| | | |
|---|---|---|
| **Course Name** | *Web Server and Application Testing* | فحص خوادم وتطبيقات الويب |

| **Course Information** | **Course Code** | **Course No.** | **Credit Hour** | **Prerequisite(s)** |
|---|---|---|---|---|
| | 0912637 | IS 637 | 3 (3-0-6) | 0914611 |

**Course Track** □ Program Core ☒ Electives

**Course Description**

Current technology has given us access to huge amounts of information on the web and simplified tasks. Web has become the primary vector for infecting computers. This course covers contemporary web application vulnerabilities and exploitation techniques based on the Open Web Application Security Project (OWASP). Students will be introduced to different methods and techniques that are used when attacking web servers including password cracking, SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) to name a few. Moreover, students will be provided with the knowledge and skills to implement protection against these attacks. Students will be familiarized with tools and techniques for performing attacks related to authentication, session management, access control, data stores, server-side components, and users. Finally, the students will be introduced to the web application hacker's methodology that provides a framework to check and implement protection schemes against popular web server and application attacks.

**Course Outcomes**

After the completion of this course, the student will be able to:

1. **Define** common web infrastructure attack vectors and database vulnerabilities. [A]
2. **Apply** techniques to identify vulnerabilities existing in web servers and applications. [B, E]
3. **Use** tools and skills to attack web infrastructures. [B, E]
4. **Discuss** and **use** different procedures to check and implement protection schemes in web servers and web based applications. [C, D]

| **Assessment Policy** | **Assignments** | 25% | **Quiz** | - | **Project** | 20% |
|---|---|---|---|---|---|---|
| | **Midterm** | 25% | **Final** | 30% | **Others** | - |

| | |
|---|---|
| **Textbook** | Juned Ahmed Ansari, "*Web Penetration Testing with Kali Linux*", 3rd Edition, Packt Publishing Ltd., 2018. ISBN: 9781788623377. |
| **References** | 1. Dafydd Stuttard and Marcus Pinto, "*The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*", 2nd Edition, Wiley, 2011. ISBN-13: 978-8126533404<br>2. Prakhar Prasad, "*Mastering Modern Web Penetration Testing*", 1st Edition, Packt Publishing Limited, 2016. ISBN-13: 9781785284588<br>3. Peter Kim "*The Hacker Playbook 2: Practical Guide to Penetration Testing*" 1st Edition, CreateSpace Independent Publishing Platform, 2015. ISBN-13: 978-1512214567 |