1. Which of the following Best describes a 'website' 
   a. A target or landing page for a URL. 
   b. An HTML page with lots of external links. 
   c. A set of related web-pages stored under a single domain. 
   d. A page that run online application

   c

2. OWASP stands for 
   a. Open Web Association Security Protocol 
   b. Only Web Association Security Principle 
   c. Open Web Application Security Project 
   d. Open Web Access Security Protocol 

   c

3. True or False: 
   To reduce the Logical Vulnerabilities of a web application we would often need design/architectural changes 

   True.

4. Name the Penetration testing tool for finding application vulnerabilities from OWASP 
   a. Zed Attack Proxy 
   b. Enterprise Security API 
   c. Security Shepherd 
   d. STRIDE 

   a

5. An application from OWASP for educating on web and mobile application security 
   a. Zed Attack Proxy 
   b. Enterprise Security API 
   c. Security Shepherd 
   d. STRIDE 

   c

6. Which of the following is a popular Web application risks? 
   a. Cross site Scripting 
   b. HTTPS Protocol 
   c. Hacker code 
   d. none of these 

   a

7 SDLC 
   a. Secure Development Life Cycle 
   b. Software Development Lifecycle
   c. Security Deployment Lifecycle 
   d. Software Deployment Livecycle 

   b
8. When a web application is vulnerable to an SQL injection, but does not return error messages, it may still be susceptible to

a. SQL Injection  
b. Blind SQL Injection  
c. URL Injection  
d. OS Command Injection

b

9. An attacker submits hostile data through a Web page that stores it in a file, database, or other data store, and depends on some other Web page or mid-tier application to use that hostile data in the construction of a SQL statement.

a. Second-order SQL injection  
b. SQL Injection  
c. Blind SQL Injection  
d. OS Command Injection

a

10. SQL Injection affects

a. Confidentiality  
b. Integrity  
c. Availability  
d. All of the above

d

11. For preventing CRSF we should use

a. GET method  
b. POST method  
c. TRACK method  
d. OPTIONS method

b

12. SSL stands for

a. Service Security Level  
b. Secure Software Layer  
c. Secure Socket Layer  
d. Service Software Language

c

13. CGI stands for

a. Common Gateway Interface  
b. Communication Gateway Interface  
c. Communication Gateway Information
d. Common Gateway Information

14. Which of the following is true for APT (Advanced persistent threat)
   a. APT often target a single organization
   b. APT is often fueled by business and political motives
   c. The operators continuously monitor the interaction in order to achieve the defined objective
   d. The APT targets only government assets

   a, b, c

15. Which of the following factors contribute to risk rating to the security of the system?
    choose many
    a. The overall prevalence of Vulnerability
    b. The easiness of Detecting the Vulnerability
    c. The technical impact of the threat
    d. The Asset Value

   a, b, c, d

16. The method of executing system level commands through a vulnerable application?
   a. SQL injection
   b. Admin Hacking
   c. Missing Authorization
   d. OS Command Injection

   d

17. When access control checks are incorrectly applied, users are able to access data or perform actions that they should not be allowed to perform. This method is called
   a. Invalid Authorization
   b. Missing Authorization
   c. Non existent Authorization
   d. Incorrect Authorization

   d

18. Pick up the safe way to retrieve a password, among the ways given below?
   a. Ask the customers phone number and message the password to the phone
   b. Ask for registered username and give link for password reset on screen
   c. Ask for registered email or phone and verify if database before giving the link for password reset on screen
   d. Ask for username and sent the password link to the registered email-id or registered phone

   d

19. Name the risk a web application possess when it does not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.
a. Cross-Site Request Forgery (CSRF)
b. SQL injection
c. Missing Authorization
d. Unrestricted Upload of File with Dangerous Type

20. Pick out the strongest password from the given lot
a. password
b. asdfg12345
c. P@33W@d
d. xk3dCOmI@s

d pick-up a password whose size is larger than 8 characters. The passwords should contain alphanumeric and special characters.

21. Pick out the information that should be leaked to user upon some error?
a. Stacktrace
b. The failed SQL Query
c. A failed Authorization
d. Database Schema Details

c

22. Choose the practices that would prevent information leakage from a web app?
a. Remove comments from HTML and JavaScript pages
b. Displaying a custom error message
c. Make sure that different error handling mechanism returns at roughly same time.
d. All of the Above

d

23. Which one of the following is an Open source DBMS?
a. Oracle Database
b. Microsoft SQL Server
c. MySQL
d. SAP Sybase

c

24. Pick out the WRONG statement
a. In HTTP, Credentials of the user need to be send on every Request
b. SSL/TLS can be used to encrypt credentials to prevent man in middle attack
c. HTTP is applicable at the transport layer in OSI Model.
d. None of the Above

c

25. What can we say about the prevalence of Cross-Site Scripting according to OWASP 2013 list?
a. Average
b. Rare
26. Verifying user authorization to access target object will help to protect against
a. XSS
b. Security misconfiguration
c. Insecure Direct Object Reference
d. injection

c
27. From the options choose measures that we can take to prevent Sensitive Data Exposure?
a. Discarding/Deleting Sensitive data as soon as possible
b. Disabling auto-complete on forms collecting sensitive data
c. Use of weak Cryptographic algorithm without proper key management
d. Data stored in plain text for long time

c
28. True or False : If your web application has XSS holes(vulnerabilities) other applications in host computer is susceptible to CSRF? True.

29. Pick out the WRONG statement about HeartBleed from the following
a. Heartbleed is a security bug in OpenSSL implementation
b. The memory buffer for the return message is allocated based on length field in requesting message
c. Heartbleed could be used to expose the machine for future attacks by exposing sensitive data
d. Heartbleed is an extension of TLS protocol

d
30. True or False: Non-validated Forwards could facilitate phishing : True.

31. The Software Assurance Maturity Model framework from OWASP would help in
a. Evaluating an organization's existing software security practices
b. Building a balanced software security assurance program in well-defined iterations
c. Defining and measuring security-related activities throughout an organization
d. all of these
e. none of these
d

32. Choose the costs associated with code review 1 in SAMM? choose many?
a. Build out or license of code review checklists
b. Ongoing project overhead from code review activities of high-risk code
c. Research and selection of code analysis solution
d. Initial cost and maintenance of automation integration

a,b
33. In Threat Modelling Tool, pick out the shape used to represent the collection of Sub processes
   a. rectangle
   b. Oval
   c. Double Oval
   d. Triangle
   c

34. From STRIDE threats, which one of the following is a Threat to Integrity?
   a. Spoofing
   b. Tampering
   c. Repudiation
   d. Denial of Service
   b

35. An unskilled attacker who uses code developed by others for attacking a system?
   a. man-in-middle
   b. Borrower
   c. Script Kiddie
   d. None of the above
   c

36. WinNuke is a popular example of?
   a. Spoofing
   b. Tampering
   c. Repudiation
   d. Denial of Service
   d

37. Pick out True statements about Directory Enumeration attack?
   a. Its aimed at finding the directory structure of our website
   b. Attack can be preformed manually
   c. Proper Implementation of Authorization can prevent the attack
   d. All of the Above
   d

38. See the change given below and identify the threat the attacker is trying to exploit?
   Assume attackers userID is 1
   original URL: http://vunerableSite.com/accountInfo?LoggedIn=True&userID=1
   changed URL: http://vunerableSite.com/accountInfo?LoggedIn=True&userID=2
   a. XSS
   b. Security misconfiguration
39. The Internet socket port number used for HTTPS communication
a. 43
b. 343
c. 443
d. 143

40. Pick out the WRONG statement?
a. UDP is a connectionless protocol.
b. TCP is suited for applications that require high reliability.
c. HTTPS uses UDP at Transport Layer
d. UDP has smaller overhead compared to TCP