Lecture 6

---

1. Finding a way to send text to a web application or browser that is interpreted as a command or cod
    a. CSRF
    b. Injection
    c. Parameterized object

2. Attacker sends simple text-based attacks that exploit the syntax of the targeted interpreter.
    a. CSRF
    b. Injection
    c. Parameterized statement

3. How to Avoid SQL injection
    a. Minimize Database privileges
    b. uses interfaces that support binding
    c. Encode all user inputs before sent it to the interpreter
    d. Always perform 'white list' input validation on all user supplied input
    e. All

4. Programming languages talk to SQL databases using
    a. Database Driver
    b. Database server
    c. Database tables

5. make sure that the parameters (i.e. inputs) passed into SQL statements are treated in a safe manner
    a. [Type an answer here]
    b. CSRF

c. Injection

d. Parameterized statement

6. Attacker uses leaks or flaws in the authentication or session management functions (e.g., exposed accounts, passwords, session IDs) to impersonate users

   a. Broken Authentication and Session management

   b. CSRF

   c. BOTH

7. Sessions can be implemented with

   a. Cookies

   b. URL Rewrite

   c. Both

8. involves placing a session id in the URL

   a. Cookies

   b. URL Rewrite

   c. Both

use $GET method

9. the use of lists of known passwords,

   a. Session time out

   b. Credential stuffing

   c. Non

10. A user uses a public computer to access an application. Instead of selecting "logout" the user simply closes the browser tab and walks away

    a. Session time out

    b. Credential stuffing

    c. Non

11. automated injection of breached username/password pairs in order to fraudulently gain access to user accounts. This is a subset of the brute force

    a. Session time out

    b. Credential stuffing

    c. Non

12. Avoiding Broken Authentication and Session Management

    a. Verify Architecture

    b. Verify implementation

    c. Both

13. Authentication should be simple, centralized, and standardized to avoid Broken Authentication

    a. true

    b. false

14. Attacker sends text-based attack scripts that exploit the interpreter in the browser

    a. XSS

    b. CSRF

    c. SSLR

15. are those in which attackers inject malicious code ,usually client-side scripts,

    a. XSS

    b. CSRF

    c. SSLR

16. To avoid Client XSS, the preferred option is to avoid passing untrusted data to JavaScript and other browser APIs that can generate active conten

    a. true

    b. false

17. Safe ways to represent dangerous characters in a web page

    a. <
    b. >
    c. both

18. A security principle that restricts how a document or script loaded from one origin can interact with a resource from another origin

    a. XSS
    b. Same Origin Policy
    c. non

19. The purpose of the same-origin policy is to prevent scripts from accessing malicious content. Without the same-origin policy

    a. XSS
    b. Same Origin Policy
    c. non

20. Page have the same origin must have

    a. Same Port
    b. same protocol
    c. same host

21. is a W3C spec that allows crossdomain communication from the browser. By building on top of the XMLHttpRequest object, CORS allows developers to work with the same idioms as same-domain requests.

    a. XSS
    b. Same Origin Policy
    c. CORS

22. attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable موقع ثغرات به web application

    a. XSS

b. CORS cross origin resource sharing --> domains

c. CSRF cross site request forgery

23. Occurs when an authenticated user unknowingly initiates a request

    a. XSS

    b. CORS

    c. CSRF

24. XSS facilitates CSRF via

    a. SQL injection

    b. Link injection

    c. non

25. parameters are sent in the URL itself

    a. post

    b. Get

26. : parameters are sent in the request body

    a. post

    b. Get

27. DO NOT use GET for anything that changes the server state or contains sensitive information

    a. true

    b. false

    c. [Type an answer here]

28. use POST for every action that changes the server state and reject all non-POST methods

    a. true

    b. false

29. Attacker accesses default accounts, unused pages, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the system.
    a. XSS
    b. CORS
    c. Security misconfiguration

30. files are the first place hackers look
    a. style.css
    b. Robots.txt
    c. vvv

31. web accessible and contains URLs you don't want indexed by a search engine. This might be the kind of data hackers want
    a. style.css
    b. Robots.txt
    c. vvv

32. Uses Google search engine and advanced query abilities to find insecure data files and misconfigured/unpatched servers indexed on the Web
    a. [Type an answer here]
    b. Google hacking
    c. Design Hacking

33. Try to force directory browsing by eliminating anything past the various "/"
    a. CSRF
    b. forced Directory Browsing
    c. XSS

34. – Keep up with updates for ALL components can avoid
    a. non
    b. Security Misconfiguration

c. style.css

35. tricking a Web user into clicking on something different

    a. Click Jacking

    b. CSRF

    c. XSS

36. takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function

    a. CSRF

    b. Click Jacking

    c. XSS

37. techniques for preventing framing by the framed site.

    a. Design fading

    b. frame busting

    c. Html busting

38.