Project Title:
Cybersecurity Capstone: Vulnerability Assessment & Secure Network Design

---

Introduction

Welcome to the Cybersecurity Capstone Project for 3MTT Cohort 2 fellows! This capstone is designed to help you apply core cybersecurity skills in a real-world scenario. Using the OWASP Juice Shop—an intentionally vulnerable web application—you'll identify security vulnerabilities and recommend secure design measures. Completing this project is essential for graduation.

Objectives

By the end of this project, you will be able to:

1. Conduct a vulnerability assessment and identify security risks in a web application.
2. Apply secure network design principles to propose defensive strategies.
3. Recommend practical remediation measures for common cybersecurity threats.

Scenario

You've been hired as a cybersecurity consultant to assess and secure the OWASP Juice Shop, an e-commerce application known for its vulnerabilities. The company requires you to identify major security risks, assess the current network design, and provide a plan for hardening the application's security posture.

Demo Link to Juice Shop: OWASP Juice Shop

OWASP Juice Shop is designed for training in vulnerability assessment and secure practices. As part of this project, treat it as a live assessment to uncover and mitigate areas where sensitive data, transactions, or user information might be at risk.

Project Parts

Part 1: Vulnerability Identification and Assessment

1. **Task**: Conduct a vulnerability assessment on OWASP Juice Shop. Use tools discussed in the course (e.g., OWASP ZAP, Burp Suite) to scan for vulnerabilities such as SQL injection, cross-site scripting (XSS), and authentication weaknesses.
2. **Deliverables**:

    - A vulnerability report listing each identified issue, including type, impact, and affected areas.
    - Screenshots or brief notes explaining how each vulnerability was identified.
3. **Skills Applied**:
    - Threat identification and vulnerability scanning.
    - Assessment of risks based on potential impact.

Part 2: Secure Network Design

1. **Task**: Based on the vulnerabilities identified in Part 1, design a secure network architecture. Consider best practices such as segmentation, firewall implementation, and intrusion prevention to mitigate the identified risks.
2. **Deliverables**:
    - A network design proposal document or diagram with detailed explanations for each security control included.
    - Brief descriptions of each network component and how it strengthens security.
3. **Skills Applied**:
    - Network security fundamentals and secure design principles.
    - Application of risk mitigation strategies.

Submission Guidelines

- **Submission Format**: Combine both Parts 1 and 2 into a single document in PDF or Google Doc format.
- **Submission Platform**: Upload the document link to the assignment portal. Ensure that view/comment access is enabled.
- **Document Requirements**: Include clear headings for each part, organized sections for each vulnerability, and a labeled network design diagram or written proposal.

Conclusion

This capstone project will allow you to practice essential skills in vulnerability assessment and network security design. By completing this project, you’ll gain hands-on experience in identifying and mitigating risks in a practical, real-world application. Use the resources from the course to support your analysis and design, and reach out to fellow classmates or instructors if you need guidance along the way. Good luck!