CSH6 CH 21 REVIEW QUESTIONS

1. Hackers today often concentrate their attacks on targets that ___
2. Cookies are usually discussed in connection with client-side risks. Why are cookies also viewed as threats to the security of a Website?
3. Enterprise Java Beans, CORBA, DCOM/COM services are foundations specifically for ___
4. What does the acronym MIMA (or MITMA) mean in discussions of Website security?
5. How can embedded user identifiers (e.g., in an unsubscribe link) be abused?
6. Relying on hidden fields on a Web page is a security risk because ___
7. Databases used in Web applications must be protected by ___
8. One of the methods for interfering with pharming is the use of ___
9. In discussions of information security, the acronym SSL stands for ___
10. A hacker introduces a very long string into a field on a Web form; the string loads program instructions into the stack for execution of unauthorized functions. This attack is best described as ___
11. Particular attention to access controls over ____ can maintain the security of Web servers.
12. One of the key tools for vulnerability analysis of a Website is ___
13. In coding HTML on a Web server, ___ are best kept to a minimum to reduce security risks.
14. Hackers often test systems they are evaluating for attacks ___
15. What does CORBA mean in discussions of Website development?
16. Which of the following methods is/are used for illegal access to Websites by attackers?
17. The Secure Electronic Transaction (SET) protocol uses ___ to protect credit-card information from access by a merchant.
18. What is the acronym for the transfer protocol using SSL in Web communications?
19. [A] major source[s] of client-side security risks is [are] ___
20. A serious danger for Web security is ___
21. Platform security measures include(s) ___
22. The de facto protocol for protecting confidential data in transit from a user to a Web server is ___
23. Web servers often use which of the following tools for the middleware that responds to user requests?
24. What does the acronym CGI mean in connection with Websites?
25. Certificates are granted to legitimate Websites by a(n) ___
26. The authors of Chapter 21 of the CSH6 strongly discourage which of the following activities?

27. If an attacker discovers a way of activating the code that accesses secured information without passing through the normal user-authentication processes, the attack can be called ___
28. Which of the following languages is/are most often used for generating CGI and PHP scripts?
29. Some malicious software funning on the client side of Web transactions funnels information about the user to servers without authorization. This kind of malware is called ___
30. One of the frequent vulnerabilities introduced by poor program design is ___
31. For improved security, data in databases used in Web applications should be ___
32. Site managers can set up dummy targets to attract attacks by hackers; these dummy targets are called ___
33. A good way of preventing attacks based on SSIs is to ___
34. Every CGI script on a Web server must ___
35. A solid foundation for effective Website security includes ___
36. Which of the following Website safeguards is/are recommended in Chapter 21 of the CSH6?