S/K/TY

Reg. No:

VIT
Vellore Institute of Technology

Final Assessment Test – November 2025

Course: BCSE320L - Web Application Security
Class NBR(s): 1452/1456/1457
Time: Three Hours
Slot: B1+TB1
Max. Marks: 100

- KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE
- DON'T WRITE ANYTHING ON THE QUESTION PAPER

COs	CO Statements
CO1	Understand security challenges and the need for Authentication and Authorization in web-based systems and applications.
CO2	Familiarize the Application Programming Interface analysis and vulnerability management of securing a web-based system.
CO3	Learn the web application hacking techniques and prevention solutions.
CO4	Apply the best practices of Secure Credentials, session management, and Security Automation in web applications.
CO5	Develop the best strategies to prevent XSS, CSRF, XXE, Injection, DOS attacks and Securing Third-Party Dependencies.

BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)

Answer ALL Questions
(10 X 10 = 100 Marks)

1.	Explain the concept of REST APIs in web application architecture. Discuss their role in enabling communication between client and server and identify common security risks associated with poorly secured APIs.	CO1	BL2
2.	A web developer is building a single-page application (SPA) using modern frameworks. Apply the concepts of authentication and authorization systems to ensure that secure access control is maintained throughout the application.	CO1	BL3
3.	An organization maintains several subdomains such as dev.example.com, test.example.com, and api.example.com. Evaluate how an attacker could exploit these using brute-force subdomain enumeration.	CO2	BL4
4.	An intern in a security firm wants to understand how APIs can reveal vulnerabilities in web systems. Explain how analyzing API endpoint shapes and discovery methods helps in evaluating the security risk of an exposed application programming interface.	CO2	BL2
5.	Analyze how detecting both client-side and server-side frameworks contributes to developing a comprehensive security strategy for a multi-layered healthcare web application.	CO2	BL4
6.	An e-commerce feedback portal is suspected to be vulnerable to Cross-Site Scripting (XSS). Make use of a systematic approach to discover and validate XSS vulnerabilities in this application.	CO3	BL3

7. ABC Bank wants to enable one-click money transfer functionality through its online portal. During a security review, you notice the application uses simple GET requests such as CO3 BL4

https://abc-bank.com/transfer?to=12345&amount=5000

Evaluate how an attacker could exploit this design to perform unauthorized transactions. Propose a comprehensive defense strategy involving anti-CSRF tokens, same-site cookies, and secure HTTP methods.

8. A healthcare web application allows users to upload XML files for importing patient data. During a security audit, it was discovered that the XML parser used in the backend is vulnerable to external entity references. As the security analyst, explain how both Direct XXE and Indirect XXE attacks could be exploited in this scenario, and discuss the potential impact these attacks might have on the backend server's confidentiality, availability, and integrity. CO5 BL4

9.a) Evaluate the behavior of the regular expression /^((pq)*)+$/ when validating different user inputs. Determine which of the following inputs are accepted or rejected by the expression and justify your reasoning based on regex evaluation rules: CO3 BL4

a) pqpqpqpqpqpqpqpqpqp
b) pqpqpqpqpqpqpqpqpqpqpqpq
c) pqpqpqpqpqpqpppqpqpqpqpqpq
d) pqpqpqpqpqpqpqpqpqpqpqpqpqpqpqpqp

Analyze how a typical backtracking regex engine processes these inputs, estimate the time complexity involved in matching them, and identify the potential Regular Expression Denial of Service (ReDoS) risk.

OR

9.b) A web application has been experiencing intermittent performance issues that you suspect are due to SQL Injection and Denial of Service (DoS) attacks. You do not have direct access to the application. Analyze network traffic logs and other indirect indicators to identify potential SQL Injection and DoS vulnerabilities. Evaluate the patterns that suggest these types of attacks and their potential impact on the application. CO3 BL4

10.a) Evaluate how a bug bounty program helps improve the overall security posture of an organization compared to traditional security audits. CO4 BL4

OR

10.b) ABC Healthcare wants to implement password reset functionality for its patient portal. Apply secure design principles to describe how password reset tokens should be generated, stored, and validated to prevent misuse and credential compromise. CO4 BL4

⇔⇔⇔ S/K/TY ⇔⇔⇔