USC Viterbi
School of Engineering
Information Technology Program

ITP 425: Web Application Security

Units: 4
Fall 2021
Lecture: Monday, 5PM – 6:50PM
Lab: Wednesday, 5PM-6:50PM

Class Location: RRB 101 & Online

Instructor: Andy Portillo
Office: TBD
Office Hours: Wednesday 5-6:50PM

- Additional office hours will be held online by appointment, use email below to contact me

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.

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. This course follows the OWASP Top Ten web application vulnerabilities.

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
Course is letter graded, with any and all materials available on Blackboard (blackboard.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.

Students will be running a virtual machine during the course and will need to have a system capable from hosting a VM running with the following:
4 GB of RAM
40+ GB of storage (external drive preferred)
2 processors

If you do not have a system capable to handle hosting the VM, please look into ITP laptop loaner program.

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%
Labs / 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 Blackboard 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 Blackboard 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 Blackboard 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 blackboard. 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 what was discovered by writing professional quality reports. These reports are held to standards that are expected by professionals in industry who are writing reports for clients, attorneys, judges and juries. 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. While you will not be writing reports in 125, please take care to properly communicate your lab and assignment findings.

If you are not a native English speaker and writer, 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 careers. 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.

Additional University policies follow the course schedule.

ITP 425 - Course Schedule

Week	Date	Topic(s)	In Class Activities	Deliverables
1	M 8/23	Course Introduction and Intro to OWASP	Lecture	--
	W 8/25	Lab 1 – Setting up Lab	Lab	**Lab 1 – Due 9/1**
2	M 8/30	OWASP A6:2017 – Security Misconfiguration	Lecture	--
	W 9/1	Lab 2 – A6:2017	Lab	**Lab 2 – Due 9/8**
3	M 9/6	OWASP A9:2017 – Using Components with Known Vulnerabilities	Lecture	--
	W 9/8	Lab 3 – A9:2017	Lab	**Lab 3 – Due 9/15**
4	M 9/13	OWASP A2:2017 – Broken Authentication	Lecture	--
	W 9/15	Lab 4 – A2:2017	Lab	**Lab 4 – Due 9/22**
5	M 9/20	OWASP A5:2017 – Broken Access Control	Lecture	--
	W 9/22	Lab 5 – A5:2017	Lab	**Lab 5 – Due 9/29**
6	M 9/27	OWASP A1:2017 – Injection Part 1: HTML and Command Injections with bypassing techniques	Lecture	--
	W 9/29	Lab 6 – A1:2017 Part 1	Lab	**Lab 6 – Due 10/6**
7	M 10/4	OWASP A1:2017 – Injection Part 2: SQL injection	Lecture	--
	W 10/6	Lab 7 – A1:2017 Part 2	Lab	**Lab 7 – Due 10/13**
8	M 10/11	Scavenger Hunt with *Guest Lecturer(s)*	Scavenger Hunt	**Scavenger Hunt – Due 10/20**
	W 10/13			
9	M 10/18	OWASP A4:2017 – XML External Entities (XXE) and A7:2017 – Cross-Site Scripting (XSS)	Lecture	--
	W 10/20	Lab 8 - A4:2017 and A7:2017	Lab	**Lab 8 – Due 10/27**
10	M 10/25	OWASP A8:2017 – Insecure Deserialization	Lecture	--
	W 10/27	Lab 9 – A8:2017	Lab	**Lab 9 – Due 11/3**
11	M 11/1	OWASP A3:2017 – Sensitive Data Exposure with *Guest Lecturer(s)*	Lecture	--
	W 11/3	Lab 10 – A3:2017	Lab	**Lab 10 – Due 11/10**
12	M 11/8	OWASP A10:2017 – Insufficient Logging and Monitoring with *Guest Lecturer*	Lecture	--
	W 11/10	Lab 11 – A10:2017	Lab	**Lab 11 – Due 11/17**
13	M 11/15	Practical Review	CTF Review	**CTF Responses - Due 12/1**
	W 11/17			
14	M 11/22			
	W 11/24			
15	M 11/29	Web Application Penetration Testing Report	Final Paper - Report Template will be provided.	**Students must submit a web app pentest report with a minimal of 10 vulnerabilities (one for each OWASP Top 10). Final Report Due **TBD****
	W 12/1	Study Days – No Class (TBD)		
Finals	M 12/6	Study Days – No Class		
	W 12/8	Final Due		

Statement on Academic Conduct and Support Systems

Academic Conduct:

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 in *SCampus* in Part B, Section 11, "Behavior Violating University Standards" policy.usc.edu/scampus-part-b. Other forms of academic dishonesty are equally unacceptable. See additional information in *SCampus* and university policies on scientific misconduct, http://policy.usc.edu/scientific-misconduct.

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