R·I·T	Rochester Institute of Technology Golisano College of Computing and Information Sciences Department of Computing Security

CSEC-380

Principles of Web Application Security

2215 Course Syllabus

REMINDER: The information presented in this syllabus is subject to expansion, change, or modification during the semester.

Instructor (section 01): Name: Rob Olson Email address rboics@rit.edu	**Office Hours (via Slack):** Th: 3:30 PM – 5:00 PM F: 10:00 AM – 12:00 PM Or via scheduled appointment **Electronic Course Resources:** **http://mycourses.rit.edu**

Course Text and Materials

Optional:
Dafydd Stuttard and Marcus Pinto - *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Wiley;* Osborne Media; 2nd edition, 2011
Handouts & Online Readings as assigned

Important RIT Deadlines

Last day of add/drop is ***January 18th***
Last day to withdraw with a grade of "W" is ***April 1rd***
NOTE: The Computer Security department policy states that a student has one semester to **challenge any grade**. After that, grades cannot be challenged.

Course Description

This course is designed to give students an understanding of the theories and ideas relating to web application security. The course will introduce students to the concepts associated with deploying and securing typical HTTP environments as well as defensive techniques they may employ.

Course Objectives

General

This course is designed to provide students with an understanding of the principles of web application security. Students will be introduced to common misconfigurations and vulnerabilities that may be present in standard web applications. Industry best practices will be studied and implement to demonstrate how to defend against such threats.

Prerequisites:
NSSA-245 and (CSEC 101 or CSEC 102 or CSEC 140)

Course Organization

MyCourses

The course is organized by using RIT's myCourses platform and the instructor's personal page. You are required to have a DCE account to access both. myCourses can be accessed at ***mycourses.rit.edu***. myCourses drop boxes may be used for the submissions of homework.

Online Exam

Exams will include multiple-choice questions and other content formats as appropriate. The written exams are designed to test your mastery of the material covered in lecture and from the assigned reading. The exams are closed book, closed notes, and closed neighbor. Access to cell phones, pagers, PDAs or any other electronic devices is prohibited. There will be a midterm and a final.

Homework

Roughly every other week homework will be assigned to students to help them understand concepts and practice techniques covered in class. Homework must be submitted according to your lab instructor's directions. Late homework will be penalized at the instructor's discretion.

Grading

Grading will be completed 2 weeks after the due date

Blog

Write a blog post related to computing security that provides new content or perspective compared to what is generally published.

Grading

The grading scale used along with the grading criteria is as follows:

Component	Weight
Homeworks	35%
Midterm Exam	10%
Final Exam	10%
Blog	10%
Quizzes	15%
Practical	15%
Reading Quizzes	5%

Range	Grade
>93%	A
90-93%	A-
87-89%	B+
83-87%	B
80-83%	B-
77-79%	C+
73-76%	C
70-73%	C-
60-69%	D
<60%	F

Course Schedule

Week	General Topics/Exams	Optional Reading
1	Foundational Concepts of Web	Chapter 1
2	Protocol Overview/History	
3	HTTP Overview	Chapter 3
4	HTTP Overview Cont.	
5	Authentication in HTTP	Chapter 6
6	Browser Defenses	
7	Midterm	
8	Client Side Attacks	Chapter 10
9	Client Side Attacks: XSS	Chapter 12
10	Server Side Defenses	Chapter 18
11	Server Side Attacks: SQLi	Chapter 9
12	Server Side Attacks: Code Execution	
13	Other Server Side Attacks	Chapter 13
14		
15	Future of Web attacks	

Cheating Policy: Please review the departmental policy on cheating as described at http://www.rit.edu/academicaffairs/policiesmanual/d080

Late Work

I expect that every effort will be made to ensure that work is submitted on time. The official due date is always the due date and time associated with the dropbox. Assignments submitted late will suffer a 20% penalty, in other words the highest possible grade you can receive is an 80.

Nevertheless, I understand that unforeseen circumstances occasionally arise. If you have a legitimate and reasonable explanation for your assignment being late, schedule an appointment with me to discuss it and I will consider rescinding the 20% penalty.

Remember, the dropbox due date, is the official due date. However, there is a 48 hour grace period in which you can still submit the assignment to the dropbox, keep in mind that if it is submitted after the due date/time it is still considered late and subject to the penalty. Do not

assume that because you are able to submit it to the dropbox successfully you submitted it on time.
After the 48 hour grace period the dropbox will close, and you will not be able to submit an assignment. In special situations late assignments may be allowed to be submitted via dropbox (It will be reopened for you). Any assignment submitted after the 48 hour grace period will receive the 20% late penalty without exception. Additionally, submitting a late assignment to the dropbox does not guarantee it will be graded, it is entirely at the discretion of the teaching assistant and/or instructor.

Exams
There will be two exams given in this course. The exams will contain a mixture of multiple choice, true/false, and short answer questions. A note sheet will NOT be allowed.

Typing
All assignments for this course, whether assigned normally or added as extra credit, are to be typed – there are no exceptions to this. Any diagrams or schematics must be done electronically as well. Use Visio or equivalent. Anything that you hand in that is not typed will not be graded, unless you have contacted me ahead of time to make other arrangements. All work should be submitted electronically to myCourses in the respective drop box.

Grading
Grading will be completed within two weeks by the instructor. For every day after the two week period, each student (or group) will receive a bonus point for each day that the grading is not completed. Work that is submitted late via dropbox is exempt from the two-week rule. It will be graded at the discretion of the professor/TA as stated in the section on late work.