Course Reform and Practice of "Web Security Programming" Under the Orientation of Applied Talent Training

Yingchao Wang, Na Li*
Xinjiang Institute of Science and Technology, Korla 841000, Xinjiang, China

Abstract: As a core elective course for the information security major, “Web Security Programming” is tasked with cultivating students' practical capabilities in Web security development and attack-defense techniques. Targeting key issues in current teaching — such as the theory-practice disconnect, simplistic attack-defense scenarios, rigid assessment methods, and insufficient coverage of cutting-edge technologies — this paper proposes a course reform plan from five dimensions: teaching content optimization, practical system upgrading, assessment method innovation, integration of ideological and political education with technology, and teaching resource expansion, in line with the course syllabus. By streamlining redundant knowledge, enhancing scenario-based combat training, improving diversified assessment, deepening immersive ideological and political education, and expanding three-dimensional resources, the reform achieves the four-in-one talent training goal of "foundation-vulnerability-practice-literacy", elevates teaching quality and students' post adaptability, and offers a reference for cultivating applied talents in information security.

***Keywords*:** web security programming, course reform, applied talents, practical teaching, integration of ideological and political education

1. Introduction

With the rapid development of information technology and the application of emerging technologies such as artificial intelligence and big data, higher requirements have been placed on applied talent cultivation. Against this backdrop, universities have actively explored curriculum teaching reforms to enhance students' practical and innovative capabilities for industry needs. Relevant practices include: the Environmental Design Materials and Construction Technology course built a "three integrations and three stages" curriculum system empowered by AI[1]; the C Language Course adopted a project-driven model to improve academic performance and practical abilities[2]; the Teochew Gongfu Tea Course established a "three-dimensional coordination, four-capability progression and five-dimensional integration" model under intangible cultural heritage education[3]; the Python Programming Course implemented project-driven teaching and diversified evaluation for AI and big data applications[4]; the Remote Sensing Software Application Course optimized objectives and content based on the OBE concept[5]; the Circuit Experiment Course reformed teaching with a "trinity" evaluation system emphasizing process over results[6];This research review summarizes the above reform experiences, discusses the Web Security Programming course reform and practice oriented to applied talent cultivation, and provides a reference for similar courses.

2. Current Situation of the Course and the Necessity of Reform

2.1 Analysis of Current Course Situation

Per our university’s Web Security Programming syllabus, the 40-hour course (20 theoretical, 20 lab hours) covers Web development fundamentals (HTML, CSS, JavaScript, PHP, JSP, Python/Flask), core vulnerability attack-defense (SQL injection, XSS, CSRF, SSRF, etc.), and network security laws. It specifies three-dimensional training goals (knowledge, ability, ideological and political literacy), includes 9 mandatory lab projects, and uses a 50/50 assessment split of usual and final performance.

2.2 Main Existing Problems

(1) Loose teaching content connection: The Web development foundation module (HTML, CSS, etc.) is disconnected from the security module, focusing only on development technologies rather than security risk analysis; traditional vulnerability cases are outdated, with no coverage of cutting-edge topics like file upload vulnerabilities and API interface security.

(2) Incomprehensive practical system: Practical projects are dominated by single-vulnerability verification (e.g., SQL

injection, XSS experiments), lacking comprehensive and confrontational tasks, which hinders students from forming a complete "development-vulnerability mining-protection and repair" thinking chain.

(3) Rigid, one-dimensional assessment: Usual performance relies on online tests and experimental report formatting, while final assessments are based on traditional written exams, failing to fully evaluate students' practical operation, vulnerability analysis and protection design capabilities.

2.3 Necessity of Reform

At present, the demand for applied talents in the network security industry is increasingly urgent, requiring practitioners to not only have a solid theoretical foundation, but also strong practical operation and problem-solving abilities. The existing course teaching model has been difficult to adapt to industry needs and talent training goals. There is an urgent need to optimize teaching content, upgrade the practical system, and innovate assessment methods through course reform, so as to achieve the training effect of "adequate theory, excellent practice and comprehensive literacy", help students quickly adapt to the requirements of network security positions, and improve the pertinence and effectiveness of the course.

3. Overall Ideas and Objectives of Course Reform

3.1 Overall Ideas

Centered on applied talent cultivation and guided by "consolidating foundation, focusing on actual combat, and prioritizing literacy", we establish a five-in-one reform system (content optimization, practical system upgrading, assessment innovation, ideological-political and technical integration, resource expansion) based on the existing syllabus. This system addresses key issues: streamlining content and integrating security with development bridges the theory-practice gap; comprehensive/attack-defense projects enrich scenarios; diversified assessment improves evaluation; scenario-based ideological education enhances literacy; and expanded 3D resources strengthen support.

3.2 Reform Objectives

(1) Knowledge Objectives: Master core Web development and secure coding principles, grasp common Web vulnerability defenses, understand cutting-edge threats and relevant laws, and form a systematic Web security knowledge system.

(2) Ability Objectives: Acquire skills in Web development, vulnerability attack-defense, and security scheme design/optimization, enabling independent resolution of practical Web security issues.

(3) Literacy Objectives: Establish the "technology for good" philosophy, develop sound engineering ethics, social responsibility and legal awareness, and become industry-ready compound security talents.

4. Specific Measures for Course Reform

4.1 Optimization of Teaching Content: Constructing a Progressive System of "Foundation-Security-Cutting-edge"

Streamline basic modules by merging redundant network content in Chapters 1 and 8 (focusing on TCP/IP-HTTP security correlations) and integrating HTML/CSS/JavaScript with front-end threats, adding injection, phishing and cross-domain vulnerability sub-modules to link development with security. Prioritize Python/Flask (widely used in security, easy vulnerability reproduction), simplify PHP/JSP as extensions, and compare language security features via cases to reduce learning load. Add 3 modules (2 hours each: 1 lecture + 1 lab) on file upload vulnerabilities, API security and logical vulnerability mining, and update SQL injection/XSS chapters with WAF bypass/HTML5 injection, replacing old cases with real CTF questions.

4.2 Upgrading of Practical System: Building a Three-level Actual Combat Platform of "Foundation-Comprehensive-Confrontation"

We upgrade HTML/CSS practices to Front-end Security Development Practice requiring post-development vulnerability identification and fixes, add parameterized query and data encryption tasks to the database module comparing spliced vs. parameterized SQL vulnerabilities; revamp development-oriented systems into security-focused projects where students complete the full "development → mining → protection" workflow to replace single-verification experiments; launch a 4-hour mid-semester CTF week via a SQLi-LABS/DVWA-based platform with group competitions on vulnerability mining and code repair and real-time teacher feedback, assigning phased EduCoder/CTFHub tasks with scores counted toward usual performance; simplify 9 reports into 3 comprehensive ones covering the full project cycle and 3 attack-defense logs to foster summary skills.

5. Expected Effects of Reform

The reform enhances student competence by shifting them from theoretical/verification-focused to proficient in development, attack-defense and compliance, equipping them with basic Web security capabilities to meet enterprise entry requirements and independently participate in CTF competitions or conduct simple security assessments; it resolves core issues like theory-practice disconnect and incomplete assessment, using scenario-based combat and diversified assessment to boost student engagement (with satisfaction projected to rise over 20%) and enhance teachers' capabilities, forming a "teaching-practice-reflection-optimization" virtuous cycle; it also builds a unique "technology + ideological and political education + actual combat" model, which aligns with the information security major's applied and compound talent goals, laying a foundation for school-level excellent course construction and providing a reference for similar course reforms.

6. Conclusion and Prospect

Aligned with applied talent cultivation and the course syllabus, the Web Security Programming reform resolves key teaching issues through five-dimensional measures — content optimization, practical system upgrading, assessment innovation, ideological-political and technical integration, and resource expansion — emphasizing theory-practice integration, technology-literacy balance, and tradition-cutting-edge connection to foster competent Web security talents. Future efforts will deepen school-enterprise cooperation with real industrial cases, update cutting-edge Web security content, adopt AI and VR for immersive training, and establish a long-term evaluation mechanism based on student employment and industry feedback to better support network security applied talent cultivation.

Acknowledgments

This paper was supported by the following fund projects: The Second Batch of New Engineering Research and Practice Projects of Xinjiang New Engineering Education Alliance: Construction and Practice of the "Three-dimensional, Four-stage and Five-improvement" Innovation and Entrepreneurship Competence Training System for Information Security Major under the Background of New Engineering (XJGK2025008); 2025 Xinjiang Uygur Autonomous Region Educational Science Planning Project: Exploration and Practice of the "One-core, Four-drive and Five-integration" High-level Application-oriented Technical Talent Training Mode for Information Security Major(HEN2025012).

References

[1] Bin Xiao. Research on Teaching Reform and Practice of "Environmental Design Materials and Construction Technology" Course Based on Artificial Intelligence[J]. Education Insights, 2025, (11): 173-180.

[2] Jun Xu. Research on the Teaching Reform and Practice of C Language Course Based on Project-driven. Advances in Computer and Communication, 6(5): 317-320.

[3] Min KE. Reform and Practice of Experimental Teaching for the Teochew Gongfu Tea Course in the Context of Intangible Cultural Heritage[J]. Agricultural Biotechnology, 2025, (6): 96-99.

[4] Qian Liu, Jiejuan Guo. Course Reform and Practice of "Python Programming" for Artificial Intelligence and Big Data Applications[J]. Journal of Computer Technology and Electronic Research, 2024, (1): 99-102.

[5] Rui Wang, Bi He. Teaching Method Reform and Practice Based on the OBE Concept: A Case Study of the Remote Sensing Software Application Course[J]. International Journal of Social Science and Education Research, 2025, (2): 95-98.

[6] Shijin Yu, Hua Zhu, Keyan Hu, Liangzu Cao, Ying Wei. The Ideological and Political Reform and Practice of the Course "Sensitive Materials and Sensing Technology"[J]. Adult and Higher Education, 2022, (6): 7-11.