2M, 4M and 8M questions are required?

Q.1	Solve any Six out of Eight?	**12Marks**	**2 marks each**
Q.2	Solve any Four out of Six?	**16 Marks**	**4 marks each**
Q.3	Solve any Four out of Six?	**16 Marks**	**4 marks each**
	OR		
Q.3	Solve any Two out of Three?	**16 Marks**	**8 marks each**
Q.4	Solve any Two out of Three?	**16 Marks**	**8 marks each**

2 Marks questions:

1. List the different application and explain anyone with example?
2. Explain with example Application Entry Points?
3. Describe the history of software security?
4. **Describe Active Reconnaissance and Passive Reconnaissance?**
5. **Explain** Automated Enigma Code Cracking?
6. **List and explain the categorization of various web application?**
7. What is Web application reconnaissance?
8. How you can secure modern web application?
9. How to test again the XSS? Explain with example?
10. Write short note on the comprehensive cod review?
11. Explain the 1) Vulnerability Discovery 2) Vulnerability Analysis?
12. What is regression testing?
13. Explain the feature requirement for loan application?
14. What is responsible disclosure program?
15. Explain the third-party penetration testing?
16. Enlist the ways to test the application included in responsible disclosure program?
17. List and draw penetration testing stages?
18. What is in-house and out-house penetration testing?
19. What is Blind and Double-Blind Penetration test?
20. Define the following
    Security Risk
    Vulnerability
21. Explain the CIA with respect to security?
22. Explain the secure software development technique?
23. Write short notes on evaluation of information security?
24. What are the unique characteristics of android?
25. What is android application sandbox?
26. Draw the android data storage model?
27. List the android component?
28. Draw the diagram of android activity and back stack?

29. Draw the Android data storage threat model?
30. Define confidentially and authentication with example?
31. Explain the encryption of data?
32. Describe the input validation type reject-known -bad?
33. Describe “SSL/TLS: The Industry Standard”?

4 Marks questions:

1. Classify and explain information gathering categorizes?
2. Explain how you find subdomain with example?
3. How you can use the search engine caches information gathering of target?
4. Describe the Hidden Manipulation with example?
5. ow you can discover vulnerability for web application of bank?
6. Illustrate Archetypical Vulnerabilities Versus Custom Logic Bugs?
7. How you decide where to start a security review?
8. Explain blacklists with example?
9. Write short note on secure coding antipattern?
10. Explain the Vulnerability management Lifecycle?
11. Illustrate the Dynamic and static analysis in vulnerability discovery?
12. Give note on cross site scripting. What are the types of cross site scripting?
13. Explain the CVSS base scoring?
14. Explain temporal scoring in CVSS?
15. Explain environmental scoring in CVSS?
16. Write short notes on HTML-entity encoding?
17. Explain the Security Risk = Vulnerability + Threat + Consequences with example?
18. Explain the Linux security model?
19. How files being isolated in android?
20. Explain the process design with example?
21. How do you generate a self-signed certificate for signing your Android application?
22. Explain the OWASP mobile top ten risks?
23. What is Intent? Intercomponent Signaling of component?
24. Explain the attacks associated with Android application components?
25. Illustrate the android activity and back stack with example?
26. Explain the services and the two forms of it with example?
27. Write a code to setup the connection using HTTP over SSL/TLS?
28. Explain Authentication of the Entities?
29. Explain the method 1) getCipherSuite () 2) getServerCertificates ()
30. Explain the hostname verification feature of SSL/TLS?
31. What Is the SSL/TLS Handshake?
32. How to fix SSL/TLS handshake failed error?

8 Marks questions:

1. How would you classify the attack type through user input if the code is not sanitized?

2. Explain Reflective XSS with example?
3. Describe the parameter tempering with example?
4. Explain the following Web Application Security Threats?
   Hidden Manipulation
   Parameter Tampering
   Cross-Site Scripting
   Buffer Overflow

5. Give the CVSS for following scenario:
   Vulnerability: -A vulnerability in the MySQL Server database could allow a remote, authenticated user to inject SQL code that MySQL replication functionality would run with high privileges. A successful attack could allow any data in a remote MySQL database to be read or modified.
   Attack: - An attacker requires an account on the target MySQL database with the privilege to modify user-supplied identifiers, such as table names. The account must be on a database which is being replicated to one or more other MySQL databases. An attack consists of logging in using the account and modifying an identifier to a new value that contains a quote character and a fragment of malicious SQL. This SQL will later be executed as a highly privileged user on the remote system(s). The malicious SQL is injected into SQL statements that are part of the replication functionality, preventing the attacker from executing arbitrary SQL statements.

6. Let's assume you want to allow the creation of JavaScript buttons that link to a page

   sourced from user input:

```
<button onclick="goToLink ()">click me</button>
const userLink = "<script>alert('hi')</script>";
const goToLink = function () {
window.location.href = `https://mywebsite.com/${userLink}`;
// goes to: https://my-website.com/<script>alert('hi')</script>
};
```

   With respect to this code how you would sanitize the hyperlink?

1. How android app stores the data? explain the two ways used to stores the data?
2. Explain with example android file system isolation?
3. Explain the attacks associated with Android application components?
4. How to store data locally in an Android app? Explain?
5. How to Generate a CSR code for Android apps?
6. Explain the APK Signing scheme?
7. How Can Android Smart Lock Be Attacked?
8. How to store data locally in an Android app? Explain?
9. How to store data locally in an Android app? Explain?
10. Discuss in detail about content providers?
11. Illustrate the principle of least privileges with example?
12. "An alternative approach to specifying the flags in an Intent is to explicitly grant a specific app permission on a Content Provider URI" explain with example?

13. Describe “Using Hostname Verifier for Other Purposes” with example?
14. Web application developers need to be extremely concerned about proper input validation because malicious input that you fail to catch can lead to dangerous vulnerabilities such as SQL injection Justify with example?
15. Write notes on 1) Authentication of entities 2) Encryption of data
16. “A SQL statement should never be formed by concatenating command and data together” Justify with example?