

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	Application Security, Vulnerability
Course Code:	2ET2070204T
Pre-requisite Course:	To give exposure to various security threats to web applications/ servers and providing security to web servers.

Course Objectives: After successful completion of the course, student will be able to

1. To impart the knowledge architecture reference layer Security issues and challenges of Web Crawling Server & Application.
2. Describe security threats faced in different application environments including software, web, database, cloud, and mobile.
3. Incorporate measures to reduce the risk of application security breach.
4. Locate resources that are up to date to address emerging application security issues.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)									Total (Marks)
					Theory (Marks)				Practical (Marks)					
	L	T	P	Total	SEE		CCA		SEE		CCA			
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.		
3	3	-	-	3	24	60	16	40	-	-	-	-	100	

Course Contents:

Unit No	Topics	Total Hours	Weight age (%)
1	Application Discovery Site Mapping & Web Crawling Server & Application Fingerprinting Identifying the entry points File extensions handling Page enumeration and brute forcing Comments in code – view source Looking for leftovers and backup files Admin interfaces Robots.txt Analysis of error code	10	20
2	What is authentication? Authentication scenarios User enumeration Guessing passwords - Brute force & Dictionary attacks Default users/passwords Weak password policy Direct page requests Parameter modification Password reset flaws Password change flaws Locking out users Lack of SSL at login pages Bypassing weak CAPTCHA mechanisms Login without SSL	10	20
3	What is authorization RBAC Authorization bypassing Parameter tampering Forceful browsing Rendering based Authorization Client side validation attacks Insecure direct object reference Business logic attacks Flow bypassing Replay attacks Abuse of functionality Path traversal Canonicalization Uploaded files backdoors Insecure file extension handling Directory listing File size File type Malware upload	12	30
4	SQL injection Common implementation mistakes - authentication bypassing using SQL Injection Cross Site Scripting (XSS) Reflected VS. Stored XSS Command injection Special chars - ' & < >, empty Session management techniques Cookie based session management Cookie properties Cookies - secrets in cookies, tampering Exposed session variables Missing Attributes – httpOnly, secure Session validity after logoff Long session timeout Session keep alive – enable/disable Session id rotation Cross Site Request Forgery (CSRF) Open redirect	12	30

Text Books:

1. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook, 2nd Edition, Wiley Publishing, Inc.
2. Stuart McClure Joel, Scamb Ray, George Kurtz, Hacking Exposed

Reference Books:

1. Network Security Secrets & Solutions, Seventh Edition, 2012, The McGraw-Hill Companies
2. Justin Clarke, SQL Injection Attacks and Defense, 2009, Syngress Publication Inc.
3. Magnus Mischel, ModSecurity 2.5, Packt Publishing

Course Learning Outcomes (CLO):

Course Outcomes	Description	Bloom's Taxonomy Level
COL1	Understand security concepts, security professional roles, and security resources in the context of systems and security development life cycle	Understanding (2) Applying (3)
COL2	Understand the business need for security, threats, attacks, top ten security vulnerabilities, and secure software development	Applying (3)
COL3	Understand information security policies, standards and practices, the information security blueprint.	Applying (3)
COL4	Analyze and describe security requirements for typical web application scenario.	Applying (3)

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	H	M	M		M											
CLO2	H	M			M							L				
CLO3	H	M	M		M											
CLO4	M	M	M		M							L				
CLO5	M	M										L				

H: High, M: Medium, L: Low