

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF COMPUTER APPLICATIONS

QUESTION BANK

Academic Year 2026-2027



III SEMESTER

PMC504 - ENGINEERING SECURE SOFTWARE SYSTEMS

(Regulation – 2024)

Prepared by

Mrs. R. Jeevitha, Assistant Professor



SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM NAGAR, KATTANKULATHUR - 603203.

DEPARTMENT OF COMPUTER APPLICATIONS



Subject Code & Name : PMC504 ENGINEERING SECURE SOFTWARE SYSTEMS

Class / Semester : II -MCA - III Sem

UNIT I NEED OF SOFTWARE SECURITY AND LOW-LEVEL ATTACKS

Software Assurance and Software Security - Threats to software security - Sources of software insecurity - Benefits of Detecting Software Security - Properties of Secure Software – Memory-Based Attacks: Low-Level Attacks against Heap and Stack - Defense Against Memory-Based Attacks.

Part A

Q.No	Questions	Marks	Competence	BT Level	CO
1	Define Software Security.	2	Remembering	BTL-1	CO1
2	What is Software Assurance?	2	Remembering	BTL-1	CO1
3	List any four threats to software security.	2	Remembering	BTL-1	CO1
4	What are the major sources of software insecurity?	2	Remembering	BTL-1	CO1
5	State the benefits of detecting software security vulnerabilities.	2	Understanding	BTL-2	CO1
6	Define secure software.	2	Remembering	BTL-1	CO1
7	List the essential properties of secure software.	2	Remembering	BTL-1	CO1
8	What is a memory-based attack?	2	Remembering	BTL-1	CO1
9	Define stack memory.	2	Remembering	BTL-1	CO1
10	Define heap memory.	2	Remembering	BTL-1	CO1
11	What is a stack overflow attack?	2	Understanding	BTL-2	CO1
12	What is a heap overflow attack?	2	Understanding	BTL-2	CO1
13	What is meant by buffer overflow?	2	Remembering	BTL-1	CO1
14	Differentiate stack memory and heap memory.	2	Understanding	BTL-2	CO1
15	What is Address Space Layout Randomization (ASLR)?	2	Remembering	BTL-1	CO1
16	What is Data Execution Prevention (DEP)?	2	Remembering	BTL-1	CO1
17	What is a stack canary?	2	Remembering	BTL-1	CO1
18	State two defense mechanisms against memory-based attacks.	2	Understanding	BTL-2	CO1

19	What is meant by code injection?	2	Understanding	BTL-2	CO1
20	What is return-oriented programming (ROP)?	2	Remembering	BTL-1	CO1
21	Why is input validation important in software security?	2	Understanding	BTL-2	CO1
22	What is the role of secure coding practices in software security?	2	Understanding	BTL-2	CO1
23	What is a vulnerability in software?	2	Remembering	BTL-1	CO1
24	Mention any two characteristics of a secure software system.	2	Understanding	BTL-2	CO1
Part B					
Q.No	Questions	Marks	Competence	BT Level	CO
1	Examine the concepts of Software Assurance and Software Security with suitable examples.	16	Applying	BTL-3	CO1
2	(i) Discover various threats to software security	8	Analyzing	BTL-4	CO1
	(ii) Inspect the threats impact on software systems.	8			
3	Analyze the different sources of software insecurity and suggest preventive measures.	16	Analyzing	BTL-4	CO1
4	Illustrate the benefits of detecting software security vulnerabilities during software development.	16	Applying	BTL-3	CO1
5	(i) Examine the properties of secure software	8	Applying	BTL-3	CO1
	(ii) Examine the contribution of secure software.	8			
6	Analyze memory-based attacks and classify different types.	16	Analyzing	BTL-4	CO1
7	Analyze the stack overflow attack with a neat diagram.	16	Analyzing	BTL-4	CO1
8	Analyze the heap overflow attack and compare it with stack overflow.	16	Analyzing	BTL-4	CO1
9	Examine the defense mechanisms including ASLR, DEP and Stack Canaries.	16	Applying	BTL-3	CO1
10	Examine a secure software development approach to minimize vulnerabilities.	16	Applying	BTL-3	CO1
11	Compare and correlate Software Assurance and Software Security.	16	Analyzing	BTL-4	CO1
12	Analyze how secure coding practices prevent memory-based attacks.	16	Analyzing	BTL-4	CO1
13	Examine the working principle of stack memory architecture and stack overflow	16	Applying	BTL-3	CO1
14	Examine the software security testing and the techniques for detecting vulnerabilities.	16	Applying	BTL-3	CO1
15	Analyze memory protection mechanisms.	16	Analyzing	BTL-4	CO1
16	Analyze a secure SDLC strategy.	16	Analyzing	BTL-4	CO1

17	Analyze a case of memory corruption vulnerabilities and propose a security solution.	16	Analyzing	BTL-4	CO1
----	--	----	-----------	-------	-----

UNIT II SECURE SOFTWARE DESIGN

Requirements engineering for secure software - SQUARE process Model – Requirements elicitation and prioritization- Isolating the Effects of Untrusted Executable Content – Stack Inspection – Policy Specification Languages – Vulnerability Trends – Buffer Overflow – Code Injection - Session Hijacking. Secure Design - Threat Modeling and Security Design Principles.

Part A					
Q.No	Questions	Marks	Competence	BT Level	CO
1	Define secure software design.	2	Remembering	BTL-1	CO2
2	What is requirements engineering for secure software?	2	Remembering	BTL-1	CO2
3	What is the SQUARE process model?	2	Remembering	BTL-1	CO2
4	What is requirements elicitation?	2	Remembering	BTL-1	CO2
5	What is requirements prioritization?	2	Remembering	BTL-1	CO2
6	Define untrusted executable content.	2	Remembering	BTL-1	CO2
7	What is stack inspection?	2	Remembering	BTL-1	CO2
8	Define policy specification language.	2	Remembering	BTL-1	CO2
9	What is a security policy?	2	Remembering	BTL-1	CO2
10	What is vulnerability trend?	2	Remembering	BTL-1	CO2
11	Define buffer overflow.	2	Remembering	BTL-1	CO2
12	What is code injection?	2	Remembering	BTL-1	CO2
13	What is session hijacking?	2	Remembering	BTL-1	CO2
14	What is threat modeling?	2	Remembering	BTL-1	CO2
15	List any four security design principles.	2	Remembering	BTL-1	CO2
16	Define least privilege principle.	2	Remembering	BTL-1	CO2
17	What is attack surface?	2	Understanding	BTL-2	CO2
18	What is trust boundary?	2	Remembering	BTL-1	CO2
19	State two objectives of secure design.	2	Understanding	BTL-2	CO2
20	What is secure architecture?	2	Remembering	BTL-1	CO2
21	Differentiate authentication and authorization.	2	Understanding	BTL-2	CO2
22	What is input validation?	2	Understanding	BTL-2	CO2
23	What is defense in depth?	2	Understanding	BTL-2	CO2

24	Mention two benefits of threat modeling.	2	Understanding	BTL-2	CO2
----	--	---	---------------	-------	-----

Part B					
Q.No	Questions	Marks	Competence	BT Level	CO
1	Examine the requirements engineering process for secure software with suitable examples.	16	Applying	BTL-3	CO2
2	Apply the SQUARE process model with a neat diagram.	16	Applying	BTL-3	CO2
3	Analyze requirements elicitation and prioritization techniques for secure software.	16	Analyzing	BTL-4	CO2
4	Identify and illustrate the methods for isolating the effects of untrusted executable content.	16	Applying	BTL-3	CO2
5	Analyze stack inspection and its role in software security.	16	Analyzing	BTL-4	CO2
6	Examine policy specification languages and their applications.	16	Applying	BTL-3	CO2
7	Analyze the vulnerability trends and their impact on secure software.	16	Analyzing	BTL-4	CO2
8	Analyze buffer overflow attacks with suitable examples.	16	Analyzing	BTL-4	CO2
9	Examine the code injection attacks and preventive techniques.	16	Applying	BTL-3	CO2
10	Develop the methods to prevent session hijacking attacks.	16	Applying	BTL-3	CO2
11	Examine threat modeling and its stages.	16	Applying	BTL-3	CO2
12	Analyze security design principles with examples.	16	Analyzing	BTL-4	CO2
13	Examine the SQUARE process and threat modeling for secure software.	16	Applying	BTL-3	CO2
14	Analyze about the code injection and session hijacking with countermeasures.	16	Analyzing	BTL-4	CO2
15	Illustrate the secure design principles and the policy specification languages.	16	Applying	BTL-3	CO2
16	Examine a secure software architecture using security design principles.	16	Applying	BTL-3	CO2
17	Analyze about buffer overflow, code injection and session hijacking and measures to protect it.	16	Analyzing	BTL-4	CO2

UNIT III SECURITY RISK MANAGEMENT

Risk Management Life Cycle – Risk Profiling – Risk Exposure Factors. Risk Evaluation and Mitigation – Risk Assessment Techniques – Threat and Vulnerability Management.

Part A					
Q.No	Questions	Marks	Competence	BT Level	CO
1	Define risk management.	2	Remembering	BTL-1	CO3
2	What is the risk management life cycle?	2	Remembering	BTL-1	CO3

3	What is risk profiling?	2	Remembering	BTL-1	CO3
4	Define risk exposure.	2	Remembering	BTL-1	CO3
5	List the risk exposure factors.	2	Remembering	BTL-1	CO3
6	What is risk evaluation?	2	Remembering	BTL-1	CO3
7	Define risk mitigation.	2	Remembering	BTL-1	CO3
8	What is risk assessment?	2	Remembering	BTL-1	CO3
9	List any two risk assessment techniques.	2	Understanding	BTL-2	CO3
10	What is threat management?	2	Remembering	BTL-1	CO3
11	What is vulnerability management?	2	Remembering	BTL-1	CO3
12	Define threat.	2	Remembering	BTL-1	CO3
13	What is vulnerability?	2	Remembering	BTL-1	CO3
14	Differentiate threat and vulnerability.	2	Understanding	BTL-2	CO3
15	What is risk identification?	2	Remembering	BTL-1	CO3
16	What is qualitative risk assessment?	2	Remembering	BTL-1	CO3
17	What is quantitative risk assessment?	2	Remembering	BTL-1	CO3
18	What is risk register?	2	Remembering	BTL-1	CO3
19	What is residual risk?	2	Remembering	BTL-1	CO3
20	What is risk acceptance?	2	Remembering	BTL-1	CO3
21	What is risk avoidance?	2	Understanding	BTL-2	CO3
22	What is risk transfer?	2	Understanding	BTL-2	CO3
23	Mention two benefits of risk management.	2	Understanding	BTL-2	CO3
24	State the importance of vulnerability management.	2	Understanding	BTL-2	CO3

Part B					
Q.No	Questions	Marks	Competence	BT Level	CO
1	Apply the Risk Management Life Cycle with a neat diagram.	16	Applying	BTL-3	CO3
2	Examine the process of Risk Profiling with suitable examples.	16	Applying	BTL-3	CO3
3	Analyze the various Risk Exposure Factors affecting software security.	16	Analyzing	BTL-4	CO3
4	Develop a summary on Risk Evaluation and Risk Mitigation strategies.	16	Applying	BTL-3	CO3
5	Analyze different Risk Assessment Techniques and compare their effectiveness.	16	Analyzing	BTL-4	CO3
6	Analyze qualitative and quantitative risk assessment methods.	16	Analyzing	BTL-4	CO3
7	Examine Threat Management and Vulnerability Management in detail.	16	Applying	BTL-3	CO3

8	Analyze the relationship between threats, vulnerabilities and risks.	16	Analyzing	BTL-4	CO3
9	Develop and Demonstrate various risk mitigation techniques for secure software systems.	16	Applying	BTL-3	CO3
10	Examine the effectiveness of vulnerability management in reducing security risks.	16	Applying	BTL-3	CO3
11	Analyze the importance of risk assessment in software security.	16	Analyzing	BTL-4	CO3
12	Analyze the role of risk profiling in information security.	16	Analyzing	BTL-4	CO3
13	Categorize Risk Management Life Cycle and Risk Assessment Techniques.	16	Analyzing	BTL-4	CO3
14	Examine about the Threat Management and Vulnerability Management with examples.	16	Applying	BTL-3	CO3
15	Examine Risk Exposure Factors and Risk Mitigation Strategies.	16	Applying	BTL-3	CO3
16	Analyze a comprehensive Risk Management Framework for a software organization.	16	Analyzing	BTL-4	CO3
17	Analyze the risks and write a suitable mitigation strategies for multiple security threats and vulnerabilities.	16	Analyzing	BTL-4	CO3

UNIT IV SECURITY TESTING

Traditional Software Testing – Comparison - Secure Software Development Life Cycle - Risk Based Security Testing – Prioritizing Security Testing With Threat Modeling – Penetration Testing– Planning and Scoping - Enumeration – Remote Exploitation – Web Application Exploitation - Exploits and Client Side Attacks – Post Exploitation – Bypassing Firewalls and Avoiding Detection- Tools for Penetration Testing

Part A					
Q.No	Questions	Marks	Competence	BT Level	CO
1	Define software testing.	2	Remembering	BTL-1	CO4
2	What is traditional software testing?	2	Remembering	BTL-1	CO4
3	What is secure software testing?	2	Remembering	BTL-1	CO4
4	Define Secure Software Development Life Cycle (SSDLC).	2	Remembering	BTL-1	CO4
5	What is risk-based security testing?	2	Remembering	BTL-1	CO4
6	What is threat modeling?	2	Remembering	BTL-1	CO4
7	What is penetration testing?	2	Remembering	BTL-1	CO4
8	What is planning in penetration testing?	2	Remembering	BTL-1	CO4
9	What is scoping in penetration testing?	2	Remembering	BTL-1	CO4
10	Define enumeration.	2	Remembering	BTL-1	CO4
11	What is remote exploitation?	2	Remembering	BTL-1	CO4
12	What is web application exploitation?	2	Remembering	BTL-1	CO4

13	What is an exploit?	2	Remembering	BTL-1	CO4
14	What is a client-side attack?	2	Remembering	BTL-1	CO4
15	What is post exploitation?	2	Remembering	BTL-1	CO4
16	What is firewall bypassing?	2	Remembering	BTL-1	CO4
17	What is intrusion detection avoidance?	2	Remembering	BTL-1	CO4
18	What is vulnerability scanning?	2	Remembering	BTL-1	CO4
19	Name any two penetration testing tools.	2	Remembering	BTL-1	CO4
20	What is Nmap?	2	Remembering	BTL-1	CO4
21	What is Metasploit Framework?	2	Remembering	BTL-1	CO4
22	Differentiate software testing and security testing.	2	Understanding	BTL-2	CO4
23	What is the purpose of security testing?	2	Understanding	BTL-2	CO4
24	List two benefits of penetration testing.	2	Understanding	BTL-2	CO4
Part B					
Q.No	Questions	Marks	Competence	BT Level	CO
1	Analyze about the Traditional Software Testing and Security Testing.	16	Analyzing	BTL-4	CO4
2	Demonstrate a Secure Software Development Life Cycle (SSDLC) with a neat diagram.	16	Applying	BTL-3	CO4
3	Analyze the Risk-Based Security Testing approach with suitable examples.	16	Analyzing	BTL-4	CO4
4	Describe the role of Threat Modeling in prioritizing security testing.	16	Applying	BTL-3	CO4
5	Develop the phases of Penetration Testing with examples.	16	Applying	BTL-3	CO4
6	Analyze the Planning and Scoping phase of Penetration Testing.	16	Analyzing	BTL-4	CO4
7	Examine Enumeration and Remote Exploitation techniques.	16	Applying	BTL-3	CO4
8	Analyze Web Application Exploitation and Client-Side Attacks.	16	Analyzing	BTL-4	CO4
9	Examine Post Exploitation techniques and Firewall Bypassing methods.	16	Applying	BTL-3	CO4
10	Discuss different Tools used for Penetration Testing.	16	Analyzing	BTL-4	CO4
11	Examine Exploits and Client-Side Attacks with examples.	16	Applying	BTL-3	CO4
12	Analyze methods for avoiding detection during penetration testing.	16	Analyzing	BTL-4	CO4
13	Demonstrate the principles of SSDLC and Risk-Based Security Testing.	16	Applying	BTL-3	CO4
14	Categorize Threat Modeling and Penetration Testing phases.	16	Analyzing	BTL-4	CO4
15	Examine Web Application Exploitation and Penetration Testing Tools.	16	Applying	BTL-3	CO4

16	Develop a comprehensive security testing strategy for a web application using SSDLC and Penetration Testing.	16	Applying	BTL-3	CO4
17	(i) Analyze about the penetration testing techniques.	8	Analyzing	BTL-4	CO4
	(ii) Discuss about an effective security testing plan.	8			

UNIT V SECURE PROJECT MANAGEMENT

Governance and security - Adopting an enterprise software security framework - Security and project management - Maturity of Practice.

Part A					
Q.No	Questions	Marks	Competence	BT Level	CO
1	Define governance in software security.	2	Remembering	BTL-1	CO5
2	What is software security governance?	2	Remembering	BTL-1	CO5
3	What is an enterprise software security framework?	2	Remembering	BTL-1	CO5
4	Define project management in software security.	2	Remembering	BTL-1	CO5
5	What is security project management?	2	Remembering	BTL-1	CO5
6	What is maturity of practice?	2	Remembering	BTL-1	CO5
7	List the levels of maturity of practice.	2	Remembering	BTL-1	CO5
8	What is a security policy?	2	Remembering	BTL-1	CO5
9	Define security governance framework.	2	Remembering	BTL-1	CO5
10	What is risk governance?	2	Remembering	BTL-1	CO5
11	What is security compliance?	2	Remembering	BTL-1	CO5
12	Define security metrics.	2	Remembering	BTL-1	CO5
13	What is security audit?	2	Remembering	BTL-1	CO5
14	What is security awareness?	2	Remembering	BTL-1	CO5
15	What is security culture?	2	Remembering	BTL-1	CO5
16	What is project governance?	2	Remembering	BTL-1	CO5
17	State the objectives of secure project management.	2	Remembering	BTL-1	CO5
18	Mention two benefits of enterprise software security framework.	2	Remembering	BTL-1	CO5
19	Differentiate governance and management.	2	Understanding	BTL-2	CO5
20	What is stakeholder management in security projects?	2	Understanding	BTL-2	CO5
21	What is security planning?	2	Understanding	BTL-2	CO5
22	What is continuous improvement?	2	Understanding	BTL-2	CO5
23	Mention two characteristics of a mature security practice.	2	Understanding	BTL-2	CO5

24	Why is governance important in software security?	2	Understanding	BTL-2	CO5
----	---	---	---------------	-------	-----

Part B					
Q.No	Questions	Marks	Competence	BT Level	CO
1	Analyze about governance and its role in software security.	16	Applying	BTL-3	CO5
2	Examine the process of adopting an enterprise software security framework.	16	Applying	BTL-3	CO5
3	Categorize the relationship between security and project management.	16	Analyzing	BTL-4	CO5
4	(i) Develop a governance framework for secure software project management.	8	Applying	BTL-3	CO5
	(ii) Discuss the concept of maturity of practice in software security.	8			
5	Analyze the benefits of implementing enterprise software security governance.	16	Analyzing	BTL-4	CO5
6	Describe the responsibilities of project managers in secure software development.	16	Applying	BTL-3	CO5
7	Analyze the key elements of security governance with suitable examples.	16	Analyzing	BTL-4	CO5
8	Examine different maturity models used in software security.	16	Applying	BTL-3	CO5
9	Discover the effectiveness of enterprise software security frameworks.	16	Analyzing	BTL-4	CO5
10	Examine the governance strategies for improving software security.	16	Applying	BTL-3	CO5
11	Apply the project management practices for secure software projects.	16	Applying	BTL-3	CO5
12	Analyze governance policies for secure software development.	16	Analyzing	BTL-4	CO5
13	Categorize enterprise software security framework and the maturity of practice.	16	Analyzing	BTL-4	CO5
14	Analyze governance and project management in software security.	16	Analyzing	BTL-4	CO5
15	Examine governance models and maturity models for software security.	16	Applying	BTL-3	CO5
16	Analyze about a comprehensive governance framework for secure software project management.	16	Analyzing	BTL-4	CO5
17	Categorize the characteristics of Initial, Repeatable, Defined, Managed, and Optimized maturity levels and explain how an organization can progress from one level to the next.	16	Analyzing	BTL-4	CO5

Staff Prepared By
[R.JEEVITHA]

HOD
[Dr.S.PARTHASARATHY]



