JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATION- 2024

B.Tech-3 Semester (CSE/IT)

COURSE CODE (CREDITS): 24B11CI312 (3) MAX. MARKS: 25

COURSE NAME: Information and Cyber Security Foundation

COURSE INSTRUCTORS: Mr. Aayush Sharma MAX. TIME: 1 Hour30 Minutes

Note:*(a)All questions are compulsory.*

(b) The candidate is allowed to make Suitable numeric assumptions wherever required for solving problems

Q.No	Question	CO	Marks
Q1	a) Analyze the differences between the OSI and TCP models, focusing on their respective layers. How does the collapse of layers in the TCP model affect network design and communication? b) A user is sending a 2000-byte message using the TCP/IP model. Given that the Maximum Segment Size (MSS) is 512 bytes, how many TCP segments will be required to transmit the message, assuming no additional headers are considered?	[CO-1] [CO-2]	[5]
Q2	Below is a code for a flask app connected to a front end which contains the Javascript code:	[CO-2] [CO-3]	[5]

```
from flask import Flask, request, jsonify
import sqlite3

app = Flask(__name__)

def get_db_connection():
    conn = sqlite3.connect('example.db')
    conn.row_factory = sqlite3.Row
    return conn

@app.route('/user', methods=['GET'])
def get_user():
    user_id = request.args.get('id')

    conn = get_db_connection()

    query = f"SELECT * FROM users
WHERE id = {user_id};"

    cursor = conn.execute(query)
    user = cursor.fetchone()
    conn.close()

    if user:
        return jsonify(dict(user))
```

```
<script>
document.getElementById('searchBtn').add
EventListener('click', function() {
        const userId =
document.getElementById('userId').value;
 fetch(`/user?id=${userId}`)
.then(response => response.json())
.then(data => {
            if (data.error) {
document.getElementById('result').innerHT
ML = 'Error: ' + data.error;
            }
else {
document.getElementById('result').innerHT
ML = 'User: ' + JSON.stringify(data);
    }
        });
    });
</script>
```

	else: **return** jsonify({"error": "User not found"}), 404 **if __name__ == '__main__':** app.run(debug=True) Based on the above answer the following: **a)** What is SQL injection, and where does it occur in the given Flask. app? **b)** Explain how cross-site scripting (XSS) can be exploited in the JavaScript front-end of the provided code. **c)** Evaluate the current architecture of the Flask and JavaScript application. Propose a redesign or security improvements to mitigate both SQL injection and XSS vulnerabilities, considering best practices in web security.			
Q3	Analyze the potential impact of both the SQL injection and XSS vulnerabilities. How could an attacker exploit these to compromise the application, and what are the consequences?		**[CO-3]**	**[5]**
Q4	a) What is the Burp Suite and why is it used? b) Explain how the Repeater tool helps in testing web application vulnerabilities like SQL injection or cross-site scripting (XSS). c) In Burp Suite's Repeater, after testing an input field, you receive different responses when sending a certain payload. Analyze the possible reasons why this variation in response occurs and how you would investigate further using the tool. d) What is the role of the Proxy tool in Burp Suite? e) In a captured request, you notice that a URL parameter is encoded. Evaluate how the Burp Suite Decoder tool can help you understand the encoded value and propose a way to manipulate it for further testing.		**[CO-2]** **[CO-3]** **[CO-4]**	**[5]**
Q5	a) You suspect that someone on your network is using an unencrypted protocol like FTP to transfer sensitive data. Describe how you would use Wireshark to detect and capture this traffic. b) A network administrator is using Wireshark to investigate a potential security breach. Evaluate the effectiveness of Wireshark in detecting the following attacks: Man-in-the-Middle (MITM) such as DHCP spoofing or ARP poisoning, Distributed Denial of Service (DDoS). c) How will you use wireshark to eavesdrop on phone calls on occurring on the network?		**[CO-2]** **[CO-3]**	**[5]**