VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering
Fall Semester 2024-25
CAT I

SLOT: D1+TD1

Programme Name & Branch: B.Tech. Computer Science and Engineering with Specialization in Information Security

Course Name & Code: Web Application Security - BCSE320L

Class Number (s): 1451/1449

Faculty Name (s): Dr.Arulkumar V, Dr.Natarajan P

Exam Duration: 90 Min. **Maximum Marks: 50**

General Instructions: Answer all the questions

Q. No.	Question	Max Marks
1.	A multistage login system requires the user's username first, followed by numerous other items in subsequent stages. If any of the provided items are invalid, the user is instantly directed to the first stage. What is wrong with this mechanism, and how can the vulnerability be addressed and how can you gather the information?	10
2.	YBC trading e-commerce website, hosted on an Apache web server, has been experiencing a sudden surge in traffic. However, the traffic seems suspicious, with many requests coming from unknown IP addresses. Upon further investigation, you notice that the requests are all targeting the same endpoint /login.php, and are attempting to submit login credentials. How you choose your web server and what web server security measure would you implement to mitigate this potential brute-force attack, and why?	10
3.	a) You are building a REST API for a social media platform to allow users to create, read, update, and delete (CRUD) their profile information. The API endpoint for updating a user's profile is /users/{userId}. Discuss how REST API works in this scenario (5 Marks) b) How SPA is ideal for modern internet-based applications? and compare them with legacy web. (5 Marks)	10
4.	a) You are a web administrator responsible for managing a domain (www.xbcbank.com) that hosts three separate web applications: - A blog at built using WordPress for customer forum. - An e-commerce platform built using Magento for transactions - A custom-built API for data store using Node.js. Discuss how this sub-domain works? And provide the sub-domain links for the above. (6 Marks) b) Infy Security administrator for an online banking platform that uses username and password authentication. Your security team has detected a surge in login attempts from a single IP address, with the attacker trying a large number of usernames and passwords in rapid succession. Discuss about the Dictionary attack and provides a solution for the above scenario? (4 Marks)	10
5.	Penetration tester tasked with assessing the security of a web application. During your reconnaissance phase, you visit the website and view the page source. You notice the following HTML comment: *<!-- Built with React, powered by Node.js and Express -->* You also observe the following HTTP response headers: *X-Powered-By: Express* *Content-Type: application/json; charset=utf-8* Based on the above information, what can you infer about the client-side and server-side frameworks used by this web application?	10