Advances in Education 教育进展, 2024, 14(12), 51-58
Published Online December 2024 in Hans. https://www.hanspub.org/journal/ae
https://doi.org/10.12677/ae.2024.14122231

Hans汉斯

基于竞赛驱动的网络安全教育教学改革探索

朱思征[1]，王山山[1]，徐　烨[1]，葛　昕[2]，王　丹[1]

[1]上海理工大学公共实验中心/计算中心，上海
[2]上海理工大学信息化办公室，上海

收稿日期：2024年10月30日；录用日期：2024年11月26日；发布日期：2024年12月4日

摘　要

在信息化时代的迅猛发展下，网络安全已成为全球关注的焦点，随着网络威胁的不断演进，网络安全人才的培养显得尤为关键。然而，当前的网络安全教育存在理论与实践脱节、课程内容更新不及时等问题，难以满足行业对高技能人才的需求。本文通过分析网络安全教育的现状与挑战，探讨了竞赛驱动教学模式在人才培养中的作用及其优势，并提出了改进网络安全教学的具体建议。将网络安全竞赛融入教学体系，有助于提高学生的实战能力，缩小课堂教学与行业需求之间的差距。该研究为网络安全教育的改革与创新提供了理论基础与实践参考，具有重要的教育和应用价值。

关键词

网络安全教育，网络安全竞赛，竞赛驱动学习，教学创新

Exploration of Competition-Driven Teaching Reform in Cybersecurity Education

Sizheng Zhu[1], Shanshan Wang[1], Ye Xu[1], Xin Ge[2], Dan Wang[1]

[1]Computer Center/Public Experiment Center, University of Shanghai for Science and Technology, Shanghai
[2]Informationization Office, University of Shanghai for Science and Technology, Shanghai

Received: Oct. 30th, 2024; accepted: Nov. 26th, 2024; published: Dec. 4th, 2024

Abstract

With the rapid development of the information age, cybersecurity has become a global focal point. As cyber threats continue to evolve, the cultivation of cybersecurity talent is crucial. However, current cybersecurity education faces issues such as disconnection between theory and practice and outdated course content, making it difficult to meet the industry's demand for highly skilled professionals. This paper analyzes the current status and challenges of cybersecurity education, explores

文章引用: 朱思征, 王山山, 徐烨, 葛昕, 王丹. 基于竞赛驱动的网络安全教育教学改革探索[J]. 教育进展, 2024, 14(12): 51-58. DOI: 10.12677/ae.2024.14122231

the role and advantages of competition-driven teaching models in talent development, and proposes specific suggestions for improving cybersecurity education. Integrating cybersecurity competitions into the teaching system helps enhance students' practical skills and bridge the gap between classroom instruction and industry needs. This study provides a theoretical foundation and practical reference for the reform and innovation of cybersecurity education, possessing significant educational and application value.

Keywords

Cybersecurity Education, Cybersecurity Competitions, Competition-Driven Learning, Teaching Innovation

1. 引言

随着全球数字化进程的加速，网络安全已成为当前社会和经济发展中的关键问题。信息技术的广泛应用虽然带来了诸多便利，但也加剧了网络安全威胁的增长。从国家的核心基础设施到企业和个人的数字资产，均面临着网络攻击的风险。频发的网络攻击事件不仅对国家安全构成威胁，还对企业运营的稳定性以及个人隐私的保护造成了严重影响。因此，各国将提升网络安全保障能力视为战略任务与重要目标。

网络安全人才的培养是增强网络防御能力的核心基础。根据《网络安全产业人才发展报告(2023 年版)》[1]，全球特别是中国在网络安全人才上存在巨大的缺口，尤其是在具备实战技能的高技术人才方面。

然而，传统的教育模式过于注重理论，无法紧跟技术的快速发展，课程更新滞后，实践环节不足，导致学生毕业时缺乏处理真实网络攻击的实战经验。这不仅限制了学生的职业发展，也无法满足行业对网络安全人才的需求。

为弥补传统网络安全教育的不足，网络安全竞赛成为培养高素质人才的一种有效方式。以 CTF (Capture The Flag)竞赛为代表的安全赛事，不仅提高了学生的实践技能，还促进了创新思维和团队协作能力。这类竞赛通过模拟真实的网络攻击与防护场景，使学生能将所学知识应用于实际操作中，并在实践中快速成长。通过竞赛的高强度实战训练，学生能够更加深入了解网络安全的最新技术和威胁趋势，从而增强应对复杂攻击场景的能力。

本论文探讨如何通过将网络安全竞赛引入教育体系，推动教学改革。通过分析当前网络安全教育中存在的问题，研究基于竞赛的教学模式，阐述竞赛在提高学生实战技能和培养高端人才方面的作用，并提出优化教学体系的具体策略。该研究不仅为高校网络安全教学改革提供了理论依据，还为培养符合产业需求的高素质网络安全人才提供了实践指导，具有重要的教育与社会价值。

2. 网络安全教育的现状与挑战

2.1. 国内外网络安全教育现状

国外大学生的网络安全教育在多个国家和地区得到了高度重视，尤其是在美国、澳大利亚、新西兰和欧盟等发达国家和地区。这些国家普遍将大学生网络安全教育纳入国家战略，通过制定相关政策、开展系统化教育计划、促进多方协作以及优化教育资源来提升大学生的网络安全意识和实战能力。美国通

过“国家网络安全教育计划”和设立“卓越学术中心”等项目，全面推动网络安全学科建设和人才培养；澳大利亚通过开展主题教育活动和推出“网络安全帮助按钮”，加强实践化教育；新西兰注重整合政府、学校、社会企业等多方力量，构建多维度的网络安全教育体系；欧盟则通过规范化师资培训和网络安全知识竞赛等手段，提升网络安全教育的软硬实力。这些国家和地区的共同目标是构建科学、系统的网络安全教育体系，为社会培养高素质的网络安全人才[2]。

我国近年来在网络安全教育方面取得了快速进展，尤其是《中华人民共和国网络安全法》颁布后，国家对网络安全人才培养的重视不断提升。自 2015 年将“网络空间安全”设为一级学科后，国内高校逐步加快了网络安全专业建设，截至 2022 年底，超过 200 所高校设立了网络安全相关专业[3]。然而，国内的网络安全教育体系尚在发展中，与发达国家相比，教育内容和实践训练环节仍需完善。

2.2. 网络安全领域的人才需求与缺口

随着信息技术的广泛应用和数字经济的快速发展，全球对网络安全人才的需求持续增长。中国的网络安全市场规模在 2022 年达到了 633 亿元，预计未来几年将保持年均 15%以上的增长。然而，网络安全人才供需严重失衡，尤其是具备实战能力的高端人才极度匮乏。2023 年，网络安全相关专业的毕业生总规模预计为 3.2 万人，但这一数量远不足以满足产业发展的需求。企业对网络安全工程师、渗透测试工程师、数据安全工程师等岗位的需求尤为迫切，尤其是《数据安全法》和《个人信息保护法》实施后，数据安全人才成为市场的紧缺资源[3]。高水平的网络安全人才不仅要掌握理论知识，还必须具备应对复杂安全威胁的实战经验。

2.3. 传统网络安全教育模式的不足

尽管网络安全教育逐渐受到重视，但传统教育模式仍存在较大问题。当前的教育体系过于注重理论教学，缺乏实战训练，导致学生在应对现实网络安全威胁时显得无力。教材和课程更新速度慢，往往无法跟上网络攻击技术的发展[3]。例如，许多高校课程内容滞后于产业需求，学生毕业时所掌握的技能难以满足企业的实际工作要求。实践教学和实验室资源匮乏也是一大难题。尽管部分高校已开始重视实践，但总体上，学生获得的实际操作机会有限。实习和实训环节的不足，使得学生在进入职场时，缺乏应对网络攻击和安全事件的实战经验。

2.4. 学生网络安全能力培养的瓶颈

网络安全领域对学生的能力要求不仅限于技术，更涉及到跨学科的知识应用。然而，现有的教学体系无法有效培养学生的综合能力。例如，渗透测试、逆向工程、密码学等高阶技能往往需要结合多门学科的知识，然而高校课程的设置较为分散，学生难以系统性地学习这些核心技能[3]。另外，由于师资力量不足，许多高校的教师缺乏实战经验，这直接影响了学生的培养质量。现有的教师队伍多以理论型为主，实际网络攻防经验有限，难以在教学中为学生提供切实可行的实战指导。

从目前看来，尽管网络安全教育体系正在逐步完善，但在人才供给、课程设置、实战能力培养等方面，仍存在诸多亟待解决的挑战。

3. 网络安全竞赛教育的特点与优势

3.1. 竞赛教育的实践性与实战性

网络安全竞赛教育的显著特点在于其较强的实践性和实战性，与传统课堂教学不同，通过模拟真实的网络攻击与防御场景，提供了一个动态的学习平台。在此过程中，学生不仅需要掌握理论知识，还必须灵活应用这些知识来解决实际问题。通过实战演练，学生能够直接接触各种网络攻击技术，如渗透测

试、漏洞发现和网络防御，积累宝贵的实战经验。事实证明，这种基于真实网络环境的竞赛模式有效地缩短了理论与实践之间的差距，使学生能够更好地应对现实中的复杂网络安全威胁。

3.2. CTF 竞赛在网络安全教育中的应用

CTF (Capture The Flag)竞赛是当前网络安全教育中最广泛应用的形式之一[4]，通过模拟真实的网络攻击与防御场景，要求参赛者利用破解、逆向分析和漏洞利用等技术手段“夺旗”，即利用安全漏洞找到指定的目标，竞赛不仅测试技术水平，还要求参赛者具备高度的灵活性和创造力。在网络安全教育中，CTF 竞赛不仅提升了学生的实战能力，还为他们提供了展示和应用技术的舞台，通过参与 CTF，学生能够深入了解网络安全的不同领域，如 Web 安全、逆向工程和密码学等。同时，竞赛题目紧跟网络安全领域的最新动态，帮助学生及时掌握前沿技术和新兴安全威胁。

3.3. 网络安全竞赛对学生技术能力和思维能力的提升

网络安全竞赛极大提升了学生的技术能力和思维能力，竞赛任务通常要求学生掌握渗透测试、漏洞修补和逆向分析等多项技能。在解决竞赛问题的过程中，学生不仅能系统巩固所学知识，还通过探索新问题学会使用多种工具进行漏洞挖掘和安全防御。不断的技术应用与练习，不仅深化了他们对网络安全的理解，也为未来职业发展奠定了坚实基础。此外，竞赛还培养了学生的逻辑思维与创新能力，由于问题通常没有固定解法，学生需要从不同角度思考并尝试多种技术手段，这种训练提升了他们解决复杂安全问题的能力，培养了批判性思维和创新意识。

3.4. 网络安全竞赛中的团队合作与应对复杂问题能力的培养

网络安全竞赛通常以团队形式进行，团队成员需要分工合作，共同应对复杂的网络安全挑战，这种合作不仅提升了学生的沟通能力，还锻炼了他们在高压环境下的协作与决策能力。在竞赛中，每位成员通常负责不同的任务，如漏洞分析、攻击测试和策略制定，这要求团队成员之间高效配合，互相支持，共同解决问题。在面对复杂挑战时，竞赛不仅考验技术水平，还要求团队具备迅速应对和调整策略的能力。面对不断变化的竞赛场景，团队需要在短时间内作出反应，并根据实际情况调整方案，以找到最佳解决方案。这种环境培养了学生在复杂情境下的决策能力和抗压能力，使他们能够更好地应对未来网络安全领域的挑战。

总体来说，网络安全竞赛通过实战训练、技术应用和团队协作等多方面的优势，弥补了传统网络安全教育的不足，为学生提供了全面提升能力的平台。通过参与竞赛，学生能够更快速、更有效地掌握网络安全技能，从而增强其在实际工作中的竞争力。

4. 网络安全竞赛融入教学的策略与实践

在网络安全教育中，融入竞赛元素不仅能够提升学生的实践能力，还能激发学生的学习兴趣。本节将探讨如何通过课程设计、项目制学习、学生自主学习、案例教学法以及竞赛结果与教学评估的关联，全面推进基于竞赛驱动的网络安全教育改革[5]。

4.1. 课程设计：如何将网络安全竞赛内容融入到课程中

课程设计是将网络安全竞赛有效融入教学的基础。首先，课程应围绕网络安全竞赛的主题和关键技能进行构建，例如网络攻防、漏洞分析和安全编程等。通过引入竞赛题目，教师可以在每个模块中展示相关内容。例如，在教授 SQL 注入时，利用历史竞赛中的具体题目，使学生能更直观地理解这一安全漏洞的实际应用。此外，课程设计应强调项目导向学习，鼓励学生参与模拟攻击与防御的项目，促进理论

与实践的结合。

4.2. 项目制学习与问题导向学习的应用

项目制学习与问题导向学习是提升学生动手能力和创新思维的重要策略。在此过程中，教师应设定与网络安全竞赛相关的真实问题，让学生在团队合作中解决实际挑战。通过将项目与竞赛场景结合，学生能够深入理解漏洞的成因及其防范措施，从而提高实战能力。

为了增强学生的自主学习能力，教师应提供丰富的学习资源，并鼓励学生根据个人兴趣进行选择。定期组织模拟竞赛，不仅可以让学生在压力环境中锻炼应对能力，还能通过反馈机制帮助学生识别自身的不足。在模拟竞赛结束后，教师应组织反思会，鼓励学生分享学习心得和遇到的挑战，这种互动形式将有助于深化学习效果。

4.3. 案例教学法的使用：通过竞赛题目反向推导知识点

案例教学法是一种有效的学习方法，通过分析历史竞赛中的经典案例，教师可以引导学生从实际问题出发，反向推导出相关的理论知识。例如，在讨论 XSS 攻击时，教师可以分析某个特定的竞赛题目，讲解如何有效防范此类攻击。通过小组讨论和案例分析，学生能够在互动中提升批判性思维能力。

4.4. 竞赛结果与教学评估的关联

竞赛结果为教学评估提供了重要依据，教师应通过分析学生在竞赛中的表现，如解题效率、正确率及团队协作能力，识别学生的强项与弱项。基于此反馈，教师可以适时调整课程内容和教学策略，确保教学的有效性。此外，将竞赛成绩纳入学期评估体系，能够激励学生积极参与，并通过设立奖学金或荣誉称号，进一步促进学生在竞赛中的努力。

通过以上多种策略与实践的结合，网络安全竞赛的融入不仅能丰富教学内容，还能有效提升学生的实战能力和创新思维，这一改革探索将推动网络安全教育的持续发展与创新。

5. 教研教改的关键措施

为了有效提升网络安全教育的质量，并更好地培养具有实战能力的高端人才，教研教改的关键措施需要聚焦于竞赛与课程体系的有机结合、教师角色的转变、跨学科融合以及校企合作等多个方面。这些措施能够推动教学创新，提高学生的实践能力和应对复杂问题的能力。

5.1. 建立竞赛与课程体系的有机结合机制

要让网络安全竞赛更好地发挥其教育作用，首先需要将竞赛内容与课程体系进行有机结合，将竞赛作为教学的一部分，不仅可以增强学生的学习兴趣，还能让学生在课程学习中实际应用所学知识，通过设计与竞赛任务紧密相关的实验课程或作业，学生能够在学期中不断实践，提升技术水平。课程中的理论教学可以通过与竞赛中真实案例相结合，帮助学生更好地理解网络安全的原理与应用。例如，利用 CTF 竞赛中的题目反向推导安全知识点，将竞赛中的复杂问题拆解成课程中的教学内容，使学生在理论学习的过程中逐步积累实践经验，实现从理论到实践的无缝衔接。

另外，为了适应不同阶段学生的学习需求，网络安全竞赛教育应设置分阶段的课程体系。基础课程可以涵盖网络安全的基本理论和技术，如计算机网络、操作系统安全、Web 安全等，帮助学生建立坚实的理论基础。随着学生能力的提升，高阶课程可以引入更复杂的竞赛内容，如漏洞挖掘、逆向分析、渗透测试等高级技能，逐步引导学生进入实战层面。

这种分阶段的竞赛课程设计能够帮助学生逐步掌握网络安全技能，避免过早接触过于复杂的问题导

致的挫败感。同时，逐步提升的课程难度也能保持学生的学习热情，使其在不断的挑战中持续进步。

5.2. 教师角色的转变：从知识传授者到引导者

随着竞赛和实践教学的重要性逐渐提升，教师的角色也需要随之发生转变。在网络安全教育中，教师应更多地成为引导者，帮助学生自主探索、发现和解决问题，可以通过设计开放式问题、引导学生参与竞赛、进行小组讨论等方式，激发学生的自主学习能力，不再仅仅是知识的灌输者，而是学生学习过程中的支持者和指导者，通过引导学生进行独立思考和合作学习，培养其分析问题和解决问题的能力。

5.3. 跨学科与多学科融合的教学方法创新

网络安全是一个跨学科的领域，涉及计算机科学、法律、管理、心理学等多个学科，教学方法的创新需要打破传统学科界限，采用跨学科和多学科融合的方式来培养学生的综合能力。例如，将密码学、法律合规、数据安全等内容引入网络安全课程，帮助学生在解决技术问题的同时，理解网络安全的法律和伦理背景。

跨学科教学可以通过项目制学习、团队协作等方式进行。例如，结合实际案例，要求学生不仅从技术角度解决问题，还要考虑法律风险和管理策略，从而培养学生的全局观和综合思维能力。

5.4. 校企合作与产教融合，利用企业资源提升学生实践能力

为了让学生能够更好地适应未来的职业需求，校企合作与产教融合至关重要，通过与网络安全企业合作，高校可以引入企业的实际项目和案例到教学中，为学生提供更多的实战机会。企业可以为高校提供实验室设备、技术支持以及网络安全竞赛中的实战平台，帮助学生在校期间积累实践经验。同时，企业可以通过提供实习机会、培训项目等形式，帮助学生了解行业前沿技术，提升其就业竞争力。通过产教融合的模式，学生不仅能够在理论学习中获得知识，还能通过企业的资源和平台，真正参与到网络安全的实际工作中，从而增强其实践能力和职业素养[6]。

通过以上措施建立竞赛与课程体系的结合机制、设置分阶段课程、转变教师角色、引入跨学科融合的教学方法以及加强校企合作，网络安全教育可以在实践性和实战性上得到进一步提升。这些教研教改措施有助于培养具备理论基础、技术能力和实战经验的高素质网络安全人才，推动网络安全人才培养体系的全面发展。

6. 网络安全竞赛教育的成果分析

6.1. 成功案例分析

2023 年，我们开设了“信息安全竞赛基础与实践”课程，并建立了 CTF 战队，以竞赛为载体将课程内容与实际应用结合，取得了显著成果。团队依托课程，积极参与国内各类网络安全竞赛，获得了多个重要奖项。其中，团队在 2023 年蓝桥杯全国总决赛中荣获一等奖第一名，这不仅体现了学生在网络安全领域的技术实力，也说明了课程设计的有效性和实用性。此外，团队还在 2023 年信息安全与对抗技术竞赛中荣获国赛二等奖、中国大学生计算机设计大赛国赛二等奖，以及全国大学生信息安全竞赛华东南赛区决赛的两项三等奖，在 2023 年省赛及以上级别的比赛中取得了超过 20 项奖项，这些奖项的获得展示了团队在不同层次和领域中的综合能力和实战经验。

此外，学生积极参与了“护网行动”等重大活动，通过参与网络安全防护任务，积累了宝贵的实战经验。2024 年，团队在信息安全与对抗技术竞赛中获得了国赛一等奖 2 项，省部级以上奖项将近 30 项，再次证明了课程与竞赛体系结合的成功。

6.2. 学生能力提升的表现

通过一系列竞赛和实践活动，学生的综合能力得到了全面提升：

技术能力的提升：通过课程与竞赛的结合，学生在渗透测试、漏洞挖掘、攻防对抗等关键技术领域取得了长足进步。特别是在蓝桥杯和信息安全与对抗技术竞赛中，学生的实战能力和技术水平得到了高度认可。这些竞赛要求学生不仅具备扎实的理论基础，还需要灵活应用最新技术工具来解决复杂问题。

创新能力的培养：竞赛中的开放性问题设计极大激发了学生的创新思维。学生在竞赛中不仅要解决常规的安全问题，还需要通过创新的思维方式来破解新的攻击手段，并提出独特的防护方案。中国大学生计算机设计大赛等竞赛中的表现也充分展示了学生的创造力。

团队合作能力的加强：网络安全竞赛通常以团队形式进行，要求成员之间紧密合作。通过参与 CTF 竞赛和护网行动等活动，学生们学会了如何在高压环境下与队友协作，制定有效的攻防策略。团队合作不仅提高了学生的沟通和协作能力，还培养了其解决复杂问题的综合能力。

6.3. 教育效果的反馈与评估

通过竞赛教育的实践，我们对教育效果进行了系统的反馈与评估。首先，学生的获奖情况反映了竞赛教育的成功和课程设计的有效性。连续取得的省赛、国赛荣誉，证明了学校在人才培养上的创新模式为学生提供了广泛的实践平台和发展空间。

其次，参与竞赛的学生在校内外的表现反馈良好，他们在竞赛中的实践经验帮助他们在课堂学习中对网络安全的理解更加深入。学生普遍反映，课程与竞赛相结合的教学模式不仅提升了他们的实际操作能力，还帮助他们巩固了理论知识，提高了学习兴趣。此外，企业对参与竞赛学生的实践能力和综合素质给予高度评价，许多学生在校企合作项目中获得了更多的实践机会。

通过数据分析，2023 年省赛以上获得的 20 多项奖项，以及学生在 2024 年进一步取得的优异成绩，说明竞赛教育显著提高了学生的综合能力，教育目标得以有效实现。这种以竞赛为主导的实践教学模式，能够为高校的网络安全人才培养提供持续的动力和方向。

7. 结论

网络安全竞赛教育已成为网络安全人才培养的重要模式之一，其实践性和实战性显著增强了学生的技术能力和问题解决能力。通过“信息安全竞赛基础与实践”课程的开设以及 CTF 战队的组建，学校实现了竞赛教育与课程教学的有机结合，学生在国内外重要赛事中屡获佳绩。这些成果表明，将竞赛嵌入教学体系，不仅能够激发学生的学习兴趣，还能提供一个将理论知识与实践技能相结合的平台，提升学生的综合能力。通过竞赛教育，学生不仅掌握了前沿的网络安全技术，如漏洞挖掘、渗透测试、逆向工程等，还在创新思维和团队协作方面得到了全面发展。实践证明，竞赛教育模式能够有效弥补传统课堂教学中实践环节的不足，并缩短理论学习与实际需求之间的差距，为学生未来的职业发展奠定了坚实基础。

网络安全教育已成为推动国家信息安全战略的重要支撑力量。通过竞赛教育模式的不断完善，网络安全教育将在未来的人才培养中发挥更加重要的作用。随着产业对网络安全人才需求的不断增加，教育机构必须不断创新教学方法、优化课程设计，以应对日新月异的技术发展。竞赛教育模式不仅培养了学生的技术能力，还为他们提供了一个与行业接轨的实战平台。未来，网络安全教育将继续在人才培养中发挥关键作用，为国家和社会培养具备综合能力、创新思维和实战经验的网络安全专业人才。

基金项目

上海理工大学本科教学研究与改革项目：产教融合推进下的网络安全实践教学创新的研究

(JGXM202341)。

参考文献

[1] 中华人民共和国工业和信息化部人才交流中心. 《网络安全产业人才发展报告（2023 年版）》正式发布[EB/OL]. https://www.miitec.cn/home/index/detail?id=3305, 2023-09-13.

[2] 谭玉, 张涛, 吕维霞. 大学生网络安全教育的国际比较及启示[J]. 电子政务, 2017(2): 117-125.

[3] 张卓群. 中国网络安全产业发展态势及对策研究[J]. 北京工业大学学报(社会科学版), 2022, 22(3): 75-85.

[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. https://doi.org/10.12677/CES.2023.119380

[5] 耿海军, 王威, 孟卓. 面向新工科的网络安全实践教育体系与实践平台构建研究[J]. 创新教育研究, 2023, 11(1): 65-71. https://doi.org/10.12677/CES.2023.111011

[6] 王高丽, 王梅, 章晴, 等. 面向网络安全领域拔尖人才培养的探索[J]. 教育进展, 2023, 13(11): 8574-8579. https://doi.org/10.12677/AE.2023.13111324