CSEC 731 – Web Server & Application Security Audits
Section 01
Spring 2022

Instructor	Prof. Robert Olson
Office Location	GCI-1789
Phone	475-4601
E-mail	rboics@rit.edu
Office Hours	Friday – 2pm to 4pm, Zoom
Course Time	Asynchronous
Course Place	Online

1. Catalog description: This course discusses the processes and procedures to perform a technical security audit of web servers and web based applications. Students will not only explore Web Servers and Applications/Services threats, but also apply the latest auditing techniques to identify vulnerabilities existing in or stemming from web servers and applications. Students will write and present their findings and recommendations in audit reports on web servers and application vulnerabilities. To be successful in this course students should be knowledgeable in a scripting language and comfortable with the administration of both Linux and Windows platforms.

2. Prerequisite(s): CSEC-600

3. Required Course Textbook: None

3a. Optional Supplemental Materials (Available from RIT Library as e-books):

- The Web Application Hacker's Handbook
- The Web Application Defender's Cookbook
- The Browser Hacker's Handbook
- Black Hat Python, 2nd Edition
- Web Security for Developers
- Designing Secure Software
- Docker Deep Dive
- DevOps with Kubernetes – 2nd Edition
- Practical Ansible
- Continuous Integration with Jenkins

4. Course Learning Outcomes:

After completing this course, the student will be able to:

- Discuss the function and construction of web servers, web browsers, and web applications
- Demonstrate knowledge of assorted web protocols and their implementations, such as HTTP

- Demonstrate knowledge of web application and server vulnerabilities such as the OWASP Top 10.
- Develop DevOps tooling for deploying and hardening web applications
- Assess the security of web applications and servers

5. Tentative Course Outline:

Week 1:	Web Architecture and Network Programing	P-A: Writing a Web Scraper
Week 2-3	Web Protocols and Parsing	(W3) P-B: Writing a Web Server
Week 4:	Network Security for Web Servers	
Week 5:	Web Application Programming	
Week 6:	Server-side Attacks	
Week 7:	Client-side Attacks	
Week 8:	Secure Programming	Midterm Exam
Week 9:	Web Application Security Assessments	P-C: Audit/Harden FOSS Web App
Week 10:	Web App Authentication Mechanisms	
Week 11:	Web App Hardening and Automation	
Week 12:	Virtualization/Containerization for Web	
Week 13:	(Tentative) Kubernetes	
Week 14:	(Tentative) CI/CD Pipelines	
Week 15:	Course Wrap-up	Final Exam

6. Grading:

The relative weight of each component of your grade is shown on the table below.

Component	**Percentage**
Projects (3)	50% Project A – 10% Project B – 20% Project C – 20%
Participation / Discussions	20%
Exams (2)	30% (15% each)

The table below lists student's grade for a given percentage achieved. Numeric grades that fall between categories will be rounded up or down at the discretion of the instructor.

94%-100%	90%-93%	88%-89%	82%-87%	80%-81%	78%-79%	72%-77%	70%-71%	60-69	0%-59%
A	A-	B+	B	B-	C+	C	C-	D	Fail

7. Exams, Projects, and Labs/Assignments:

All exams must be taken on the day(s) specified. All projects and lab assignments are due on the date listed in the hand-out provided by the instructor. Exceptions will be made at the sole discretion of the instructor. Some valid reasons may include:

1. Illness of the student or serious illness of a member of the student's immediate family.
2. A death in the student's immediate family
3. Trips sponsored by official RIT student groups, academic units, or athletic teams.
4. Major religious holidays

A student requiring special considerations for reasons 3 or 4 should talk to the instructor at least a week in advance, whenever possible.

8. Class Attendance

All students are expected to participate in this course for the entire duration of the semester. "Attending class" is recommended, although it may take different forms because of the COVID-19 pandemic. It is my intention to stream all lecture content via Zoom for this course, allowing students to participate even if they cannot attend in-person.

At the time of writing this syllabus, it is unclear if I'll be able to record these streamed lectures and distribute them via MyCourses.

You should not physically attend class if you are feeling sick and you do not need to ask my permission to attend via Zoom instead of in person. There are a host of valid reasons, ranging from transportation challenges to mental health, why a student may choose not to attend CSEC 731 in person. This course will move at a rapid pace, however, and it is your responsibility to ensure that you are continuing to actively participate.

This is one of my standard syllabus clauses and does not apply to classes taught entirely asynchronously.

9. Academic Honesty

The following statement is the Policy on Academic Dishonesty for the Computing Security Department.

The Computing Security Department (CSEC) does not condone any form of academic dishonesty. Any act of improperly representing another person's work as one's own (or allowing someone else to represent your work as their own) is construed as an act of academic dishonesty. These acts include, but are not limited to, plagiarism in any form or use of information and materials not authorized by the instructor during an examination or for any assignment.

If a faculty member judges a student to be guilty of any form of academic dishonesty, the student will receive a failing grade for the course. Academic dishonesty involving the abuse of RIT computing facilities may result in the pursuit of more severe action.

If the student believes the action by the instructor to be incorrect or the penalty too severe, the faculty member will arrange to meet jointly with the student and with the faculty member's immediate supervisor. If the matter cannot be resolved at this level, an appeal may be made to the Academic Conduct Committee of the college in which the course is offered.

If the faculty member or the faculty member's immediate supervisor feels that the alleged misconduct warrants more severe action than failure in the course, the case may be referred to the Academic Conduct Committee. The Academic Conduct Committee can recommend further action to the dean of the college including academic suspension or dismissal from the Institute.

The following definitions will be used to clarify and explain unacceptable conduct.
This is not intended to be an exhaustive list of specific actions but a reasonable description to guide one's actions.

CHEATING includes knowingly using, buying, stealing, transporting or soliciting in whole or part the contents of an administered/un-administered test, test key, homework solution, paper, project, software project or computer program, or any other assignment.
It also includes using, accessing, altering, or gaining entry to information held in a computer account or disk owned by another.

COLLUSION means the unauthorized collaboration with another person in preparing written work or computer work (including electronic media) offered for credit. Final work submitted by a student must be substantially the work of that student. Collaboration on an assignment is expressly forbidden unless it is explicitly designated as a group project. When there is any doubt, a student should consult the instructor (NOT ANOTHER STUDENT) as to whether some action Is considered collusion.

Whenever there is any question as to whether a particular action is considered academic dishonesty, the instructor should be consulted PRIOR to commencing that action.

10. Responsible Disclosure

During the course of the semester, students in CSEC 731 may uncover previously unknown security vulnerabilities in mobile applications or mobile devices. In the event that this happens, students will be expected to practice responsible disclosure practices, in consultation with the instructor. This includes, but may not be limited to, submitting the vulnerability to a bug bounty program or notifying the company of the vulnerability far enough in advance of releasing details to give the company sufficient time to respond. The instructor reserves the right to penalize a students' grade if the student fails to practice responsible disclosure and to recommend the student for further academic discipline if needed.

11. Course Success

Success in this course depends heavily on your personal health and wellbeing. Recognize that stress is an expected part of the college experience, and it often can be compounded by unexpected setbacks or life changes outside the classroom. Moreover, those with marginalized identities may be faced with additional social stressors. Your other instructors and I strongly encourage you to reframe challenges as an unavoidable pathway to success. Reflect on your role in taking care of yourself throughout the term, before the demands of exams and projects reach their peak. Please feel free to reach out to me about any difficulty you may be having that may impact your performance in this course as soon as it occurs and before it becomes unmanageable. In addition to your academic advisor, I strongly encourage you to contact the many other support services on campus that stand ready to assist you.

12. COVID-19, Year 3 Addendum

Please be advised that, under emergency circumstances, I may be required to alter course requirements, assignment deadlines, attendance expectations, and grading procedures. Please also be advised that the university may have to alter the academic calendar in response to a university. This addendum added as the result of a recommendation in a mass email sent from Dr. Ellen Granberg's office titled "Continuity of Instruction".