VARDHAMAN
COLLEGE OF ENGINEERING

CURRICULUM
For
Bachelor of Technology
Cyber Security (Minors)

Under
Choice Based Credit System (CBCS)

B. Tech. - Minors Degree Program

(For batches admitted from the Academic Year 2025 - 2026)

August 2025

VARDHAMAN COLLEGE OF ENGINEERING
(Autonomous)
Affiliated to **JNTUH,** Approved by **AICTE,** Accredited by **NAAC** with **A++** Grade
Kacharam, Shamshabad, Hyderabad- 501 218, Telangana, India
www.vardhaman.org, info@vardhaman.org

II B.Tech. II Semester													
#	Course Code	Title of the Course	Category	Teaching and Learning Scheme				Hours	Credits	Assessment Marks		
				CI		LI	TW + SL	H	C	CIE	SEE	Total
				L	T	P	SL					
Theory Courses												
1	M2601	Foundations of Cryptography	PC	45	-	-	45	90	3	40	60	100
2	M2602	Information Theory for Cybersecurity	PC	45	-	-	45	90	3	40	60	100
Total				90	0	0	90	180	6	80	120	200

III B.Tech. I Semester												
#	Course Code	Title of the Course	Category	Teaching and Learning Scheme				Hours	Credits	Assessment Marks		
				CI		LI	TW + SL	H	C	CIE	SEE	Total
				L	T	P	SL					
Theory Courses												
Elective–I: Cybersecurity & Steganography												
1	M2603	Steganography and Digital Watermarking	PC	45	-	-	45	90	3	40	60	100
	M2604	Ethical Hacking Fundamentals										
Elective–II: Forensics												
2	M2605	Digital Forensic	PC	45	-	-	45	90	3	40	60	100
	M2606	Privacy & Security in Online social media										
Total				90	0	0	90	180	6	80	120	200

III B.Tech. II Semester												
#	Course Code	Title of the Course	Category	Teaching and Learning Scheme				Hours	Credits	Assessment Marks		
				CI		LI	TW + SL	H	C	CIE	SEE	Total
				L	T	P	SL					
Theory Courses												
Elective–III: Web & Security Assessment												
1	M2607	Security Assessment and Risk Analysis	PC	45	-	-	45	90	3	40	60	100
	M2608	Web and Mobile Application Security										
Practical Courses												
2	M2609	Web and Mobile Application Security Laboratory	PC	-	-	30	-	30	1	40	60	100
Total				45	0	30	45	120	4	80	120	200

IV B.Tech. I Semester												
#	Course Code	Title of the Course	Category	Teaching and Learning Scheme				Hours	Credits	Assessment Marks		
				CI		LI	TW + SL	H	C	CIE	SEE	Total
				L	T	P	SL					
Experiential Learning Course												
1	M2810	Mini Project in Minor Specialization	PW	-	-	-	90	90	2	40	60	100
Total				0	0	0	90	90	2	40	60	100

II B.Tech. II Semester

M2601 - Foundations of Cryptography

Teaching and Learning Scheme				Hours	Credits	Assessment Marks		
CI		LI	TW+SL	H	C	CIE	SEE	Total
L	T	P	SL					
45	0	0	45	90	3	40	60	100

Course Description

Course Overview

This course aims a thorough understanding of cryptographic techniques essential for secure communication. It begins with classical cryptography and its evolution into modern approaches, including private-key encryption and the concept of perfect secrecy. Students learn about computational security, pseudo randomness, and methods for constructing encryption schemes resilient to chosen-plaintext and chosen-ciphertext attacks. The course covers message authentication codes, hash functions for integrity, and the design of block ciphers like DES and AES. It also explores real-world cryptanalysis methods such as differential and linear attacks. Finally, the course introduces public-key cryptography, key exchange mechanisms like Diffie-Hellman, and RSA encryption, addressing the limitations of symmetric systems.

Course Pre/Co-requisites

No Pre-requisites required.

Course Outcomes

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

M2601.1. Understand and differentiate between classical and modern cryptographic techniques, including the principles of private-key encryption and perfect secrecy.

M2601.2. Apply computational approaches to construct secure encryption schemes and evaluate their strength under CPA and CCA attack models.

M2601.3. Design and implement secure message authentication codes and collision-resistant hash functions to ensure data integrity and authenticity.

M2601.4. Analyze the structure and security of block cipher algorithms such as DES and AES, and understand cryptanalysis techniques like differential and linear attacks.

M2601.5. Explain the limitations of symmetric cryptography and apply public-key encryption methods, including RSA and Diffie-Hellman, for secure key exchange and hybrid encryption.

Course Syllabus

Unit-I:

Introduction and Classical Ciphers:

Classical Cryptography and Modern Cryptography, The Setting of Private-Key Encryption, Historical Ciphers and Their Cryptanalysis, The Basic Principles of Modern Cryptography. Perfectly-Secret Encryption: Definitions and Basic Properties, The One-Time Pad (Vernam's Cipher), Limitations of Perfect Secrecy.

Unit-II:

Private-Key Encryption and Pseudo randomness:

A Computational Approach to Cryptography, A Definition of Computationally-Secure Encryption, Pseudo randomness, Constructing Secure Encryption Schemes, Security under Chosen-Plaintext Attacks (CPA), Constructing CPA-Secure Encryption Schemes, Security Against Chosen-Ciphertext Attacks (CCA).

Unit-III:

Message Authentication Codes and Collision-Resistant Hash Functions:

Secure Communication and Message Integrity, Encryption vs. Message Authentication Codes - Definitions, Constructing Secure Message Authentication Codes, Collision-Resistant Hash Functions.

Unit-IV:

Pseudorandom Objects in Practice (Block Ciphers):

Substitution-Permutation Networks, Feistel Networks, DES – The Data Encryption Standard, Increasing the Key Size for Block Ciphers, AES – The Advanced Encryption Standard, Differential and Linear Cryptanalysis.

Unit-V:

Private-Key Management and the Public-Key Revolution:

Limitations of Private-Key Cryptography, Public-Key Revolution, Diffie-Hellman Key Exchange. Public-Key Encryption: Public-Key Encryption - An Overview, Definitions, Hybrid Encryption, RSA Encryption, Chosen Ciphertext Attacks.

Books and Materials

Text Books:

1. Katz, Jonathan, and Yehuda Lindell. Introduction to Modern Cryptography. 3rd ed., Chapman & Hall/CRC, 2020.

Reference Books:

1. Goldreich, Oded. Foundations of Cryptography: Basic Tools. Cambridge University Press, 2004.

M2602-Information Theory for Cyber Security

Teaching and Learning Scheme				Hours	Credits	Assessment Marks		
CI		LI	TW+SL	H	C	CIE	SEE	Total
L	T	P	SL					
45	0	0	45	90	3	40	60	100

Course Description

Course Overview

This course explores the fundamental principles of information theory and their practical applications in cyber security. Students will gain a deep understanding of entropy, data compression, and error correction, and how these concepts form the theoretical backbone of secure communication, encryption, authentication, and anomaly detection systems. The course bridges the gap between theory and practice by analyzing real-world cryptographic protocols, security systems, and cyber-attack detection methods from an information-theoretic perspective.

Course Pre/Co-requisites

No Pre requesites

Course Outcomes

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

M2602.1. Explain the core concepts of Information theory such as entropy, mutual information, and channel capacity.

M2602.2. Demonstrate how information theory is used in data compression, encryption, and error detection or correction.

M2602.3. Apply theoretical principles to analyze and improve cybersecurity systems

M2602.4. Evaluate the role of information theory in detecting and preventing cyber threats

M2602.5. Assess Modern applications in Cryptography, secure communications and information leakage mitigation.

Course Syllabus

Unit-I:

Introduction to Information Theory:

Shannon's foundation of Information theory, Random Variables, Probability distribution factors, Uncertainty/entropy information measures, Leakage, Quantifying Leakage and Partitions, Lower bounds on Key Size: Secrecy, authentication and Secret sharing, provable security, computationally- secure, Symmetric Cipher.

Unit-II:

Key Concepts in Cybersecurity and Authentication:

Secrecy, Authentication, Secret Sharing, Optimistic results on perfect secrecy, secret key agreement, Unconditional Security, Quantum Cryptography, Randomized Ciphers, Types of codes: Block codes Hamming and Lee metrics, description of linear block codes, parity check codes, cyclic codes, masking techniques.

Unit-III:

Engineering Cryptography Key Concepts & Security Techniques:

Information theoretic security and Cryptography, basic introduction to Diffie – Hellman, AES, and Side Channel attacks.

Unit-IV:

Secrecy Metrics:

Strong, weak, semantic security, partial secrecy, Secure Source Coding: Rate-Distortion Theory for Secrecy Systems, Side Information at Receivers, Differential privacy, Distributed channel synthesis.

Unit-V:

Digital Forensics Overview

Digital and Network Forensics, Public Key Infrastructure, Light Weight Cryptography, Elliptic Curve Cryptography, and applications.

Books and Materials

Text Books:

1. Kulkarni, Muralidhar, and K. S. Shivaprakasha. Information Theory and Coding. 1st ed., Wiley India Pvt. Ltd., 2015.
2. Singh, R. P., and S. D. Sapre. Communication Systems: Analog & Digital. 3rd ed., Tata McGraw Hill, 2012.
3. Borda, Monica. Fundamentals in Information Theory and Coding. Springer, 2011.
4. Bose, Ranjan. Information Theory, Coding and Cryptography. 3rd ed., McGraw Hill Education, 2016.

Reference Books:

1. Andleigh, Prabhat K., and Kiran Thakrar. Multimedia Systems Design. Pearson India, 2015.

III B.Tech. I Semester

ELECTIVES COURSE - I

M2603 - Steganography and Digital Marketing

Teaching and Learning Scheme				Hours	Credits	Assessment Marks		
CI		LI	TW+SL	H	C	CIE	SEE	Total
L	T	P	SL					
45	0	0	45	90	3	40	60	100

Course Description

Course Overview

This course explores the principles, techniques, and applications of steganography and digital watermarking for secure communication, copyright protection, and authentication in the digital domain. It covers both spatial and transform domain methods for embedding and extracting hidden information in multimedia content such as images, audio, video, and text, while maintaining imperceptibility, capacity, and robustness. Students will learn to analyze the trade-offs in designing information hiding systems, evaluate their resilience against steganalysis and removal attacks, and implement practical solutions using modern tools and algorithms. Ethical considerations and real-world case studies will also be discussed to provide a comprehensive understanding of the role of information hiding in cybersecurity and digital rights management.

Course Pre/Co-requisites

M2601-Foundations of Cryptography

Course Outcomes

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

M2603.1. Understand the history and importance of Watermarking and Steganography.

M2603.2. Analyze applications and properties of watermarking and steganography.

M2603.3. Demonstrate Models and algorithms of watermarking.

M2603.4. Develop the passion for acquiring knowledge and skill in preserving authentication of information .

M2603.5. Identify the theoretic foundations of Steganography and Steganalysis.

Course Syllabus

Unit-I:

Introduction:

Steganography Overview, History of hiding (text, images, audio, video, speech etc.), theoretic foundations of Steganography

Unit-II:

Steganalysis:

Active and Malicious Attackers, Active and Passive Steganalysis.

Unit-III:

Steganography Frameworks:

Frameworks for secret communication (Pure Steganography, Secret Key, Public Key Steganography), Steganography algorithms (Adaptive and Non-adaptive).

Unit-IV:

Steganography Techniques:

Substitution systems, Spatial domain, transform domain techniques, Spread Spectrum, Statistical Steganography.

Unit-V:

Digital Watermarking:

Introduction, Difference between Watermarking and Steganography, Classification (Characteristics and Applications), types and techniques (Spatial – domain, Frequency – domain, and vector quantization-based watermarking), watermarking security & authentication

Books and Materials

Text Books:

1. Digital Watermarking and Steganography, Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, Morgan Kaufmann Publishers, New York, 2008.
2. Information Hiding: Steganography and Watermarking – Attacks and Countermeasures by Neil F. Johnson, Zoran Duric, Sushil Jajodia.

Reference Books:

1. Sahu, Aditya Kumar, editor. Multimedia Watermarking: Latest Developments and Trends. Springer, 2024.

M2604 – Ethical Hacking Fundamentals

Teaching and Learning Scheme				Hours	Credits	Assessment Marks		
CI		LI	TW+SL	H	C	CIE	SEE	Total
L	T	P	SL					
45	0	0	45	90	3	40	60	100

Course Description

Course Overview

This course provides an in-depth study of cybersecurity threats, vulnerabilities, and defense measures. It covers ethical hacking concepts, terminologies, and phases of the hacking process. Students learn foot printing, port scanning, and reconnaissance techniques.System hacking topics include password cracking, sniffing, spoofing, and keystroke logging.Web security modules address SQL injection, cross-site scripting, and session hijacking.Wireless hacking covers WEP/WPA cracking, sniffing traffic, and DOS attacks.Practical sessions emphasize ethical penetration testing and security auditing.By course end, students can identify vulnerabilities and implement countermeasures effectively.

Course Pre/Co-requisites

M2602-Information Theory for Cyber Security

Course Outcomes

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

M2604.1. Explain vulnerabilities, mechanisms to identify vulnerabilities or threats or attacks.

M2604.2. Perform penetration & security testing.

M2604.3 Explain various methods of password cracking.

M2604.4 Interpret web services and session hacking.

M2604.5 Discuss about hacking wireless networks.

Course Syllabus

Unit-I:

Ethical Hacking Overview & Vulnerabilities:

Understanding the importance of security, Concept of ethical hacking and essential Terminologies- Threat, Attack, Vulnerabilities, Target of Evaluation, Exploit. Phases involved in hacking.

Unit-II:

Foot printing and Port Scanning:

Foot printing - Introduction to foot printing, Understanding the information gathering methodology of the hackers, Tools used for the reconnaissance phase. Port Scanning - Introduction, using port scanning tools, Ping sweeps, Scripting Enumeration-Introduction, Enumerating windows OS & Linux OS

Unit-III:

System Hacking:

Aspect of remote password guessing, Role of eavesdropping, Various methods of password cracking, Keystroke Loggers, Understanding Sniffers, Comprehending Active and Passive Sniffing, ARP Spoofing and Redirection, DNS and IP Sniffing, HTTPS Sniffing

Unit-IV:

Hacking Web Services & Session Hijacking:

Web application vulnerabilities, application coding errors, SQL injection into Back-end Databases, cross-site scripting, cross-site request forging, authentication bypass, web services and related flaws, protective http headers- Clickjacking Understanding Session Hijacking, Phases involved in Session Hijacking, Types of Session Hijacking, Session Hijacking Tools

Unit-V:

Hacking Wireless Networks:

Introduction to 802.11, Role of WEP, Cracking WEP Keys, Sniffing Traffic, Wireless DOS attacks, WLAN Scanners, WLAN Sniffers, Hacking Tools, Securing Wireless Networks

Books and Materials

Text Books:

1. Kimberly Graves, "Certified Ethical Hacker", Wiley India Pvt Ltd, 2010.

Reference Books:

1. Michael T. Simpson, "Hands-on Ethical Hacking & Network Defense", Course Technology, 2010
2. Rajat Khare, "Network Security and Ethical Hacking", Luniver Press, 2006
3. Ramachandran V, backtrack 5 Wireless Penetration Testing Beginner's Guide (3rd ed.), Pack Publishing, 2011
4. Thomas Mathew, "Ethical Hacking", OSB publishers, 2003.

ELECTIVES COURSE - II

M2605 – Digital Forensics

Teaching and Learning Scheme				Hours	Credits	Assessment Marks		
CI		LI	TW+SL	H	C	CIE	SEE	Total
L	T	P	SL					
45	0	0	45	90	3	40	60	100

Course Description

Course Overview

This course will cover the fundamentals of digital forensics. Provides an in-depth study of the rapidly changing and fascinating field of computer forensics. Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes. Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools E-evidence collection. It provides preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics.

Course Pre/Co-requisites

M2601-Foundations of Cryptography M2602-Information Theory for Cyber Security

Course Outcomes

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

M2605.1. Understand relevant legislation and codes of ethics.

M2605.2. Investigate computer forensics and digital detective and various processes, policies and procedures data acquisition and validation, e-discovery tools.

M2605.3. Analyze E-discovery, guidelines and standards, E-evidence, tools and environment.

M2605.4. Apply the underlying principles of email, web and network forensics to handle real life problems.

M2605.5. Use IT Acts and apply mobile forensics techniques.

Course Syllabus

Unit-I:

Digital Forensics Science:

Forensics science, computer forensics, and digital forensics. Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber criminalistics area, challenges faced by digital forensics.

Unit-II:

Cyber Crime Scene Analysis:

Identifying digital evidence, collecting evidence in private-sector incident scenes, processing law enforcement crime scenes, preparing for a search, securing a computer incident or crime scene, seizing digital evidence at the scene

Unit-III:

Evidence Management & Presentation:

Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Types of Evidence, Define who should be notified of a crime, parts of gathering evidence.

Unit-IV:

Computer Forensics:

Preparing a computer case investigation, Procedures for corporate hi-tech investigations, conducting an investigation, Complete and critiquing the case. Network Forensics: Overview of network forensics, open-source security tools for network forensic analysis.

Unit-V:

Mobile Forensics:

Mobile forensics techniques, mobile forensics tools, recent trends in mobile forensic technique and methods to search and seizure electronic evidence. Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008.

Books and Materials

Text Books:

1. B Nelson, A. Phillips, and C. Steuart, Guide to Computer Forensics and Investigations, 4th edition, Course Technology 2010.

Reference Books:

1. John Sammons, The Basics of Digital Forensics, 2nd Edition, Elsevier, 2014
2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, Laxmi Publications,2025.

M2606– Privacy and Security in Online Social Media

Teaching and Learning Scheme				Hours	Credits	Assessment Marks		
CI		LI	TW+SL	H	C	CIE	SEE	Total
L	T	P	SL					
45	0	0	45	90	3	40	60	100

Course Description

Course Overview

This course introduces students to the foundational concepts, challenges, and technologies related to privacy and security in online social networks (OSNs). It focuses on how modern online platforms like Facebook, Twitter, LinkedIn, and Instagram manage data, user identity, and trust, while also exposing learners to real-world security threats and mitigation techniques. Students will learn the working principles of online social networks, the evolution of social media platforms, and explore privacy risks, trust issues, and information disclosure concerns. The course dives deep into access control models, identity management strategies, and trust management systems that are critical to protecting user data in Unthorough a combination of theoretical frameworks and real-world case studies, students will acquire the skills to analyse, design, and evaluate privacy-preserving and security-enhancing mechanisms used in online social platforms.

Course Pre/Co-requisites

M2602-Information Theory for Cyber Security

Course Outcomes

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

M2606.1. Understand working of online social networks.

M2606.2. Describe privacy policies of online social media.

M2606.3. Analyze countermeasures to control information sharing in Online social networks.

M2606.4. Apply knowledge of identity management in Online social networks.

M2606.5. Compare various privacy issues associated with popular social media..

Course Syllabus

Unit-I:

Introduction to Online Social Networks:

Introduction to Social Networks, From offline to Online Communities, Online Social Networks, Evolution of Online Social Networks, Analysis and Properties, Security Issues in Online Social Networks, Trust Management in Online Social Networks, Controlled Information Sharing in Online Social Networks, Identity Management in Online Social Networks, data collection from social networks, challenges, opportunities, and pitfalls in online social networks, APIs; Collecting data from Online Social Media.

Unit-II:

Trust Management in Online Social Networks:

Trust and Policies, Trust and Reputation Systems, Trust in Online Social, Trust Properties, Trust Components, Social Trust and Social Capital, Trust Evaluation Models, Trust, credibility, and reputations in social systems; Online social media and Policing, Information privacy disclosure, revelation, and its effects in OSM and online social networks; Phishing in OSM & Identifying fraudulent entities in online social networks.

Unit-III:

Controlled Information Sharing in Online Social Networks:

Access Control Models, Access Control in Online Social Networks, Relationship-Based Access Control, Privacy Settings in Commercial Online Social Networks, Existing Access Control Approaches

Unit-IV:

Identity Management in Online Social Networks:

Identity Management, Digital Identity, Identity Management Models: From Identity 1.0 to Identity 2.0, Identity Management in Online Social Networks, Identity as Self-Presentation, Identity thefts, Open Security Issues in Online Social Networks

Unit-V:

Case Study:

Privacy and security issues associated with various social media such as Facebook, Instagram, Twitter, LinkedIn etc.

Books and Materials

Text Books:

1. Security and Privacy-Preserving in Social Networks, Editors: Chbeir, Richard, Al Bouna, Bechara (Eds.), Springer, 2013.

Reference Books:

1. Security and Trust in Online Social Networks, Barbara Carminati, Elena Ferrari, Marco Viviani, Morgan & Claypool publications.
2. Security and Privacy in Social Networks, Editors: Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N., Pentland, A. (Eds.), Springer, 2013
3. Security and privacy preserving in social networks, Elie Raad & Richard Chbeir, Richard Chbeir & Bechara Al Bouna, 2013
4. Social Media Security: Leveraging Social Networking While Mitigating Risk, Michael Cross, 2013

III B.Tech. II Semester

ELECTIVES COURSE - III

M2607 – Security Assessment and Risk Analysis

Teaching and Learning Scheme				Hours	Credits	Assessment Marks		
CI		LI	TW+SL	H	C	CIE	SEE	Total
L	T	P	SL					
45	0	0	45	90	3	40	60	100

Course Description

Course Overview

This course explores the principles, techniques, and applications of steganography and digital watermarking for secure communication, copyright protection, and authentication in the digital domain. It covers both spatial and transform domain methods for embedding and extracting hidden information in multimedia content such as images, audio, video, and text, while maintaining imperceptibility, capacity, and robustness. Students will learn to analyze the trade-offs in designing information hiding systems, evaluate their resilience against steganalysis and removal attacks, and implement practical solutions using modern tools and algorithms. Ethical considerations and real-world case studies will also be discussed to provide a comprehensive understanding of the role of information hiding in cybersecurity and digital rights management.

Course Pre/Co-requisites

M2602-Information Theory for Cyber Security

Course Outcomes

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

M2607.1. Describe basic information security concepts and critical information characteristics.

M2607.2. Apply risk assessment methods to identify threats and vulnerabilities.

M2607.3. Analyze security policies and disaster recovery planning mechanisms.

M2607.4. Examine personnel security practices and security auditing processes.

M2607.5. Evaluate OPSEC strategies and security controls using case studies.

Course Syllabus

Unit-I:

Security Basics:

Information Security (INFOSEC) Overview: Critical information characteristics,availability information states –processing security countermeasures-education, training and awareness, critical information characteristics – confidentiality critical information characteristics – integrity, information states – storage, information states – transmission, security countermeasures-policy, procedures and practices, threats, vulnerabilities.

Unit-II:

Threats and Vulnerabilities of Systems:

Threats, major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS). Countermeasures: assessments (e.g., surveys, inspections). Concepts of Risk Management: consequences (e.g., corrective action, risk assessment), cost/benefit analysis and implementation of controls, monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information).

Unit-III:

Security Planning:

Directives and procedures for policy mechanism. Contingency Planning/Disaster Recovery: agency response

procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event.

Unit-IV:

Personnel Security Practices and Procedures:

Access authorization/verification, contractors, employee clearances, position sensitivity, security training and awareness, systems maintenance personnel. Auditing and Monitoring: conducting security reviews, effectiveness of security programs, investigation of security breaches, privacy review of accountability controls, review of audit trails and logs.

Unit-V:

Operations Security (OPSEC):

OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography-encryption (e.g., point-to-point, network, link). Case study of threat and vulnerability assessment

Books and Materials

Text Books:

1. Information Systems Security, 2ed: Security Management, Metrics, Frameworks and Best Practices, Nina Godbole, John Wiley & Sons.
2. Principles of Incident Response and Disaster Recovery, Whitman & Mattord, Course Technology.

Reference Books:

1. Digital Watermarking and Steganography: Fundamentals and Techniques. 2nd ed., CRC Press, 2017.
2. Multimedia Watermarking: Latest Developments and Trends. Springer, 2024.

M2608– Web and Mobile Application Security

Teaching and Learning Scheme				Hours	Credits	Assessment Marks		
CI		LI	TW+SL	H	C	CIE	SEE	Total
L	T	P	SL					
45	0	0	45	90	3	40	60	100

Course Description

Course Overview

The course has been designed to equip students with the relevant skills, tools and tech- niques to identify vulnerabilities and flaws within web and mobile applications.

Course Pre/Co-requisites

M2602-Information Theory for Cyber Security

Course Outcomes

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

M2608.1. Understand the Knowledge of Web Application hacking and attack for evasion techniques.

M2608.2. Apply the different techniques for hijacking and fixation.

M2608.3. Discover and exploit through techniques for Web services vulnerabilities.

M2608.4. Analyze the android and iOS for Mobile Application Security.

Course Syllabus

Unit-I:

Web Applications:

Introduction to web applications, Web application hacking, Overview of browsers, extensions, and platforms, Attacks, detection evasion techniques, and coun- termeasures for the most popular web platforms, including IIS, Apache, PHP, and ASP.NET Attacks and countermeasures for common web authentication mechanisms, including password-based, multifactor (e.g., CAPTCHA), and online authentication services like Windows Live ID.

Unit-II:

Advanced session analysis:

hijacking, and fixation techniques, cross-site scripting, SQL injection, classic categories of malicious input, Overlong input (like buffer over- flows), canonicalization attacks (like the infamous dot-dot-slash), and meta characters (including angle brackets, quotes, single quote, double dashes, percent, asterisk, under- score, newline, ampersand, pipe, and semicolon), beginner-to-advanced SQL injection tools and techniques, stealth-encoding techniques and input validation/ output-encoding countermeasures.

Unit-III:

Web services vulnerabilities discovery:

Web services vulnerabilities discovery and exploited through techniques including WSDL disclosure, input injection, external entity injection, and XPath injection. Web application management attacks against remote server management, web content manage- ment/authoring, admin misconfigurations, and developer-driven mistakes. Web browser exploits.

Unit-IV:

Android Architectures:

Setting up a Testing Environment, Android Build Process, Reversing APKs, Device Rooting, Android Application Fundamentals, Network Traffic, Device and Data Security, Tapjacking, Static Code Analysis, Dynamic Code Analysis

Unit-V:

iOS Architecture:

Device Jailbreaking, Setting up a Testing Environment, iOS Build Process, Reversing iOS Apps, iOS Application Fundamentals, iOS Testing Fundamentals, Network Traffic, Device Administration, iOS: Dynamic Analysis.

Books and Materials

Text Books:

1. Hacking Exposed Web Applications, 3rdEdition, JOEL SCAMBRAY, VINCENT LIU, CALEB SIMA
2. The Web Application Hacker's Handbook Discovering and Exploiting Security Flaws By Dafydd Stuttard, Marcus Pinto
3. Rich Bowen, Ken Coar, "Apache Cookbook", O'Reilly
4. "Mobile Application Security" by David Thiel, Chris Clark, Himanshu Dwivedi Re- leased February 2010 Publisher(s): McGraw-Hill ISBN: 9780071633574

Reference Books:

1. McDonald, Malcolm. Grokking Web Application Security. Manning, 2024

M2609 – Web and Mobile Application Security Laboratory

Teaching and Learning Scheme				Hours	Credits	Assessment Marks		
CI		LI	TW+SL	H	C	CIE	SEE	Total
L	T	P	SL					
0	0	60	0	60	2	40	60	100

Course Description

Course Overview

This laboratory course provides practical exposure to identifying and exploiting security vulnerabilities in web and mobile applications. Students gain hands-on experience with common attacks such as broken authentication, injection, XSS, XXE, insecure deserialization, and mobile-specific threats like tapjacking and reverse engineering. The course emphasizes understanding attacker techniques, analyzing system responses, and documenting security flaws in line with OWASP guidelines

Course Pre/Co-requisites

M2602-Information Theory for Cyber Security

Course Outcomes

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

M2609.1. Apply the Knowledge of Web Application Hacking and attack for evasion techniques.

M2609.2. Analyze the different techniques for hijacking and fixation.

M2609.3. Discover and exploit through techniques for Web services vulnerabilities.

M2609.4. Analyze the android and iOS for mobile application security.

Course Syllabus

List of Experiments:

1. Enumeration: Perform enumeration on a target system and document the responses obtained.
2. Security Misconfiguration: Identify and analyze security misconfigurations in a system, and record the responses.
3. Using Components with Known Vulnerabilities: Detect and assess components with known vulnerabilities, and document the findings.
4. Broken Authentication: Exploit broken authentication mechanisms and record the observed responses.
5. Broken Access Control: Test and evaluate broken access control scenarios, and document the results.
6. Injection Attacks: Perform injection attacks (such as SQL, Command, or LDAP injection) and capture the system responses.
7. XML External Entities (XXE) and Cross-Site Scripting (XSS): Conduct XXE and XSS attacks and document the output.
8. Insecure Deserialization: Test for insecure deserialization vulnerabilities and record the system behavior.
9. Sensitive Data Exposure: Identify instances of sensitive data exposure and document the findings.
10. Bypassing Security Controls: Demonstrate methods to bypass security controls and record the observed outcomes.
11. Tapjacking: Perform a tapjacking attack and analyze the application's response.
12. eLS_LogIn (Reverse Engineering Lab): Conduct reverse engineering of the eLS_LogIn application and document the findings.

13. eLS_LogIn (Dynamic Analysis Lab): Perform dynamic analysis of the eLS_LogIn application and document the findings.
14. Secure OTP Generator: Design, implement, and evaluate a secure OTP generator and document its functionality.

Laboratory Equipment/Software/Tools Required:

1. Computer Systems (PCs) installed with Ubuntu OS (Open source/ Freeware)
2. GCC Compiler (Open source/ Freeware)
3. Burp Suite, SQLMap,Metasploit,Wireshark

Books and Materials

Text Books:

1. Hacking Exposed Web Applications, 3rdEdition, JOEL SCAMBRAY, VINCENT LIU, CALEB SIMA
2. The Web Application Hacker's Handbook Discovering and Exploiting Security Flaws By Dafydd Stuttard, Marcus Pinto
3. Rich Bowen, Ken Coar, "Apache Cookbook", O'Reilly
4. "Mobile Application Security" by David Thiel, Chris Clark, Himanshu Dwivedi Released February 2010 Publisher(s): McGraw-Hill ISBN: 9780071633574

Vision

To be a pioneer institute and leader in engineering education to address societal needs through education and practice.

Mission

To adopt innovative student centric learning methods.
To enhance professional and entrepreneurial skills through industry institute interaction.
To train the students to meet dynamic needs of the society.
To promote research and continuing education.

Quality Policy

We at Vardhaman College of Engineering, endeavor to uphold excellence in all spheres by adopting the best practices in effort and effect.

VCE
VARDHAMAN
COLLEGE OF ENGINEERING

VARDHAMAN COLLEGE OF ENGINEERING

(Autonomous)

Affiliated to **JNTUH,** Approved by **AICTE,** Accredited by **NAAC** with **A++** Grade
Kacharam, Shamshabad, Hyderabad- 501 218, Telangana, India
www.vardhaman.org, info@vardhaman.org