网络安全意识培养融入计算机类专业课程教学的路径初探——以《网页设计与制作》课程为例

冯容
湖南化工职业技术学院，湖南 株洲 412000
DOI: 10.61369/TACS.2025090035

摘　　要： 当前网络安全意识培养在计算机网络专业课程教学中面临三大核心问题：目标割裂导致安全素养与专业能力培养脱节，路径单一限制实践转化效能，内容抽象难以激发学习主动性。本文以《网页设计与制作》课程为实践载体，突破传统教学中安全意识培养与专业技能教学的二元对立，形成“知识传授－能力训练－意识养成”三位一体的培养闭环，通过双目标协同框架设计、模块化安全知识嵌入、三维教学法创新及多元化评价体系构建，系统验证了融合培养模式的有效性。研究成果为计算机网络专业人才安全素养的系统化提升提供了可操作的实施范式，具有重要的理论参考价值与实践指导意义。

关 键 词： 网络安全意识；计算机网络专业；课程教学；教学改革

A Preliminary Exploration of the Path of Network Security Awareness Cultivation into Computer-Related Professional Courses --Take the Course "Web Design and Production" as an Example

Feng Rong
Hunan Vocational College of Chemical Technology, Zhuzhou, Hunan 412000

Abstract: The cultivation of cybersecurity awareness in computer network education currently faces three core challenges: fragmented objectives leading to disconnection between security literacy and professional skills development, limited pathways restricting practical application effectiveness, and abstract content failing to stimulate learning initiative.This study employs the "Web Design and Production" course as a practical platform, breaking the traditional dichotomy between security awareness cultivation and professional skill instruction. It establishes a three-in-one integrated framework encompassing "knowledge transmission, skill training, and awareness development." Through dual-objective collaborative design, modular integration of security knowledge, innovative three-dimensional teaching methodologies, and diversified evaluation systems, the research systematically validates the effectiveness of this integrated training model.The findings provide actionable implementation paradigms for systematically enhancing cybersecurity literacy among computer network professionals, offering significant theoretical reference value and practical guidance significance.

Keywords: network security awareness; computer network major; course teaching; teaching reform

一、研究背景和目的

随着《网络安全法》的颁布实施及数字经济的深度发展，网络安全已成为国家战略与行业发展的核心议题，计算机网络专业人才的安全意识培养因此具备了鲜明的时代必要性。当前计算机网络专业课程教学中，网络安全意识培养存在三大核心问题亟待解决：一是教学目标上普遍存在“重技能训练、轻意识塑造”的倾向；二是培养路径过度依赖独立安全课程或短期专题活动，导致知识覆盖面有限且难以形成持续教育；三是教学内容抽象化严重，与实际应用场景脱节，造成学生安全知识利用率低下。

通过将网络安全意识有机融入课程教学全过程，既响应了国家网络安全战略对人才培养的要求，也为解决当前专业教学中安全教育碎片化问题提供了新的实践方向[1]。

二、网络安全意识培养融入课程教学的理论基础

（一）网络安全意识培养的理论框架

网络安全意识培养的理论构建需以系统性模型为基础，其核

心在于四维度能力体系的协同发展。该模型具体包含风险合规响应意识、边界安全知识、管理技能及职业行为规范四个层面，为明确培养目标提供了结构化指导，确保学习者在认知、技能与素养层面形成闭环发展。在此基础上，引入“三全育人”理念，强调网络安全意识培养需贯穿教学全过程，实现课前引导、课中渗透与课后巩固的有机衔接[2]。

结合渗透式教学模式提出的“目标－知识－行为”三融合逻辑，将培养目标分解为可操作的知识模块与行为指标[3]，为课程教学中的意识培养提供了可迁移的实施路径。

这一理论框架突破了传统安全教学的技术导向局限，通过认知建构、技能训练与职业伦理的三维联动，实现从知识传递到素养内化的深层转化，为计算机网络专业课程融入安全意识培养提供了完整的理论支撑[4]。

（二）计算机网络专业课程教学的改革需求

当前计算机网络专业课程教学体系已难以适应网络安全人才培养的现实需求，其改革紧迫性主要体现在三个维度。首先是教学内容与行业发展脱节，胡向海的研究指出，现有教材更新周期过长，部分内容已显著滞后于技术发展，如传统杀毒软件相关知识占比过高，而云计算安全、物联网安全等前沿领域内容缺失[5]。其次是教学方法存在理论与实践失衡，多数专业教师仍采用口头宣讲的方式传授安全知识，缺乏沉浸式实践训练环节，导致学生难以将安全理论转化为防护能力[6]。最后是评价体系存在结构性缺陷，现有考核机制过度侧重技能操作熟练度，对安全意识养成、规范操作习惯等软能力的评估长期缺位，形成”重技术轻意识”的培养偏向。

这种教学体系的结构性矛盾，直接导致学生在进入职场后普遍存在安全防护意识薄弱、规范操作能力不足等问题，凸显了将网络安全意识培养融入专业课程教学的必要性与迫切性。

三、网络安全意识培养融入课程教学的实施路径

（一）目标定位：三维目标的融合

在计算机网络专业课程教学中融入网络安全意识培养，需构建“三维目标协同”定位框架，实现知识、能力与素质目标的三维融合。在知识目标层面，应系统嵌入网络安全核心知识，如 HTTPS 协议原理与数据加密技术，夯实学生的理论基础；在能力目标层面，通过基础层、进阶层、高阶三级梯度实现分学段培养，从聚焦风险识别能力，培养学生对常见网络安全威胁的感知与判断能力，到强化合规开发能力，要求学生在实践中遵循安全标准与规范，最终提升应急响应能力，训练学生应对安全事件的处置策略与流程；在素质目标层面，重点培养安全意识与合规素养，例如《网页设计与制作》课程可新增“合法合规获取素材”的专项能力目标，引导学生树立规范开发理念。

这种梯度化目标设计既符合学生认知规律，又能使网络安全意识培养与专业技能提升形成有机整体，为课程教学提供清晰可操作的实施路径[7]。

（二）内容设计：网络安全知识与专业技能的融合

在网络安全意识培养与专业课程教学的融合实践中，采用“模块化嵌入”设计思路具有显著的系统性优势。

以《网页设计与制作》课程为例，其安全内容融入采用“理论－演示－实践”三位一体的教学闭环。具体而言，将国际权威的 OWASP Top 10漏洞（如跨站脚本攻击 XSS、跨站请求伪造 CSRF）拆解为三个紧密衔接的教学环节：首先通过理论讲解建立漏洞认知框架，随后进行实时漏洞演示揭示攻击原理，最终指导学生完成防御代码的编写与部署。为强化抽象知识的具象化理解，课程设计“伪造淘宝网站”对比实验，通过抓包工具直观展示 HTTP 明文传输与 HTTPS 加密传输的安全性差异，使学生深刻理解数据传输层安全的核心机制。

（三）教学方法创新：案例驱动与项目实践的结合

为实现网络安全意识与专业课程的深度融合，本研究构建了以案例教学、项目实践、竞赛驱动为核心的“三维教学法”体系。在案例教学环节，通过分析真实 XSS 攻击事件，对比演示攻击代码与防御代码的差异，使学生直观理解漏洞原理与防护机制；项目实践采用分组开发模式，要求学生在网站开发中完成 HTTPS 配置、表单验证、敏感数据加密等安全功能实现；竞赛驱动环节则依托技能月赛，强制要求作品集成安全知识模块与漏洞防护功能，形成教学闭环。

以《网页设计与制作》课程的“安全表单设计”项目为例，教学实施遵循需求分析－方案设计－测试优化的工程化流程：在需求分析阶段强调用户信息收集的合规性，方案设计阶段要求嵌入 CSRF Token 等防护机制，测试优化阶段引入 OWASP ZAP 工具进行自动化漏洞扫描。

该教学体系通过“理论解析－实践应用－竞技提升”的递进式培养，有效解决了网络安全知识碎片化、实践环节薄弱的问题，为计算机网络专业课程的安全教学改革提供了可复制的实施路径[8]。

四、《网页设计与制作》课程中的实践案例设计

（一）课程安全模块的具体切入点

在《网页设计与制作》课程中融入网络安全意识培养，需根据不同教学章节的技术特点设置针对性安全模块。在“HTML 表单”章节，重点强化输入验证机制，通过限制特殊字符输入、实施长度验证规则构建第一道安全防线，同时引入CSRF 防护技术，指导学生在表单中嵌入验证 Token 以抵御跨站请求伪造攻击。进入“JavaScript 基础”章节，聚焦 DOM 型 XSS 漏洞防御，系统讲解输出编码规范与内容安全策略（CSP）的配置方法，帮助学生理解客户端脚本安全的核心原理。在“综合项目”实践环节，要求学生实现敏感数据加密功能，如采用 MD5算法对用户密码进行加密存储，并通过 Chrome 开发者工具查看 HTTPS 证书信息，掌握传输层安全配置技能。

通过章节化渗透与实验化教学相结合的方式，使学生在掌握网页开发技能的同时，建立”安全优先”的开发思维，实现技术

能力与安全素养的协同培养。典型教学案例实施过程为实现网络安全意识与《网页设计与制作》课程教学的有机融合，本研究以“用户登录表单安全开发”为典型教学案例，构建“法律规范－漏洞认知－防御实践－能力评估”的四阶教学实施路径，具体过程如下：

1. 需求分析：法律框架下的安全开发定位

教学实施首阶段聚焦网络安全法律规范与开发需求的转化衔接。依据《网络安全法》对个人信息保护的要求，明确用户登录表单开发需满足两大核心准则：一是用户信息收集必须获得明确授权同意，二是数据传输过程需采用加密技术保障机密性。通过解读法律条文与实际开发场景的对应关系，引导学生建立“安全合规优先”的开发思维，为后续漏洞分析与防御实现奠定法律认知基础。

2. 漏洞演示：攻防视角的风险可视化

采用“逆向教学法”设计无安全验证的登录表单原型，故意保留 SQL 注入漏洞风险点。教学中使用 OWASP ZAP 漏洞扫描工具对该表单进行安全检测，实时展示工具扫描发现的 SQL 注入漏洞细节，并通过模拟攻击演示未授权数据访问、数据库篡改等典型攻击后果。这一环节使抽象的安全风险转化为可感知的攻击场景，有效强化学生对漏洞危害性的认知，激发主动防御的学习动机。

3. 防御实现：分层防护的工程化实践

基于漏洞演示环节暴露的安全风险，组织学生以小组为单位开展防御方案设计与技术实现。实践任务涵盖三大核心防护技术：在前端开发中添加输入验证函数，过滤特殊字符以阻断注入攻击路径；在后端逻辑中嵌入 CSRF Token，构建跨站请求伪造防护机制；采用 SHA-256加密算法对用户密码进行不可逆加密存储，防止明文数据泄露。通过分组协作与技术攻关，学生系统掌握“输入验证－请求校验－数据加密”的多层防御体系，将安全理论转化为实际开发能力。

4. 效果评估：工具检测与方案论证结合

教学效果评估采用“技术检测＋方案阐述”的双维度评价体系。教师使用专业漏洞扫描工具对学生提交的防御方案进行自动化检测，验证输入验证、CSRF 防护、密码加密等功能的有效性；同时要求学生提交防御方案说明文档，阐述技术选型依据、防护原理及潜在优化方向。

教学实施逻辑链：通过法律规范锚定开发底线，利用漏洞演示揭示风险本质，依托分层实践构建防御能力，最终以量化评估验证教学成效，形成“问题识别－原理探究－工程实现－效果验证”的闭环教学体系，实现网络安全意识与网页开发技能的同步培养[9]。

五、网络安全意识培养的评价体系构建

（一）多元化评价指标设计

为实现网络安全意识培养与课程教学的深度融合，需构建“知识－技能－行为”三维评价指标体系。知识维度通过网络安全法规、漏洞原理笔试进行考核；技能维度聚焦漏洞检测工具使用与安全配置实操能力评估；行为维度则关注开发过程中的安全习惯养成，如定期备份代码、规范日志记录等关键行为。

在《网页设计与制作》课程中，该评价体系的落地呈现为：理论考试增设“HTTPS 工作原理”简答题，强化网络安全理论认知；实操考核要求学生使用 OWASP ZAP 工具扫描并修复至少2个网页漏洞，提升安全实践技能；行为评价通过“安全开发日志”追踪学生对“输入验证－输出编码－加密传输”安全开发流程的遵循情况。

（二）评价实施路径

为确保网络安全意识培养的教学效果，需构建“校内＋校外”联动的评价体系。校内通过技能月赛和课程实操考核实施过程性评价，重点检验学生在真实开发场景中的安全防护能力；校外联合企业开展实习评价，要求学生提交企业真实项目的安全开发报告（如参与企业网站漏洞修复实践），实现理论学习与行业需求的无缝对接[10]。

六、结论与展望

本研究通过《网页设计与制作》课程教学实践，构建了网络安全意识培养的”目标－知识－行为”三融合实施路径，验证了课程安全模块对提升学生安全防护能力的实践价值，并形成了包含过程性评价、漏洞挖掘实践、企业案例分析的多元化评价体系。

未来将从三方面推进实践：一是扩大试点至《局域网组建》《数据库原理》等5门核心课程；二是深化校企合作，引入企业真实漏洞案例库；三是迭代完善评价指标，重点强化安全行为量化评估，最终形成可复制的计算机网络专业安全意识培养融合范式。

参考文献

[1] 郭阳，董杨．基于＂三全育人＂视阈下高校网络思想政治教育的路径研究[J]. 杨凌职业技术学院学报，2023，22(02)：57-59.

[2] 梁海峰．移动互联网时代大学生网络安全教育研究[J]. 计算机产品与流通，2020(01)：246.

[3] 胡向海．中职计算机网络信息安全实践课程教学改革研究[J]. 现代职业教育，2020(47)：200-201.

[4] 方文超．基于总体国家安全观的面向在粤就读香港籍大学生课程思政建设研究——以＂网页设计与制作＂课程为例[J]. 当代教育实践与教学研究，2023(2)：171-173.

[5] 杜鑫．美国国家安全硕士培养模式研究[D]. 中国人民公安大学，2023.

[6] 王广丽．当代大学生自主网络安全意识宏观培养路径研究[J]. 改革与开放，2023(17)：62-66.

[7] 邱红丽，张舒雅．网页设计与制作课程思政实施探究[J]. 女报，2023(10)：0082-0084.

[8] 李若瑜，陈蔚，朱元彩，等．基于OBE理念的高职院校课程教学改革探索——以＂网页设计与制作＂课程为例[J]. 淮北职业技术学院学报，2023，22 (04)：63-66. DOI：10.16279/j.cnki.cn34-1214/z.2023.04.015.

[9] 李蔷．从＂讲授项目＂升华到知识建构教学——以＂网页设计与制作＂为例[J]. 电脑知识与技术，2021(31)：183-185.

[10] 贾丽．网络授课环境下教学内容及资源对学习效果影响的探究——以计算机专业相关课程为例[J]. 网络安全技术与应用，2020，(07)：102-103.

