系统安全综合实训课程的教学实践与探索

姚慧
湖北工程学院，湖北 孝感 432000
DOI: 10.61369/TACS.2026040023

摘　　要： 作为网络空间安全专业的关键实践环节，系统安全综合实训课程致力于全面构建学生在 Web 渗透测试与安全防护领域的核心实践技能。本文以 Vulnhub 靶场作为核心实践平台，采用以实战为导向的教学模式，详细阐述了课程的教学目标设定、内容模块化构建、多元化教学方法以及综合性考核评价机制。通过对2022级学生课程目标达成度的量化评估，验证了教学效果，并基于教学实践中识别的问题，提出了具有可操作性的课程优化与持续改进方案，旨在为同类专业实践课程的建设与改革提供借鉴。

关 键 词： 网络空间安全；系统安全综合实训；Web 渗透测试；实践教学；课程目标达成度

Teaching Practice and Exploration of the Comprehensive Training Course on System Security

Yao Hui
Hubei Engineering University, XiaoGan, HuBei 432000

Abstract: As a critical practical component of the Cybersecurity program, the System Security Comprehensive Training course is dedicated to comprehensively cultivating students' core practical competencies in Web penetration testing and security defense. This paper employs Vulnhub as the core practical platform and adopts a practice-driven teaching model, elaborating in detail on the course's teaching objective formulation, modular content design, diversified teaching methodologies, and integrated assessment and evaluation mechanism. Through quantitative evaluation of the course objective achievement of the 2022 cohort, the teaching effectiveness is validated. Based on the issues identified during teaching practice, actionable strategies for course optimization and continuous improvement are proposed, with the aim of providing insights for the development and reform of similar professional practical courses.

Keywords: cybersecurity; system security comprehensive training; Web penetration testing; practical teaching; course objective achievement

一、课程定位与教学目标

系统安全综合实训是网络空间安全专业一门连接理论知识与工程实践的核心专业实践课程，共计48学时（全部为实验学时），对应3学分。其先修课程涵盖计算机网络、网络安全、网络攻防技术等，是学生进行毕业设计前至关重要的综合性能力训练环节[1]。本课程以 Vulnhub Web 渗透靶场为主要实践载体，构建了高度仿真的网络攻防对抗环境。通过一系列结构化的 Web 渗透测试项目实践，使学生深入理解 Web 系统常见安全漏洞的机理与攻击方法。

结合专业毕业要求，课程确立了四项核心教学目标：一是掌握 Web 渗透测试的标准技术流程（涵盖信息收集、漏洞利用、权限提升等环节），能够熟练运用 Burp Suite、SQLMap 等主流工具完成对指定 Vulnhub 靶场的渗透任务；二是能够针对 SQL 注入、跨站脚本（XSS）等典型 Web 安全漏洞，构思并设计基础性的安全防护方案，并理解安全系统设计与开发的基本逻辑；三是在防御方案设计过程中，能够综合考虑法律、安全等多重约束条件，展现出初步的创新思维，例如对防御策略进行优化改进；四是通过实践操作，深刻认识 Web 渗透测试活动可能对网络环境、服务器资源等方面产生的潜在影响。上述课程目标分别对毕业要求中的“设计 / 开发解决方案”、“使用现代工具”、“环境与可持续发展”等指标点形成了强支撑或中等支撑，是达成专业人才培养目标的关键实践环节[2]。

二、课程教学内容与方法设计

（一）模块化教学内容体系构建

课程紧密围绕四项教学目标，构建了由“环境部署与工具使用”、“Web 渗透核心技术”、“安全防御方案设计”及“综合项目实践”四大知识模块组成的教学内容体系。各模块内容循序渐进、相互衔接，总学时为48，分配比例为6:16:12:14，实现了从基础技能训练到复杂综合应用的能力培养闭环。

1. 环境部署与工具模块：本模块核心内容包括 Vulnhub 靶场镜像的安装与配置，以及在 Kali Linux 环境下 Nmap、Burp

Suite、SQLMap 等渗透测试工具的配置与基础操作。重点在于培养学生搭建实验环境和操作核心工具的基本技能，同时强调所有渗透测试活动必须基于合法授权的前提，帮助学生树立牢固的合规意识。

2. Web 渗透技术模块：本模块全面覆盖渗透测试的核心流程，包括信息收集（如 Nmap 端口扫描、Web 目录枚举）、漏洞利用（如 SQL 注入的手工测试与 SQLMap 自动化利用、XSS 攻击载荷的构造）以及权限提升技术。通过贴近实战的操作训练，使学生掌握 Web 渗透测试的全流程技术要点，并结合非法渗透行为的法律追责案例教学，强化学生的法律底线意识。

3. 防御方案设计模块：本模块聚焦于典型 Web 漏洞的防护实现技术，例如针对 SQL 注入的参数化查询防护、针对 XSS 的输入过滤与输出编码等。要求学生不仅掌握技术实现方法，还需在方案中主动融入《网络安全法》等法律法规的合规性要求，并鼓励探索轻量化、高效率的防御策略优化路径，从而培养学生的安全防护设计能力与初步的创新思维。

4. 综合项目实践模块：本模块以自定义的综合性 Web 靶场为项目载体，要求学生以小组协作形式，完整实施一次渗透测试全流程，并撰写专业的渗透测试报告与对应的安全防御方案报告。课程组织小组答辩与项目复盘讨论，并结合“护网行动”等国家级网络安全实战演练的经典案例进行讲解，激发学生维护国家网络安全的使命感，强化其团队协作能力与职业规范。

（二）“实战驱动 + 多维互动”教学模式

课程突破了以理论讲授为主的传统教学模式，综合运用实战教学、案例分析、小组协作项目及对抗演练（拓展环节）等多种教学方法，突出学生在学习过程中的主体地位，构建了“教、学、练、战”一体化的教学模式[3]。

1. 实战教学：以 Vulnhub 靶场为具体操作对象，教师通过多媒体演示结合实时屏幕投屏，详细讲解渗透技术的操作流程与工具使用技巧，学生同步进行实操练习。教师巡回指导，及时解决学生操作中遇到的问题，实现“边讲边练、讲练深度融合”，促进学生快速将理论知识转化为实际操作能力。

2. 案例分析：选取 Struts2远程代码执行、Heartbleed 等具有代表性的经典 Web 安全漏洞案例，深入剖析其漏洞原理、具体攻击过程以及有效的防御技术应用。组织学生进行交互式课堂讨论，引导其分析漏洞利用的关键环节与防御策略的核心思想，从而提升学生的技术深度分析与复杂问题研判能力。

3. 小组协作项目：将学生划分为4-6人的项目小组，布置针对自定义 Web 靶场的攻防综合项目。要求各小组通过协作，完成从信息收集、漏洞发现与利用到最终防御方案设计的全流程。教师定期组织项目进度汇报，针对各小组遇到的技术难点与团队协作问题进行针对性指导，着力培养学生的团队协作精神与解决复杂工程问题的能力。

4. 对抗演练（拓展选做）：将学生分为攻击方（红队）与防守方（蓝队）。攻击方实施 Web 渗透测试，防守方则需实时监控、发现攻击并部署漏洞修复与防御策略。通过屏幕共享、日志分析等方式展示对抗过程，演练结束后组织全面的复盘讨论，总结渗透技巧的有效性与防御策略的优劣，极大强化学生的实战应用与安全应急处置能力。

此外，课程在各个教学环节中有机融入了课程思政元素，将合法合规意识、维护国家网络安全的责任感与使命感、团队协作的职业规范等贯穿于教学全过程，实现学生专业实践能力与综合职业素养的协同培养[4]。

三、课程考核体系与达成度分析

（一）多元化考核体系设计

各项课程目标在总评成绩中的考核权重进行了差异化设计：课程目标1（基础技术）和课程目标4（环境认知）各占10%，侧重于考核学生的基础操作与理论认知能力；课程目标2（防御设计）和课程目标3（合规创新）各占40%，重点突出对学生安全方案设计能力与综合创新素养的考核。该考核体系与教学目标高度契合，能够较为全面地反映学生的综合实践能力水平。

课程摒弃了单一的期末笔试考核模式，构建了由“项目实践过程”（占40%）、“项目答辩”（占30%）和“项目报告”（占30%）三部分构成的多元化综合考核体系。考核内容与四项课程目标精准对应，旨在实现“以考核促进学习，以评价驱动能力提升”。

1. 项目实践：此项考核支撑全部四项课程目标。以团队形式完成实践任务，评分依据包括实践文档的完整性、测试逻辑的合理性、操作过程的规范性等。团队负责人需根据各成员的实际贡献度，在0.80至1.10的范围内设定个人评分系数（团队平均系数不超过1，且系数不重复），最终个人成绩由团队基础分结合个人系数计算得出。

2. 答辩：此项考核主要支撑课程目标2和3。以团队为单位进行答辩，成绩由“答辩过程分”（占60%，考核项目讲解的清晰度、技术阐述的准确性及回答问题的能力）和“答辩 PPT 质量分”（占40%，考核 PPT 结构的完整性、内容的全面性与呈现效果）两部分组成，再结合个人贡献系数折算为个人最终成绩。

3. 项目报告：此项考核主要支撑课程目标2和3。以团队提交的电子版项目报告为评价对象，从渗透测试步骤的完整性、漏洞分析的清晰度与深度、工具使用的规范性、技术细节的准确性以及文档格式的规范性等多个维度进行评分，同样结合个人贡献系数计算个人成绩。

（二）2022级学生课程目标达成度分析

2022级网络空间安全专业共有51名学生修读本课程。课程总评成绩平均值为83.06分，中位数为83.00分，标准差为7.21。最高分为96.99分，最低分为66.40分，无不及格学生。成绩分布情况为：优秀（≥90分）10人，占比19.61%；良好（80-89分）24人，占比47.06%；中等（70-79分）16人，占比31.37%；及格（60-69分）1人，占比1.96%。成绩分布基本符合正态分布，表明整体教学效果良好。

四项课程目标的达成度均显著高于0.6的预设合格标准，具体表现如下：课程目标1的达成度为0.88，表明学生能够熟练使用各

类渗透测试工具完成靶场任务，技术基础较为扎实，较2021级提升了0.10；课程目标2的达成度为0.82，表明学生能够有效识别典型 Web 漏洞并设计出基础防御方案，对系统设计开发流程有较好理解，较2021级提升了0.08；课程目标3的达成度为0.82，表明学生能够在防御方案中融入法律、安全等约束因素，并体现出一定的创新意识，合规与创新能力较2021级提升了0.08；课程目标4的达成度为0.88，表明学生能够深入认知 Web 渗透测试对环境的潜在影响，理论联系实际的能力较2021级提升了0.06。

整体而言，2022级学生在 Web 渗透基础技术操作和环境认知方面表现突出，在防御方案设计与合规创新能力方面也呈现出稳步提升的态势。各课程目标达成度均实现了同比（较2021级）增长，这证明课程现行的教学内容设计、教学方法应用以及考核评价体系是科学且有效的，能够有力地支撑学生实践应用能力的培养。

四、课程教学存在的问题与持续改进措施

（一）教学过程中存在的核心问题

尽管课程整体教学效果良好，目标达成度较高，但结合教学实践反馈与达成度分析的深层次解读，仍可识别出一些亟待优化的问题：一是 Web 渗透技术教学目前主要依托于标准化靶场场景，与企业真实、复杂的网络环境存在一定差距，导致学生在面对多因素交织的复杂场景时，其技术应变与综合应对能力尚有提升空间；二是在漏洞防御方案设计环节，教学多侧重于基础防护方法的实现，学生对漏洞产生的底层机制理解不够深入，导致所设计的方案在针对性与创新性方面有待加强；三是法律法规与安全因素在方案中的融入目前多作为基础性要求提出，学生对法律条款的理解深度及其在工程实践中的具体应用能力（即合规设计能力）有待进一步深化[5]。

（二）针对性持续改进措施

针对上述问题，结合课程教学目标与专业人才培养的总体要求，拟从四大教学模块出发，制定分层、可操作的持续改进措施，以推动课程教学质量实现螺旋式上升：

1. 优化 Web 渗透技术教学：在现有靶场基础上，引入基于企业真实事件改编的网络安全案例与高仿真网络环境，增设复杂场景下的渗透测试实操项目，例如多漏洞链式利用、内网横向移动渗透等。同时，建立学生“技术互助学习小组”，鼓励学生分享在解决复杂问题过程中的经验与思路，从而提升其在复杂、动态场景下的技术应对与协同攻关能力。

2. 深化防御方案设计教学：在教学中增加对典型漏洞底层原理的深入剖析，结合 CVE 漏洞数据库详情、OWASP Top 10年度安全报告等资源，引导学生从源代码、协议机制等根源上理解漏洞成因。引入“项目式学习”（PBL）模式，要求学生以小组为单位，针对一个模拟的企业级 Web 应用，设计一套完整的安全防御体系方案，并组织跨小组的方案互评与公开展示，以提升方案设计的系统性、针对性与创新性。

3. 强化合规与创新意识培养：系统性地将《网络安全法》、《数据安全法》、《个人信息保护法》等关键法律法规的核心条款融入相关教学模块，并结合近期真实的网络安全违法处罚案例开展警示教育[6]。在考核中设立“防御方案创新奖”评比环节，明确鼓励学生探索轻量化部署、低资源消耗、高效率防护的创新型防御策略，并对评选出的优秀创新方案进行课堂专题展示与推广，有效激发学生的创新思维与探索热情。

课程教学团队将持续跟踪上述各项改进措施的实施效果，结合后续年级学生的课程目标达成度数据、教学满意度反馈以及行业技术发展动态，对教学内容、教学方法与考核体系进行动态评估与优化，建立并完善“教学－实践－考核－反馈－改进”的闭环质量管理机制，确保课程建设始终与网络空间安全行业的技术演进趋势及人才能力需求保持同步。

五、结语

系统安全综合实训作为网络空间安全专业人才培养体系中的核心实践课程，是锤炼学生 Web 渗透测试与安全防御实战能力、塑造其合法合规职业素养的关键环节。本文通过对课程定位、教学目标、内容体系、教学方法及考核评价机制的系统性梳理，结合对2022级学生课程目标达成情况的实证分析，明确了当前课程教学的优势所在与不足之处，并据此提出了具有针对性的持续改进策略。网络空间安全技术日新月异，面临的威胁态势持续演变，与之相应的实践课程教学也必须保持动态发展与持续革新[7]。展望未来，系统安全综合实训课程将继续坚持“实战驱动、能力为本、素养协同”的教学理念，紧密对接网络安全行业的技术前沿发展与企业的实际人才需求，不断优化课程教学内容与实战载体，创新教学方法与考核模式，持续提升课程教学质量和育人成效，为培养能够适应并引领网络空间安全行业发展的高素质、应用型专业人才奠定更为坚实的实践能力基础。

参考文献

[1] 牛晓博，胡正高，刘曼琳 . 网络安全课程对抗式教学方法探索与实践 [J]. 网络安全技术与应用 ,2025,(04):122-124.

[2] 王怀习，束妮娜，王晨，等 . 科研学术反哺教学在网络空间安全学科中的教学探索与实践 [J]. 高教学刊 ,2025,11(13):22-25.DOI:10.19980/j.CN23-1593/G4.2025.13.006.

[3] 曾晟珂，何明星，牛宪华，等 . 课程思政视角下研究生案例教学探索与实践——以西华大学密码学与网络安全课程为例 [J]. 软件导刊 ,2024,23(08):198-203.

[4] 游海晖，廉龙颖，陈荣丽，等 . 网络安全课程思政的教学框架研究 [J]. 电脑知识与技术 ,2025,21(26):169-171.DOI:10.14004/j.cnki.ckt.2025.1338.

[5] 曹越，杜雪茹，陈治宏，等 . 信息化时代下网络安全课程创新探索 [J]. 计算机教育 ,2025,(09):55-60.DOI:10.16512/j.cnki.jsjjy.2025.09.013.

[6] 胡雪丽，马旭攀，丁文博 . 以实战能力为导向的网络信息安全课程教学改革 [J]. 计算机教育 ,2025,(08):22-27.DOI:10.16512/j.cnki.jsjjy.2025.08.012.

[7] 杨玉丽，陈永乐，于丹 . 新工科背景下网络协议安全课程教改探索 [J]. 大学教育 ,2024,(10):52-54+63.

