USC Viterbi
School of Engineering
Information Technology Program

ITP 425: Web Application Security

Units: 4
Fall 2024
Lecture: Tuesday, 6PM-7:50PM – KAP 267
Lab: Thursday, 6PM-7:50PM – RRB 101

Class Location: KAP 267 & RRB 101

Instructor: Andy Portillo
Office: N/A
Office Hours/Open Lab: By appointment
Contact Info:

- andy.portillo@usc.edu
- E-mails will be responded to within 48 hours

IT Help: Viterbi Information Technology
Hours of Service: Monday-Friday 8AM – 9PM
Contact Info: Phone: 213-740-0517; Email: engrhelp@usc.edu

Program Mission: The goal of the Digital Forensics and Cyber Security program at USC is to develop the critical thinking, analytical reasoning, and technical writing skills that are necessary to effectively work in a junior level digital forensic or cyber security analyst role. This is accomplished through utilizing industry standard tools and techniques to investigate labs and cases based upon real-world investigations and intrusions. Students will study various areas of cyber investigations, including digital evidence gathering, reporting, examinations, and court presentations. Students will study cyber security tenants of risk analysis, remediation, as well as penetration testing and network security design.

Piazza Enrollment: https://piazza.com/usc/fall2024/itp425

Course Description

This course will examine web applications from an offensive security standpoint. The topics for the semester will discuss information gathering, vulnerability detection, infiltration, and privilege escalation. Each portion of the course will involve understanding the web application architecture, penetration testing a web application, and hardening a vulnerable application.

Catalogue Description

Examine web applications from an offensive security standpoint. Topics include information gathering, vulnerability discovery and validation, exploitation and privilege escalation techniques. Real-case scenario analysis and reporting.

Learning Objectives

- Web application and their modern-day usage and capabilities
- Information gathering methodologies
- Systematic vulnerability detection
- Exploitation and lateral movement
- Web application security controls

Prerequisite(s): ITP 301 (Interactive Web Development) OR ITP 325 (Ethical Hacking & Systems Defense) OR ACAD 275 (Dev I)

Course Notes

The course is letter graded, with any and all materials available on Brightspace (Brightspace.usc.edu). Assignments will be conducted in the classroom during assigned class or lab time or outside of the classroom.

Technological Proficiency and Hardware/Software Required

It is assumed that the student has baseline technical knowledge (basic computer usage, basic internet usage). For any upper-division course (300-level and above), it is assumed that you have refined your technical abilities in ITP 125, including basic Python scripting.

Required Readings and Supplementary Materials

It is recommended that you keep up to date on the occurrences in the world of technology. The following listing of sources has been provided for your convenience: https://www.owasp.org, https://www.owasp.org/index.php/OWASP_Testing_Project, https://www.github.com/OWASP/CheatSheetSeries/tree/master/cheatsheets

Complete Modules 1-4 of the First.org training for CVSS version 3.1: https://learning.first.org/courses/course-v1:FIRST+CVSSv3.1+2020/about

Description and Assessment of Assignments

The assignments will be a combination of in-class and out-of-class laboratory exercises. They will typically involve some form of procedural work (we will provide instructions), with some reflection on the work performed including researching processes and procedures performed. All laboratory exercises will be graded on a point-scale, typically between 10 and 20 points.

Grading Breakdown

	% of Grade
Class Participation / Attendance	20%
Lab Assignments	35%
Final Report	45%
Total:	**100%**

Grading Scale

Course final grades will be determined using the following scale

A	93-100
A-	90-92
B+	87-89
B	83-86
B-	80-82
C+	77-79
C	73-76
C-	70-72
D+	67-69
D	63-66
D-	60-62
F	59 and below

Grading Policies

The lab assistants, graders, and instructors will do their best to return assignments graded to students within one week of the submission. Certain assignments that are longer in length, including exams, case reports, and final projects, may require more time.

The grading rubric is posted. There is no curve, and grades are based on performance in the class. While we understand the importance of grades and maintaining a high GPA, we cannot hand out high marks without justified performance in the class. Do not rely upon an expectation of a guaranteed minimum final grade in this class regardless of its impact on your overall GPA, financial situation, familial situation, or the fate of the galaxy.

The instructor is the ultimate authority over any grade for any assignment, exam or class.

University policy states that no extra credit may be afforded to individual students without the same opportunity made available to everyone in the class. Should there be extra credit in the class, it will be made available to the entire class. Do not ask the instructor for additional extra credit.

Grades will be posted on Brightspace and it is your responsibility to ensure that the grades online are accurate and to follow your progress in the class.

Assignment Policies

The labs will be posted on Brightspace under the “Assignments” or “Labs” section. Each lab will include instructions, a due date, and a link for electronic submission. Labs must be submitted using this link. Do not email your assignments to the instructor, lab assistants, or graders

Unless otherwise noted, all lab assignments are due at the beginning of class the next class period, unless otherwise modified by Brightspace announcement and/or email from the instructor and/or Lab Assistants. Some assignments (typically longer in length) will have a due date on 11:59:59 PM on the Friday or Sunday of the following week. Do not expect a timely response from the lab assistants, graders, or instructors if emailed after normal business hours particularly on the date the assignment is due.

If you join the class after the semester has started, you will have two weeks from the date of enrollment to complete all assignments due before you joined the class unless a written extension is granted from the instructor, typically via email.

It is your responsibility to submit your assignments on or before the due date and verify it has been successfully submitted. Assignments turned in up to 24 hours late will have 25% of the total points deducted from the graded score. Assignments turned in between 24 and 48 hours late will have 50% of the total points deducted from the graded score. After two days, submissions will not be accepted and you will receive no credit for the assignment.

The lab assistants and graders are not authorized to grant an extension on any assignment. Any extensions must be requested of the instructor in writing and confirmed in writing. If you ask for an extension on the day the assignment is due, without expressing an emergency such as family crisis, it will probably not be granted.

Certain assignments will require a paper submission, and you may be asked to submit them to the main ITP office. There have been previous allegations of student rudeness to the ITP Staff. If the staff complains about you being rude, you will have 25% automatically deducted from your assignment. Don’t be rude.

The instructor and lab assistants reserve the right to not answer certain questions about the lab assignment. This is normally due to the nature of the question being directly related to the learning objectives of the lab. You are encouraged to use online resources to further your understanding of the material to successfully answer questions related to the lab assignment (in other words, use your research skills).

All lab assignments have been tested by the instructor and/or lab assignments. Due to the nature of certain software packages and configurations in the lab, the assignments may or may not work as intended. You are encouraged to ask questions if something appears to not work correctly. However, there are certain instances where things are intended to not work correctly and the instructor and lab assistant will indicate as such. When in doubt, do a little research.

Contacting the Instructor, Lab Assistants or Graders

When emailing the lab assistants, graders or instructor, please be sure to include your full name, student ID, class name and number, and class section (day and time) in the email.

Emails sent to the lab assistants or graders will be responded to within two business days. The instructor will endeavor to respond to emails within two business days. Do not email anyone with the expectation of an immediate response within the hour. Please do not complain when we have not responded to your email ten minutes before the assignment deadline.

Questions regarding individual clarification or regrade must be made through email to both the grader and the instructor. When requesting a regrade, the instructor has the prerogative to alter a grade higher or lower based upon a review of the entire assignment. Be absolutely certain before requesting a regrade of any assignment or exam – if you are going to roll the dice, be certain of your gamble.

Questions about lab assignments should be submitted through the class discussion board (typically Piazza). This will have a faster response rate. Do not post code or answers on Piazza.

The instructor will post his/her regular office hours on Brightspace. You may request a meeting with the instructor outside of normal office hours. Should you go to the instructor's office outside of normal office hours or outside of a scheduled meeting, do not expect the instructor to be able to meet with you. We do have other responsibilities outside of the class.

Attendance Policy

You are expected to be in class, on time, and distraction free. As this class meets once a week and as it is lecture and lab any student who misses more than two classes is in danger of failing the course. Please see the instructor immediately if you have missed at least two class meetings.

This is a lab-based class. Certain class sections will be lecture, lab, or a combination of lecture and lab. Attendance is vital to success in the class, and punctuality is vital to success in your professional careers. The lab assistants will be taking attendance for every class meeting. If you anticipate missing a class due to an event, please email the lab assistants and instructor prior to the start of class. If you are sick, we want you to get better and not infect your fellow classmates – please email the lab assistants and instructor. Should you miss a class with a lab assignment, contact the lab assistants to determine available times to come to the lab and finish your assignment.

Writing Skills

A significant portion of the cyber security and digital forensics curriculum involves communicating by writing professional quality case reports. These reports are held to standards expected by professionals in the industry who are writing reports for clients, executives attorneys, judges, juries, congresspeople, senators – individuals who may be very technical or individuals who while intelligent are not technical.

It is expected that the reports will be written with correct spelling, grammar, and language nuances of the American English language. A component of each report grade will be based on writing style, grammar, and word choice. These reports must be accessible to technical and non-technical readers alike.

It is recommended that you visit the USC American Language Institute (http://ali.usc.edu/) for resources to assist you in this course and your professional career. Writing assistance is also available from the Dornsife Writing Center (https://dornsife.usc.edu/writingcenter/). You do not need to be a Dornsife student to take advantage of the services from the Writing Center. Additional writing assistance is also available from the Viterbi Writing Center in the form of Writing Consultations (http://viterbi.usc.edu/students/undergrad/varc/writing-consultations.htm). In accordance with university standards, plagiarism of any type will not be tolerated.

Course Content Distribution and Synchronous Session Recordings Policies

USC has policies that prohibit the recording and distributing any synchronous and asynchronous course content outside of the learning environment. Recording a university class without the express written permission of the instructor and announcement to the class, or unless conducted pursuant to an Office of Student Accessibility Services (OSAS) accommodation. Recording can inhibit free discussion in the future and thus infringe on the academic freedom of other students and the instructor. (Living our Unifying Values: The USC Student Handbook, page 13). Distribution or use of notes, recordings, exams, or other intellectual property, based on university classes or lectures without the express written permission of the instructor for purposes other than individual or group study. This includes but is not limited to providing materials for distribution by services publishing course materials. This restriction on unauthorized use also applies to all information that had been distributed to students or in any way had been displayed for use in relation to the class, whether obtained in class, via email, on the internet, or via any other media. (Living our Unifying Values: The USC Student Handbook, page 13)

Academic Integrity

The University of Southern California is foremost a learning community committed to fostering successful scholars and researchers dedicated to the pursuit of knowledge and the transmission of ideas. Academic misconduct is in contrast to the university's mission to educate students through a broad array of first-rank academic, professional, and extracurricular programs and includes any act of dishonesty in the submission of academic work (either in draft or final form).

This course will follow the expectations for academic integrity as stated in the USC Student Handbook. All students are expected to submit assignments that are original work and prepared specifically for the course/section in this academic term. You may not submit work written by others or "recycle" work prepared for other courses without obtaining written permission from the instructor(s). Students suspected of engaging in academic misconduct will be reported to the Office of Academic Integrity.

Other violations of academic misconduct include but are not limited to, cheating, plagiarism, fabrication (e.g., falsifying data), knowingly assisting others in acts of academic dishonesty, and any act that gains or is intended to gain an unfair academic advantage.

The impact of academic dishonesty is far-reaching and is considered a serious offense against the university and could result in outcomes such as failure on the assignment, failure in the course, suspension, or even expulsion from the university.

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences that can include expulsion. Please familiarize yourself with the discussion of plagiarism and academic integrity in the USC Student Handbook: https://policy.usc.edu/studenthandbook

Other forms of academic dishonesty are equally unacceptable. See additional information and university policies on scientific misconduct, http://policy.usc.edu/scientific-misconduct

For more information about academic integrity, see the student handbook or the Office of Academic Integrity's website, and university policies on Research and Scholarship Misconduct.

Policy on Generative AI

Since creating, analytical, and critical thinking skills are part of the learning outcomes of this course, all assignments should be prepared by the student working individually or as allowed by the instructor in groups. Students may not have another person or entity complete any substantive portion of the assignment. Developing strong competencies in these areas will prepare you for a competitive workplace. Therefore, using AI-generated tools is prohibited in this course, will be identified as plagiarism, and will be reported to the Office of Academic Integrity.

ChatGPT:

ChatGPT and similar programs and platforms represent great promise for the field of information technology, cybersecurity, and just about every other part of our world. Our policy on ChatGPT is as follows: you may use ChatGPT or similar programs for your assignments for this class, but treat them as a research tool and not a primary or secondary source. This means 1) cite your original source(s), and they can't be ChatGPT or similar tools directly, 2) treat everything those tools tell you to do or information they provide with a strong grain (pound?) of salt, and 3) never copy and paste or treat their output as a source or knowledgebase of ultimate authority. We want to emphasize the concept of using them as tools since they may guide you to the right answers; however, they can't and don't always do this correctly, and you may not know when they're telling the truth or making something up.

Our team is exceptionally good at recognizing answers from ChatGPT and similar tools. AI detection tools and real humans will both be used to validate your assignments in this class. If we suspect or determine that your assignments are being produced by AI-based tools or otherwise violate the guidelines above, your submissions will be treated as violations of the university's academic integrity policy and handled as such.

ITP 425 - Course Schedule

Week	Date	Topic(s)	Deliverables
1	T 8/27	Course Introduction and Intro to OWASP	--
	TH 8/29	Lab 1 – Enumeration	**Lab 1 – Due 9/5**
2	T 9/3	OWASP A1:2021 – Security Misconfiguration	--
	TH 9/5	Lab 2 – A1:2021	**Lab 2 – Due 9/12**
3	T 9/10	OWASP A6:2021 – Vulnerable and Outdated Components	
	TH 9/12	/ Lab 3 – A6:2021	**Lab 3 – Due 9/19**
4	T 9/17	OWASP A7:2021 – Identification and Authentication Failures	--
	TH 9/19	Lab 4 – A7:2021	**Lab 4 – Due 9/26**
5	T 9/24	OWASP A1:2021 – Broken Access Control	--
	TH 9/26	Lab 5 – A1:2021	**Lab 5 – Due 10/3**
6	T 10/1	OWASP A3:2021 – Injection Part 1: Command Injection and Cross-site Scripting (XSS)	--
	TH 10/3	Lab 6 – A3:2021 Injection Part 1	**Lab 6 – Due 10/10**
7	T 10/8	OWASP A3:2021 – Injection Part 2: SQL and PHP injection	--
	TH 10/10	Lab 7 – A3:2021 Injection Part 2	**Lab 7 – Due 10/17**
8	T 10/15	Mid-Term: Scavenger Hunt	**Scavenger Hunt – Due 10/24**
	TH 10/17		
9	T 10/22	OWASP A10:2021 – A10:2021 Server-Side Request Forgery (SSRF)	--
	TH 10/24	Lab 8 – A10:2021	**Lab 8 – Due 10/31**
10	T 10/29	OWASP A08:2021 – Software and Data Integrity Failures	--
	TH 10/31	Lab 9 – A8:2021	**Lab 9 – Due 11/7**
11	T 11/5	OWASP A2:2021 – Cryptographic Failures with *Guest Lecturer(s)*	--
	TH 11/7	Lab 10 – A2:2021	**Lab 10 – Due 11/14**
12	T 11/12	OWASP A9:2021 – Security Logging and Monitoring Failures with *Guest Lecturer(s)*	--
	TH 11/14	Lab 11 – A9:2021	**Lab 11 – Due 11/21**
13	T 11/19	Practical Review	**CTF Responses - Due 11/28**
	TH 11/21		
14	T 11/26		
	TH 11/28		
15	T 12/3	Web Application Penetration Testing Report	**Students must submit a web app pentest report with a minimum of 10 vulnerabilities (one for each OWASP Top 10).**
	TH 12/5	Study Days – No Class	
Finals	T 12/10	Study Days – No Class	
	TH 12/12	**Final Due**	

Final Exam: As stated in the USC Schedule of Classes at https://classes.usc.edu/term-20243/final-examinations-schedule/

Statement on Academic Conduct and Support Systems

Students and Disability Accommodations:

USC welcomes students with disabilities into all of the University's educational programs. The Office of Student Accessibility Services (OSAS) is responsible for the determination of appropriate accommodations for students who encounter disability-related barriers. Once a student has completed the OSAS process (registration, initial appointment, and submitted documentation) and accommodations are determined to be reasonable and appropriate, a Letter of Accommodation (LOA) will be available to generate for each course. The LOA must be given to each course instructor by the student and followed up with a discussion. This should be done as early in the semester as possible as accommodations are not retroactive. More information can be found at osas.usc.edu. You may contact OSAS at (213) 740-0776 or via email at osasfrontdesk@usc.edu.

Support Systems:

Student Counseling Services (SCS) – (213) 740-7711 – 24/7 on call
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention. engemannshc.usc.edu/counseling

National Suicide Prevention Lifeline – 1 (800) 273-8255
Provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week. www.suicidepreventionlifeline.org

Relationship and Sexual Violence Prevention Services (RSVP) – (213) 740-4900 – 24/7 on call
Free and confidential therapy services, workshops, and training for situations related to gender-based harm. engemannshc.usc.edu/rsvp

Sexual Assault Resource Center
For more information about how to get help or help a survivor, rights, reporting options, and additional resources, visit the website: sarc.usc.edu

Office of Equity and Diversity (OED)/Title IX Compliance – (213) 740-5086
Works with faculty, staff, visitors, applicants, and students around issues of protected class. equity.usc.edu

Bias Assessment Response and Support
Incidents of bias, hate crimes and microaggressions need to be reported allowing for appropriate investigation and response. studentaffairs.usc.edu/bias-assessment-response-support

The Office of Disability Services and Programs
Provides certification for students with disabilities and helps arrange relevant accommodations. dsp.usc.edu

Student Support and Advocacy – (213) 821-4710
Assists students and families in resolving complex issues adversely affecting their success as a student EX: personal, financial, and academic. studentaffairs.usc.edu/ssa

Diversity at USC
Information on events, programs and training, the Diversity Task Force (including representatives for each school), chronology, participation, and various resources for students. diversity.usc.edu

USC Emergency Information
Provides safety and other updates, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible. emergency.usc.edu

USC Department of Public Safety – UPC: (213) 740-4321 – HSC: (323) 442-1000 – 24-hour emergency or to report a crime.
Provides overall safety to USC community. dps.usc.edu