CSIS 485 Cybersecurity Capstone I Project
Statement of Work (SOW)

In this capstone course you will operate as a member of a consulting contractor team providing secure software engineering as governed by a SECDEVOPS project Statement of Work (SoW) in response to the customer's Request for Proposal (RFP). The SoW will be used to govern a SECDEVOPS project to deliver the RFP product(s) meeting all applicable customer provided, or team developed, requirements and specifications as documented by the contractor team responding to the RFP. Within this SoW SECDEVOPS project you will incorporate the applicable software and system security requirements-based modifications into an already available opensource system, or project team developed updated version of an opensource application, integrated with proprietary products in use by a customer to solve a business problem with a team customized Proof of Concept (PoC) product architecture.

Each consultant team will be assigned a product to test and harden using customer requirements and specifications, industry best practices, and meeting all relevant customer regulatory compliance requirements (PCI, FFIEC/FDIC, SEC, HIPAA, FISMA, DoD, etc.).

Each team assigned application will require the SECDEVOPS development, definition, and documentation of security requirements, use cases, risk and vulnerability assessments, test cases, test plans, user acceptance results, and project plans. In this first of two capstone projects, you will not actually "hack" the applications but, instead you will conduct "black-box" and "white-box" security testing to learn each application's exploitable vulnerabilities and design, test, and implement design changes to prevent real-world exploitation of the identified vulnerabilities in each assigned application operating as components within a defined infrastructure system architecture.

The steps incorporated into this capstone course are common tasks and activities for professional software security engineers engaged in planning and implementing new systems or making improvements in the security of an existing application or system.

Each team development project is a unique opportunity to research, analyze, and correct previously unknown vulnerabilities within application source code previously developed by capstone student teams and provided to you for the security requirement engineering done within the context of this course.

Since this project is using opensource code originally developed by other developers, integrally operating with commercial proprietary applications and systems, it is not completely an open source or commercial proprietary project. There will be extremely limited documentation of the development work done by previous developers. Therefore, each project will require an inordinate level of individual and team effort to analyze and understand any opensource code, determine its vulnerabilities, integrate it within the various proprietary systems, and design the appropriate security engineering responses based on the application use cases within the timeframe of this semester. This Secure-SDLC (S-SDLC) SECDEVOPS work will require various project related documents, reports, and meetings to plan for success and evaluate team progress throughout this SoW project. The project management documentation will be the responsibility of the contractor SECDEVOPS team unless otherwise directed.

CSIS 485 Cybersecurity Capstone I Project
Statement of Work (SOW)

This is work typical of a professional software development team, as well as a security testing team.

This is a senior capstone course, and you are expected to know most of the actions necessary to complete the secure software development life cycle (S-SDLC) process and will be considered independently accountable contractors for each project task, with minimal instructor assistance provided.

A critical skill within the Cybersecurity field is the ability to critically analyze and independently accomplish complex tasks with minimal supervision and reporting all results to management. Demonstrating this ability within a safe academic environment during this capstone course provides each team member with a unique opportunity to be challenged and prove their professional skills.

Note: In the professional business world, fraud is the intentional incorrect reporting of effort expended on a task, hours worked during a job, progress made on tasking, success in meeting task objectives, etc., Fraud is subject to immediate termination of employment and often prosecution in a court of law. This same burden of professional integrity for documentation and reporting exists in this SoW project and academic environment for this course, in addition to the burden of academic integrity typically codified under the term of plagiarism. Academic integrity is an expectation within the Kingdom of Christ, therefore all violations will be handled in accordance with university academic policies. We are training ethical professionals, who aspire to a higher standard of integrity than the rest of the world.

Capstone I Course SoW Organization

Phase 1: Weeks 1 – 2 Establish Source Code Access and Test/Development Environments/Tools

1. Form teams
2. Get Access to the Source Code (if available)
3. Coordinate with other capstone teams as applicable
    a. Determine software engineering project state and adapt accordingly
4. Research and document resource requirements, including systems, network designs, and other infrastructure requirements to provide to program and project management.
5. Identify status reporting, documentation, and project process format requirements
6. Identify test environment and testing toolsets based on assigned application technology
7. Begin the first 2 steps of the SQUARE-lite methodology to prepare the initial project plan.
    a. **Agree on definitions.** Using the OWASP website, perform research and describe the elements of the 2017 OWASP top 10 list, in your own words, giving proper credit when due (Harper, 2018). https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
    b. **Agree on developer frameworks and customer governance requirements**. As an example, if the customer provides applications to the DoD, there are

compliance requirements that the developer must meet to assure the customer of effective application security. Your team is responsible for identifying, documenting, and satisfying all the requirements.

c. **Identify Assets, users, and security goals.** Begin to identify and describe the assets (all forms of valuable information), application use cases, application users and security goals of the assigned application (intended and unintended) (Harper, 2018).

Deliverables: The project deliverables for this phase are 2 client contact status update meeting reports. For weeks 1 and 2 acquire access to and learn any available application source code to fully understand its functionality and begin research necessary to prepare the initial project management plan using the SQUARE-Lite Methodology.

Phase 2: Weeks 3 – 6 Project Planning, Risk Assessment, Security Baseline Testing

Complete an initial attempt at the 4 steps of the SQUARE-lite methodology.

1. Deploy required infrastructure to complete the SoW SECDEVOPS project as designed by the contractor teams in Phase 1.
2. Complete the listed steps of the SQUARE-lite methodology to prepare the initial project plan.
    a. **Agree on definitions.** Using the OWASP website, perform research and describe the elements of the 2017 OWASP top 10 list, in your own words, giving proper credit when due (Harper, 2018). https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
    b. **Identify Assets, users, and security goals.** Begin to identify and describe the assets (all forms of valuable information), application use cases, application users and security goals of the assigned application (intended and unintended). (Harper, 2018)
    c. **Perform a Risk Assessment.** To perform a basic risk assessment for this course, use the following steps (Harper, 2018).
        i. For each 2017 OWASP top 10 risk, in the context of the assigned application, calculate a likelihood and impact based risk score, using the OWASP Risk Rating Methodology (Harper, 2018): https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
        ii. For each risk, consider the realistic answers to each impact and likelihood factor question and determine if that risk is ultimately a High, Medium, or Low possibility (Harper, 2018).
        iii. Provide evidence of the analysis including tables where factors are calculated for each of the 10 risk (Harper, 2018).
    d. **Security Requirements and Prioritization.** Employ the final step of SQUARE-light methodology: Elicit security requirements and prioritize the requirements (Harper, 2018).

Note: **Risk Assessment**. Your team will operate with a limited schedule and budget. Only identified high risks will be addressed during this semester. “Based on the results of the risk

assessment of phase 1, for all high risks, identify a set of security requirements from the catalog in chapter 4 to reduce each risk to an acceptable level (Medium)." (Harper, 2018) "In other words, only select requirements of Critical or High priority, due to budget and schedule constraints at this time" (Harper, 2018).

If the risk analysis did not find at least 5 high risk items from the OWASP 10 ten list, then manually choose 5 of the highest scoring risks, for this SoW (Harper, 2018).

Build an OWASP Risk Matrix table that has 6 columns: Category, the identified high risk and the selected security requirements: ID, Name, Requirement, Priority. You may copy/paste this information, as needed. You will have multiple security requirements for each identified risk. The table should be formatted in APA format (Harper, 2018).

This portion can be in Landscape orientation to maximize space in table.

Category	OWASP High Risk Item	SR ID	Name	Requirement	Priority

3. **Incorporate the STRIDE Threat Model as the Category of Risk for the assigned application.** Perform research and determine the process for STRIDE threat modeling and apply it to the assigned application. This should be done for the High-Risk threats (Harper, 2018).
4. **Select appropriate Risks for the Security Test Plan Test Cases.** Provide a table of security requirements and associated security test cases in the following format. Only provide the reduced security requirements list for Phase 1 (Harper, 2018).

   This portion can be in Landscape orientation to maximize space in table.

SR ID	SR Name	STC ID	STC Name	STC Description, Constraints, and Comments

5. **Compare static and dynamic software testing methodologies.** Provide at least one page, supported by peer reviewed journal articles and the textbook (Harper, 2018).
6. **Develop a Security Test Plan**. Draft at least 3 pages, but not more than 5 pages of a security testing plan, investigating the following options and including those applicable for the assigned application into subsequent testing (Harper, 2018):
   a. Manual Source Code Review.
   b. Automated Source Code Review.
   c. Automated Dynamic Testing.
   d. Penetration Testing.

CSIS 485 Cybersecurity Capstone I Project
Statement of Work (SOW)

Deliverables:

1. Week 3 delivery of the initial project plan. The initial project plan must provide a 2 page DRAFT SoW with a 300 word length executive summary, plus a project steps roadmap including schedule milestones in the form of a Gantt chart, incorporating the findings of the SQUARE-Lite analysis Risk Assessment and Requirements definition results within the planning. Include the Risk Matrix Test Case tables.
2. Week 4 setup of the application test environment
3. Week 5 Client Contact/Project Status Report 1
4. Week 5 Use Case/Security Requirements Documentation
5. Week 6 Baseline Security Test

Phase 3: Weeks 7 – 13 Security and Iterative Test Planning, updated Risk Analysis, and initial Project Budget Estimate

1. **Analysis of budget and impact on risk assessment, prioritization, and implementation of security requirements.** Conduct some research in the JFL library and provide at least 2 complete pages of analysis of budget impact on the risk assessment process and the prioritization and implementation of security requirements within an organization. Be sure to provide at least 3 peer reviewed journal citations and references along with at least one biblical citation concerning the need for good stewardship (Harper, 2018).
2. **Iterative Security testing** to resolve identified vulnerabilities associated with the risks and updated project and test plans based on results (Harper, 2018).
3. **Apply best practices of converting security requirements to secure software designs.** Update the project status reports with the testing results and mitigation of vulnerabilities or risks based on testing. Keep the reporting brief and incorporate the risk matrix table defined in Phase 1 (Harper, 2018).

Deliverables:

1. Week 7 Security Test 1
2. Week 7 Project/Test Plan Version 2
3. Week 8 Security Test 2
4. Week 9 Security Test 3
5. Week 9 Project/Test Plan Version 3
6. Week 10 Security Test 4
7. Week 10 Project/Test Plan Version 4
8. Week 11 Security Test 5
9. Week 11 Project/Test Plan Version 5
10. Week 12 Security Test 6
11. Week 12 Project/Test Plan Version 6
12. Week 13 Security Test 7
13. Week 13 Project/Test Plan Version 7

Phase 4: Week 14 Application Final Acceptance Security Test

CSIS 485 Cybersecurity Capstone I Project
Statement of Work (SOW)

1. **Design Review**. Apply the Microsoft Developers Network (MSDN) Architecture and Design Review Checklist to review the assigned application design based on testing. Although we do not have a design document for this application, some of the elements of the design are apparent by the implementation. A cybersecurity engineer will often reverse engineer a design document as they are often not available during development. By reviewing the functionality and source code, complete the following portions of the provided MSDN Architecture and Design Review Checklist (only) and include it as a document in the next subsequent project plan revision (Harper, 2018):
   - Input Validation
   - Configuration
   - Sensitive Data
   - Parameter Manipulation

   A copy of the MSDN Architecture and Design Review Checklist is provided in the course material. The results will be incorporated into the next project/test plan revision as a single page report containing the above 2 sections (highlighted in bold). The paper should be at least 5 pages in length and contain at least 3 peer reviewed journal articles, in addition to the textbook, properly cited in APA format. Be sure to add a title page, including your name, the title, course name, school, date, and brief comments plus evidence or rationale for each (Harper, 2018).

Deliverables:

1. Final Acceptance Test for all planned test cases and delivery of updated source code accompanied by all project, testing, and design documentation.

Phase 5: Week 15 – 16 Project Completion and Application Delivery

1. Final wrap up of the project and class/customer presentation of all documentation as well as lessons learned.

Deliverables:

1. In class presentation of project lessons learned after action report.

References:

Harper, A. (2018). CSIS 485 Cybersecurity Capstone 1 Project Instructions, *CSIS 485 Cybersecurity Capstone 1*