高校网络安全课程中的实践教学体系构建与优化

凤泽元

上海大学信息化工作办公室，上海市，200444；

摘要：本文聚焦高校网络安全实践教学，指出其存在需求错位（内容滞后于行业、忽视学生个性）与设施不足（设备陈旧、实验环境单一、软件资源短缺）两大问题。随后从三方面构建教学体系：通过联合调研、内容模块化设计及综合应用优化课程以对接行业需求；借助多元化教学方法植入与虚拟仿真等场景创设激发学习兴趣；通过校内资源统筹、校外校企合作及资源管理优化完善教学保障，旨在提升实践教学质量，弥合学生能力与行业需求的差距。

关键词：高校；网络安全；课程；实践教学；体系构建；优化

DOI：10.64216/3080-1494.25.11.090

1 高校网络安全课程中的实践教学存在的问题

1.1 需求错位

高校网络安全课程中实验教学还存在需求错位的问题，具体而言，网络安全行业技术更新迭代迅速，新的攻击手段、防御技术和安全标准持续涌现，然而高校网络安全课程的实践教学内容往往难以及时跟上行业发展的步伐，这就导致学生所学习的知识与实际工作需求之间存在明显差距。并且，不同学生对网络安全的不同方向可能有着不同的兴趣和天赋，但实践教学却未能充分考虑学生的个性化需求，普遍采用“一刀切”的教学模式，最终使部分学生对所学内容缺乏兴趣，学习积极性也随之不高。

1.2 设施不足

高校开展网络安全实践教学需要依托一套完善的测试设备，但随着网络安全技术的不断发展，部分高校的网络安全实验设备却未跟上时代发展步伐进行实时更新，无法满足实践教学的需求。

同时网络安全实践教学需要构建多样化的实验环境，包括不同的网络拓扑结构、操作系统与应用软件。但是，部分高校由于场地、资金等限制，导致实验环境过于单一，难以为学生提供丰富的实践机会。

此外，网络安全实践教学中需要使用到各种专业的软件工具，如漏洞扫描工具、渗透测试工具、安全评估工具等，但部分高校可能由于软件授权、资金等问题，无法为学生提供充足的软件资源支持。

2 高校网络安全课程中的实践教学体系构建

2.1 优化课程内容，对接现实需求

2.1.1 课程调研

针对课程调研，需组织联合调研小组，专业教师凭借其学术视野梳理网络安全领域的基础理论框架与核心知识要点，行业专家则依据实际工作中的技能需求、业务场景以及新兴威胁类型，提供关于课程内容实用性与前瞻性的重要意见，在校学生从学习体验与知识吸收角度反馈现有课程优缺点，多方通过定期研讨、问卷调查、实地访谈，精准定位课程内容与现实需求之间的差距，从而为后续内容优化提供详细依据。

例如，为解决渗透测试课程与行业需求脱节、学生实践能力不足的问题，某校组建由专业教师、行业专家、在校学生构成的联合调研小组，通过多维度调研明确优化方向。专业教师梳理渗透测试核心知识，涵盖OWASPTop10漏洞原理、渗透测试标准流程及报告规范；行业专家结合企业实践，指出电商支付接口检测、内网渗透工具应用及云环境渗透等技能缺口；学生反馈现有课程缺乏真实业务场景练习，对自动化工具高阶应用讲解不足。调研小组通过研讨、问卷、实地访谈，最终定位核心差距——学生缺乏“真实场景综合渗透能力”与“工具高阶应用能力”，为课程优化提供依据。

2.1.2 内容模块化设计

基于调研结果可开展课程内容模块化设计，要依据网络安全行业不同岗位能力要求以及技术发展趋势，将课程内容划分为基础理论、技术实践、综合应用以及前沿探讨4个模块——基础理论模块聚焦网络安全基本概念、密码学原理、网络协议安全等核心知识，为学生提供坚实理论根基；技术实践模块围绕渗透测试、漏洞挖掘、安全加固等关键技术，设置一系列具有针对性的实践任务，培养学生实践操作与问题解决能力。

例如，该校将渗透测试课程拆分为三个子模块，确保技能培养层层递进。基础工具应用子模块聚焦核心工具实操，教师演示 BurpSuite 代理配置、抓包分析等功能，布置“模拟电商登录弱口令破解”任务，要求学生用 Intruder 模块破解账号并提交报告；专项漏洞测试子模块针对高危漏洞训练，结合真实案例讲解 SQL 注入、XSS 漏洞原理，让学生在虚拟 CMS 系统中挖掘并验证漏洞，获取后台权限；综合场景渗透子模块模拟企业内网环境，学生需通过文件上传漏洞获取 Web 服务器权限，利用工具横向移动至域控，提交符合企业标准的渗透报告。

2.1.3 综合应用

综合应用模块通过模拟真实网络环境下的安全攻防演练、应急响应处理等项目，提升学生系统思维与团队协作能力；前沿探讨模块关注人工智能安全、区块链安全、量子计算安全等新兴领域，引导学生接触并研究行业前沿科技，拓宽知识视野和创新思维，各模块之间相互独立又紧密关联，形成层次分明、逻辑严谨的课程内容体系。

2.2 创新教学方法，激发学习兴趣

2.2.1 多元化教学方法植入

高校在推动网络安全课程实践教学的过程中，应当创新教学方法以激发学生的学习兴趣：在教学方法筛选环节，教师要深入剖析网络安全课程实践教学的特点与目标，结合学生的认知规律与学习风格，从众多教学方法中筛选出适合本课程的教学方法组合——项目驱动教学法因其能将理论知识与实践操作紧密结合，让学生在完成项目的过程中掌握知识技能，可作为主要教学方法之一；问题导向教学法通过引导学生自主发现问题、分析问题并解决问题，培养学生批判性思维与创新能力，也应当纳入教学方法体系之中；小组协作教学能够促进学生之间交流与合作，提升团队协作能力，同样不可或缺。教师可根据不同教学内容与教学阶段灵活应用这些教学方法，形成优势互补、协同增效的教学格局。

例如，以“提升实操与思维能力”为目标，该校灵活应用多种教学方法。项目驱动教学法以“模拟政务网站安全评估”为核心项目，学生分组完成需求分析、方案设计、测试执行及报告交付，教师分阶段指导；问题导向教学法围绕“WAF 绕过 SQL 注入”等难点，引导学生讨论方案并在虚拟环境验证；小组协作教学明确分工，设信息收集、漏洞扫描、漏洞利用、报告撰写岗，各组展示成果并接受质疑，深化技术理解。

2.2.2 教学场景创设

在教学场景创设方面，教师需要充分利用现代信息技术手段为学生打造丰富的学习场景，增强学习趣味性与吸引力：一方面可构建虚拟仿真实验平台，通过虚拟化技术模拟真实网络环境与安全事件，让学生在虚拟场景中进行实践操作，突破时间、空间和设备条件限制，能够反复练习与探索，加深对知识的理解和掌握。

另一方面可搭建在线学习社区，为学生提供一个交流互动、资源共享的平台，学生可以在社区中分享学习心得、讨论技术问题、展示实践成果，教师也可以及时给予指导和反馈，形成良好的学习氛围与互动机制；此外需引进游戏化学习元素，将网络安全知识与技能融入到游戏任务中，让学生在游戏过程中完成学习任务，有效激发学习动力与竞争意识。

例如，为突破传统教学的时空限制，该校构建了多维度的教学场景。在虚拟仿真实验平台方面，该校与某网络安全企业合作搭建“云安全实验平台”，平台包含 10 个模拟业务系统（电商、政务、OA、医疗、金融），每个系统预设近 3 年的高危漏洞（如 Log4j2 远程代码执行、SpringCloudGateway 代码注入、ApacheLog4j 漏洞），学生可通过浏览器登录平台，申请独立实验环境（环境包含 WindowsServer2019、CentOS8、Ubuntu20.04 等操作系统，预装 BurpSuiteProfessional、Nessus、MetasploitFramework、CobaltStrike 等工具），例如学生可申请“模拟医疗预约系统”环境，练习文件上传漏洞的利用——将包含一句话木马的“预约表单.pdf”伪装为图片文件上传，通过中国菜刀连接获取服务器权限，并查看数据库中的患者信息。

2.3 整合教育资源，完善教学保障

资源整合是推动实践教学开展的关键手段，教师要从校内资源统筹、校外资源引入以及资源管理优化等多个层面系统推进相关工作。

2.3.1 校内资源统筹

对于校内资源统筹，要求高校对现有网络安全相关设施设备、实验室等资源进行全面梳理整合——在师资方面，要打破院系壁垒，将计算机科学、信息工程、数学等多个学科中从事网络安全教学与研究的教师汇聚起来，依据教师专业特长与教学经验组建跨学科教学团队；在设备与实验室资源整合方面，要对分散在各院系的网络安全实验设备进行集中管理，建立起统一的网络安全实验教学中心，根据实践教学需求合理调配设备资源，提高设备利用效率，同时对实验室进行功能升级，

打造集教学、科研、实践于一体的综合性实验平台。

例如，在师资整合方面，该校打破计算机学院、数学学院、信息工程学院的院系壁垒，组建跨学科渗透测试教学团队，团队成员包括计算机学院“网络攻击与防御”方向教师（负责讲解渗透测试技术操作与实战案例）、数学学院“密码学”方向教师（负责剖析漏洞背后的数学原理，如 RSA 加密算法缺陷与漏洞利用的关联）、信息工程学院“网络协议”方向教师（负责讲解 TCP/IP 协议安全，如 ARP 欺骗、DNS 劫持在渗透测试中的应用），团队每周召开 1 次教学研讨会，确定课程的实验项目设计（如“基于 ARP 欺骗的内网流量劫持实验”）、教学难点突破方法（如“如何通过案例让学生理解缓冲区溢出漏洞的原理”）。

2.3.2 校外资源的引入

对于校外资源的引入，高校需要与网络安全企业、科研机构建立起长期稳定的合作关系，通过签订合作协议、共建实践基地等方式，引入企业的先进技术、实际案例与行业专家资源——企业可为学生提供实习机会，让学生参与真实的网络安全项目，接触行业最前沿技术与工作流程，提升实践能力和职业素养；科研机构则可以为高校提供科研合作项目，引导学生参与科研工作，培养学生的科研创新能力；此外高校还可邀请企业技术骨干与科研机构专家担任兼职教师，定期到学校开展讲座、授课以及实践指导活动。

例如，在企业资源引入方面，该校与本地 2 家知名网络安全企业（A 企业专注于 Web 安全服务，B 企业专注于内网安全与渗透测试）签订 3 年合作协议，共建“渗透测试实践基地”，企业每学期派 2 名技术骨干到学校开展 2 次线下实践课程，课程内容结合企业真实项目，如 A 企业技术骨干讲解“电商平台支付接口的逻辑漏洞挖掘”，通过演示某客户项目中“支付金额篡改”漏洞的发现过程（通过抓包分析支付请求参数，修改“amount”字段值从 100 改为 1），指导学生在模拟电商环境中复现该漏洞。

2.3.3 资源管理优化

资源管理优化是保障教育资源有效利用与持续发展的关键环节，高校需建立起完善的资源管理制度，明确资源管理责任和使用规范，对校内资源的采购、调配、维护进行全过程监控，确保资源合理使用与安全管理，对校外引入的资源则需要建立起资源共享与利益分配机制，明确双方的权利与义务，保障双方合作的合法性，促进资源可持续利用。

例如，针对校内资源，该校每学期末开展资源使用评估，通过统计设备使用率（目标不低于 85%）、教师与学生的满意度调查（发放问卷收集反馈，满意度目标不低于 90%），分析资源配置的合理性，如发现“漏洞复现区”设备使用率仅 60%，则调整该区域的漏洞环境，增加学生关注度高的新兴漏洞（如近期热门的 AI 模型安全漏洞）；针对校外资源，该校制定《校企合作资源共享与利益分配机制》，明确双方权利义务——高校负责提供学生资源、实践场地，协助企业开展人才培养；企业负责提供技术、师资、实习岗位，优先录用合作培养的学生；双方共同开发实践课程教材，教材版权归双方共有；建立合作评估机制，每学期末双方召开评估会议，通过查看学生实践报告、实习反馈、课程满意度数据，总结合作成效，如发现“企业实习学生的技术能力仍需提升”，则调整校内课程内容，增加实战演练课时；同时该校设立“校企合作专项基金”，每年投入 20 万元用于支付兼职教师课酬、购买企业提供的技术资源（如漏洞环境、工具授权），保障合作可持续开展。

3 结束语

总体来说，本文构建的高校网络安全实践教学体系，该体系不仅能切实提升学生的实践操作与创新思维，更为高校与行业协同培养网络安全人才提供了可复制的框架。未来需进一步跟进技术前沿，动态调整课程模块与合作模式，让教学体系始终适配网络安全领域的发展需求，持续为行业输送高质量人才。

参考文献

[1]刘军,王小金,余铁青. 情感分析驱动的高校课程教学策略优化研究——以“信息检索与网络安全”课程为例 [J]. 广东职业技术教育与研究, 2025, (05): 84-88+108. DOI:10.19494/j.cnki.issn1674-859x.2025.05.024.

[2]张彦华. 新质生产力背景下高校网络安全课程教学改革探讨 [J]. 产业与科技论坛, 2025, 24 (07): 179-181. DOI:CNKI:SUN:CYYT.0.2025-07-058.

[3]张金丹. 移动互联网时代高校网络安全教育教学建设研究 [J]. 办公自动化, 2025, 30 (02): 82-84. DOI:CNKI:SUN:BGDH.0.2025-02-024.

作者简介：凤泽元（1996.09—），男，汉族，上海市，硕士研究生学历，助理工程师，研究方向为校园网安全态势感知与运营、云原生安全，单位为上海大学信息化工作办公室。