QUESTIONS

1. Which of the following is used to disable file extensions in Apache servers?
   - **A.** disable_FS
   - **B.** mod_negotiation
   - **C.** stop_files
   - **D.** httpd.conf
2. You are examining connection logs from a client machine and come across this entry:

   http://www.business123.com/../../../../../Windows/system.ini

   Which attack does this most likely indicate?
   - **A.** Parameter manipulation
   - **B.** XSS
   - **C.** SQL injection
   - **D.** Directory traversal
3. A hacker is looking at a publicly facing web front end. One of the pages provides an entry box with the heading "Forgot password? Enter your e-mail address." In the entry, he types **anything' OR '1'='1**.

   A message appears stating "Your login information has been sent to a_username@emailaddress.target.com."

   Which of the following is true?
   - **A.** The cross-site scripting attempt has succeeded.
   - **B.** The SQL injection attempt has succeeded.
   - **C.** The parameter tampering has succeeded.
   - **D.** The buffer overflow attempt has succeeded.
4. Which of the following uses HTML entities properly to represent <script>?
   - **A.** <script>
   - **B.** (script)
   - **C.** &script&
   - **D.** "script"
5. A pen tester is examining a web front end on a target network. The page displays a Search text box form entry, allowing the user to search for items on the site. Instead of entering a search text string, the tester enters the following:

   <script> function myFunction() { alert("It worked!"); } </script>

After the tester clicks the Search button beside the entry box, a pop-up appears stating "It Worked." Which of the following is true regarding this attempt?

A. The site is vulnerable to XSS.

B. Coding on the site is poor, and a buffer overflow attack may result in a DoS.

C. The attacker's next entry in the Search box should be **' OR '1'='1**.

D. This is expected behavior on properly configured sites.

6. Which of the following is used by SOAP services to format information?

A. Unicode

B. HTML entities

C. NTFS

D. XML

7. A security administrator is called for advice. The sales staff has noticed a large number of orders being filled at prices far below those posted on the site. After some research, it does not appear that the web server or the underlying SQL database has been directly compromised. Next, the security administrator reviews the IDS logs and finds nothing unusual. Additionally, the local logs on the server itself do not show anything indicating a problem. Which of the following is the most likely explanation for the false orders?

A. The website uses hidden fields for price values, which have been altered by the attacker.

B. SQL injection has been used to update pricing in the database. After the order was placed, pricing was reset to normal, to cover tracks.

C. Server-side scripting was used to alter the price.

D. A tool such as Metasploit was used to carry out the attack.

8. Which of the following is a common SOA vulnerability?

A. SQL injection

B. XSS

C. XML denial of service

D. CGI manipulation

9. The source code of software used by your client seems to have a large number of gets() alongside sparsely used fgets(). What kind of attack is this software potentially susceptible to?

A. SQL injection

B. Buffer overflow

C. Parameter tampering

D. Cookie manipulation

10. Which code entry will stop input at 100 characters?
    - **A.** if (I > 100) then exit (1)
    - **B.** if (I >= 100) then exit (1)
    - **C.** if (I <= 100) then exit (1)
    - **D.** if (I < 100) then exit (1)
11. You are examining log files and come across this URL:

    http://www.example.com/script.ext?template%2e%2e%2e%2e%2e%2f%2e%2f%65%74%63%2f%70%61%73%73%77%64

    Which of the following best describes this potential attack?
    - **A.** This is not an attack but a return of SSL handshakes.
    - **B.** An attacker appears to be using Unicode.
    - **C.** This appears to be a buffer overflow attempt.
    - **D.** This appears to be an XSS attempt.
12. Which of the following tools can be used to clone a copy of a website to your machine, to be scrutinized later?
    - **A.** BurpSuite
    - **B.** NetCraft
    - **C.** HttpRecon
    - **D.** BlackWidow
13. Which character is your best option in testing for SQL injection vulnerability?
    - **A.** The @ symbol
    - **B.** A double dash
    - **C.** The + sign
    - **D.** A single quote
14. An angry former employee of the organization discovers a web form vulnerable to SQL injection. Using the injection string SELECT * FROM Orders_Pend WHERE Location_City = 'Orlando', he is able to see all pending orders from Orlando. If he wanted to delete the Orders_Pend table altogether, which SQL injection string should be used?
    - **A.** SELECT * FROM Orders_Pend WHERE Location_City = Orlando';DROP TABLE Orders_Pend --
    - **B.** SELECT * FROM Orders_Pend WHERE 'Orlando';DROP_TABLE --
    - **C.** DROP TABLE Orders_Pend WHERE 'Orlando = 1' --
    - **D.** WHERE Location_City = Orlando'1 = 1': DROP_TABLE --

15. Efforts to gain information from a target website have produced the following error message:

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e08'
[Microsoft]{OBDC SQL Server Driver}
```

Which of the following best describes the error message?

A. The site may be vulnerable to XSS.

B. The site may be vulnerable to buffer overflow.

C. The site may be vulnerable to SQL injection.

D. The site may be vulnerable to a malware injection.

16. Which buffer overflow attack is designed to make use of memory that remains in use while a program is running?

A. Stack

B. Heap

C. Active

D. Permanent

17. Which of the following is a standard method for web servers to pass a user's request to an application and receive data back to forward to the user?

A. SSI

B. SSL

C. CGI

D. CSI

18. An attacker performs a SQL injection attack but receives nothing in return. She then proceeds to send multiple SQL queries, soliciting TRUE or FALSE responses. Which attack is being carried out?

A. Blind SQL injection

B. SQL denial of service

C. SQL code manipulation

D. SQL replay

19. Which of the following can be used for remote password cracking of web servers? (Choose all that apply.)

A. Brutus

B. Nikto

C. THC-Hydra

D. Nessus

20. An attacker is attempting to elevate privileges on a machine by using Java or other functions, through nonvalidated input, to cause the server to execute a malicious piece of code and provide command-line access. Which of the following best describes this action?

    A. Shell injection

    B. File injection

    C. SQL injection

    D. URL injection

21. An attacker is successful in replaying a secure cookie, stolen during an XSS attack, even during an invalid session on the server. How is this possible?

    A. A cookie can be replayed at any time, no matter the circumstances.

    B. Encryption was accomplished at the application layer, using a single key.

    C. Authentication was accomplished using XML.

    D. Encryption was accomplished at the network layer.

22. HTML forms include several methods for transferring data back and forth. Inside a form, which of the following encodes the input into the Uniform Resource Identifier (URI)?

    A. HEAD

    B. PUT

    C. GET

    D. POST

23. An attacker is looking at a target website and is viewing an account from the store on URL http://www.anybiz.com/store.php?id=2. He next enters the following URL:

    http://www.anybiz.com/store.php?id=2 and 1=1

    The web page loads normally. He then enters the following URL:

    http://www.anybiz.com/store.php?id=2 and 1=2

    A generic page noting "An error has occurred" appears.

    Which of the following is a correct statement concerning these actions?

    A. The site is vulnerable to cross-site scripting.

    B. The site is vulnerable to blind SQL injection.

    C. The site is vulnerable to buffer overflows.

    D. The site is not vulnerable to SQL injection.

24. Which of the following is the hexadecimal value of a NOP instruction?

    A. 0x60

    B. 0x70

    C. 0x80

    D. 0x90

25. An attacker is viewing a blog entry showing a news story and asking for comments. In the comment field, the attacker enters the following:

```
Nice post and a fun read
<script>onload=window.location='http://www.badsite.com'</script>
```

    What is the attacker attempting to perform?

    A. A SQL injection attack against the blog's underlying database

    B. A cross-site scripting attack

    C. A buffer overflow DoS attack

    D. A file injection DoS attack

26. An attacker attempts to manipulate an application by advancing the instruction pointer with a long run of instructions containing no action. What is this attack called?

    A. File injection

    B. Stack flipping

    C. NOP-sled

    D. Heap based

27. You are examining website files and find the following text file:

```
# robots.txt for http://www.anybiz.com/
User-agent: Googlebot
Disallow: /tmp/
User-agent: *
Disallow: /
Disallow: /private.php
Disallow: /listing.html
```

    Which of the following is a true statement concerning this file?

    A. All web crawlers are prevented from indexing the listing.html page.

    B. All web crawlers are prevented from indexing all pages on the site.

    C. The Googlebot crawler is allowed to index pages starting with /tmp/.

    D. The Googlebot crawler can access and index everything on the site except for pages starting with /tmp/.