



CS 4177

Software Vulnerabilities

This course focuses on security issues and their remediation through the use of hands-on, practical exercises. Students will learn of the potential risks that accompany the use of networks, devices, and systems by using cyber security tools and techniques to uncover and analyze their inner workings. Students will learn to apply defenses and mitigations to alleviate risks.

Course URL:

<http://cssrvlab01.utep.edu/4177>

Note: the site is only accessible from UTEP and through UTEP's VPN

Office Hours:

T 9am-10am @ Zoom
(link is on blackboard)

Instructor:

- Dr. Jaime C. Acosta
Office: Prospect Hall Rm 120
Email: jcacosta@utep.edu

Class location and time:

The course codes are CRN 17444 for CS4177.
Class will be held in CCSB G.0208 on Thursdays from 4:30pm to 5:50pm.

Course materials:

Students are required to bring a laptop to every class to complete assignments, tests, and the course project. If this is an issue, please notify the professor.

This course does not require the purchase of a textbook; all resource material will be posted on the course website and/or Blackboard.

Course Policies:

- Homework assignments are due at the beginning of the class, unless specified otherwise.
- Assignments may be discussed with others, but solutions must be designed, written, and tested by you or, in the case of group assignments, by your group.
- No make-up exams or assignments will be given except under extreme conditions.
- It is the student's responsibility to independently cover any material missed.

Grades:

| | |
|-------------|-----|
| Assignments | 50% |
| Tests | 20% |
| Project | 30% |

Final letter grades will be assigned as follows:

A = 90% through 100%

B = 80% through 89%

C = 70% through 79%

D = 60% through 69%

F = Less than 60%

Submission of late work:

Homework assignments are due at the beginning of class. Late work will be accepted at most two days late, unless specified by the instructor, and will be marked down two letter grades. After two days the assignment will not be accepted.

Standards of Conduct and Academic Dishonesty

You are expected to conduct yourself in a professional and courteous manner, as prescribed by the UTEP Standards of Conduct: <https://www.utep.edu/student-affairs/osccr/student-conduct/>

Academic dishonesty includes but is not limited to cheating, plagiarism and collusion. Cheating may involve copying from or providing information to another student, possessing unauthorized materials during a test, or falsifying data (for example program outputs) in laboratory reports. Plagiarism occurs when someone represents the work or ideas of another person as his/her own. Collusion involves collaborating with another person to commit an academically dishonest act. Professors are required to - and will - report academic dishonesty and any other violation of the Standards of Conduct to the Dean of Students.

When in doubt, please ask. On exams you must submit your own work and you may not give or receive help. On assignments you must submit your own work. Submissions that are "identical" will be considered as a clear evidence of cheating.

Students Needing Special Accommodations

In accordance with the UTEP procedure, if you need accommodations for equal access in this course, please do the followings:

- Contact Center for Accommodations and Support Services (CASS) at cass@utep.edu or by phone at (915) 747-5148 to verify your eligibility.
- Contact me before or at the beginning of the first class to discuss your individual needs for accommodations, with an official letter of accommodation or other documents.

COVID-19 Precaution Statement

Please stay home if you have been diagnosed with COVID-19 or are experiencing COVID-19 symptoms. If you are feeling unwell, please let me know as soon as possible, so that we can work on appropriate accommodations. If you have tested positive for COVID-19, you are encouraged to report your results to covidaction@utep.edu, so that the Dean of Students Office can provide you with support and help with communication with your professors. The Student Health Center is equipped to provide COVID-19 testing.

The Center for Disease Control and Prevention recommends that people in areas of substantial or high COVID-19 transmission wear face masks when indoors in groups of people. The best way that Miners can take care of Miners is to get the vaccine. If you still need the vaccine, it is widely available in the El Paso area, and will be available at no charge on campus during the first week of classes. For more information about the current rates, testing, and vaccinations, please visit epstrong.org.

Ethics and Security Vulnerabilities:

During this course, you will learn skills used by professional security evaluators to identify and remediate vulnerabilities. Tampering with systems and exploiting vulnerabilities without written consent has severe consequences including academic suspension and legal prosecution and could prevent you from ever working in your field of study.

In two words: **Act Responsibly!**

Tentative Schedule: (may change as the semester progresses)

| |
|--|
| Decoding Malware Communication |
| <ul style="list-style-type: none">• Uncovering malware communications (Wireshark and Volatility)• Reversing the encoding scheme (Ghidra)• Building a decoder (Dshell)• Test |
| Sandboxes and Innovation exercises |
| <ul style="list-style-type: none">• Environment development (Kali Linux, Ubuntu, Metasploitable)• Project planning |
| Dynamic Reversing |
| <ul style="list-style-type: none">• Create and reverse your own binary (IDA Pro)• Recover passcodes (IDA Pro debugger)• Automated reversing (Angr)• Test |
| Process Analysis |
| <ul style="list-style-type: none">• Ransomware analysis and mitigation• Ransomware key recovery• Password security and deep memory analysis |
| Projects |
| <ul style="list-style-type: none">• Presentations• Walkthroughs• Reports |