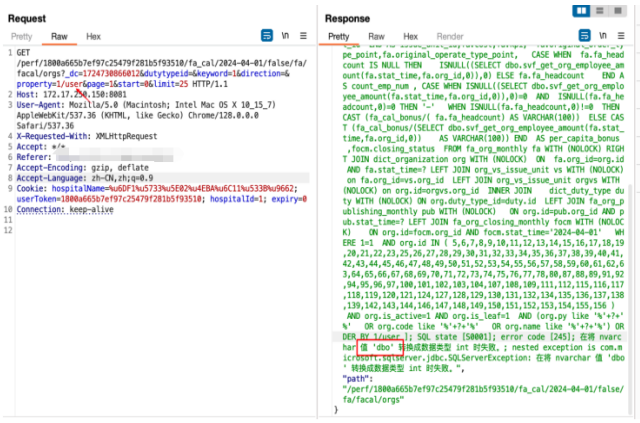

图1 RBRVS系统sql注入的数据包

5.3越权访问。

(1)笔者登录登陆低权限账号1KYK，获取其token信息，如图所示。(2)然后再登录高权限账号palline，获取token。(3)最后将高token替换成低权限token，可垂直越权使用高权限功能。

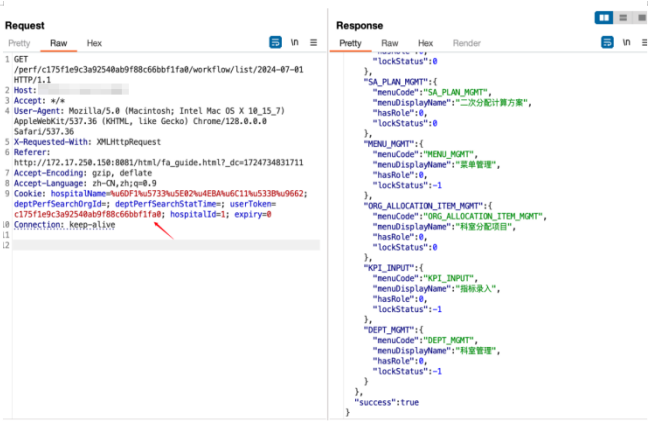

图2 低权限账号1KYK的token的数据包

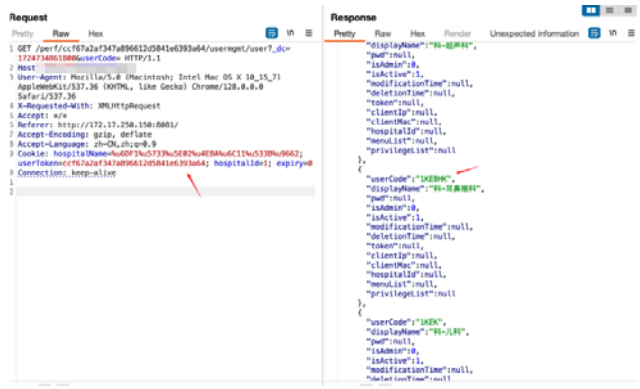

图3 高权限账号palline的token的数据包

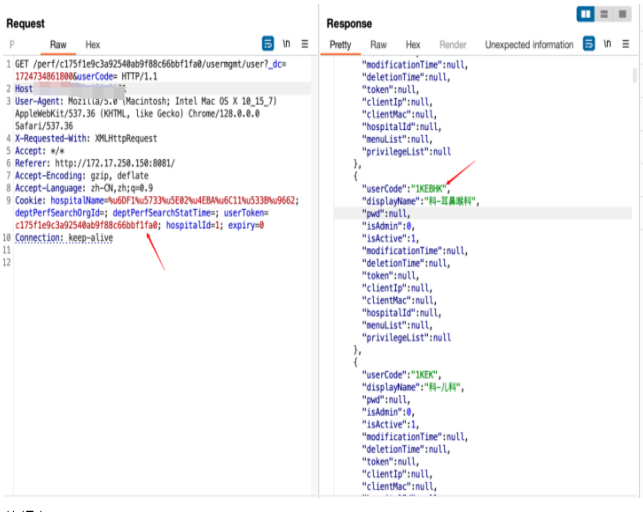

图4 高token替换成低权限token的数据包

5.4接口未授权漏洞。(1)笔者在前端发现一个接口。(2)通过拼接访问,可未授权获取用户uuid信息。

5.5报错信息泄漏。笔者通过破坏数据格式,发现该系统抛出异常返回包,泄漏了组件相关信息。

6 RBRVS系统的漏洞整改

针对测试中发现的问题和风险,笔者对系统的开发厂家提出以下建议,并跟进整改。

6.1弱口令整改。在代码层面用正则表达式设置8位以上的强口令,密码需同时包括数字、大小写字母和特殊字符。

6.2 sql注入整改。对property参数进行预编译,或者进行关键字过滤。

6.3越权访问整改。对用户操作进行权限校验,防止通过修改参数进入未授权页面及进行非法操作,建议在服务端对请求的数据和当前用户身份做校验检查。

6.4接口未授权漏洞整改。对该接口进行鉴权,使用sessionID和token进行绑定。

6.5报错信息泄漏整改。使用throwable类优化程序,防止数据抛出异常。

7 讨论

本文通过对某医院的RBRVS系统进行渗透测试,发现了其中存在的安全漏洞和风险点,并提出了相应的改进建议。这对于保障医院信息系统的安全性和稳定运行具有重要意义。

未来,随着医院数字化建设的深入推进,医院信息系统的安全问题将越来越受到重视。因此,需要建立完善的安全机制,包括加强员工安全意识教育、设置安全审计机制、建立紧急响应机制等,以应对更加复杂和隐蔽的网络安全威胁。同时,网络安全技术人员也需要继续探索和完善渗透测试方法和技术,确保其在医院信息系统安全检测中的正确性和有效性。

8 本次检测的不足

8.1测试时间存在不妥。本次测试均在正常的工作时间进行,测试工作对被测试系统带来一定的压力。

8.2本次测试的系统为正式系统,为更大程度的避免风险产生,应对备份系统进行测试。备份系统与正式系统所安装的应用和承载的数据差异较小,而其稳定性要求又比正式系统低。

8.3鉴于笔者的渗透测试经验和水平,可能未发现该系统的一些其他漏洞。

9 结语

本文通过对某医院的RBRVS信息系统进行渗透测试,发现其中存在的安全漏洞和风险点,并提出了相应的改进建议。本文旨在通过实践,验证渗透测试方法的有效性,并为其他医院信息系统安全管理提供一些参考。

[参考文献]

[1]舒婷,赵韡,徐帆,等.患者安全目标:智慧医院建设中的网络安全风险[J].中国卫生质量管理,2020,11(6):24-27.

[2]王卫国,陈东,王贤,等.数字化本质与运营模式进化的探讨[J].信息系统工程,2021,(11):10-13.

[3]孟晓阳,朱卫国,黄迎萍,等.医院网络渗透测试与数据包分析技术实践[J].中国卫生信息管理杂志,2017,14(6)838-842.

[4]王莹.HTML5下的流媒体内容保护系统的设计与实现[D].北京交通大学,2017.

作者简介：

彭俊标(1997--),男,汉族,广东省梅州市人,研究生,高级工程师,从事的研究方向：医院信息化、网络安全。