PRESIDENCY UNIVERSITY

(Established under the Presidency University Act, 2013 of the Karnataka Act 41 of 2013)
[2024-25 EVEN SEMESTER]
COURSE HAND OUT [Revision 03-July 2023]

SCHOOL: PSCS **DATE OF ISSUE: 09/01/2025**

NAME OF THE PROGRAM	**: B.TECH. COMPUTER SCIENCE & ENGINEERING - CYBER SECURITY (CCS)**
P.R.C. APPROVAL REF.	: PU/AC-18/CSE16/CCS/2021-2025/22
SEMESTER/YEAR	: 6th Sem, 3rd Year
COURSE TITLE & CODE	: Web Security & CSE3097
COURSE CREDIT STRUCTURE	**: 2-0-2-3**
CONTACT HOURS	**: 60 Sessions**
COURSE IC	**: Ms. Sreelatha PK**
COURSE INSTRUCTOR(S)	**: Ms. Sreelatha PK**
COURSE URL	: Presidency University (Linways)
PROGRAM OUTCOMES	:

Graduates of the B. Tech. Program will have the following abilities:

PO-1 Engineering Knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO-2 Problem analysis: identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first of mathematics, natural sciences and engineering sciences.

PO-3 Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal and environmental considerations.

PO-4 Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data and synthesis of information to provide valid conclusions.

PO-5 Modern tool usage: Create, select, and apply appropriate techniques, resources and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO-6 The Engineer and the Society: Apply reasoning informed by the contextual knowledge to assess, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO- 7 Environment and sustainability: Understand the impact of the professional solutions in societal and environmental contexts, and demonstrate the knowledge of and need for sustainable development.

PO-8 Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO- 9 Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO-10 Communication: Communicate effectively on complex engineering activities with the engineering community and society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO-11 Project Management and Finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO -12 Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES:

PSO1: [Problem Analysis]: Identify, formulate, research literature, and analyze complex engineering problems related to Software Engineering principles and practices, Programming and Computing technologies reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PSO2: [Design/development of Solutions]: Design solutions for complex engineering problems related to Software Engineering principles and practices, Programming and Computing technologies and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PSO3: [Modern Tool usage]: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities related to Software Engineering principles and practices, Programming and Computing technologies with an understanding of the limitations.

COURSE PREREQUISITES: Fundamental knowledge in Advanced Computer Networks.

COURSE DESCRIPTION: The purpose of this course is to introduce you to the field of web security by understanding web functionality and various security validations. The web is our gateway to many critical services and is quickly evolving as a platform to connect all our devices. Web vulnerabilities are growing on a year-to-year basis and designing secure web applications is challenging. The course covers fundamental concepts of web security principles, web vulnerability and exploitation, various attacks on web applications, and a few basic topics on web encryption.

COURSE OBJECTIVES: The objective of the course is to familiarize the learners with the concepts of **Web Security** and attain **Skill Development** through **Experiential Learning** techniques.

COURSE OUTCOMES: On successful completion of the course the students shall be able to

TABLE 1: COURSE OUTCOMES		
CO Number	**CO**	**Expected BLOOMS LEVEL**
CO1	**Define** the fundamentals of web applications and validation	**L1(Remember)**
CO2	**Recognize** the significance of password and authentication in web applications	**L2(Understand)**
CO3	**Explain** the importance of session management in web	**L2(Understand)**
CO4	**Apply** web attack techniques to find vulnerabilities in web applications	**L3(Apply)**

MAPPING OF C.O. WITH P.O.
[H-HIGH, M- MODERATE, L-LOW]

TABLE 2a: CO PO Mapping ARTICULATION MATRIX												
CO. No.	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CO1	M				M			M				M
CO2	H	M		M	H			H				M
CO3	M	M		M	H			H				H
CO4	M			M				M				M

CO. No.	**PSO1**	**PSO2**	**PSO3**
CO1	L		
CO2	M	L	
CO3	H	H	H
CO4	H	H	M

COURSE CONTENT (SYLLABUS):

Module 1 **[14 Hrs-L[08]+P[06]][Remember]**

Introduction

Web Functionality, Encoding Schemes, Mapping the Application - Enumerating the Content and Functionality, Analyzing the Application Bypassing, Client-Side Controls: Transmitting Data via

the Client, Capturing User Data, Handling Client-Side Data Securely - Input Validation, Blacklist Validation - Whitelist Validation - The Defense in-Depth Approach - Attack Surface Reduction, Rules of Thumb, Classifying and Prioritizing Threats.

Module 2 **[16 Hrs – L[08] +P[08]] [Understand]**

WebApplicationAuthentication

Authentication Fundamentals- Two Factor and Three Factor Authentication, Web Application Authentication- Password Based, Built-in, HTTP, Single Sign-on, Custom Authentication, Validating credentials - Secured Password Based Authentication: Attacks against Password, Importance of Password Complexity - Design Flaws in Authentication Mechanisms - Implementation Flaws in Authentication Mechanisms - Securing Authentication.

Module 3 **[16 Hrs – L[08] +P[08]] [Understand]**

Session Management &Web Security Principles

Need for Session Management, Weaknesses in Session Token Generation, Weaknesses in Session Token Handling, Securing Session Management; Access Control: Access Control Overview, Common Vulnerabilities, Attacking Access Controls, Securing Access Control. Origin Policy, Exceptions, Browser security Principles- Cross Site Scripting and Cross Site Request Forgery, File Security Principles: Source Code Security, Forceful Browsing, Directory Traversals.

Module 4 **[14 Hrs – L[06] +P[08]] [Apply]**

Web Application Vulnerability

Attacking data-stores and backend components- Injecting into Interpreted Contexts, injecting into SQL, NoSQL, XPath, LDAP, Injecting OS Commands, Manipulating File Paths, Injecting into XML Interpreters, Injecting into Back-end HTTP Requests, Injecting into Mail Services, Attacking application logic-real world logic flaws, Attacking users-Cross site scripting-varieties of XSS,XSS attacks in action, finding and exploiting XSS vulnerabilities, preventing XSS attacks, Other techniques-cookie based Attacks, HTTP Header Injection

DELIVERY PROCEDURE (PEDAGOGY):

TABLE 3: SPECIAL DELIVERY METHOD/ PEDAGOGY PLANNED WITH TOPICS

S. No	Lecture Number	Subtopic as per lesson Plan	Pedagogy title/ short explanation of adopted pedagogy	** At end of semester please update whether activity was done
1	L21	Origin Policy, Exceptions	Self Learning	
2	L23	Forceful Browsing	Flipped Classroom	
3	L25	SQL injection	Problem based Learning	

REFERENCE MATERIALS:

Textbook(s)

T1. Dafydd Stuttard, Marcus Pinto, "The Web Application Hacker's Handbook", Willey Publishing Inc. ,2008

Reference Book(s)

R1. B. Sullivan, V. Liu, and M. Howard, "Web Application Security", A B Guide. New York: McGraw-Hill Education, 2012.

R2. Web Application Security: Exploitation and Countermeasure for Modern Web Applications, by Andrew Hoffman.

E**-book Links**

- T1: https://www.oreilly.com/library/view/web-application-security/9780071776165/
- T2: https://www.oreilly.com/library/view/web-application-security/9781492053101/

Additional web-based resources

W1. **NPTEL course** : Introduction to Information Security I, IIT Madras https://nptel.ac.in/courses/106106129

W2. **Coursera Link** : https://www.coursera.org/learn/security-and-authentication

SPECIFIC GUIDELINES TO STUDENTS:

Self-Learning topics, Participative Learning and Problem based learning topics should be taken seriously as it will be assessed in the course and it will also help in understanding the course better. It is up to the student to put required effort and meet faculty for reinforcing learning.

COURSE SCHEDULE:

TABLE 4: COURSE BROAD SCHEDULE

Sl. No.	ACTIVITY	STARTING DATE	CONCLUDING DATE	TOTAL NUMBER OF PERIODS
01	Overview of the course & Module 01	20.01.2025	13.02.2025	**14** [8 L +6 P]
02	Continuous Assessment 1	14.02.2025	14.02.2025	
03	Module: 02	17.02.2025	13.03.2025	**16** [8 L + 8P]
04	Continuous Assessment 2	14.03.2025	14.03.2025	
05	Mid Term	17.03.2025	21.03.2025	**4**
06	Module: 03	24.03.2025	18.04.2025	**12** [6 L + 6 P]
07	Assignment	-	-	-
08	Module: 04	21.04.2025	16.05.2025	**14** [6 L+ 8 P]
09	End Term	26.05.2025	6.06.2025	

SCHEDULE OF INSTRUCTION For theory component:

TABLE 5: DETAILED COURSE SCHEDULE / LESSON PLAN (THEORY)								
Sl. no	**Session no**	**Lesson Title**	**Topics**	**Low Order Learning**	**High Order Learning**	**Course Outcome Number**	**Delivery Mode**	**Reference**
1	L1	Module I - Introduction to Web Security	Course Integration LO1-Recognize the different modules of the courses LO2-Analyze the importance of the course	LOL1 LOL2			Chalk & Talk / Interactive Learning	
2	L2		Topics: Web Functionality LO1: Define web functionality. LO2: Illustrate examples of web functionality.	LOL1 LOL2		CO1	Chalk & Talk / Interactive Learning	T1 Chap3 (Pg no. 47 – 55)
3	L3		Topics: Encoding Schemes LO1: Explain encoding schemes. LO2: Analyze the role of encoding in web applications.	LOL2 LOL4		CO1	Chalk & Talk / Interactive Learning	T1 Chap3 (Pg no. 56 – 59)
4	L4		Topics: Enumerating Content and Functionality LO1: Identify steps for mapping applications LO2: Develop strategies to enumerate content.	LOL2 LOL3		CO1	Chalk & Talk / Interactive Learning	T1 Chap4 (Pg no.62-79)
5	L5		Topics: Analyzing the Application and Bypassing Controls LO1: Analyze security controls. LO2: Demonstrate bypassing techniques.	LOL3 LOL4		CO1	Chalk & Talk / Interactive Learning	T1 Chap4 (Pg no.79-91)
6	L6		Topics: Transmitting Data via the Client and Capturing User Data LO1: Explain client-side controls. LO2: Evaluate data security risks.	LOL2 LOL4		CO1	Chalk & Talk / Interactive Learning	T1 Chap5 (Pg no.95 - 110)
7	L7		Topics: Handling Client-Side Data Securely - Input Validation LO1: Describe input validation techniques. LO2: Compare blacklist and whitelist validation.	LOL1 LOL5		CO1	Chalk & Talk / Interactive Learning	T1 Chap5 (Pg no.128 - 131)
8	L8		Topics: The Defense-in-Depth Approach and Attack Surface Reduction, Classifying and Prioritizing Threats LO1: Define defense-in-depth, threats LO2: Assess methods for reducing attack surfaces.	LOL2 LOL5		CO1	Chalk & Talk / Interactive Learning	R1 Chap2 (Pg no.24 - 44)

			Continuous Assessment1 & Discussion					
END OF MODULE- 1								
9	L9	Module II - Web Application Authenticati on	Topics: Two-Factor and Three-Factor Authentication LO1: Define two-factor and three-factor authentication. LO2: Compare two-factor vs three-factor methods.	LOL1 LOL3		CO2	Chalk & Talk / Interactive Learning	R1 Chap3 (Pg no. 54-60)
10	L10		Topics: Password-Based, Built-in, HTTP, Single Sign-on, and Custom Authentication LO1: Explain types of web application authentication. LO2: Analyze use cases for each type.	LOL2 LOL4		CO2	Chalk & Talk / Interactive Learning	R1 Chap3 (Pg no. 61-69)
11	L11		Topics: Validating Credentials LO1: Identify methods for validating credentials. LO2: Apply secure practices to credential validation.	LOL2 LOL3		CO2	Chalk & Talk / Interactive Learning	R1 Chap3 (Pg no. 69)
12	L12		Topics: Attacks Against Passwords, Importance of Password Complexity LO1: Describe common password-based attacks. LO2: Evaluate password complexity requirements.	LOL1 LOL5		CO2	Chalk & Talk / Interactive Learning	R1 Chap3 (Pg no. 70-74)
13	L13		Topics: Design Flaws in Authentication Mechanisms LO1: Identify common design flaws. LO2: Propose strategies to mitigate design flaws.	LOL3 LOL5		CO2	Chalk & Talk / Interactive Learning	T1 Chap6 (Pg no. 135-155)
14	L14		Topics: Implementation Flaws in Authentication Mechanisms LO1: List common implementation flaws. LO2: Analyze real-world examples of implementation flaws.	LOL1 LOL4		CO2	Chalk & Talk / Interactive Learning	T1 Chap6 (Pg no. 156-161)
15	L15		Topics: Securing Authentication LO1: Explain the principles of secure authentication. LO2: Evaluate methods for securing authentication mechanisms.	LOL2 LOL5		CO2	Chalk & Talk / Interactive Learning	T1 Chap6 (Pg no. 162-172)

16	L16		**Continuous Assessment 2**					
17	L17	Mid Term						
18	L18	Mid Term						
END OF MODULE- 2								
19	L19	Module III - Session Management &Web Security Principles	Topics: Need for Session Management, Weaknesses in Session Token Generation LO1: Define session management and its importance. LO2: Analyze weaknesses in session token generation.	LOL1 LOL4		CO3	Chalk & Talk / Interactive Learning	T1 Chap7 (Pg no. 175 - 187)
20	L20		Topics: Weaknesses in Session Token Handling, Securing Session Management LO1: Explain secure practices for session token handling. LO2: Propose strategies to secure session management.	LOL2 LOL5		CO3	Chalk & Talk / Interactive Learning	T1 Chap7 (Pg no. 191-212)
21	L21		Topics: Access Control Overview, Common Vulnerabilities, Attacking Access Controls, Securing Access Control LO1: Describe access control, common vulnerabilities and access control. LO2: Evaluate the effectiveness of access control mechanisms.	LOL1 LOL5		CO3	Chalk & Talk / Interactive Learning	T1 Chap8 (Pg no. 217-234)
22	L22		Topics: Origin Policy, Exceptions, LO1: Explain Origin Policy LO2: Analyze browser security principles and their exceptions.	LOL2 LOL4		CO3	Chalk & Talk / Self Learning	R1 Chap5 (Pg no. 149-166)
23	L23		Topics: Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) LO1: Explain XSS LO2: Analyze XSS and CSRF vulnerabilities.	LOL2 LOL4		CO3	Chalk & Talk / Interactive Learning	R1 Chap6 (Pg no. 170-210)
24	L24		Topics: Source Code Security, Forceful Browsing, Directory Traversals LO1: Define file security principles and risks. LO2: Evaluate mitigation techniques for file security vulnerabilities. **Assignment 1 & Discussion**	LOL1 LOL5		CO3	Chalk & Talk / Interactive Learning	R1 Chap8 (Pg no. 253-280)

END OF MODULE- 3								
25	L25	Module IV - Web Application Vulnerability	Topics: Injecting into Interpreted Contexts, SQL, NoSQL, XPath, LDAP LO1: Define injection attacks on data stores. LO2: Analyze the impact of SQL and NoSQL injections.	LOL1 LOL4		CO4	Chalk & Talk / Interactive Learning	T1 Chap9 (Pg no. 237-285)
26	L26		Topics: Injecting OS Commands, Manipulating File Paths, Injecting into XML Interpreters LO1: Explain OS and XML injection techniques. LO2: Evaluate real-world scenarios of OS and XML inject.	LOL2 LOL5		CO4	Chalk & Talk / Interactive Learning	T1 Chap9 (Pg no. 285-300)
27	L27		Topics: Injecting into Back-End HTTP Requests, Injecting into Mail Services LO1: Identify vulnerabilities in back-end components. LO2: Develop secure practices to mitigate such attacks.	LOL1 LOL6		CO4	Chalk & Talk / Interactive Learning	T1 Chap9 (Pg no. 300-330)
28	L28		Topics: Real-World Logic Flaws LO1: Describe common application logic flaws. LO2: Analyze and design secure application logic to prevent flaws.	LOL2 LOL6		CO4	Chalk & Talk / Interactive Learning	T1 Chap11 (Pg no. 350-368)
29	L29		Topics: Cross-Site Scripting (Varieties, Attacks, Exploitation, and Prevention) LO1: Explain different types of XSS attacks. LO2: Evaluate methods to detect and prevent XSS vulnerabilities.	LOL2 LOL5		CO4	Chalk & Talk / Interactive Learning	T1 Chap18 (Pg no. 580-583)
30	L30		Topics: Cookie-Based Attacks, HTTP Header Injection LO1: Define cookie-based attacks and HTTP header injection. LO2: Assess techniques to prevent cookie-based and header injection attacks.	LOL1 LOL5		CO4	Chalk & Talk / Interactive Learning	T1 Chap19 (Pg no. 623-642)
END OF MODULE- 4								

SKILL SETS TO BE DEVELOPED:

SK1. An attitude of enquiry.

SK2. Confidence and ability to tackle new problems.

SK3. Ability to interpret events and results.

SK4. Ability to work as a leader and as a member of a team.

SK5. Assess errors in systems/processes/programs/computations and eliminate them.

SK6. Observe and measure physical phenomena.

SK7. Write reports.

SK8. Select suitable equipment, instrument, materials & software

SK9. Locate faults in system/Processes/software.

SK10. Manipulative skills for setting and handling systems/Process/ Issues

SK11. The ability to follow standard /legal procedures.

SK12. An awareness of the Professional Ethics.

SK13. Need to observe safety/General precautions.

SK14. To judge magnitudes/Results/issues without actual measurement/actual contacts

Skill sets maaping on Pos

Sl. No.	Description	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
1.	An Attitude of Enquiry		✔										
2.	Confidence and ability to tackle new problems	✔	✔	✔		✔							
3.	Ability to interpret events and results			✔									✔
4.	Assess errors and eliminate them			✔									
5.	Write reports										✔		
6.	Select suitable software					✔							✔

7.	To predict the required output for the given problem.		✔	✔									

COURSE CONTENT &TASK SCHEDULE FOR LABORATORY COMPONENT:

Sl. No.	Task No	Task Learning Outcome	Level 01	Level0 2	Number of Lab Sessions required to complete the task	Skills to be developed	Course Outcome to be developed
1	P1	Practical knowledge of known vulnerabilities in CGI, LAMP stacks, REST APIs cross-site scripting: i.Basic Network scanning ii. Advanced scanning in general search iii. Netstat port scanning:	LOL1		2	SK1,SK2, SK4,SK6	CO1
2	P2	Use the Nessus tool to scan the network for vulnerabilities: I.Vulnerability Mapping ii.Policies iii.Plugins iv.General Scanning v.Port Scanning	LOL1, LOL2		2	SK1,SK2, SK4,SK6	CO1
3	P3	HTTP and setting up stacks	LOL1, LOL2		2	SK1,SK2, SK4,SK6	CO2
4	P4	Various types of databases Access Controls Various types of databases Access Controls	LOL1		2	SK1,SK2, SK4,SK6	CO2
5	P5	Vulnerability: Study and work with KF Sensor	LOL1, LOL2		2	SK1,SK2, SK4,SK6	CO3
6	P6	Study of web authoring tool: Study and work with Snort	LOL1, LOL2		2	SK1,SK2, SK4,SK6	CO3

7	P7	Study of web authoring tool: Study and work with Nmap	LOL1, LOL2		2	SK1,SK2, SK4,SK6	CO3
8	P8	Testing web applications I. Create an Online Community website and test the website ii.Showcase Your Work Online and test its worth	LOL3		2	SK1,SK2, SK4,SK6	CO4
9		Continuous Assessment 3			2		
10		Mid Term					
11	P9	Testing web applications: Create a Local Business Website and test the website		L3	2	SK1,SK2, SK4,SK6	CO4
12	P10	SQL injection and prevention From the given data set: i.Put limits on all result sets ii.Cleanse and Validate Freeform User Input iii.Remove Freeform User Input When Possible iv.Validate Data Prior to Processing v.Ensure Errors are Not User-Facing vi.Use Stored Procedures to Abstract Business Logic and Control parameters vii.Use LIKE Operators Carefully	LOL3		2	SK1,SK2, SK4,SK6	CO4
13	P11	Cross site request forgery attack With the usage of Virtual Machines: i.Configure the Virtual Machines ii.Observing HTTP Request in Victim VM iii.CSRF Attack using GET Request iv.CSRF Attack using POST Request	LOL3		2	SK1,SK2, SK4,SK6	CO4

		v. implementing a countermeasure					
14	P12	Web tracking Tracking the Web based scenario by i.Environment Configuration ii.clear history and cookies iii.open a new private window in Firefox	LOL3		2	SK1,SK2, SK4,SK6	CO4
15		Continuous Assessment 4					

ASSESSMENT SCHEDULE FOR THEORY AND LABORATORY COMPONENT:

Sl. No	Components of Continuous Assessment	Weightage (% of Total Marks)	Duration of Assessment
1	Continuous Assessment 1 – Theory	5%	1 hour
2	Continuous Assessment 2 -Theory	5%	1 hour
3	Continuous Assessment 3 -Lab	6.25%	1 hour
4	Mid Term Examination - Theory	25%	1.5 hours
5	Assignment	2.5%	-
6	Continuous Assessment 4 -Lab	6.25%	1 hour
7	End Term Final Examination – Theory	50%	3 hours
Total		100%	

Topics relevant to "EMPLOYABILITY SKILLS":

- Session Management &Web Security Principles and Web Application vulnerability for **Skill Development** through **Experiential Learning Techniques. This is attained through the Lab Experiments as mentioned in the assessment component**

ASSESSMENT DETAILS:

Si. No	Assessment type	Contents	Course outcome Number	Duration in Hours	Marks	Weightage	Venue, Date and Time
1	CA1 – Theory (Surprise Test 1)	Module 1	CO1	1 hour	10	5%	14.02.2025
2	CA2 – Theory (Surprise Test 2)	Module 2	CO2	1 hour	10	5%	14.03.2025

3	Lab exercises execution + Viva + Record	Module 1,2	CO1,CO2,	6 programs	12.5	6.25%	14.03.2025
4	Midterm Examination	Module1, 2	CO1, CO2	1.5 Hours	50	25%	17.03.2025 TO 21.03.2025
5	Assignment	Module 3	CO3		5	2.5%	-
6	Lab exercises execution + Viva + Record	Module 3,4	CO3,CO4	6 programs	12.5	6.25%	20.05.2025
7	End-term examination	All Modules	CO1,CO2, CO3, CO4	3 Hours	100	50%	26.05.2025 TO 06.06.2025

COURSE CLEARANCE CRITERIA:

Self-learning topics, Topics of participate learning and Technology enabled learning should be taken seriously as it will be assessed in the course and also it will help in understanding better. Hence, it is required to make maximum effort and meet faculty for reinforcing learning.

- Students are required to maintain class work which will be reviewed / evaluated at the end of every month.
- Students are required to strictly adhere to assignments and other assessment deadlines.
- Students are required to actively participate in online / offline classroom and other discussions.
- Course Clearance Criteria will be as per the Program Regulations

MAKEUP EXAM POLICY:

As per academic regulations of the university

Contact timings in the chamber for any discussions: University-wide free hour

CONTACT TIMINGS IN THE CHAMBER FOR ANY DISCUSSIONS:

Students are encouraged for any clarifications and discussions on this course during free hours in person (offline mode) or through online class platform such as Microsoft Teams.

SAMPLE THOUGHT PROVOKING QUESTIONS:

Sl. No.	**QUESTION**	**MARKS**	**COURSE OUTCOME NO.**	**BLOOM'S LEVEL**
1	How would you perform a security/penetration test on a web application covering the following scenarios? • Unauthenticated tests on log-in page. Test for brute forcing, password cracking, rainbow table attacks, account lockouts, clickjacking, session fixation, and so on. • Authenticated tests with one user account. Test for the usual suspects from the OWASP Top 10.	5	CO2	Understand

	• Authenticated tests with multiple user accounts. Test for horizontal privilege escalation, vertical privilege escalation, and forceful browsing.			
2	Explain a DOM-based cross-site scripting attack.	2	CO3	Understand
3	Is input validation sufficient to prevent cross-site scripting?	2	CO1	Remember
4	You have a log-in page with “username” and “password” fields. How do you test for SQL injection without using any tool?	10	CO4	Apply

TARGET SET FOR COURSE OUTCOME ATTAINMENT:

TABLE 8: TARGET SET FOR ATTAINMENT OF EACH CO and ATTAINMENT ANALYSIS AFTER RESULTS

Sl.no	C.O. No.	Course Outcomes	Threshold Set for the CO	Target set for attainment in percentage	Actual C.O. Attainment In Percentage *	Remarks on attainment &Measures to enhance the attainment *
01	CO1	Define the fundamentals of web applications and validation [Remember]	50%	55%		
02	CO2	Recognize the significance of password and authentication in web applications [Understand]	50%	60%		
03	CO3	Explain the importance of session management in web [Understand]	60%	60%		
04	CO4	Apply web attack techniques to find vulnerabilities in web applications [Apply]	60%	60%		

(Ms. Sreelatha PK)

Signature of the course Instructor

This course has been duly verified Approved by the D.A.C.

Signature of the Chairperson D.A.C.

BLOOM'S TAXONOMY SAMPLE VERBS

Learning Outcomes Verbs at Each Bloom Taxonomy Level to be used for writing the course Outcomes.

TABLE 9: REFERENCE SAMPLES OF BLOOMS TAXONOMY VERBS		
Cognitive Level	Illustrative Verbs	Definitions
Remember	Arrange, define, describe, duplicate, identify, label, list, match, name, order, outline, recite, recognize, relate, repeat, reproduce, select, state, tabulate, tell	remembering previously learned information
Understand	Classify, compare, compute, convert, contrast, defend, describe, differentiate, distinguish, estimate, explain, extrapolate, generalize, interpolate, locate, paraphrase, predict, recognize, review, summarize, translate	grasping the meaning of information
Apply	Apply, change, choose, calculate, classify, demonstrate, determine, employ, examine, illustrate, interpret, modify, operate, practice, predict, prepare, produce, restructure, schedule, sketch, solve, use	applying knowledge to actual situations
Analyze	Analyze, appraise, breakdown, calculate, categorize, compare, contrast, criticize, debate, diagram, differentiate, discriminate, distinguish, examine, experiment, identify, infer, inventory, relate, separate, subdivide, test	breaking down objects or ideas into simpler parts and seeing how the parts relate and are organized
Evaluate	Appraise, argue, assess, choose, compare, contrast, criticize, defend, discriminate, estimate, evaluate, explain, interpret, judge, measure, predict, rank, rate, recommend, select, support, validate	rearranging component ideas into a new whole
Create	Arrange, assemble, construct, collect, compose, create, design, develop, formulate, integrate, manage, organize, plan, prepare, prescribe, produce, propose, specify, synthesize, write	put elements together to form a new coherent or functional whole; reorganize elements into a new pattern or structure