## **CYBR 465: Web Applications Security (3 credits)**

This course will examine web applications from an offensive security standpoint. The course covers in-depth, the critical web application vulnerabilities defined by OWASP and uncovers underlying attacks and their mitigations. Topics will cover infiltration, injections, authentication violations, web design related vulnerabilities, configurations and privilege escalation, and security compliance of web application. Each portion of the course will involve core understanding of the complex web application architecture and hardening a vulnerable application using specialist methods. *(Prerequisite: COSC 312, CYBR 310)*

**Course Learning Outcomes:**

By the end of the course, students will be able to:

A1. Demonstrate critical knowledge of the specialized concept and theories related to web application vulnerabilities, exploits and their mitigation.

A2. Apply specialized methods, tools and standards to detect and mitigate the sophisticated web application threats.

B1. Analyze the core web application vulnerabilities to identify the security requirements in formulating specialist web application security solution.

B2. Design specialist counter strategies to overcome the critical web application attacks.

B3. Exhibit the specialist skills of expressing and communicating web application security compliance effectively in written and oral forms.

C1. Demonstrate effective teamwork and collaboration skills in the context of web application security, working collaboratively to diagnose and resolve potential web application vulnerabilities.

**Course Learning Materials:**

* Andrew Hoffman, “Web Application Security: Exploitation and Countermeasures for Modern Web Applications”, 1st Edition (2020), O'Reilly Media, ISBN: 978-1492053118.
* Malcolm McDonald, “Web Security Basics For Developers: Real Threats, Practical Defense”, illustrated (2020), No Starch Press, ISBN: 978-1593279943
* Simone Onofri, Donato Onofri, Matteo Meucci, “Attacking and Exploiting Modern Web Applications: Discover the mindset, techniques, and tools to perform modern web attacks and exploitation”, (2023), Packt Publishing, ISBN: 978-1801816298.
* Colin Watson and Tin Zaw, “OWASP Automated Threat Handbook: Web Applications”, Version 1.2 (2018), OWASP Foundation, ISBN: 978-1-329-42709-9.

**Course Content:**

1. Introduction to Web Application Security
2. Web Application Security design and Compliance:
3. Web Application Vulnerabilities
4. OWASP A04:2021 – Insecure Web Application Design
5. OWASP A05:2021 – Security Misconfiguration
6. OWASP A07:2021 – Identification and Authentication Failure
7. OWASP A01:2021 – Broken Access Control
8. OWASP A02:2021 – Sensitive Data Exposure
9. OWASP A03:2021 – Injections
10. OWASP A03:2021 – Cross-Site Scripting (XSS)
11. OWASP A08: 2021– Insecure Deserialization
12. OWASP A09:2021 – Insufficient Logging and Monitoring
13. OWASP A01:2021 – Cross-Site Request Forgery (CSRF).
14. OWASP A10:2021 Server-Side Request Forgery (SSRF).