Course Curriculum

Course Code :	SE 3206
Course Title :	Software Security Lab
Course Credit:	1 Credit (Lab course)
Credit Hour :	14 X 2 = 28 hours (1 class equivalent to 2 hours lab)

Week	Content (Lesson Plan) or Lab Activity
W-01	Attacks: Browser, Web, User Data, Email
W-02	SQL Injection Attack and Countermeasure
W-03	XSS (Cross-site Scripting) with Javascript CSRF and Clikcjacking
W-04	Password Cracking and Identity Theft
W-05	Session Management
W-06	Operating System Security: String Handling, Memory Corruption
W-07	Buffer Overflow: Attacks and Defence
W-08	DoS (Denial of Service) Attack and Defence
W-09	Intrusion Detection and Prevention
W-10	Anomaly Detection
W-11	Program Analysis: Static and Dynamic
W-12	Mobile Application Security
W-13	Security Testing: Penetration Testing
W-14	Risk- Based Security Testing Abuse Cases- Operational testing
Lab Final and Viva Voce	

Reference Books:

CSJ *Security in Computing* (5th Edition). Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies. Pearson Education, Inc. 2015

JEH *Hacking: The Art of Exploitation* (2nd Edition). Jon Erickson. No Starch Press. 2008

DMH *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws* (2nd Edition). Dafydd Stuttard, Marcus Pinto. Wiley Publishing, Inc. 2007

GWP *Penetration Testing: A Hands-On Introduction to Hacking* (1st Edition). Georgia Weidman. No Starch Press. 2014

WSL *Computer Security: Principles and Practice* (3rd Edition). William Stallings, Lawrie Brown. Pearson Education, Inc. 2015

Marks Distribution:

Topic or Activities		**Evaluation Percentage**	
Security Flaw Detection & Defense (Lab Work: Continuous Assessment)			
	Web Attack	20%	**40%**
	Software Vulnerabilities Detection	20%	
	Anomaly Detection	15%	
	Program Analysis	15%	
	Mobile Application Security	10%	
	Security Testing	20%	
Design & Implementation (Mini Project)			
	Defensive Programming	50%	**20%**
	Security Testing	15%	
	Use of Tools	10%	
	Evaluate security, robustness, usability etc.	15%	
	Auditing & Logging	10%	
Hacking Contest (Lab Final)			
	Attack on a System	30%	**25%**
	Penetration Testing of the System	15%	
	System/Design Flaws Identification	20%	
	Countermeasure or Secure the System	25%	
	Documentation	10%	
Viva Voce (Final)			
	Security Issues	20%	**15%**
	Design Principles	15%	
	Countermeasure	25%	
	Infrastructure Security	25%	
	Threat Modeling	10%	
	Emerging Topics	5%	