Faculty of Computer Science & Applications
Master of Computer Application with Cyber Security
(W. E. F.: 2023-24)

Document ID: SUTEFCAM-01

Name of Faculty	:	Faculty of Computer Science & Applications
Name of Program	:	Master of Computer Application with Cyber Security
Course Code	:	2MCA08
Course Title	:	Web & Data Base Security
Type of Course	:	Professional Core
Year of Introduction	:	2023-24

Prerequisite	:	Basic Statistics
Course Objective	:	The goal of this course is to introduce students to the Web & Data Base Security, It is used in both the research and business environments.
Course Outcomes	:	At the end of this course, students will be able to:
	CO 1	Understand the importance of security of web application and database.
	CO 2	Launch cross site scripting attacks, forgery attack, SQL injection attack on vulnerable web application.
	CO 3	Carry out vulnerability analysis of source code in different languages and platforms.
	CO 4	Implement security policy for a database & Create database links.
	CO 5	Configure SSL on Server & Use PKI tools for database security.

Teaching and Examination Scheme

Teaching Scheme (Contact Hours)			Credits	Examination Marks				
				Theory Marks		Practical Marks		Total Marks
L	T	P	C	SEE	CIA	SEE	CIA	
3	0	2	4	70	30	30	20	150

*Legends: **L**-Lecture; **T**–Tutorial/Teacher Guided Theory Practice; **P**–Practical, **C** – Credit, **SEE** – Semester End Examination, **CIA** - Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.))*

Course Content

Unit No,	Topics	Teaching Hrs.	Weightage	Mapping with CO
1	**Web Application Basics:** Introduction, HTTP Protocol, Web Functionality, Encoding Schemes, Enumerating Content and Functionality, Analyzing the Application	3	5%	CO1
2	**Authentication Security:** Authentication Techniques, Design Flaws in Authentication, Implementation Flaws in Authentication, Securing Authentication, Path Traversal Attacks	3	5%	CO1
3	**Injection Attacks:** Injecting into Interpreted Contexts, SQL Injection, NoSQL Injection, XPath Injection, LDAP Injection, XML Injection, Http	4	10%	CO1

	Injection, Mail Service Injection			
4	Cross Site Scripting (XSS): Types of XSS, XSS in Real World, Finding and Exploiting XSS Vulnerabilities, Preventing XSS Attacks	4	10%	CO2
5	**User Attacks:** Inducing User Actions, Capturing Cross-Domain Data, Client-Side Injection Attacks, Local Privacy Attacks, ActiveX Control attacks, Browser Attacks	5	10%	CO2
6	**Vulnerability Analysis of Source Code:** Approaches to Code Review, Signatures of Common Vulnerabilities, Analysis of Java platform, Analysis of ASP.NET platform, Analysis of PHP, Analysis of Perl, Analysis of Javascript, Analysis of SQL	6	15%	CO3
7	**Introduction To Database Security**: Fundamental Data Security Requirements, Data Security Concerns, Compliance Mandates, Security Risks, Developing Enterprise Security Policy, Defining a Security Policy, Implementing a Security Policy, Techniques to Enforce Security	3	5%	CO4
8	**Database Access Control:** User Authentication, Protecting Passwords, Creating Fixed Database Links, Encrypting Database Link Passwords, Using Database Links Without Credentials, Using Database Links And Changing Passwords, Auditing With Database Links, Restricting A Database Link With Views, Trust Management & Negotiation	4	10%	CO4
9	**Database Security Issues:** Database Security Basics, Security Checklist, Reducing Administrative Effort, Applying Security Patches, Default Security Settings, Secure Password Support, Enforcing Password Management, Protecting The Data Dictionary, System and Object Privileges, Secure Data Outsourcing, Security in Advanced Database Systems, Managing Enterprise User Security	6	15%	CO5
10	**Framework For Database Security:** Security for Workflow Systems, Secure Semantic Web Services, Spatial Database Security, Security, Reengineering, Strong Authentication, Single Sign-On, Public Key Infrastructure (PKI) Tools, Configuring SSL on the Server, Certificates, Using Kerberos for Authentication	6	15%	CO5

Suggested Distribution of Theory Marks Using Bloom's Taxonomy						
Level	Remembrance	Understanding	Application	Analyse	Evaluate	Create
Weightage	**45%**	**45%**	**10%**	**-**	**-**	**-**

NOTE: This specification table shall be treated as a general guideline for the students and the teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Suggested List of Experiments/Tutorials

Sr. No.	Name of Experiment/Tutorials	Teaching Hours
1.	Reset password of Ubuntu and Cent OS (I forget the password of my machine).	02
2.	Create the password less Authentication between 2 machines. a) Two Linux machine One window and another is Linux). Use key based authentication.	02
3.	Set strong password policy in Linux machine for authentication perform this task in Windows machine. Prevent reusing old password. Set minimum password length. Set password complexity. Set password expiration period. Also set accounts lock out policy after 5 attempts.	03
4.	Make a vulnerable web application.	03
5.	Launch the Cross-site Scripting Attack, Cross-Site Request Forgery Attack, and Sql injection attack on a vulnerable web application and also perform Web Tracking using web tracking technology based on Elgg based labs on Seeds lab.	03
6.	Install Game over in your VMWARE and access it through browser. Study and perform the tests given in Section 1 and 2 also prepare the report according to your understanding.	03
7.	Install Nginx in Linux and secure it (https) by creating your own certificate. Use different keys for encryption.	03
8.	Collect Log Events from Windows Server by using Log Parser tool.	03
9.	Collect Log Events from Windows Server by using Log Parser tool.	03
10.	Configure SQUID proxy server and block social websites and chat application.	03

Major Equipment/ Instruments and Software Required

Sr. No.	Name of Major Equipment/ Instruments and Software
1	Intel-compatible 64-bit dual-core CPU i5 or higher (a faster processor is recommended).
2	8 GB RAM (more memory is recommended)
3	60 GB of available disk space (more space is recommended)
4	USB port 2.0 or higher (USB port 3.0 is recommended)
5	Ethernet network interface card (NIC) or adapter
6	Wi-Fi card or adapter
7	Virtualization support enabled in the BIOS; this is sometimes called Intel Virtualization
8	Technology (also known as Intel VT) or AMD-V

Reference Books

Sr. No.	Name of Reference Books
1	"The Web Application Hacker's Handbook", Dafydd Stuttard, Wiley India Pvt. Ltd.
2	" Database Security" , S.Castano, M. Fugini, G. Martella,P. Samarati, Addision-Wesley
3	" Database Security " Alfred Basta, Melissa Zgola, Cengage Publication