College and Job 职业教育发展, 2025, 14(8), 390-396
Published Online August 2025 in Hans. https://www.hanspub.org/journal/ve
https://doi.org/10.12677/ve.2025.148397

Hans汉斯

融入CTF竞赛和高校信息中心的网络空间安全基础课程改革实践

姜婧妍[1*]，于丽娜[2#]，王树兰[1]，傅向华[1]，曹劲舟[1]

[1]深圳技术大学大数据与互联网学院，广东 深圳
[2]深圳技术大学城市交通与物流学院，广东 深圳

收稿日期：2025年7月14日；录用日期：2025年8月15日；发布日期：2025年8月26日

摘 要

随着网络空间安全上升为国家战略，高校网络安全人才培养面临新的挑战和机遇。本文基于深圳技术大学大数据与互联网学院网络空间安全基础课程的改革实践，探讨了将CTF竞赛训练与高校信息中心实践环境相结合的教学模式创新。通过构建“理论 + 竞赛 + 实战”三位一体的教学体系，有效提升了学生的网络安全实践能力和专业兴趣，为网络安全人才培养提供了新的思路和方法。

关键词

网络空间安全基础，CTF竞赛，高校信息中心，教学改革，实践教学

Curriculum Reform Practice of Integrating CTF Competition and University Information Center into Cyberspace Security Foundation Course

Jingyan Jiang[1*], Lina Yu[2#], Shulan Wang[1], Xianghua Fu[1], Jinzhou Cao[1]

[1]School of Big Data and Internet, Shenzhen Technology University, Shenzhen Guangdong
[2]School of Urban Transportation and Logistics, Shenzhen Technology University, Shenzhen Guangdong

Received: Jul. 14th, 2025; accepted: Aug. 15th, 2025; published: Aug. 26th, 2025

*第一作者。
#通讯作者。

文章引用: 姜婧妍, 于丽娜, 王树兰, 傅向华, 曹劲舟. 融入 CTF 竞赛和高校信息中心的网络空间安全基础课程改革实践[J]. 职业教育发展, 2025, 14(8): 390-396. DOI: 10.12677/ve.2025.148397

Abstract

With cyberspace security rising to the level of national strategy, cybersecurity talent cultivation in universities faces new challenges and opportunities. Based on the curriculum reform practice of the Cyberspace Security Foundation course at the School of Big Data and Internet, Shenzhen Technology University, this paper explores the teaching model innovation that combines CTF competition training with the practical environment of university information centers. By constructing a trinity teaching system of "theory + competition + practice", it effectively enhances students' cybersecurity practical abilities and professional interests, providing new ideas and methods for cybersecurity talent cultivation.

Keywords

Cyberspace Security Foundation, CTF Competition, University Information Center, Curriculum Reform, Practical Teaching

1. 引言

网络空间的重要性日益凸显，已成为与陆、海、空、天同等重要的国家战略领域，网络空间安全已成为国家安全体系的重要组成部分。2016 年国家互联网信息办公室颁布《国家网络空间安全战略》[1]，将网络空间安全提升为国家战略高度。同年，中央网信办等六部委联合发文《关于加强网络安全学科建设和人才培养的意见》[2]，明确提出了网络安全人才培养的战略要求。然而，传统的信息安全教学模式主要以理论讲授和基础实验为主，难以满足行业对实战型安全人才的需求。企业在招聘安全工程师时，普遍要求应聘者具备“真实攻击和黑灰产对抗经验，具备 CTF 大赛获奖证明、CVE 漏洞证明”等实践能力。这种理论教学与实践需求之间的鸿沟，成为制约网络安全人才培养质量的关键问题。

基于这一现状，深圳技术大学大数据与互联网学院结合“腾讯安全英才班”建设，对网络空间安全基础课程进行了深度改革，将 CTF 竞赛训练与高校信息中心的丰富实践环境相结合，构建了全新的教学模式。该改革不仅充分利用了高校信息中心的网络设备、服务器集群、多样化操作系统和真实业务环境等资源优势，还通过引入 CTF 竞赛这一国际流行的网络安全技术竞技形式，有效激发了学生的学习兴趣和实践能力。经过一个完整学期的教学实践验证，这种融合模式在提升学生实践能力、增强学习兴趣、改善教学质量等方面取得了显著成效。

2. 改革背景与现状分析

2.1. 改革背景

深圳技术大学大数据与互联网学院于 2022 年与腾讯公司合作创建了“腾讯安全英才班”，这是国内首个依托腾讯安全实验室设立的安全方向特色班。该班级的创建为网络空间安全基础课程改革提供了良好的平台支撑和企业资源支持。网络空间安全基础作为网络安全专业的核心基础课程，承担着为学生构建完整知识体系、激发专业兴趣的重要使命，主要涵盖密码学基础与应用、网络安全技术、环境与系统

安全技术、操作系统安全技术、数据库安全技术等核心内容。

在改革前，网络空间安全基础课程采用传统的理论教学与验证性实验相结合的模式[3]-[6]，存在理论与实践脱节、实践环境局限、竞赛体系缺失、产业需求差距等主要问题。课程内容偏重理论知识和密码算法的实现，缺乏对抗性实践环节，学生难以建立对网络攻防的直观认识。传统实验多为验证性操作，缺乏真实的网络攻防环境，学生无法体验实际的安全威胁和防护场景。同时，学校缺乏 CTF 竞赛队伍建设，学生对网络安全竞赛了解甚少，难以通过竞赛提升实践能力。此外，课程内容与企业实际需求存在差距，学生毕业后难以快速适应安全岗位的工作要求。

深圳技术大学信息中心拥有丰富的网络设备和实践环境，这些资源为网络空间安全基础课程改革提供了得天独厚的实践基础。信息中心具备完善的网络基础设施，包括核心交换设备、安全设备、服务器集群等硬件资源，多样化的操作系统和应用环境，涵盖 Windows、Linux、数据库等多种平台，真实的网络拓扑结构和业务系统，为攻防演练提供接近实际的环境，以及专业的技术团队，能够为教学提供技术支持和安全保障。这些优质资源的合理利用，成为课程改革成功的重要保障。

2.2. 网络安全实践教学研究现状

传统的网络安全教学多采用“理论讲授 + 验证性实验”的模式。然而，大量研究表明，这种模式因其环境虚拟、场景固化、缺乏对抗性等缺陷，难以有效培养学生的实际问题解决能力。为突破此困境，学术界和工业界进行了多方面的探索。一种主流的改进是构建高度仿真的虚拟实验室(Cyber Range)，通过虚拟化技术模拟复杂的网络环境和攻击场景。尽管网络靶场在很大程度上提升了实践的真实感，但其构建和维护成本高昂，且场景设计仍依赖于预设脚本，与真实网络环境的动态性和复杂性仍有差距。

2.3. CTF 竞赛在教学中的应用

作为一种流行的网络安全竞技形式，CTF 因其高度的趣味性、对抗性和实践性，被广泛引入教学过程。研究表明，基于 CTF 的教学法能显著提升学生的学习动机、团队协作能力和技术应用能力。例如，吴昊等人[7]通过分析 CTF 赛题来构建网络安全知识体系，证明了其对教学内容的有效反哺。然而，多数研究将 CTF 作为一门独立课程或课外活动，如何将其系统性地融入核心基础课程的日常教学，并与课程的理论体系紧密结合，仍是值得深入探讨的课题。

2.4. 本研究的理论框架与定位

本研究的教学模式设计主要基于两种教育学理论：建构主义[8]和情境学习[9]。建构主义理论认为，学习是学习者在与环境互动中主动建构知识意义的过程，而非被动接收信息。情境学习理论则强调，知识的掌握与应用深度嵌入在具体的“情境、活动和文化”之中，在真实或接近真实的环境中学习效果最佳。

将这两种理论应用于网络安全教学，意味着教学活动不应止步于抽象概念的讲授，而应为学生创设一个可以主动探索、实践和“建造”知识的环境。CTF 竞赛恰好提供了一个以问题为导向的“建构”场景，而高校信息中心则提供了一个无与伦比的“真实情境”。

综合上述分析，现有研究分别探讨了虚拟实验室、CTF 教学法等路径，但鲜有研究将 CTF 竞赛的系统化训练与高校信息中心这一独特的、现成的真实物理环境进行整合。本研究恰好填补了这一空白，通过“理论 + 竞赛 + 实战”的融合，探索在真实情境中实现知识建构的教学改革，旨在回答“如何有效利用现有高校资源，低成本地构建高保真实践教学环境”这一关键问题。

3. 课程改革设计与实施

本次改革的核心目标是构建“理论 + 竞赛 + 实战”三位一体的教学体系，通过融入 CTF 竞赛训练

和高校信息中心实践环境，提升学生的网络安全实践能力和专业素养。改革遵循实战导向、竞赛驱动、产教融合、能力本位的基本理念，教学设计深度融合了建构主义与情境学习理论，强调学生在真实情境中主动构建知识与技能。以真实的网络攻防场景为教学背景，让学生在实践中掌握安全技术，通过 CTF 竞赛激发学生学习兴趣，培养团队协作和问题解决能力，结合企业需求和行业标准，缩短教学与实践的差距，以培养学生的实际操作能力和创新思维为核心目标。

网络空间安全基础课程设计为 4 学分，18 周教学，每周包含 2 课时理论教学和 2 课时实践教学。课程整体架构分为四个层次，见图 1：理论教学层涵盖密码学基础、网络安全技术、系统安全、应用安全等核心内容；实践教学层包括信息中心实训、攻防演练、漏洞挖掘、安全工具使用等实践环节；竞赛训练层融入 CTF 基础训练、专项技能提升、团队协作、实战竞赛等竞赛要素；评价体系层建立理论考核、实践评价、竞赛成绩、项目作品等多元化评价机制。

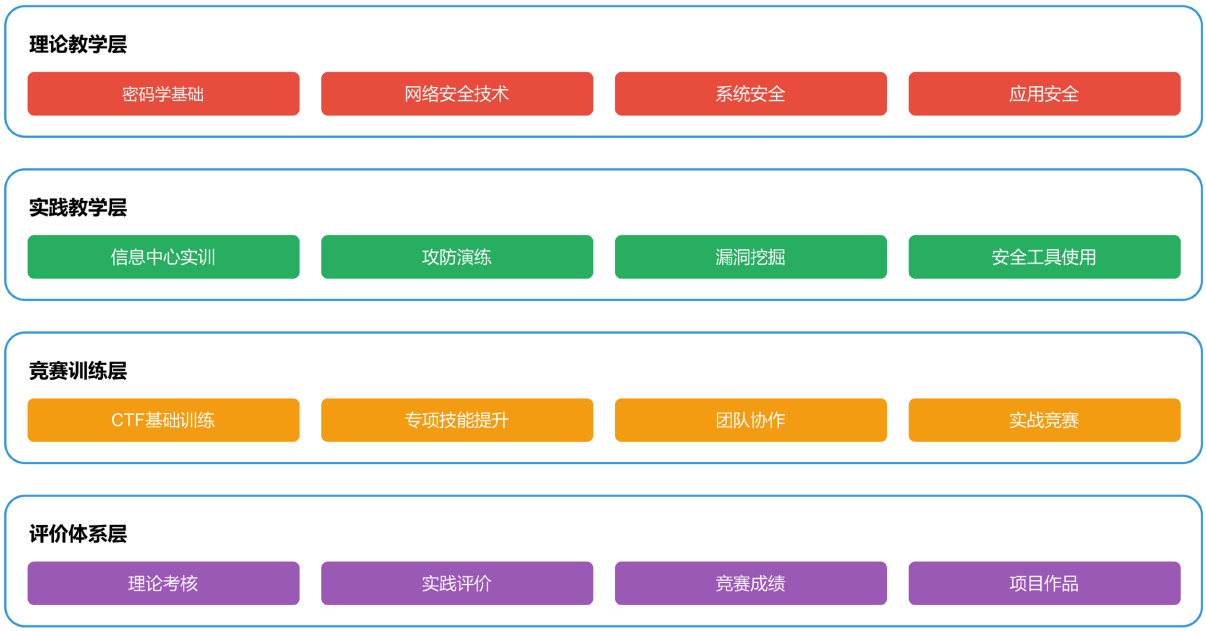

Figure 1. Curriculum framework for cyberspace security foundation course
图 1. 网络空间安全基础课程架构图

理论教学采用“知识点 + 案例 + 工具”的模式，将传统的理论知识与实际应用场景紧密结合。课程内容按照 18 周进行精心安排，第 1~2 周进行信息安全概论教学，涵盖信息安全基本概念、威胁模型、安全属性等基础知识，结合近期重大网络安全事件分析和威胁情报平台使用；第 3~6 周讲授密码学基础，包括对称加密、非对称加密、数字签名等核心技术，以 HTTPS 协议安全机制为案例，实践 OpenSSL、GPG 等工具使用；第 7~8 周学习网络安全技术，涵盖网络协议安全、防火墙、入侵检测等内容，结合企业网络安全架构设计案例，掌握 Wireshark、Nmap、Snort 等工具；第 9~12 周深入系统安全，学习操作系统安全机制、访问控制等知识，通过 Linux 系统加固实践，熟悉 SELinux、AppArmor 等安全机制。第 13~14 周专注 Web 应用安全，学习 OWASP Top 10、注入攻击、XSS 等漏洞类型，分析真实 Web 漏洞案例，掌握 Burp Suite、OWASP ZAP 等渗透测试工具；第 15~16 周学习安全管理，包括风险评估、安全策略、合规要求等内容，结合企业安全管理体系建设案例，使用风险评估工具进行实践；第 17~18 周介绍前沿技术与趋势，涵盖 AI 安全、IoT 安全、区块链安全等新兴领域，分析新技术安全挑战，体验专业安全检测工具。

实践教学充分利用高校信息中心的设备和环境，设计了三个层次的实践内容。为保障实践教学的安全性与可控性，我们采取了严格的技术隔离措施。所有实践操作均在通过 VLAN 技术划分的专用教学网络中进行，与校园网生产环境物理或逻辑隔离，并部署了行为监控与回滚机制，确保实验操作不影响信息中心正常运行。基础实践环节在信息中心的实验室环境中进行，学生学习基本的安全工具使用和安全配置，包括防火墙配置、入侵检测系统部署、漏洞扫描等基础操作，这些实践帮助学生建立对网络安全技术的基本认识。进阶实践环节利用信息中心的网络拓扑，构建真实的攻防演练环境，学生分组进行红蓝对抗，体验真实的网络攻击和防御过程，通过角色扮演和实战演练，深化对攻防技术的理解。例如，红队需利用指定的 Web 漏洞(如 SQL 注入)获取服务器权限，而蓝队则需通过分析 WAF 日志、修复代码来完成防御。高级实践环节结合信息中心的实际业务系统，开展安全评估和渗透测试实践，让学生在真实环境中提升安全技能，这种“准生产环境”的实践经验是传统实验室环境无法提供的。

CTF 竞赛训练贯穿整个学期，采用递进式培养模式。第 1~6 周进行 CTF 基础知识普及，介绍竞赛形式和题型，开展新手入门训练，让学生了解 CTF 竞赛的基本规则和参与方式，激发学生的参与兴趣。此阶段题目以基础知识为主，如一道 Web 方向题目可能要求学生通过分析 HTTP 响应头找到隐藏的 Flag。第 7~12 周开展分类别专项训练，包括 Web 安全、密码学、逆向工程、二进制安全等方向的深度训练，根据学生的兴趣和特长进行分组指导，提升专项技能。第 13~18 周进行团队组建和实战演练，组织校内 CTF 比赛，选拔优秀队伍参加外部竞赛，通过真实竞赛锻炼学生的实战能力和心理素质。

课程实施采用多种创新的教学方法和策略。项目驱动教学法以真实的安全项目为载体，让学生在解决实际问题的过程中掌握知识和技能；翻转课堂模式让学生课前通过在线资源自学理论知识，课堂时间主要用于讨论、实践和答疑；团队协作学习模拟 CTF 竞赛的团队模式，培养学生的协作能力和沟通技巧。同时，通过校企合作引入企业导师和真实项目案例，校内协同整合信息中心、网络中心等部门资源，为教学提供全方位支持，社区共建建立 CTF 兴趣社团，形成学习共同体，促进知识传承和经验分享。

4. 实施效果分析

经过一个完整学期的教学实践，课程改革在学生能力提升、学习兴趣激发、教学质量改善等方面取得了显著成效。为确保评估的客观性，本研究对修读该课程的 40 名学生进行了全过程跟踪。在未来的研究中，计划设置一个采用传统教学模式的平行班级作为对照组，以进行更严谨的比较分析。学生在技术能力方面表现出显著提升，掌握了 20 余种主流安全工具的使用，能够独立完成基础的渗透测试和安全评估任务，95%的学生能够在期末 CTF 考核上独立解决基础难度的题目。此处的“实践能力”通过一个包含 15 个评估点的评分细则进行量化，涵盖工具使用熟练度、漏洞分析逻辑、报告撰写规范性等维度。通过信息中心的真实环境实践，学生对网络安全技术有了更直观的认识，学生反馈表明实践环节帮助他们更好地理解了理论知识的应用价值。

教学质量的改善主要体现在课程满意度显著提升、学习成效明显改善、教学互动增强等方面。课程满意度通过期末匿名问卷调查进行，采用李克特五点量表法收集数据。学生对课程的满意度从改革前的70%提升到 92%，特别是实践环节得到了学生的高度认可，学生普遍认为实践训练更贴近实际工作需求，有助于提升就业竞争力。期末考试成绩分布更加合理，实践能力评分从平均分数增长 10 分，学生在安全工具使用、漏洞发现、攻防技术等方面的能力得到明显提升。课堂讨论更加活跃，学生提问和交流的频次明显增加，形成了良好的学习氛围，师生互动质量显著提高。

5. 特色与创新

本次课程改革的最大创新在于构建了“三层融合”的教学模式。理论与实践的深度融合不是简单的

理论 + 实验模式，而是让理论知识在实践中得到验证和深化，实践过程中发现的问题又推动理论学习的深入，形成了良性的学习循环。课程与竞赛的有机结合将 CTF 竞赛训练融入日常教学，让竞赛成为检验学习效果和激发学习兴趣的重要手段，既提升了学生的技术能力，又培养了团队协作和抗压能力。校内与校外的协同育人充分利用高校信息中心的资源优势，同时引入企业导师和项目，实现多方协同育人，为学生提供了从理论学习到实践应用的完整培养链条。

资源利用创新体现在信息中心资源的教学化改造和真实环境的安全实践两个方面。将原本用于学校信息化建设和运维的设备、网络、系统等资源，通过合理规划和安全隔离，转化为丰富的教学实践资源，这种资源的二次利用不仅降低了教学成本，还提供了更加真实的实践环境。在确保安全的前提下，让学生在真实的网络环境中进行安全实践，这种“准生产环境”的实践经验是传统实验室环境无法提供的，学生能够体验到真实工作环境中的复杂性和挑战性。

评价体系创新建立了多元化的评价体系，包括过程性评价、能力导向评价、团队协作评价等多个维度，具体权重分配为：小组展示 + 课堂讨论(30%)，实验报告(40%)，团队 CTF 竞赛成绩(20%)，以及课程项目报告(20%)。通过日常的实践操作、CTF 训练表现等进行过程评价，重点考察学生解决实际安全问题的能力，而不仅仅是理论知识的掌握，将团队合作能力纳入评价体系，培养学生的协作精神。这种多元化的评价方式更加全面地反映了学生的综合能力和素质，为学生的个性化发展提供了更好的支持。

6. 结论

通过融入 CTF 竞赛和高校信息中心资源的网络空间安全基础课程改革实践，成功构建了“理论 + 竞赛 + 实战”三位一体的教学模式，有效提升了学生的网络安全实践能力和专业素养。改革取得的成效表明，这种教学模式创新是可行的和有效的，为网络安全人才培养提供了新的思路和方法。课程改革的成功关键在于充分利用高校现有资源，将 CTF 竞赛训练有机融入日常教学，建立产教融合的协同育人机制，构建多元化的评价体系。这些经验对于其他高校开展类似的教学改革具有重要的参考价值。

然而，本研究也存在一些局限性。首先，该教学模式对师资力量和硬件环境要求较高，教师不仅需要扎实的理论功底，还需具备丰富的安全实战和 CTF 竞赛指导经验；同时，需要信息中心等部门的深度配合与资源投入，这在部分院校可能难以复制。其次，在实践教学过程中，如何实现更大规模学生的有效管理和风险控制，仍是需要持续探索的挑战。

面向未来，将继续深化课程改革，完善教学体系，为培养更多高质量的网络安全人才做出贡献。同时，期待与更多院校和企业开展合作，共同推动网络安全教育事业的发展。网络安全人才培养是一项长期而艰巨的任务，需要教育界和产业界的共同努力。通过不断地教学改革和实践创新，相信能够为国家网络安全战略的实施提供强有力的人才支撑，为提升全社会的网络安全水平贡献力量。

基金项目

广东省教育厅高等教育教学改革项目“高质量应用型计算机领域人才培养体系探索与构建”(20251056060005)；广东省教育厅教育科学规划课题(高等教育专项)“面向应用型本科教育的卓越成长型信息安全人才培养理论与应用研究”(2024GXJK283)；深圳技术大学校级教研项目“结合腾讯安全教学平台与 CTF 竞赛的信息安全导论课程教学创新研究”(20231009)。深圳技术大学校级教研项目“应用型大学‘数据科学与大数据技术专业’人才培养方案改革实践”(20251013)。

参考文献

[1] 国家互联网信息办公室. 国家网络空间安全战略[EB/OL].

http://www.cac.gov.cn/2016-12/27/c_1120195926.htm, 2016-12-27.

[2] 中央网络安全和信息化领导小组办公室等六部门. 关于加强网络安全学科建设和人才培养的意见[EB/OL]. http://www.moe.gov.cn/srcsite/A08/s7056/201607/t20160707_271098.html, 2016-06-12.

[3] 杨金宝, 高飞, 吴邱涵, 等. 基于 OBE 理念的网络空间安全专业实验体系构建[J]. 网络安全技术与应用, 2022(3): 96-97.

[4] 吴昊. 基于 CTF 赛题分析的网络安全学科知识体系研究[J]. 创新教育研究, 2023, 11(9): 2578-2584.

[5] 张成姝, 林捷. 信息安全技术课程校企合作中的教学改革探索[J]. 创新教育研究, 2019, 7(2): 237-241.

[6] 李忠伟, 刘哲理. 基于敏捷教学模式的网络空间安全基础课程建设与实践思考[J]. 计算机教育, 2020(3): 12-15.

[7] 吴昊. 基于 CTF 赛题分析的网络安全学科知识体系研究[J]. 创新教育研究, 2023, 11(9): 2578-2584.

[8] Vygotsky, L.S. (1978) Mind in Society: The Development of Higher Psychological Processes. Harvard University Press.

[9] Lave, J. and Wenger, E. (1991) Situated Learning: Legitimate Peripheral Participation. Cambridge University Press.