Course Name	*Information Systems Security*			
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0912620	IS 620	3(3-0-6)	0912610
Course Track	☐Program Core ☒Electives			

Course Description

The security design principles are discussed and applied to eliminate typical vulnerabilities in implementing an information system. The course includes discussion on several emerging threats including next-generation phishing, drive-by-pharming, online extortion, multi-application botnets, crimeware, mobile worms. Emerging defense techniques are also discussed with all threats. The latest web vulnerabilities covered in this course include client-state manipulation, cookie-based attacks, SQL injection, cross domain attacks (XSS/XSRF/XSSI), and HTTP header injection. Security issues that arise specifically in Web 2.0 applications taking advantage of AJAX, XmlHttpRequest, and mash-ups are discussed. The course also covers Same-Origin-Policy (SOP) violations that can occur due to DNS rebinding, timing, and user tracking attacks.

Course Outcomes

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

1. Recognize the importance of Penetration Testing, in providing security for web information systems for organizations.
2. Explain the phases of Penetration Testing along with in depth study of many exploiting techniques for selected latest web vulnerabilities.
3. Analyze the information systems to identify attack surface for security vulnerabilities and threats by following a standard methodology.
4. Design and Implement the penetration testing plan to launch attacks for selected vulnerabilities to evaluate security of the web-based systems.
5. Show experience in solving security problems and writing report as a team leader or a team member.

Assessment Policy	**Assignments**	-	**Quiz**	10%	**Project**	20%
	Midterm	25%	**Final**	45%	**Others**	-

Textbook	1. Dafydd Stuttard, Marcus Pinto, “Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws”, 2nd Edition, Wiley, 2011.
References	1. Offensive Security material on Kali Linux and Penetration Testing