Scholars Journal of Arts, Humanities and Social Sciences

OPEN ACCESS

Abbreviated Key Title: Sch J Arts Humanit Soc Sci
ISSN 2347-9493 (Print) | ISSN 2347-5374 (Online)
Journal homepage: https://saspublishers.com

Discussion on Experiment Teaching for Code Security Audit

Jiazhong Lu[1*], Yuanyuan Huang[1]

[1]School of Cybersecurity, Chengdu University of Information Technology, Chengdu, 610225, Sichuan, China

DOI: 10.36347/sjahss.2021.v09i12.006 | **Received:** 22.11.2021 | **Accepted:** 26.12.2021 | **Published:** 30.12.2021

***Corresponding author:** Jiazhong Lu

Abstract **Review Article**

Code Security Audit is a special professional course for information security majors in Chengdu University of Information Technology, which includes a theoretical part and an experimental part. In the context of the teaching reform of this course, this article analyzes the current situation of the experimental curriculum, and summarizes some of the deficiencies of the experimental curriculum in terms of teaching content and teaching methods. In order to further improve the teaching quality of this experimental course, some improvement methods in the teaching content and teaching methods of the experimental course are proposed, which are conducive to improving students' practical ability and innovative consciousness, and cultivating high-quality innovative talents.

Keywords: Code security audit, experimental teaching, discussion of reform.

1. INTRODUCTION

The "Code Security Audit" course is a special course for computer majors in Chengdu University of Information Technology. The course includes PHP code audit environment construction methods, PHP code audit ideas, common vulnerability audit methods, secondary vulnerability mining methods, PHP security programming specifications and C safety programming specification [1-3]. Courses are offered to sophomores and juniors majoring in computer science. The prerequisites for this course are "Network Attack and Defense" and "PHP Programming". Students are required to be able to systematically master the basic skills and engineering applications of PHP code security audit, and have strong engineering practice. Through the study of this course, you can further lay a theoretical foundation for subsequent professional courses (such as "Advanced Attack and Defense Technology", "Engineering Practice", etc.), and engage in practical work such as information security detection, application system design and development. Therefore, the course needs to create an opportunity for students to integrate theory with practice and thinking to expand and innovate through experimental teaching, so as to strengthen students' understanding of code security audit-related knowledge, and cultivate and diversify students' code security auditing of other computer programming languages. Comprehensive application ability is also a key link to improve teaching quality.

2. The current situation and shortcomings of experimental teaching

At present, most of the computer professional courses of Chengdu University of Information Technology are mainly based on theoretical teaching, and the experimental teaching is less than the theoretical teaching, and the computer major is a major that mainly focuses on practice and programming. In recent years, with the country's emphasis on experimental courses, schools have paid more attention to experimental teaching. Taking the "Code Security Audit" course as an example, the college has made the following improvements in the curriculum and experimental teaching.

(1) This year, the curriculum setting has been adjusted, and the ratio of the number of hours of the theoretical part and the experimental part has been increased from 2:1 to 5:3. Increasing experimental class hours is conducive to enhancing students' hands-on ability and improving teaching quality. Secondly, in terms of curriculum arrangement, it is required that the theoretical and experimental classes of this course be interspersed, the basic knowledge is instilled through theoretical teaching, and the use of knowledge is strengthened in the experimental link. This is not only conducive to the organic combination of the two types of teaching content, but also facilitates students to consolidate knowledge. Third, in terms of the final grade evaluation of the course, the experimental class performance and normal performance account for 50%

of the total grade, which can arouse students' enthusiasm for practical operation.

(2) In terms of the experimental environment, the laboratory purchased a batch of new computers and redeployed the teaching location of the laboratory, turning the classroom in the previous format into a circular classroom. At the same time, a general laboratory and two independent laboratories for experimental classes have been added, and related software environments have been configured for experimental teaching. A good experimental environment is the basic guarantee for the experimental teaching of this course.

Nevertheless, in the course of "Code Security Auditing", the author still found that this course has deficiencies in experimental teaching content and teaching methods [4, 5], as follows:

(1) The experimental case emphasizes the theory too much, which is inconsistent with the actual application. Taking Discuz’s Cross-site Request Forgery (CSRF) as an example, the experiment included the website’s source code and database details. There is a str_replace function in the source/admincp/admincp_db.php file. The table name and file are submitted directly by GET. The directory name consists of a fixed backup plus a six-digit number. After the backup is successful, the vulnerability can be exploited directly. Obviously, in practical applications, backing up the database tables in the installation directory is meaningless, because the installation directory is on the server side and not in the local folder. Such a vulnerability case is very tasteless.

(2) Cannot teach students in accordance with their aptitude. Different students differ greatly in their learning ability and practical ability, and their foundations are different, but the content and requirements of the experiment are the same for all students. Therefore, under the same requirements, some students can complete the vulnerabilities reproduction required by the experiment in less than ten minutes. For students with a weak foundation and weak hands-on skills, the entire class may still be setting up the environment needed for the experiment. In addition, some students participated in the network attack and defense team of the college, and often participated in various network attack and defense competitions. Their grasp of code rhythm and sensitivity to vulnerabilities were very different. The experiments in the book were easy for them.

(3) The experiment lacks engineering application and deviates from actual demand. The main purpose of this course is to learn about the preparation of PHP code auditing, common web vulnerabilities auditing methods, secondary vulnerabilities mining methods, code auditing skills, PHP security programming specifications, etc., and then master the use of code security auditing techniques. The ability to solve complex engineering problems in the field of information security. However, there is often a lack of engineering application background in experimental content, and it has no obvious effect on improving students' engineering practice ability. Secondly, the vulnerabilities involved in the experiment are common vulnerabilities in the PHP language. The lack of digging and exploring unknown vulnerabilities or other multi-programming language architecture system vulnerabilities will cause experimental teaching to deviate from the cutting-edge changes and actual needs of the IT industry, and it is also not conducive to promoting the spirit of exploration of students.

3. Discussion on the content setting of experimental courses

3.1 Close to reality and increase actual combat training

The existing experimental content is for the purpose of verifying the theory. With the popularity of network security today, it is difficult to reproduce the vulnerabilities in the experiment with the existing programming architecture and defense schemes. This course is about webpage, server and database penetration technology and vulnerability mining technology, which has the characteristics of strong practicality, fast technology update and fleeting vulnerabilities. This led to the inability of early attack techniques to meet current actual combat needs. As far as the content of this course is concerned, both the vulnerability mining technology and the vulnerability defense technology used are all earlier technologies. It can only be aimed at the early system framework and environment, and it is difficult to have such loopholes in reality, and it can only play a role in a specially configured experimental environment. Therefore, the current experimental courses can only improve students' mastery of theoretical knowledge, but are slightly inferior to improving students' practical ability. For this reason, the author suggests that the design of experimental content in the future needs to be closer to reality, reduce the proportion of verification experiments, and combine the current Internet frontier architecture and defense schemes to increase the complexity of the experiment, and to improve the actual combat ability of students in a true sense.

3.2 Teamwork and increase the difficulty of the experiment

Most of the existing experiments reproduce Web vulnerabilities before 2014. The vulnerabilities are simple in principle, few in types, and easy to operate. Moreover, the experiments do not require students to read through the entire code of the program, and students can review relevant information within a specified time and complete them independently. Therefore, it is not possible to fully exercise the students' exploration ability and problem-solving ability, or to reflect the ability of teamwork, or to achieve the actual combat effect. For this reason, the author recommends reducing the proportion of simple and reproducible experiments, using these experiments as after-school exercises, and increasing the proportion of team collaboration experiments. Cooperative experiments need to have higher requirements in content, difficulty, operation, and exploration, and must be combined with the real environment. For example, when vulnerabilities in large apps or web pages are reproduced, firewalls can be turned on. At the same time, it should be noted that for cooperative experiments, tasks should be allocated reasonably according to the students' own situation and advantages, so as to achieve a clear division of labor and an average amount of tasks.

3.3 Keep pace with the times and focus on innovation

The current experiment focuses on: (1) the method of building the PHP environment and the tools that need to be prepared for the PHP code audit. (2) The idea of PHP code audit. (3) Auditors of common vulnerabilities such as SQL injection, XSS, file operations, command execution, variable coverage, and logic processing. (4) Methods of mining vulnerabilities. These tools, ideas and methods have appeared or proposed several years ago or even more than ten years ago. After years of development, many more advanced tools and techniques have emerged. Therefore, in the experimental class, it is necessary not only to enable students to design information security system solutions that meet the needs of complex information security problems, but also to reflect the sense of innovation in the design process, taking into account social, health, safety, legal, cultural, and environmental factors. It also enables students to develop, select and use appropriate technologies, resources, modern tools and information technology tools for complex engineering problems in the field of information security, including the prediction and simulation of complex engineering problems, and to understand their limitations. At the same time, students can effectively communicate and communicate with industry colleagues and the public on complex engineering issues in the field of information security, including writing reports and design manuscripts, making statements, expressing clearly or responding to instructions. It also needs and possesses a certain international perspective, able to communicate and exchange in a cross-cultural context. Therefore, the author suggests that in the content arrangement of this course in the future, exploratory and innovative experiments can be appropriately added for interested students to broaden their horizons, enhance their interest in scientific research, and stimulate creativity.

4. Exploration on the reform of experimental teaching methods

4.1 Increase the proportion of experimental classes based on actual conditions

For highly practical courses such as "Code Security Audit", the proportion of experimental courses in the entire course should be appropriately increased based on the college's own situation. The author's college is divided into experimental class and parallel class. Most of the students in the experimental class are students with strong hands-on ability, rich practical experience, good foundation, and familiarity with code. For this type of students, the number of experimental class hours should be increased, and on this basis, the difficulty of the experiment should be increased, and the ability of teamwork can be improved. The ratio of experimental class to theoretical class can be adjusted to 1:1 or 2:3. However, students in parallel classes should first lay a solid foundation, understand the principles of each experiment, and the content of the experiment should be simple and easy to understand, and can be mutually corroborated with the knowledge of the theory class. Of course, it is not enough to just increase the proportion of experimental class hours. More importantly, it is to increase the proportion of experimental classes in the performance assessment, so as to stimulate students' interest in experimental classes. In view of the existing experimental class assessment, generally based on the experimental report, students can also be required to perform experimental demonstrations in batches and make demos in a more in-depth manner. For this reason, the author suggests that the proportion of different experimental scores can be increased for different classes. For this reason, the author recommends that different experimental scores can be increased for different classes. For example, the experimental class can be increased to 60-70%, and the parallel class can be maintained at least 50%.

4.2 Incorporate into the college students' innovation and entrepreneurship training program

The college student innovation and entrepreneurship training program is a national-level college student innovation and entrepreneurship training program that the Ministry of Education decided to implement during the "Twelfth Five-Year Plan" period. Through the implementation of the national-level college student innovation and entrepreneurship training program, colleges and universities can change their educational ideology, reform the talent training model, strengthen the training of innovation and entrepreneurship, enhance the innovation ability of college students and the entrepreneurial ability on the basis of innovation, and cultivate adaptation to an innovative country High-level innovative talents needed for construction. In the author's experimental courses, a large number of students have the ability to learn and develop independently. The content of the experimental courses can be combined with the project to form a network security-related development project. Let the code security audit course become one of the effective measures to improve network security, which not only helps to enhance the experimental teaching value of this course, but also can be integrated into practice so that students have project experience and improve their own abilities.

4.3 Join the Syclover team

The Syclover team was established in March 2005 and was created by students from the School of Information Security Engineering of Chengdu University of Information Technology. And a safety technical team organized and led by the students. The group's research directions include penetration testing, reverse engineering, mobile security, secure programming, and vulnerability exploitation. And in the National College Student Security Technology Competition, Alibaba Security Technology Competition, Baidu Cup Network Security Competition, the third 360 Information Security Technology Competition and other competitions have achieved excellent results. At the same time, it has successfully held the first National Information Security Technology League XCTF Chengdu Sub-station SCTF, the second XCTF International Cyber Security Technology Confrontation League Chengdu Sub-station SCTF, CUIT Information Security Technology Competition, and Geek Challenge. Based on the above information, students with outstanding practical ability can be selected in the author's experimental class and invited to join the team. The advantage of this is that it can maximize the talents and advantages of students, learn more cutting-edge information security knowledge while participating in the team, and can also obtain interview opportunities for some domestic and foreign scientific research institutions and enterprises.

5. CONCLUSION

This article summarizes the problems existing in the experimental course of "Code Security Audit" and puts forward the ideas for the course reform. In teaching: One is to increase practical training close to reality, especially to increase project training. The second is teamwork to increase the difficulty of the experiment. The third is to keep pace with the times and focus on innovation. In teaching method: It is recommended to increase the proportion of experimental courses according to the actual situation, and combine it with college student innovation and entrepreneurship training program, and join the Syclover team. This article will help to further promote the reform of curriculum teaching, teach students in accordance with their aptitude, guide students in the overall improvement of basic knowledge, personal ability, teamwork and engineering practice ability, and also help stimulate students' spirit of innovation and exploration.

6. REFERENCES

1. Robert, C. Sicord. (2015). C Security Coding Standard [M]. Mechanical Industry Press.
2. Yin, Y. (2015). Code Auditing [M]. Machinery Industry Press.
3. Guo, X., Chen, X. (2021). Web security vulnerabilities and code audit [M]. Publishing House of Electronics Industry.
4. Chen, T., Wang, X., Zhang, X [J]. (2015). Discussion on experimental teaching of network and system attack technology. Experiment Science and Technology, 13; 1.
5. Huang, Y., Li, F., Wang, J., Zhang, L [J]. (2015). Discussion on the experimental teaching of Oracle database application development based on CDIO, 52; 0250-02.