**崑山科技大學資工系IPAS證照輔導班 練習**

**名稱:** CEH v10 \_CH03\_Security Foundations

|  |  |  |
| --- | --- | --- |
|  | | |
| 答案 | 編號 | 題目 |
|  | 1. | In nmap, the http-methods script can be used to test for potentially risky HTTP options supported by a target. Which of the following methods would be considered risky per the script? A.CONNECT B.GET C.POST D.HEAD |
|  | 2. | OWASP, an international organization focused on improving the security of software, produces a list called “OWASP Top 10 Most Critical Web Application Security Risks” for web applications. Which item is the primary concern on the list?  A. XSS B. Injection Flaws  C. Insufficient Logging and Monitoring  D. Broken Authentication and Session Management |
|  | 3. | A web application developer wants to test a new application for security flaws. Which of the following is a method of testing input variations by using randomly generated invalid input in an attempt to crash the program? A.Insploit B.Finglonger C.Metasplation  D.Fuzzing |
|  | 4. | Which of the following uses HTML entities properly to represent <script>? A. &lt;script&gt; B. &#40;script&#41;  C. &amp;script&amp; D. &quot;script&quot; |
|  | 5. | An attacker tricks a user into visiting a malicious website via a phishing e-mail. The user clicks the e-mail link and visits the malicious website while maintaining an active, authenticated session with his bank. The attacker, through the malicious website, then instructs the user’s web browser to send requests to the bank website. Which of the following best describes this attack? A.CSPP B.XSS C.CSRF D.Hidden form field |
|  | 6. | Which of the following is used by SOAP services to format information? A.Unicode B.HTML entities C.NTFS D.XML |
|  | 7. | A web application developer is discussing security flaws discovered in a new application prior to production release. He suggests to the team that they modify the software to ensure users are not allowed to enter HTML as input into the application. Which of the following is most likely the vulnerability the developer is attempting to mitigate against? A. Cross-site scripting  B. Cross-site request forgery C.Connection string parameter pollution  D.Phishing |
|  | 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 of the following would be the best choice in the prevention of XSS?A. Challenge tokens B. Memory use controls  C. HttpOnly flag in cookies D. Removing hidden form fields |
|  | 11. | You are examining log files and come across this URL: Images Which of the following best describes this potential attack?   1. This is not an attack but a return of SSL handshakes. 2. An attacker appears to be using Unicode. 3. This appears to be a buffer overflow attempt. 4. This appears to be an XSS attempt. |
|  | 12. | Which MSFconsole command allows you to connect to a host from within the console?A. pivot B. connect C. get D. route |
|  | 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?   1. SELECT \* FROM Orders\_Pend WHERE Location\_City = Orlando';DROP TABLE Orders\_Pend – 2. SELECT \* FROM Orders\_Pend WHERE 'Orlando';DROP\_TABLE – 3. DROP TABLE Orders\_Pend WHERE 'Orlando = 1' – 4. WHERE Location\_City = Orlando'1 = 1': DROP\_TABLE -- |
|  | 15. | Efforts to gain information from a target website have produced the following error message: Images Which of the following best describes the error message?   1. The site may be vulnerable to XSS. 2. The site may be vulnerable to buffer overflow. 3. The site may be vulnerable to SQL injection. 4. The site may be vulnerable to a malware injection. |
|  | 16. | An attacker discovers a legitimate username (user1) and enters the following into a web form authentication window:  Which of the following attacks is most likely being attempted?  A. SQL injection B. LDAP injection C. URL tampering D. DHCP amplification |
|  | 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. | A tester is attempting a CSPP attack. Which of the following is she most likely to use in conjunction with the attack?  **A.; B.: C.‘ D.“ E. - - F.~** |
|  | 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 using a cookie, stolen during an XSS attack, during an invalid session on the server by forcing a web application to act on the cookie’s contents. 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 statements is not true regarding WebGoat?   1. WebGoat is maintained and made available by OWASP. 2. WebGoat can be installed on Windows systems only. 3. WebGoat is based on a black-box testing mentality. 4. WebGoat can use Java or .NET. |
|  | 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?   1. A SQL injection attack against the blog’s underlying database 2. A cross-site scripting attack 3. A buffer overflow DoS attack 4. A file injection DoS attack |
|  | 26. | Which of the following is one of the most common methods for an attacker to exploit the Shellshock vulnerability?   1. SSH brute force B. CSRF C. Form field entry manipulation   D.Through web servers utilizing CGI (Common Gateway Interface) |
|  | 27. | You are examining website files and find the following text file: Images 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/. |