Question Bank
Web and Mobile Security (20CST-333)

Short Answer Type(2 Marks)

1. Who are more knowledgeable hackers and why?
2. Who are green hat hackers?
3. What is DMZ?
4. What is the use of CAPTCHA?
5. Define blue-bugging.
6. What do you mean by blue-snarfing.
7. How blue-jacking is done?
8. What are different types of captcha?
9. What is dictionary attack?
10. Define ping of death attack.
11. Define directory traversal attack.
12. How buffer overflow is used to perform malicious activities?
13. Explain SIM/UICC Security.
14. What is browser exploit?
15. What are canonicalization attacks?
16. What are basic security and cryptographic techniques?
17. Discuss the advantages and disadvantages of Mesh topology.
18. Define security misconfiguration.
19. What is Bluetooth security?
20. Write down the advantages and disadvantages of bus topology.
21. Write down the advantages and disadvantages of star topology.
22. Define X-path injection attack.

Long Answer Types(5 Marks, 10 Marks)

1. Explain different session hijacking and fixation techniques. How session hijacking is done?
2. Explain GSM security network and its security algorithms.
3. How input injection attack is performed? Explain all methods.
4. How client side scripts help to execute any web application?
5. Explain different ways to perform session hijacking. How is it mitigated?
6. Explain network topologies along with advantages and disadvantages.

7. How android and IOS security is maintained? Explain with their layer architecture.

8. Explain Creaser cipher with an example.

9. Explain encryption and decryption process of Monoalphabetic cipher with an example

10. Discuss polyalphabetic algorithm with example.

11. What types of attacks are performed on remote server? Explain each with their countermeasures.

12. Explain the working of CAPTCHA program.

13. Differentiate between Window and Linux.

14. Explain security measures of WI-FI attacks.

15. How SQL injection is performed? Explain methods and solutions.

16. How HTML injection is performed? Explain methods and solutions.

17. How CSS and CSRF are performed? Explain methods and solutions.

18. Explain different types of mobile malwares and security practices.

19. What types of attacks are performed through Bluetooth connection? Explain.

20. Explain Attacks and countermeasures for common web authentication.

21. What attacks are performed on VoIP? How is it made secure? Explain.

22. Elaborate the countermeasures or mitigations for SQL INJECTION attack.

23. Discuss the countermeasures or mitigations for wifi attack.

24. How VPN is used to provide security in public network? Explain.

25. How hashing is different from encryption? Explain.

26. Explain the working process of session hijacking using Burpsuite.

27. Discuss the working of Digital Signatures.

28. What security practices are applied to keep your Mobile phone safe?

29. Why IOS is more secure than android? Explain.

30. Explain the security countermeasures for Android and IOS.

31. How to ensure security of window phone?

32. Explain the following in detail(types, methods and solutions):

    a) Wi-fi Security

       b)   ASP.net and PHP attacks

       c)   Apache and IIS server attacks

d)   Admin misconfiguration attack

e)   Security of Mobile VoIP Communications.

33.   Elaborate following: (methods and mitigations)

a) LTE network security

b)   Stealth-encoding techniques

c) Emerging Trends in Mobile Security-Mobile Geo-location

d) XSS Attack

e)   XML injection attacks