Metropolitan State University of Denver
Regular Course Syllabus

CSS - 3751 - Application Security   Fall 2016

Status	completed
Tracking:	LAS1617-29
Department	Mathematical and Computer Sciences, Department of
Prefix:	CSS
Course Number:	3751
Course Type:	Computer Science Studies
Course Title:	Application Security
Transcript Course Title:	Application Security
Equivalent/ Crosslisted?	
List all equivalent courses:	
List all crosslisted courses:	
Check All That Apply:	Elective
Credit Hours:	3
Schedule Type:	Lecture
Grade Mode:	Letter
Lecture:	45
Lab:	
Internship:	
Practicum:	
Other:	
Additional Student Work Hours per course:	90
Variable topics umbrella course:	No
If yes, number of credits/ repeats allowed	
Specified repeatable course:	No
If yes, number of credits/ repeats allowed	
Prerequisite(s):	CSS 2751 and CSS 2752 or permission of instructor
Corequisite(s):	
Prerequisite(s) and/or Corequisite(s):	
Banner Prerequisite(s):	CSS 2751 and CSS 2752
Banner Corequisite(s):	
Banner Prerequisite(s) and/or Corequisite(s):	
Level	
Class	
Program/Major	
Student attribute	
Catalog Course Description:	Writing applications so that they are less susceptible to compromise is a critical aspect of cybersecurity. This course explores how applications are compromised and the steps that must be taken to make them more secure. Several different languages and platforms are covered.

Required Reading and Other Materials will be equivalent to:	Michael Howard, David LeBlanc, John Viega, (2009) 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them 1st Edition, ISBN-13: 978-0071626750
Specific, Measurable Student Behavioral Learning Objectives:	1. Analyze the various types of memory corruption used for compromises. 2. Plan for static and dynamic tests to detect memory corruption. 3. Evaluate a programming language for security. 4. Measure the likelihood that a specific program could be compromised. 5. Create steps to harden an SQL database. 6. Select appropriate defenses for a web application. 7. Assess the results of several types of testing against an application.

Detailed Outline of Course Content (Major Topics and Subtopics) or Outline of Field Experience/ Internship	I. Memory management
	  A. The stack and heap
	  B. Buffer overflows
	  C. Heap sprays
	  D. Use after free, multiple frees
	II. Language design
	  A. Garbage collection
	  B. Safe programming techniques
	III. Database security
	  A. SQL injection and mitigation
	  B. Role enforcement
	  C. Protection mechanisms
	IV. Web application security
	  A. XSS
	  B. JavaScript
	  C. Input checking
	V. Browser security
	  A. Same origin policy
	VI. Secure coding
	  A. Buffer overflows
	  B. Numeric overflows
	  C. String formatting issues
	VII. Testing
	  A. Unit, integration, system
	  B. Static and dynamic
	  C. Penetration
	  D. Fuzz

Evaluation of Student Performance	Required: a midterm and final exam and four papers. Optional: quizzes. participation, classwork, homework, projects.
Learning Objectives	
Distribution of Credit Hours	3 (3+0)

Steps	Decision	Date	
Originator			
Steve Beaty	approve	09/12/2016 10:09AM	
Department Curriculum Committee Chair			
Clark Dollard	approve	09/12/2016 02:58PM	
Department Chair			
Lindsay Packer	approve	09/12/2016 03:41PM	

Dean's Office Tracking Assignment			
Cynthia Philbrook	approve	09/14/2016 08:42AM	
Substantive College Level			
Linda Lang-Peralta	approve	12/07/2016 04:43PM	
Mona Mocanasu	approve	12/05/2016 10:12AM	
Steve Beaty	approve	10/07/2016 10:41AM	
Faculty Senate President			
Matthew Makley	None		
Erica Buckland	force-approve	01/05/2017 10:59AM	
AVP Academic and Student Affairs			
Bernice Harris	approve	01/05/2017 11:14AM	