CYBR 515: SOFTWARE SECURITY COURSE SYLLABUS

Summer 2024

COURSE INTRODUCTION

Course number and name: CYBR 515, Software Security
CRN(s): 51831/ 52184, 3 credits.
Class meets : Asynchronous
Class duration: 5/13/2024 - 6/21/2024
Prerequisite Courses: Acceptance into the MS CYBR Program.
Instructor: Mohammad Jamil Ahmad, Ph.D.
Course Materials: All material is posted on eCampus (https://ecampus.wvu.edu).

Course Introduction: This course will cover a wide range of topics essential for understanding and managing software security within a business context. Starting with basic software concepts and the integration of security practices, we delve into the Software Development Life Cycle (SDLC) and how security can be woven into each phase to mitigate risks effectively. We will explore advanced topics such as bug detection and classification, vulnerability management using common frameworks like CWE and CVE, the application of OWASP guidelines, and best practices in secure coding. Throughout this course, the material will be sourced from a selected range of peer-reviewed publications, ensuring that you receive the most current and rigorously validated information. Additionally, we will supplement our discussions with relevant chapters from online books to provide a well-rounded understanding of each topic. This approach ensures that our content remains at the cutting edge of technology and business management, preparing you to handle real-world software security challenges effectively.

INSTRUCTOR INFORMATION

Office location: 2109 Reynolds Hall. **Tel:** +1(304)293-7939

Office hours: Wednesday, Thursday, Friday Please use this link to book an appointment.

Email: mohammad.ahmad@**mail**.wvu.edu (Emails sent to @mix.wvu.edu account will be ignored).
The best and preferred method of communication is via email.

Additional and optional channel of communication: Zoom when needed.

INSTRUCTIONAL MATERIALS

Course Required Textbook:

1. * Kohnfelder, Loren. *Designing Secure Software: A Guide for Developers*. No Starch Press, 2021. Available immediately for free for WVU students (need to login using your mix account): https://learning.oreilly.com/library/view/designing-secure-software/9781098129804/
2. ** Olmsted, Aspen. *Security-Driven Software Development*. Packet Publishing, 2024. Available immediately for free for WVU students (need to login using your mix account): https://learning.oreilly.com/library/view/security-driven-software-development/9781835462836/

3. (**Recordings**) *** Oni, Alexander. *A Detailed Guide to the OWASP Top 10*. Packer Publishing. 2022. Available immediately for free for WVU students (need to login using your mix account): https://learning.oreilly.com/course/a-detailed-guide/9781837630554/
4. Walsh, John and Alion, Uzi ****. *Identity Security for Software Development*. O'Rilly Media, Inc. 2025. Available immediately for free for WVU students (need to login using your mix account): https://learning.oreilly.com/library/view/identity-security-for/9781098158026/
5. **Additional material**: Selected peer reviewed publications, online articles, book chapters, and/or recordings of related content.

COURSE LEARNING OUTCOMES

Upon successful completion of this course, the student will be able to:

1. Define key concepts in software security, including bugs, faults, errors, and vulnerabilities.
2. Understand and explain the software development life cycle (SDLC) and the integration of security practices into SDLC.
3. Identify and use tools for detecting, classifying, and managing software bugs and vulnerabilities.
4. Analyze and interpret code from software repositories to identify security risks and understand the evolution of code.
5. Apply knowledge of OWASP and other security frameworks to analyze and improve software security.
6. Implement secure coding practices and understand the methodology behind developing secure software applications.

COURSE DESIGN AND ORGANIZATION

This class is scheduled during Summer Session I of the 2024 semester, beginning on Monday, May 13, 2024, and concluding on Friday, June 21, 2024. The course is structured into six distinct modules, with each module released at the start of the week (Monday at 12:01 AM). Designed to be completed within one week, each module includes various educational activities and assessments, all of which are due by the end of the week (Sunday at 11:59 PM).

Given the compressed nature of this summer course, it is essential to manage your time effectively to keep up with the pace. Staying proactive and organized will help you "ride the wave" of coursework rather than being overwhelmed by it. Should you have any questions or need assistance, please feel free to email me at any time.

Each weekly module typically includes text readings, lectures focused on key content, assigned assessments (which may be individual or team-based), and occasional hands-on practices related to security. This blend of activities is designed to enhance both your theoretical understanding and practical skills in software security.

There will be two team-based homework assignments, two individual exams (midterm and final) a team-based research paper of a topic that students and the instructor need to agree upon. The general atmosphere of the classroom is expected to be as if one is present at a business meeting of executives trying to solve a real-world software security systems problem. To maintain transparency, you are

expected to evaluate each of your peers twice throughout the semester.

COURSE OVERVIEW

This 6-week course is designed to introduce students to the critical field of software security, bridging the gap between technical security measures and business management. The class will provide students with a foundational understanding of how software is developed and secured, focusing on the integration of security into business processes. Each week tackles a different aspect of software security, ensuring that students appreciate the impact of security on business and learn to manage risks associated with software vulnerabilities effectively. No extensive background in software development or coding is required, making this course ideal for professionals aiming to enhance their cyber management capabilities in business settings.

REQUIRED SOFTWARE AND PRE-REQUISITE KNOWLEDGE

To excel in this class, we will be using this software provided below, in addition to other external tools that the instructor will make available throughout the course.

1. Web browser
2. Pdf reader
3. Word and text processors (MS Word).
4. GitHub / GitHub Desktop.
5. SonarQube: Will be used for static and dynamic code analysis. Access will be provided through a cloud setup or local installation guide.
6. SourceTree (optional): A GUI for managing Git repositories, enhancing ease of use for those less familiar with command-line tools.
7. Basic Computer Skills: Comfort with operating systems (Windows/Mac/Linux) and general computer usage.

ASSESSMENTS

The online lectures, online class discussions, and online quizzes and final exam are all designed to explore business network security topics:

- **Learning.** Students are required to read the assigned text and any additional supplemental materials hosted on eCampus.

- **Homework Assignments**: There will be two team-based homework assignments given throughout the semester (worth 30% of total grade). Each homework assignment will cover one or more modules and will require each student to submit one document of their answers on eCampus or other means that will be provided in the instructions of the assignment.

- **Exams**: There will be two individual exams, a midterm (worth 15% of the total grade) and a final (worth 20% of the total grade). These exams are open book and will be multiple choice focusing on the most important concepts of the covered modules.

- **Research Paper:** One team-based in-depth research paper (25% of total grade) where each student group will find a topic of interest in software security, software vulnerabilities detection or classification, or software secured practices and research it in depth with a minimum of 10 sources of published peer reviewed articles, conferences, symposiums, speaker notes, online talks, or book chapters. The paper should follow the template provided on eCampus, students can use Microsoft Word to write their paper however, students are encouraged to use Overleaf or Latex. Proper citation is expected, and examples will be posted on eCampus.

- **Peer evaluations: Two individual submissions (10% of the grade) where each student is** required to evaluate each member of their group. One evaluation around the third week of classes, and one evaluation at the end of the semester. The evaluations are will simply ask each student to evaluate each member by assigning a letter grade (i.e., A, B, C, D, or F).

- **Course Discussion Forums**: These optional, ungraded discussions will be used to address anything in the class and respond to any questions. Students are encouraged to use these discussions to post their questions, comments, ideas, and responses which could be beneficial to the entire class.

GRADES

Performance on graded assessments will be recorded in the eCampus grade book. Anticipate grades to appear within a week following the due date. If the count of any assessment changes, the total percentage of that assessment type will remain the same.

- **Grading Scale**: >90% A; 80-89.9% B; 70-79.9% C; 60-69.9% D; <60% F
- Course Grading:

Assessment	Delivery	Count	% Of total grade
Homework Assignments	Team-based	2	30
Midterm Exam	Individual	1	15
Final Exam	Individual	1	20
Research Paper	Team-based	1	25
Peer Evaluation	Individual	2	10
Total			**100 %**

CLASS POLICIES

Attendance Policy:

There is no residency associated with this course. The course is designed for asynchronous learning. If needed, there will be periodic opportunities to meet online for supplementary presentations via Zoom, which all WVU students have access to through their Mix accounts.

Class Meetings and Virtual Meetings:
The presentation of this course will occur through asynchronous delivery of course material in the form of eCampus content, annotated slide lectures, activities, and optional videos. The course has been divided into 6 modules. Each module has an opening and a closing date, functioning as a window in which all lesson material must be completed. The instructor will respond to all student emails during the class session period within 24 hours M-F.

Team-based assessments Policy:
In the first week of classes, students will self-select into working groups for the semester. Each group can have up-to 4 group members, please refer to the enroll in a group link on eCampus to view and join groups. Students are expected to collaborate professionally with all group members to submit team-based assessments. For groups to function efficiently and fairly, you may like to find a common time to meet regularly via Zoom by using a website such as Doodle or Calendly. The groups are expected to distribute the work among the group members equally. If there are any issues the arise regarding the groups or group-based assessments, please do reach out to your instructor ASAP.

Assessment Submission Policy:
Students are responsible for all material covered in the course, keeping track of assignments and examination dates. All materials will be posted on eCampus, and your assessments must be submitted in the expected formats by the given due dates on eCampus or other means per the instructions. Submissions over email are not accepted. Any late work may be rejected without a grade except when a policy indicates otherwise. You should keep secure copies of your work in case of data loss.

Makeup Assignments: Should outside commitments cause a problem in meeting a due date, contact the instructor in advance to arrange a resolution to the conflict.

General Comments: The instructor reserves the right to change this syllabus as time and circumstances dictate.

RELATED STATEMENTS

Institutional Policies: Students are responsible for reviewing policies (https://tlcommons.wvu.edu/qualitymatters/syllabus-policies-and-statements) on inclusivity, academic integrity, incompletes, sale of course materials, sexual misconduct, adverse weather, as well as student evaluation of instruction, and days of special concern/religious holiday statements.

Student Evaluation of Instruction: Effective teaching is a primary mission of West Virginia University. Student evaluation of instruction provides the university and the instructor with feedback about your experiences in the course for review and course improvement. Your participation in the evaluation of course instruction is both strongly encouraged and highly valued. Results are strictly confidential, anonymous, and not available to the instructor until after final grades are released by Admissions and Records. Information about how you can complete this evaluation will be provided later. I faithfully

read my evaluations and incorporate improvements to our future classes based on useful criticism from your SEI's, so please be sure to complete these forms.

- **Instructor Access**: I am always happy to meet with you then, or else any time that is mutually convenient by appointment. It is easy for me to set up a Zoom for a video chat that meets with your convenience. You are always welcome to email me with questions or to arrange a meeting. I will always respond to your emails within 24 hours, Monday through Friday. If you choose to email me, please always include the course number in the title of your email and which assessment/ issue you are reaching out about. For example, if you have a question regarding HW 2, please use something like this in your email title "CYBR515- HW #2 question". If your email relates to a team-based assessment, please make sure you always include your group number in your email. I enjoy meeting with students during my office hours, am also happy to discuss possible research and collaboration research in any cybersecurity topics, or any issues which are important to you about the class.

USEFUL LINKS

- **2023-2024 Academic Calendar**

EXPECTED TIMELINE

The following schedule is an estimate schedule of the topics covered in this class along with the designated week. This might change depending on the progress of students in the class.

Module / Week #	Date (2024)	Topics	Covered course material	Assessments due
1	5/13 – 5-19	Introduction to Software and Security Concepts	• Chapter 1*: Foundations • Bug, Fault, Error, or Weakness: Demystifying Software Security Vulnerabilities	Group sign up
2	5/20 – 5-26	Software Development Life Cycle (SDLC) and Security Integration	• Chapter 1** : Security Principles • Security risks in the software development lifecycle: A review	Homework #1
3	5/27 – 6/2	Software Bugs	• Software Dysfunction: Why Do Software Fail? • Predicting Software Defectiveness by Mining Software Repositories	Midterm Exam
4	6/3 – 6/9	Software Vulnerabilities	• Chapter 9 **: Standard Web Application Vulnerabilities • TBD	• Research Paper Overview • Evaluation #1
5	6/10 – 6/16	OWASP and Software Security Frameworks	• Recording ***: A Detailed Guide to the OWASP Top 10 • Additional resources TBD	Homework #2
6	6/16 – 6/21	Secure Coding Practices	• Chapter 4 ****: Secure Coding Practices for Identity Security • Additional resources TBD	• Final Exam • Final Research Paper • Evaluation #2