COURSE OUTLINE: NASA201 - WEB PROG + SECURITY

Prepared: Rodney Martin
Approved: Martha Irwin, Dean, Business and Information Technology

Course Code: Title	NASA201: WEB PROGRAMMING AND SECURITY
Program Number: Name	2196: NETWRK ARCH & SEC AN
Department:	COMPUTER STUDIES
Academic Year:	2024-2025
Course Description:	This course will delve into the current scripting and computer languages used by modern web clients and servers, with a focus on the programming methodologies used to prevent exploitation of web security vulnerabilities.
Total Credits:	3
Hours/Week:	3
Total Hours:	45
Prerequisites:	There are no pre-requisites for this course.
Corequisites:	There are no co-requisites for this course.
Vocational Learning Outcomes (VLO's) addressed in this course: **Please refer to program web page for a complete listing of program outcomes where applicable.**	**2196 - NETWRK ARCH & SEC AN** VLO 2 Perform network monitoring, analysis and troubleshooting to determine efficient and secure operations. VLO 3 Develop a security architecture plan to incorporate both perimeter and endpoint security controls and devices to provide layers of security. VLO 7 Deploy servers to host web applications, focusing on securing the server and web from identified security risks.
Essential Employability Skills (EES) addressed in this course:	EES 1 Communicate clearly, concisely and correctly in the written, spoken, and visual form that fulfills the purpose and meets the needs of the audience. EES 2 Respond to written, spoken, or visual messages in a manner that ensures effective communication. EES 4 Apply a systematic approach to solve problems. EES 5 Use a variety of thinking skills to anticipate and solve problems. EES 7 Analyze, evaluate, and apply relevant information from a variety of sources.
Course Evaluation:	Passing Grade: 50%, D A minimum program GPA of 2.0 or higher where program specific standards exist is required for graduation.

Other Course Evaluation & Assessment Requirements:	A+ = 90-100%
	A = 80-89%
	B = 70-79%
	C = 60-69%

D = 50-59%
F < 50%

Students are expected to be present to write all tests in class, unless otherwise specified. If a student is unable to write a test due to illness or a legitimate emergency, that student must contact the professor prior to class and provide reasoning. Should the student fail to contact the professor, the student shall receive a grade of zero on the test.

If a student is not present 10 minutes after the test begins, the student will be considered absent and will not be given the privilege of writing the test.
Students exhibiting academic dishonesty during a test will receive an automatic zero. Please refer to the College Academic Dishonesty Policy for further information.

In order to qualify to write a missed test, the student shall have:
a.) attended at least 75% of the classes to-date.
b.) provide the professor an acceptable explanation for his/her absence.
c.) be granted permission by the professor.

NOTE: The missed test that has met the above criteria will be an end-of-semester test.

Labs / assignments are due on the due date indicated by the professor. Notice by the professor will be written on the labs / assignments and verbally announced in advance, during class.

Labs and assignments that are deemed late will have a 10% reduction per academic day to a maximum of 5 academic days at 50% (excluding weekends and holidays). Example: 1 day late - 10% reduction, 2 days late, 20%, up to 50%. After 5 academic days, no late assignments and labs will be accepted. If you are going to miss a lab / assignment deadline due to circumstances beyond your control and seek an extension of time beyond the due date, you must contact your professor in advance of the deadline with a legitimate reason that is acceptable.

It is the responsibility of the student who has missed a class to contact the professor immediately to obtain the lab / assignment. Students are responsible for doing their own work. Labs / assignments that are handed in and are deemed identical or near identical in content may constitute academic dishonesty and result in a zero grade.

Students are expected to be present to write in-classroom quizzes. There are no make-up options for missed in-class quizzes.

Students have the right to learn in an environment that is distraction-free, therefore, everyone is expected to arrive on-time in class. Should lectures become distracted due to students walking in late, the professor may deny entry until the 1st break period, which can be up to 50 minutes after class starts or until that component of the lecture is complete.

The total overall average of test scores combined must be 50% or higher in order to qualify to pass this course. In addition, combined tests, Labs / Assignments total grade must be 50% or higher.

Course Outcomes and Learning Objectives:

Course Outcome 1	Learning Objectives for Course Outcome 1
Describe the nature of web applications	1.1 Describe the nature of clients and servers on the internet 1.2 Explain how clients and servers communicate using HTTP 1.3 Define the meaning and purpose of protocols, systems, and terms such as DNS, TCP, IP, CDN, API, etc. 1.4 Explain what constitutes a web application and how they

	are distinct from other kinds of applications 1.5 Explain the role databases play in application data storage 1.6 Discuss common approaches to web application architecture 1.7 Explain the following principles of secure application design: least privilege, separation of duties, defence in depth, zero trust, security in the open
Course Outcome 2	**Learning Objectives for Course Outcome 2**
Manipulate web application code	2.1 Create simple web pages using HTML and CSS 2.2 Add dynamic behaviour to web applications using a programming language such as JavaScript and/or Python 2.3 Explain the meaning of simple SQL statements 2.4 Identify code that is vulnerable to common cyberattacks
Course Outcome 3	**Learning Objectives for Course Outcome 3**
Describe common cyberattacks	3.1 Discuss the history of and motivation for cyberattacks 3.2 Analyze the attack vectors, response, and mitigation techniques of recent cyberattacks 3.3 Discuss at a high-level the typical attack vectors and mitigation techniques for the following kinds of cyberattacks: social engineering, insider threats, man-in-the-middle, malware, denial-of-service, software vulnerability exploitation
Course Outcome 4	**Learning Objectives for Course Outcome 4**
Manage application authentication and access control	4.1 Explain the nature and necessity of authentication and access control 4.2 Discuss common methods of bypassing authentication and access control measures and corresponding mitigation techniques 4.3 Discuss the nature and importance of multi-factor authentication 4.4 Create and implement policies that help ensure proper authentication and access control measures are in place for a given application 4.5 Explain the role cookies and tokens play in authentication and the measures required to ensure secure authentication 4.6 Describe how loopholes in the Same-Origin policy give rise to Cross-Site Request Forgery (CSRF) vulnerabilities, and discuss common mitigation techniques 4.7 Perform penetration tests to identify authentication and access control vulnerabilities
Course Outcome 5	**Learning Objectives for Course Outcome 5**
Prevent common cyberattacks	5.1 Discuss the nature and utility of Firewalls, VPNs, IDSs and IPSs in the prevention of cyberattacks 5.2 Describe how loopholes in the Same-Origin policy give rise to Cross-Site Scripting (XSS) vulnerabilities and discuss common mitigation techniques 5.3 Discuss the impact of XSS and injection attacks 5.4 Idenitfy XSS and injection attack vulnerabilities in application code

	5.5 Perform penetration tests to identify XSS and injection attack vulnerabilities 5.6 Use parameterized queries to prevent SQL injection attacks 5.7 Set a Content Security Policy on web applications to reduce attack surface 5.8 Discuss the importance of preparing and rehearsing system backups
Course Outcome 6	**Learning Objectives for Course Outcome 6**
Store and transmit data securely	6.1 Identify data that must be stored and transmitted securely to meet relevant security and privacy regulations 6.2 Discuss the nature and kinds of symmetric encryption, asymmetric encryption, and hashing 6.3 Store and verify passwords securely using password hashing algorithms 6.4 Explain the process of digital signing 6.5 Explain the steps involved in a typical TLS handshake 6.6 Enable HTTPS on a website using a signed TLS certificate

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Activities and Formative Assessments	10%
Labs	30%
Tests	60%

Date: June 16, 2024

Addendum: Please refer to the course outline addendum on the Learning Management System for further information.