|  |  |  |
| --- | --- | --- |
|  |  | **CPSC 507 Advanced Cyber Security**  This second course in cyber security explores advanced technological techniques and tools in cyber security, with a deeper hands-on approach to diagnosing and remediating software application vulnerabilities and web application vulnerabilities. |
| **CPSC 50700-001, Spring I 2018**  **<Meeting time>**  **3 Credits**  **Computer Science / Master of Science** | |

**Instructor:**

Office:

Office Hours:

Office phone:

E-mail:

**Optional Textbook** Du, Wenliang, *Computer Security: A Hands-on Approarch,* ISBN-13: 978-1548367947

**Online Resources** Course Blackboard Site

## Course Rationale & Student Learning Outcomes

Greater and greater portions of our lives and identities consist of interactions with networked computing devices, and more and more data important to our lives is stored on computers and communicated through computer networks. This means that the need for understanding the principles of computer and network security is vitally important. Highly publicized security breaches affect the lives of millions of people, with no end in sight. Computer security also interacts with social/ethical issues of privacy, surveillance, and constitutional rights.

**Course Outcomes:** Upon successfully completing this course, you will be able to:

* Explain the core concept behind software security issues;
* Edit, compile, and test C programs in a Unix environment;
* Understand security issues relating to environment variables and privileged programs;
* Describe how a process’s memory address space, including the call stack, are laid out;
* Identify security vulnerabilities related to buffer overflows in the address space;
* List defense techniques to prevent buffer overflow exploits;
* Modify C programs to eliminate buffer overflow-causing bugs;
* Safely use format strings so as to avoid vulnerability-causing bugs;
* Describe the interactions and data flow of a client-server web application;
* Understand the GET and POST methods of the HTTP protocol;
* Create Cross-Site Request Forgery and Cross-Site Scripting attacks to test a website’s security;
* Describe the types of input sanitization that can prevent XSS attacks;
* Describe the back-end structure of a web application that connects to an SQL database;
* Read and write basic SQL queries and update statements;
* Test the safety of web applications by construct inputs that perform a command injection attack;
* Write PHP code that safely issues queries to a database and harvests the results.
* Discuss ways in which the issues of security and privacy on the web sometimes overlap, and sometimes are opposed to each other;
* Explain how cookies enable storing of user profile data and tracking across multiple site visits;
* Manage how your web browser stores and transmits your personal data.

**Program Outcomes**, Master of Science in Computer Science, Cyber Security concentration:

1. Identify the risks an organization faces due to cyber threats, and recommend steps to take to combat those risks.
2. Apply skills and knowledge to create new responses to emerging cyber security problems so that they can respond to new attacks as they evolve.
3. Describe how cyber attacks against an organization can be monitored and investigated for actionable intelligence.
4. Explain how symmetric and asymmetric encryption and authentication systems safeguard data, and recommend encryption and authentication systems suited to particular tasks and settings.
5. Identify components of a modern information system and the threats that challenge their security.
6. Design software and networks that resist and mitigate cyber attacks.
7. Specify tools and architectures to help secure information systems both proactively and reactively.

Of these, this course addresses program learning outcomes 1, 2, 5, 6 and 7 at the “reinforced” level.

**Graduate Student Learning Outcomes:** Lewis Graduate students will:

* Synthesize theoretical and research concepts from multiple perspectives to inform inquiry and practice.
* Formulate creative responses to complex issues through critical analysis.

Model ethical and professional behaviors to guide inquiry and practice in a global and diverse society.

## Schedule of Topics and Assigned Work

|  |  |  |
| --- | --- | --- |
| **Unit** | **Topics** | **Assignments** |
| Week 1 | Linux OS and C language intro; SetUID security | Lab 1: Environment and SetUID Discussion Board 1  Week 1 Quiz |
| Week 2 | Address spaces; Buffer overflow vulnerabilities | Lab 2: Buffer Overflow Discussion Board 2  Week 2 Quiz |
| Week 3 | Return-to-libc and Heap Overflow; the “Heartbleed” attack | Lab 3: Heartbleed Discussion Board 3  Week 3 Quiz |
| Week 4 | Format string vulnerabilities; Software security retrospective | Lab 4: Format Strings Discussion Board 4  Week 4 Quiz |
| Week 5 | Intro to Web Applications; Cross-site Request Forgery | Lab 5: CSRF Discussion Board 5  Week 5 Quiz |
| Week 6 | Cross-Site Scripting | Lab 6: Cross-Site Scripting Discussion Board 6  Week 6 Quiz |
| Week 7 | SQL and PHP; Command Injection Vulnerabilities | Lab 7: SQL Injection Discussion Board 7  Week 7 Quiz |
| Week 8 | Security and Privacy Issues | Lab 8: Web Tracking Discussion Board 8 |

## Course Requirements

Your grade in this course will be computed from three in-class exams and a final exam, homework assignments, and participation as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Percent of Final Grade** |  | **Grading Scale** | |
| Lab Assignments | 70 |  | **A** | 100% to 90% |
| Quizzes | 15 |  | **B+** | 89% to 87% |
| Forum discussions | 15 |  | **B** | 86% to 83% |
|  |  |  | **B**- | 82% to 80% |
| **Total** | **100** |  | **C+** | 79% to 77% |
|  |  |  | **C** | 76% to 73% |
|  |  |  | **C-** | 72% to 70% |
|  |  |  | **D+** | 69% to 67% |
|  |  |  | **D** | 66% to 63% |
|  |  |  | **F** | 59% or less |

## Course Format, Blackboard, and Announcements

The course will be managed primarily through the Lewis University Blackboard site (<https://lewisuniversity.blackboard.com>). Your first responsibility at the beginning of the semester is to make sure that you can access the course’s Blackboard page. If for some reason you cannot do so even though you are registered for the class, please let me know.

The course Blackboard site is purposely designed to make it as simple as possible for you to keep up with the course requirements. There is a dedicated page for each week of the course, with all the material and assignments for that week accessible from this single page.

You should get an email for every announcement posted on Blackboard; if you do not, please let me know. Because of the importance of staying informed of course updates, ***it is a class requirement to check your Lewis email account (the one that Blackboard announcements go to) once per class day.*** The instructor will not be responsible for missed assignments or deadlines due to failure to follow this requirement.

## Lab Assignments

The primary take-home work for this course will be a lab assignment given each week, in which you do a hands-on investigation of issues relating to software security. You will be given a lab document describing the procedures in detail. Each lab assignment is divided into *lab tasks* which require carrying out one component of a security investigation and reporting on the results.

For each lab assignment, you will be required to submit a report in Word or PDF format and, if applicable, code files. You will submit the homeworks on Blackboard.

Each lab assignment is graded on a 100-point scale, and is due by the beginning of the next week’s lecture (or, in the case of the final lab, the end of the term.)

**Late Policy: If you have a need to turn in an assignment after the due date,** **you must contact me by email *before* the due date. No automatic late grades will be given.**

## Forum Discussions

Interaction with your peers through in-depth discussion is an important part of the graduate learning process. In fact, you may often learn from each other better than you learn from the instructor. Each week of the course, a new open-format discussion question relating to that week’s lecture topic will be posted to the “Discussions” section of the course site.

By **Thursday at 11:59pm** each week, you should post a single thread giving a substantial, well-argued response to the given discussion prompt. Then, by **Sunday at 11:59pm**, you should respond to **two** other students’ posts. Your forum posts will be graded on information content, depth of analysis and clarity of communication.

## Quizzes

In each week of the course except for the last, there will be a 5-question multiple-choice quiz posted to Blackboard. The purpose of the quizzes is to confirm that you are grasping the high-level concepts presented in the lecture and class materials. Once you begin each quiz, you must complete it within a single 15-minute session.

**Grade Reports**

I will post grades for individual assignments on Blackboard as soon as they are graded. I may also include a “Weighted Grade” column in Blackboard to give you an idea of your total score based on assignments already graded. However, I cannot guarantee that the value in this column is perfectly accurate at any given point in the semester; please remember that its calculation can only include assignments and tests that have already been graded, and any missing assignments will become zeroes in the final grade. When I compute your final grade, I will download the scores from Blackboard and re-compute the total weighted score offline, to verify it.

If you have any questions about a grade on any assignment or your overall grade in the class, please contact me as soon as possible. I will not consider any requests at the end of the semester to “do more work” to raise your grade.

**Contacting the Instructor**

Success in this class requires that you communicate with me whenever you have questions. If you are having problems with the course content or administration, **you need to let me know as soon as possible.** My job is to help you learn, but without feedback it is difficult for me to know what is wrong.

* If you need to contact me, please email me at <instructor email>.
* Barring unusual circumstances, I will check my email at least once a day Monday through Friday. Customarily I respond to your email within 24 hours, and often faster than that. I occasionally may take longer. You might receive responses at night or on weekends, but this is not to be expected. If you do not receive a reply by the second day, please resend your message.

**Course Relationship to Mission**

Lewis University is a Catholic University in the Lasallian Tradition. Our Mission is integrated into all aspects of University life, including this course. This course embraces the Mission of the University by fostering an environment in which each student is respected as an individual within a community of learners. In the spirit of the vision of Lewis University, the goals and objectives of this course seek to prepare students to be successful, life-long learners who are intellectually engaged, ethically grounded, socially responsible, and globally aware.

## Required Information for Students

**STUDENTS REQUIRING SPECIAL ACCOMMODATIONS**

Lewis University is committed to providing equal access and opportunity for participation in all programs, services and activities. If you are a student with a disability who would like to request a reasonable accommodation, please speak with the Learning Access Coordinator, at the Center for Academic Success and Enrichment (CASE). Please make an appointment by calling 815-836-5593 or emailing [learningaccess@lewisu.edu](mailto:learningaccess@lewisu.edu). For more information about academic support services, visit the website at: [www.lewisu.edu/CASE](http://www.lewisu.edu/CASE). Since accommodations require early planning and are not provided retroactively, it is recommended that you make your request prior to or during the first week of class.  It is not necessary to disclose the nature of your disability to your instructor.

**SANCTIFIED ZONE**

This learning space is an extension of Lewis University’s Sanctified Zone, a place where people are committed to working to end racism, bias and prejudice by valuing diversity in a safe and nurturing environment. This active promotion of diversity and the opposition to all forms of prejudice and bias are a powerful and healing expression of our desire to be Signum Fidei, “Signs of Faith,” in accordance with the Lewis Mission Statement. To learn more about the Sanctified Zone, please visit: <http://www.lewisu.edu/sanctifiedzone>

**ACADEMIC HONESTY**

Scholastic integrity lies at the heart of Lewis University. Plagiarism, collusion and other forms of cheating or scholastic dishonesty are incompatible with the principles of the University. Students engaging in such activities are subject to loss of credit and expulsion from the University. Cases involving academic dishonesty are initially considered and determined at the instructor level. If the student is not satisfied with the instructor’s explanation, the student may appeal at the department/program level. Appeal of the department /program decision must be made to the Dean of the college/school. The Dean reviews the appeal and makes the final decision in all cases except those in which suspension or expulsion is recommended, and in these cases the Provost makes the final decision.

**Specific academic honesty policy for this course**: First of all, *all submitted work, whether in the form of writing, diagrams, mathematics, or computer code, must be your own composition.* If I find that you have copied any portion of a homework assignment, project, or quiz, you will receive **0** points for that work, and your grade will be reduced by one level at the end of the semester. This includes copying from websites and journals. If you are found cheating a second time, you will receive an F for the course. This policy does *not* mean that you can’t discuss how to solve a problem with your classmates. Copying work, however, defeats the purpose of the educational enterprise. I will not be lenient in enforcing this policy. Instances of cheating on examinations will also be investigated and given their full penalties according to University Policy.

**COMPUTER ETHICS**

All Lewis students must abide by the Lewis University *Information Services Acceptable Use Policy.* This is an agreement between members of the Lewis community and Lewis University regarding use of the Internet, on-campus network, Web Page, Course Management Systems, Student Information System, and all electronic systems. See: <http://www.lewisu.edu/welcome/offices/infoservices/All_AcceptableUsePolicy.htm> **Attention to the regulations in this policy is of particular importance for this class, given the nature of the material. No unethical hacking will be tolerated.**

For more information, refer to the *Academic Honesty*, *Computer Ethics*, and *Copyright Laws* policies in the University Catalog.

**STUDENT COMPLAINT POLICY**

Please see <http://www.lewisu.edu/welcome/studentcomplaints.htm> for the process.

**UNIVERSITY COPYRIGHT AND INTELLECTUAL PROPERTY GUIDELINES**

Please visit <https://www.lewisu.edu/osp/pdf/Intellectual%20Property%20Rights%20Policy.pdf>

**UNIVERSITY GRADE APEAL POLICY**

Please see <http://www.lewisu.edu/welcome/studentcomplaints.htm> for the process

## Note on Potential Modifications

The instructor reserves the right to modify, change, or waive any part of the syllabus or the evaluation criteria for this course. The instructor will provide prior notification of any modifications.