人工智能赋能软件漏洞分析与利用课程思政教学探索*

彭碧涛** 刘珍

广东外语外贸大学信息科学与技术学院，广州 510006

摘 要 软件漏洞分析与利用作为培养网络空间安全专业人才的核心课程之一，其课程思政面临多重挑战，AI 技术的发展为问题解决提供了有效的实现路径。本文从多个维度深入剖析了软件漏洞分析与利用思政教学的难点，构建了 AI 赋能的课程思政策略，重构了课程教学育人目标和教师思政能力，结合课程具体内容，设计了详细的专业知识与思政元素融合内容，给出了“课前-课中-课后”的智能育人闭环，最后构建了多元统一的教学成效评价体系，教学实践显示 AI 赋能的课程思政实施从多个维度有效提升了教学效果，本文提出的解决方案对于推动网络空间安全人才培养具有重要意义。

关键词 人工智能赋能，课程思政，软件漏洞

AI-Empowered Curriculum Ideological and Political Reform of Software Vulnerability Analysis and Exploitation

Peng Bitao Liu Zhen

School of Information Science and Technology, Guangdong University of Foreign Studies
Guangzhou 510006, China

Abstract—As one of the core courses for cultivating professionals in cyberspace security, Software Vulnerability Analysis and Exploitation faces multiple challenges in implementing curriculum ideological and political education. The advancement of AI technologies offers an effective pathway to address these issues. This paper systematically examines the difficulties in curriculum ideological and political education for this course across multiple dimensions, An AI-empowered strategy is then constructed, which involves redesigning the educational objectives and enhancing instructors' ideological-political competencies. By integrating specific course content, we design a detailed fusion matrix that aligns professional knowledge with ideological-political elements. Furthermore, a closed-loop intelligent education framework covering the "pre-class, in-class, and post-class" stages is proposed, alongside a multidimensional and unified teaching effectiveness evaluation system. Teaching practices demonstrate the AI-enhanced curriculum ideological and political education implementation significantly improves instructional outcomes across various dimensions. The solutions proposed in this study hold substantial implications for advancing the talent cultivation system in cyberspace security.

Keywords—Artificial Intelligence Empowerment, Course Ideology and Politics, Software Vulnerability

1 引 言

在当今数字化、网络化、智能化交汇的时代，网络空间已成为继陆、海、空、天之后的第五大主权空间[1]，更是大国博弈的核心战略高地。习近平总书记多次强调，“没有网络安全就没有国家安全”[2]，人才的综合素质是网络空间对抗环境中决定胜负的因素[3]。作为网络空间安全专业的专业核心课程，《软件漏洞分析与利用》聚焦底层系统安全、漏洞挖掘机理及利用技术，具有极强的工程实践性与攻防对抗属性。然而，漏洞技术本质上是一把“双刃剑”，若缺乏正确的价值引领与法治观念约束，极易导致技术的滥用甚至滑向网络黑灰产。近年来，人工智能(AI)技术的爆发式演进，基于大语言模型的生成式人工智能以及多模态技术的突飞猛进，不仅推动了生产力的跃升，也为高校教育教学模式带来了颠覆性变革。利用人工智能重塑教学流程、优化资源供给、精准追踪学情，已成为解决传统硬核工科课程思政“生硬化”、“表面化”问题的有效途径。高校通过 AI 赋能企业真实案例的引入、智能技术的教学化应用以及价值观的隐形渗透，实现知识传授与价值引领的有效统一[4]。本文旨在深入剖析 AI 赋能《软件漏洞分析与利用》课程思政的

*基金资助：教育部人文社科规划项目“总体国家安全观视域下网络空间安全专业人才培养机制与实现路径研究”（项目编号：23YJAZH106）；广东省本科高校教学质量与教学改革工程建设项目“课程思政背景下网络空间安全专业的法律法规课程教学模式改革与实践”（粤高教函[2024]9 号）

**通讯作者：彭碧涛 pengbitao@gdufs.edu.cn。

内在机理，突出“AI 全面赋能+网安硬核攻防课思政融合”的创新点，探索构建漏洞课程专属的数智化思政体系，以期为国家培养具备坚实技术基础与高尚道德操守的新时代网络安全战士。

2 软件漏洞分析与利用课程思政现状

当前还没有针对《软件漏洞分析与利用》课程的思政研究论文，仅有的几篇相关课程思政研究论文均以《软件安全》课程为研究对象，且思政研究内容只是课程建设的一个子模块。例如张淼等在融入课程思政的《软件安全》深度学习中，提到了课程思政学习的五个目标，但是并未展开具体讨论[5]；牛伟纳等进一步在软件安全各个模块点提到了相关思政建设点，但并对课程思政如何实施进行具体阐述[6]。《软件漏洞分析与利用》的课程思政建设还处于起步阶段，相关成果非常匮乏。本文通过收集网络空间安全相关课程的教学思政研究成果，结合《软件漏洞分析与利用》的教学实践，总结其课程思政的难点主要体现在表 1 所示几个方面。

首先，该课程的现有教学内容中思政元素明显不足，专业教师在授课时存在“重技术、轻思政”的倾向，导致难以达到人才培养的复合目标。其次，专业教育与思政教育易出现“两张皮”的现象，思政元素未能与专业知识深度融合，传统思政元素常以“案例点缀”形式存在，难以应对深层育人需求，从而难以实现“润物细无声”的育人效果。漏洞分析与利用技术具有极强的实战性和破坏潜力，由于网络安全专业的特殊性，在科研实践中难免会学到网络攻击方法。若缺乏正确的价值观引导和法治观念约束，学生极易受到外部不良信息的误导，甚至可能无意识地利用所学技术进行违法违规活动。 而且，传统的思政教学以教师讲授 PPT 为主，一方面缺乏有效的思维互动，另一方面学生也无法实现对软件漏洞思政的直观感知，导致学生思政接受度低。最后，教学评价与反馈机制不健全，目前的考核评价往往偏重于理论成绩或纯技术实践，缺乏对思政育人情况及学生综合素质的考核，导致学生对课程思政内容的重视程度不够。

表 1 当前《软件漏洞分析与利用》课程思政教学难点分析

难点维度	现存主要问题	带来不良后果	传统模式的局限性
思政内容匮乏	该课程思政研究成果少，已有成果也都较简单，缺乏全面深入的研究。	学生难以理解软件漏洞的安全伦理、难以真正体会到软件漏洞的法律边界。	缺乏丰富的思政元素来培养道德红客。
内容融合度低	思政元素多以“贴标签”形式硬性插入，与逆向分析、内存溢出等底层硬核知识结合生硬。	形成“两张皮”现象，学生产生抵触情绪，无法实现思想上的共鸣与内化。	缺乏智能化手段对海量时政案例与底层技术进行图谱级别的深度语义关联。
伦理约束乏力	漏洞挖掘具有强破坏性，传统授课缺乏对“非法越权探测”、“漏洞黑市交易”的沉浸式警示。	学生法治红线意识淡薄，可能在好奇心驱使下无意识触碰网络违法犯罪底线。	缺乏直观的违法场景感知与交互式的伦理困境推演。
教学手段固化	依赖静态 PPT 讲授，思政教育单向灌输，缺乏对软件漏洞真实场景的融合展现。	课堂沉闷，抬头率低，难以激发学生打破核心技术“卡脖子”的使命担当。	缺乏 VR/AR 及生成式 AI 等多模态工具来构建生动、立体的历史与现实场景。
评价体系模糊	考核“唯分数论”，缺乏对学生操作合规性、社会责任感等隐性思政素养的量化跟踪。	思政成效缺乏评价，难以实现动态反馈与持续改进。	没有采集全过程学习数据，缺少多模态数据分析与价值认知评价。

2 人工智能赋能下课程思政实施策略

2.1 人工智能赋能下课程教学目标与思政育人目标

针对上述问题，本课程将生成式人工智能与大数据分析作为底层技术基础，重构“知识传授、能力培养、价值塑造”三位一体的育人体系，实现专业教学目标和思政育人目标的统一。在专业教学上：使学生熟练掌握各类软件漏洞的原理，能够运用各种分析工具进行基础漏洞的分析与利用，能够掌握多种漏洞挖掘方法的机理同时实现对软件漏洞的挖掘，进一步回溯分析软件漏洞的成因，并对漏洞代码进行修复，最终具备独立解决复杂软件漏洞相关问题的系统能力。在思政育人上：将国家网络安全战略、网络空间主权、攻防伦理红线、团队合作精神等元素融入教学；引导学生认清技术双刃剑效应，自觉杜绝黑灰产，肩负起新时代网络安全人才的科技报国使命；将思政教育融入课程课程知识传授和能力培养全过程，实现课程多维育人目标[7]。

2.2 提升教师思政站位和思政教学能力

教师是课程思政的“主力军”，人工智能的引入要求教师不仅要具备深厚的网安专业功底，还需掌握课程思政方面的教学素养。

首先，教师必须提高政治站位，坚定思想信念，深入领会总体国家安全观；能够明辨各种网络意思形

态风险，抵制各种网络错误思潮；熟悉国家网络安全战略、网信指导方针，思政立意高。同时，教师需要熟悉网络安全法、数据安全法、个人信息保护法、国家安全法等相关法律法规、以及刑法与网络犯罪相关条款，在此基础上构建网络法治思维，在教学中能把守法、合规不触碰法律红线融入教学中。

其次，有效的课程思政需要教师具备过硬的专业知识和行业素养，教师需要精通网络空间安全的专业知识，同时了解网络安全行业现状、国内外网络安全形势、各种网络安全 APT 热点攻击事件、大国之间的网络博弈、以及相关数据泄漏事件、网络战和漏洞安全相关现实事件，能够在专业知识讲解同时用专业案例来支撑思政育人。

与此同时，教师需要思政教学的核心能力，能够将课程思政有效的融入专业能力的学习中。通过选取合适的思政案例，结合教学设计，灵活运用多种形式，在教案、课件、实验、作业与考核中全过程的融入思政元素，实现专业知识学习与价值引领的自然融合。

2.3 人工智能赋能下课程思政教学内容设计

课程内容的无缝融合是防止“贴标签”的关键。本课程紧密结合大纲中的 48 学时教学内容，利用多种生成式 AI 工具，构建思政案例，并自动生成“核心知识点—安全事件—思政映射”的结构化知识图谱，实现专业知识与思政元素的有效融合。

（1） 第一部分：软件漏洞基础

① 技术知识点：软件漏洞基本概念

思政映射点：保护国家安全设施、国家安全大局观、防患于未燃的工匠精神。

安全案例事件：震网病毒利用 0Day 漏洞摧毁伊朗离心机的网络攻击事件。该事件借助 4 个 Windows 0day 漏洞，导致伊朗近千台离心机批量报废，是全球首个通过软件漏洞直接造成大规模物理设施损毁的实战级网络战。引导学生意识到软件漏洞不是简单的代码缺陷，是可以用来攻击的战略武器，守护漏洞就是守护国家安全；同时警示在编写代码时要严谨、防范代码中的漏洞。

教学形式：事件推演视频播放

② 技术知识点：漏洞分级与发展

思政映射点：国家网络空间安全主权、网络安全责任意识。

安全案例：CNNVD 处置 PrintNightmare 漏洞（CVE-2021-34527）真实事件。以该远程执行漏洞为例，CNNVD 第一时间定义为高危，并向全国政府、金融和能源等关键信息基础设施推送预警与加固方案。引导学生理解：漏洞是国家网络安全战略资源，树立漏洞上报、合规处置、为国护网的责任意识。

教学形式：时政解读+课堂问答

③ 技术知识点：汇编与堆栈结构、PE 文件分析

思政映射点：工匠精神、严谨求实、零缺陷

安全案例：曾引发广泛影响的 CVE-2021-3156 Sudo 堆溢出漏洞。程序处理参数解析时，对反斜杠转义字符的处理逻辑存在漏洞，导致超出缓冲区长度的数据被写入，覆盖了相邻的内存数据；该漏洞可以实现权限提升，普通用户获取 root 权限。引导学生理解：即使是最成熟的工具也可能存在最基本的缓冲区处理错误，导致严重的安全问题，培养严谨的工匠精神。

教学形式：关键漏洞代码及补丁前后代码对比分析

④ 技术知识点：软件逆向、注入和破解

思政映射点：法治底线、遵纪守法、职业伦理

安全案例：全国首例“故意避开或者破坏技术措施型”侵犯著作权案（上海刘某生案）。该案中，刘某生等人未经授权破解医疗设备软件加密狗，销售金额 100 余万元，被判刑 1 年制 3 年 2 个月。明确逆向、注入仅限授权安全检测；强化技术无善恶，用法有边界的职业伦理，违反《网络安全法》、《刑法》必担责。

教学形式：最高检典型案例宣读+法条对照

（2） 第二部分：漏洞原理与利用

① 技术知识点：栈溢出、堆溢出、整数溢出、格式化字符串漏洞

思政映射点：守护人民财产安全、防护关键基础设施

安全案例：WannaCry 勒索病毒利用 MS17-010 溢出漏洞瘫痪公共基础设施。黑客利用 MS17-010 溢出漏洞全球传播病毒，瘫痪机场、银行、医院等在内的很多基础设施，造成极大的破坏。让学生理解：漏洞可能会被恶意利用危害公共安全，树立技术守护安全而不是制造危害的职业伦理价值观。

教学形式：视频播放+小组讨论

② 技术知识点：结构化异常处理、虚函数利用

思政映射点：系统性思维、攻防辩证哲学

安全案例：奇安信 A-TEAM 发现 Windows 域高危漏洞 CVE-2019-1040 获微软致谢。介绍我国安全团队合法挖掘、规范披露 Windows 域认证高危漏洞。从

“攻”的角度延伸到“防”的知识体系，体现以攻促防、守正创新的安全哲学与红客精神。

教学形式:微软官方致谢页展示+攻防转化与红客精神小组讨论

③ 技术知识点:Shellcode 编写，加壳脱壳、DEP/ASLR 原理与绕过

思政映射点：合规攻防、授权边界、法治底线

安全案例：最高法指导案例 145 号。行为人未经授权，采用技术手段绕过系统安全防护机制，非法获取服务器控制权限,构成非法控制计算机信息系统罪。强化无授权即违法的思想，渗透测试、漏洞利用、以及防护绕过必须获得授权；强化无授权不操作、无授权即违法的合规底线。

教学形式：攻防场景模拟+合规底线强调

④ 技术知识点：复合漏洞、攻击链、综合案例

思政映射点：国家网络防御、团队协作、使命担当

安全案例：CNCERT 发布 2024 年我国某先进材料设计研究院遭遇 APT 攻击。境外 APT 组织使用漏洞利用→提权→持久化→数据窃取完整攻击链企图入侵关键关键设备。我方安全团队协同研判、阻断、溯源，守护科研机密。强化团队作战、为国护网的使命。

教学形式：CNCERT 调查报告展示+小组攻防演练

（3） 第三部分：漏洞挖掘技术

① 技术知识点：词法分析、数据流分析、程序切片

思政映射点：自主创新、科研报国

安全案例:南京大学 PASCAL 实验室发布软件的静态分析框架和实验平台“太阿”。该作品面向 Java 语言，在程序分析的多项指标均优优于国际主流框架，同时更可靠、更易用,该软件也获得 2024 年 CCF NASAC 青年软件创新奖。鼓励学生在基础软件上实现自主可控、突破“卡脖子”安全难题。

教学形式：展示“太阿”平台相关报道、引入“太阿”平台

② 技术知识点：程序插桩、AFL 模糊测试、符号执行、污点分析

思政映射点：主动防御、负责任的披露、以及白帽价值观

安全案例:360 漏洞研究院获 2025 开源鸿蒙社区漏洞挖掘突出贡献团队奖。360 漏洞研究院运用漏洞挖掘技术，助力国产操作系统安全建设，体现白帽守护、自主创新和为国铸盾的职业精神；同时引导学生做白帽守护者，拒绝黑灰产。

教学形式：展示相关报道+白帽价值观

2.4 人工智能赋能下思政教学实施

本课程采用线上线下相结合的混合式教学法，并在各个环节深度融合思政内容，形成全周期的智能思政育人闭环。

（1） 课前：AI 学情画像与个性化精准推送。利用线上数据采集功能，分析学生个性测试答题情况，AI 依据数据自动生成个体的“价值认知画像”。对于法治观念薄弱的学生，系统优先推送包含《信息安全法》和《数据安全法》等解读的相关视频；对于专业自信心不足的学生，推送中国科学家在密码学、软件分析、漏洞挖掘的突破性贡献，以及中国学生在国际网络安全比赛方面获得的顶级奖励。

（2） 课中：融合知识点的沉浸式伦理思辨。在讲解各个漏洞思政切入点时，教师首先讲解对应的知识点的原理，然后通过具体的例子来帮助学生理解对应的知识点，学生分组并结合例子探讨并掌握对应的知识点。在此基础上，教师发布对应的思政材料，引导进一步扩展技术后面的安全伦理，同时会穿插交互式的问题讨论；比如教师抛出议题：“如果你发现了一个 0day 漏洞，在厂商为修复前，某安全论坛高价收购此漏洞，你该如何抉择？”，通过课堂交互，教师可以洞察学生的思想倾向，进行及时的价值观纠偏，同时深刻宣讲道德黑客下负责任的漏洞披露机制，强化学生的职业伦理等。

（3） 课后：课后作业安全伦理行为审计。在布置的课后作业中，要求学生提交不同的伦理日志，同时发布网安思政小作业。例如在漏洞挖掘与利用综合实验中要求学生记录整个过程中可能会触发的非授权访问以及违反安全伦理的点；在系统攻防实践中，要学生记录获得系统权限后，进一步做了哪些操作，是否访问了非授权的资源等；发布小作业，要求完成网络安全与国家发展、个人网安责任方面的小短文作业。基于这些伦理日志生成合规性行为报告，提醒学生要遵循安全伦理对应的行为规范；基于相关主题作业打造学生守法敬业、责任担当的职业价值观。

2.5 构建多元化、数据驱动的教学成效评价体系

传统的唯分数论无法衡量思政育人成效。本课程借助大数据与 AI 技术，重构以过程为导向的多维综合评价体系（如表 2 所示）。通过思政考核融入综合评价，将学生在课堂互动中的伦理判断倾向以及转化、漏洞项目实操的安全规范、以及课后报告中的安全责

任反思等隐形数据设计为显性指标，结合专业知识的理论和实践项目完成情况综合评价教学成效。

表 2 教学改革多维度评价指标体系表

评价维度	考核内容与方法	对应思政素养
专业知识	漏洞原理、利用、防御和挖掘等理论作答。	科学严谨的钻研态度与自主创新能力。
实战能力	漏洞项目实操、以及安全规范性检测。	坚守道德黑客红线，守法意识以及合规操作能力。
思政素养	小组伦理辩论表现、个性化引导后观念转化轨迹、作业安全报告等。	高度的信息安全职业素养和科技报国使命感。

2.6 教学成效

经过一个学期的教改实践，成效明显。基于学期评教的反馈数据进行分析，表 3 分别给出了价值引领、教学内容、教学方法、课程认知、思维启迪、能力提升等多个维度的对比数据，两行数据分别为改革前后两个学期的评教为优秀的百分比。从表 3 可以看出，各个评价维度都得到了提升。

表 3 教学评价结果对比

价值引领	教学内容	教学方法	课程认知	思维启迪	能力提升
97.14	94.29	94.29	94.29	94.29	94.29
100	100	100	100	100	100

此外，在教学实践中，一方面学生对网络安全、数据安全、和个人信息保护的认知有了较大提升，在课程后期的课堂主题讨论、课程作业、以及在最终课程报告中都能明确意识到网络操作的安全红线，在完成对应的网络安全技能的同时，能够明确网络安全访问的边界，做到清晰地遵守网络安全伦理。另一方面，依托人工智能提供的多元丰富的多媒体演示和案例，学生能够更加容易理解知识点的原理，同时且更好地掌握对应的案例应用，在更好的掌握网络空间安全知识的同时，学生对软件逆向、漏洞分析与利用等产生强烈的探索欲，在单元作业和大作业的完成质量上有明显提升，同时参与各种网络安全攻防大赛的人数明显增加。在学生提交的各种作业、以及综合评价中，可以看出学生更加感受到了作为网安人守护网络安全的责任感。

3 结束语

在网络空间安全专业中，将人工智能赋能《软件漏洞分析与利用》课程思政建设，是解决网安专业核心技术中价值引领不足、法治观念淡薄的有效途径。本文从顶层目标构建，教师素质提升、思政要素构建、全程融合实践、以及综合考核评价等多个方面系统构建网安专业特色的思政体系。通过将人工智能引入学情分析、攻防案例伦理辩论以及风险防范等场景，实现了软件漏洞相关技能与国家安全、攻防伦理、法律意识和科技报国的有机结合。未来将进一步优化思政系统的综合评价机制，同时挖掘课程的思政元素，建设前沿的网络安全思政素材库，为建设网络强国培养更多技术过硬、爱国守法的网络空间安全创新人才。

参 考 文 献

[1] 李古月,胡爱群.网络空间安全专业课程思政教学探索与实践---以东南大学“网络空间安全新进展”课程为例[J]. 网络与信息安全学报. 2022,8(2):183-189

[2] 习近平. 没有网络安全就没有国家安全[EB/OL].（2014-02-28）[2014-02-28].https://www.cac.gov.cn/2014-02/28/c_126205811.htm

[3] 黄文华,吴昊,杨晓艺等.《网络安全基础》课程思政示范课程建设与实践[J].计算机技术与教育学报. 2025,13(4):158-164

[4] 李树一,陈玺羽,王兵书等. 数值赋能下的课程思政教学探索—以智能信息处理综合实践课程为例[J]. 计算机教育. 2026(4):137-141

[5] 张淼, 张华, 佟晓筠等. 融合课程思政的《软件安全》课程深度学习模型研究[C].2023 中国高校计算机教育大会. 中国. 厦门.2023:214-219

[6] 牛伟纳,张小松,陈厅. 新工科背景下软件安全分析课程改革与实践[J]. 软件导刊. 2024,23(8):49-55

[7] 许莹,钟雄虎,周旭等. 数字赋能的人工智能导论课程思政多维育人模式及案例[J]. 计算机技术与教育学报.2025, 13(6):293-296