Instruction of Security in Web Development

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Helina Solomon

Spring, 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Daniel Graham, Department of Computer Science

Instruction of Security in Web Development

CS 4991 Capstone Report, 2022

Helina Solomon
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
hs6bg@virginia.edu

ABSTRACT

The demand for the instruction of developing secure web applications is inflated as the internet becomes more readily available. I propose a synthesis of ideas from two Computer Science (CS) courses, Intro to Cybersecurity (CS 3710) and PL for Web Applications (CS 4640). Cyber-attacks are everyday compromising web applications. Thus, students should be equipped with the knowledge of how to approach such threats in any given situation. The fusion of the two courses would teach students how they may build web applications while employing different techniques for maintaining best security practices. Learning the two dissimilar, but related, classes simultaneously would enable students to graduate with the knowledge of designing secure applications.

1 INTRODUCTION

The expansion of the internet has spawned new and more sophisticated vulnerabilities, exposing users and developers to copious threats online. The FBI has announced a 300% increase in reported cybercrimes since the Covid-19 pandemic [2]. With many companies transitioning to remote work, the risk of data exposure is greater than ever. For instance, statistics from Deloitte indicate that a quarter of employees have noticed an increase in fraudulent emails, spam, and phishing attempts in their corporate emails [2]. Cyber-attacks are mostly unpredictable and practicing cyber security measures has now become a necessity to businesses. Learning and mastering systems of protection measures and protocols will further protect websites or web applications from hacking [3].

The course objectives of CS 3710 are to understand fundamental cybersecurity principles, as well as how to better safeguard one′s personal computer. Web security is defined as a means of protecting a website or web application by detecting, preventing, and responding to cyber threats [3]. Without proper security, cyber criminals can access devices connected to the internet and steal personal information. By employing real-world applications and hands-on experience, students work on realistic security scenarios to understand threats and prevention.

In CS 4640, students learn to develop dynamic web software with several programming languages including HTML, CSS, JavaScript, PHP, JSON, and more. In the course, students implement the various programming languages by working on front-end development, user interface design, back-end development, and web-based information retrieval and processing. The overarching focus is on fundamental concepts of web development, which allows students to create reliable and usable web software.

A fusion of the two classes would consider concepts that directly correlate with each other. This proposed course would provide undergraduate students pursuing front-end or web development occupations with the tools and knowledge they need to succeed.

2 RELATED WORKS

The traditional approach of software development life cycle may not suit well as the internet broadens, where security in web applications comes into picture [1]. Although the content covered in both CS 3710 and CS 4640 are interconnected, there are not many courses offered at universities that provide a comprehensive learning experience. Only a few

schools have incorporated web development and security combined courses in their computer science curriculums. Identifying and minimizing security risks while writing code is a great skill to attain. The following related work is focused on corresponding course designs from different universities.

2.1 University of Chicago Illinois

Offered at the University of Illinois Chicago, the course, CS 491: Secure Web Application Design (Fall 2017), provides a similar overview of topics covered in this proposed course. In this class, students will learn the concepts and techniques that enable web applications to maintain high performance in the face of numerous users and attackers [5]. The course offers a hands-on learning experience in which students build their knowledge on how to maintain web applications when unknown attacks occur. It begins with building a foundation on security fundamentals and HTTP. This introduction lays the basis for the rest of the course. Successive topics include building web applications with JavaScript and dynamic web programming. After understanding the development of applications, students will then learn client-side security and best practices for server-side applications. The last several relevant topics in this course consist of defending web applications, attacking and defending user privacy, and usable web security [5]. In the end, students will be able to design, deploy, and defend modern web applications.

2.2 Stanford University

The course CS 155: Computer and Network Security (Spring 2011), provided by Stanford University, is split into two parts: web and network security. The beginning of the class is focused on an introduction to cyber security. This in turn will aid students in understanding the foundations of web security and emphasize its importance. In the following weeks, topics on the web security model and web application security are discussed. Students will learn concepts including the security architecture of the chromium browser, secure session management with cookies for web applications, cross site scripting, injection attacks, protecting high-security web sites from network attacks, and detecting and defeating interception attacks against SSL [4]. The last third of the course is focused on network security. Overall, the objective of this course for students is to attain the skill of identifying vulnerabilities and attack techniques so that they can defend against them.

3 PROPOSED COURSE DESIGN

This new proposed course includes concepts derived from CS 3710 and CS 4640 that directly correlate with one another. Students will leave the course with the knowledge of developing secure web applications.

3.1 Prerequisites

Students wishing to enroll in either CS 3710 and CS 4640 must complete CS 2150 or equivalent with a C- or higher. For this proposed course, the same requirement would be applied. Those considering the course do not need to have prior experience in web development programming languages. However, due to the amount of content covered, students should be prepared for and have a willingness to learn content at a fast pace.

3.2 Course Objectives

This course provides students with a basic level of understanding of web development and security risks. The following learning objectives were determined by corresponding ideas from CS 3710 and CS 4640 syllabi:

1. Understand core concepts of web development
2. Understand how to better safeguard one's personal computer
3. Develop dynamic web software with commonly used programming languages
4. Understand the ethical and policy context for cybersecurity in society today.
5. Understand the modern concepts in cybersecurity attacks and prevention

3.3 Course Topics

The class will begin with an introduction to web development. Students will learn the web software model and understand important factors to consider while designing a website. The following week will be an introduction to cybersecurity and a discussion on the Internet of Things (IoT). The purpose of this is to give students a basic foundation of web security and to prepare them for the rest of the course. Next,

programming languages, specifically HTML, CSS and Bootstrap, and PHP, will be taught. Students will be practicing interactive in-class and out-of-class with activities tailored to real-world applications.

Content covered at this point of the course will give students a basic understanding of web development and cyber security principles. In addition, students will be able to create usable and interactive software. As students begin to master the programming languages, the web attack topic of injections will be introduced. During this time, class discussions will consist of command, HTML, and PHP injections. Students will learn the dangers of the cyber-attack and how to minimize the risk of getting their sites hacked. A brief overview of SQL and databases will be taught in the course. Students will learn to implement SQL in their PHP code as well as have their web applications interact with a database. Lastly, the course will discuss the most commonly used web hacking technique, SQL injections. Students will learn how to prevent hackers from retrieving sensitive data.

4 EXPECTED BENEFITS

A more integrated process of learning web security and development would benefit students throughout their academic and professional journey. They will be able to apply security concepts using self-made web applications, utilizing the instructed programming languages. Students would also gain a deeper understanding of cyber security patterns, and how they relate to the applications they are creating.

Overall, the new proposed course would better prepare students for the world outside of university. This would particularly benefit those seeking front-end development occupations and projects. The potential knowledge gained would directly relate to assigned tasks in future jobs. Students are taught to be aware of security risks while designing and developing web applications. The course would add these compelling skills on a resume that recruiters would value.

5 CONCLUSION

Web applications have a large attack surface and are a popular target of remote attacks on the Internet. Statistically, they exhibit a track record of a high number of vulnerabilities and incidents [1]. While CS 3710 and CS 4640 are significant classes independently, the advantages of instructing a fused course are persuasive. Building modern web applications requires integrating concepts from software engineering, systems programming, and computer security. In order to effectively build these applications, one must be aware of potential malicious attacks and how to defend against them.

6 FUTURE WORK

To further the work completed, class assignments and projects should be produced. Due to the intensive nature of the proposed course, homework administered to students should not be too challenging. However, assignments should encourage innovative thinking as the purpose of this course is to prepare students for the professional workspace. Furthermore, topics should be updated annually so that they match concepts relating to real world applications. Faculty willing to instruct the class should consult those teaching CS 3710 and CS 4640. This would aid in establishing contemporary material as topics are directly derived from the two courses.

REFERENCES

[1] Asish Kumar Dalai and Sanjay Kumar Jena. 2011. Evaluation of web application security risks and secure design patterns. In Proceedings of the 2011 International Conference on Communication, Computing & Security (ICCCS '11). Association for Computing Machinery, New York, NY, USA, 565‑568. DOI:https://doi.org/10.1145/1947940.1948057

[2] Clare Stouffer. (2021). 115 cybersecurity statistics and trends you need to know in 2021. https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html#

[3] GoodFirms. (2020). What is Web Security? Good Firms.

https://www.goodfirms.co/glossary/web-security/

[4] Stanford. (2011). CS115: Computer and Network Security. https://crypto.stanford.edu/cs155old/cs155-spring11/

[5] University of Illinois Chicago. (2017). CS 491: Secure Web Application Design. https://www.cs.uic.edu/~ckanich/swad/f17/