BAKER COLLEGE
STUDENT LEARNING OUTCOMES

ITS4050 Internet and Web Security

3 Semester Credit Hours

Student Learning Outcomes and Enabling Objectives

1. Analyze the impact of the Internet and Web applications on the business world.
    a. Explore the evolution of web security threats and defenses over the years.
    b. Discuss the principles of secure design and their application in web environments.
    c. Identify e-commerce areas of risk, security concepts, and how to manage those risks.
    d. Compare online security threats and risks
2. Analyze OWASP, top web threats, and web-based analytics.
    a. Describe common website attacks and weaknesses.
    b. Explain the value, best practices, and importance of vulnerability and security assessments for Web applications.
    c. Discuss various protection mechanisms against DDoS attacks, such as CDN, WAF, and anti-DDoS services.
    d. Describe the Web Application Security Consortium (WASC) Threat Classification and its role in identifying web application vulnerabilities.
3. Describe the attributes and qualities of the software development life cycle (SDLC) and secure coding practices.
    a. Describe how to integrate security practices in different phases of SDLC, from requirements gathering to deployment and maintenance.
    b. Discuss secure coding practices to prevent common vulnerabilities like SQL injection and XSS.
    c. Explore various SCM tools (e.g., Git, SVN) and best practices for their secure use.
    d. Utilize automated and manual security checks and compliance using SCM tools.
4. Analyze web application vulnerabilities and how to mitigate them with secure coding best practices.
    a. Explore the role and importance of auditing and compliance with web application security.
    b. Describe vulnerability scanning tools and techniques to identify security weaknesses in web applications.

    c. Audit findings from both automated and manual vulnerability scans.
5. Identify security risks on popular mobile devices as well as their communications technologies.
    a. Analyze unique security challenges posed by mobile devices and applications.
    b. Investigate strategies for securing mobile applications, including secure storage, data encryption, and secure communications.
    c. Explore emerging threats in the mobile landscape and future trends in mobile security.
6. Explain common areas of the IT industry and the roles each plays in creating secure environments.
    a. Investigate other Web application security organizations, both federal and private.
    b. Identify organizations in web application security, such as OWASP, SANS, and ISACA.
    c. Explore various web security certifications (e.g., CISSP, CEH, OSCP, GWAPT).

Big Ideas and Essential Questions

Big Ideas

- Internet and web application Security.
- OWASP, WASC, and DDoS Attacks
- SDLC and Secure Coding
- Web Application Auditing and Compliance
- Risk Management and Mobile Device Security
- Web Application Security Organizations and Certifications

Essential Questions

1. Why are internet and web security vital to users and organizations?
2. How do you protect websites and web applications from security vulnerabilities?
3. How can the SDLC process help with securing confidential data?
4. Why are auditing and compliance important within web application security?
5. How can we use risk management approaches to secure various mobile devices?
6. How do different web security certifications and their corresponding security organizations impact web security?

These SLOs are approved for experiential credit.

Effective: Fall 2024