CYBR C234: WEB APPLICATION SECURITY

Item	Value
Curriculum Committee Approval Date	10/27/2023
Top Code	070800 - Computer Infrastructure and Support
Units	3 Total Units
Hours	68 Total Hours (Lecture Hours 54; Lab Hours 14)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Open Entry/Open Exit	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

This course introduces the concepts of the Open Web Application Security Project (OWASP) top 10 vulnerabilities for websites and web applications. A survey of secure configurations and software development pertaining to web servers and web applications provides students with the fundamental information needed to protect systems against cyberattacks. Hands-on exercises using industry-recognized tools for application security audit and assessment help students develop skills to prepare for careers as an Application Security Architect or Software Engineer. ADVISORY: CYBR C132 and CYBR C230. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Analyze and test a web application to identify common vulnerabilities.
2. Demonstrate the ability to configure tools to test a web application considering both internal and external attacks.
3. Identify potential solutions to prevent exploitation of an application or system.

Course Objectives

- 1. Identify the ethical and legal issues related to vulnerable web applications.
- 2. Demonstrate the use of industry tools used for web application security auditing as performed by security professionals.
- 3. Discuss emerging trends in the field of cybersecurity and specialized areas such as application security testing and research.

Lecture Content

Introduction and Information Gathering Threat Surface Popular Security Testing Tools Open-Source Tools and Challenges Open Web Application Security Project (OWASP) Top 10 Vulnerabilities Documentation Tools Forums Ethical and Legal Implications of Security Testing Basic Tests SQL Injection and Blind SQL Injection Java Script and XSS (Cross-Site Scripting) Broken Authentication Security Misconfigurations Sensitive Data Exposure Logs and Monitoring CSRF (Cross-Site Request Forgery), Logic Flaws, and Advanced Tools

Lab Content

Students will use tools to develop an understanding of the techniques used by security professionals to test for web application vulnerabilities. Using Kali Linux in AWS Installing Kali Linux in Docker Advanced Metasploit Framework Attacks Service Fingerprinting Advanced MySQL Attacks Advanced MSSQL Attacks Anti-Virus Avoidance Using Threat Harvester Advanced Web Application Attacks with Burpsuite Advanced Web Application Attacks with the Zed Attack Proxy Advanced File Inclusion Attacks Lateral Movement Using Web-Based Command and Control (C2) Servers

Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)
- Lab (04)
- DE Live Online Lab (04S)
- DE Online Lab (04X)

Instructional Techniques

This course will utilize a combination of lecture, hands-on guided laboratory assignments, classroom/discussion student interactions, problem solving, quizzes, tests, and troubleshooting assignments to achieve the goals and objectives of this course. All instructional methods are consistent across all modalities.

Reading Assignments

Read about topics such as session hijacking, cross-site scripting, and injection flaws. Read about the Open Web Application Security Project (OWASP) top 10 vulnerabilities. Read about specialized cybersecurity careers.

Writing Assignments

Write lab reports to describe the configuration for application security testing tools. Conduct a security assessment of vulnerable websites and web applications. Report test results and recommend solutions for proper security configuration.

Out-of-class Assignments

Using the remote lab environment, test web applications with Interception Proxy Tools. Survey penetration testing tools from commercial organizations and open-source platforms.

Demonstration of Critical Thinking

Select appropriate security tool and settings for specific vulnerability testing of web applications. Assess web server configuration to find potential security flaws and recommend solutions.

Required Writing, Problem Solving, Skills Demonstration

Develop lab report identifying web application design flaws using security tools in the remote lab environment. Discuss solutions for top 10 web application vulnerabilities.

Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelor's degree and two years of professional

experience, or any associate degree and six years of professional experience. Computer service technology: Any bachelor's degree and two years of professional experience, or any associate degree and six years of professional experience.

Textbooks Resources

1. Required Girdhar, I. Shah, D. Kali Linux Intrusion and Exploitation Cookbook, 1st ed. Packt Publishing, 2017 Rationale: Low cost

Other Resources

1. Coastline Library 2. IT white papers are available at no charge to all IT students through the Microsoft IT Academy website.