**Review Questions**

|  |  |  |
| --- | --- | --- |
| **1.** | Entering **Password::blah'** or **1=1-** into a web form in order to get a password is an example of what type of attack?   1. Buffer overflow 2. Heap-based overflow 3. Stack-based overflow 4. SQL injection | [Use of a single quote indicates a SQL injection attack.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N14) |
| **2.** | Replacing NOP instructions with other code in a buffer overflow mutation serves what purpose?   1. Bypassing an IDS 2. Overwriting the return pointer 3. Advancing the return pointer 4. Bypassing a firewall | [The purpose of mutating a buffer overflow by replacing NOP instructions is to bypass an IDS.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N47) |
| **3.** | Which of the following is used to store dynamically allocated variables?   1. Heap overflow 2. Stack overflow 3. Heap 4. Stack | [A heap is using to store dynamic variables.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N72) |
| **4.** | What is the first step in a SQL injection attack?   1. Enter arbitrary commands at a user prompt. 2. Locate a user input field on a web page. 3. Locate the return pointer. 4. Enter a series of NOP instructions. | [The first step in a SQL injection attack is to locate a user input field on a web page using a web browser.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N97) |
| **5.** | What command is used to retrieve information from a SQL database?   1. INSERT 2. GET 3. SET 4. SELECT | [The command to retrieve information from a SQL database is SELECT .](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N122) |
| **6.** | Which of the following is a countermeasure for buffer overflows?   1. Not using single quotes 2. Securing all login pages with SSL 3. Bounds checking 4. User validation | [Performing bounds checking is a countermeasure for buffer overflow attacks.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N159) |
| **7.** | What does NOP stand for?   1. No Operation 2. Network Operation Protocol 3. No Once Prompt 4. Network Operation | [NOP is an acronym for No Operation.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N184) |
| **8.** | What information does a hacker need to launch a buffer overflow attack?   1. A hacker needs to be familiar with the memory address space and techniques of buffer overflows in order to launch a buffer overflow attack. 2. A hacker needs to understand the differences between heaps and stacks. 3. A hacker must be able to identify a target vulnerable to a buffer overflow attack. 4. A hacker must be able to perform a port scan looking for vulnerable memory stacks. | [All a hacker needs to be able to do to launch a buffer overflow attack is to identify a target system. A hacker can run a prewritten exploit to launch a buffer overflow.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N209) |
| **9.** | Why are many programs vulnerable to SQL injection and buffer overflow attacks?   1. The programs are written quickly and use poor programming techniques. 2. These are inherent flaws in any program. 3. The users have not applied the correct service packs. 4. The programmers are using the wrong programming language. | [Programs can be exploited because they're written quickly and poorly.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N234) |
| **10.** | Which command would a hacker enter in a web form field to obtain a directory listing?   1. Blah';exec master..xp\_cmdshell “dir \*.\*”— 2. Blah';exec\_cmdshell “dir c:\\*.\* /s >c:\directory.txt”— 3. Blah';exec master..xp\_cmdshell “dir c:\\*.\* /s >c:\directory.txt”— 4. Blah';exec cmdshell “dir c:\\*.\* “— | [The command Blah';exec master..xp_cmdshell  dir c:\*.* /s -c:\directory.txt - obtains a directory listing utilizing SQL injection.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N259) |
| **11.** | What are two types of buffer overflow attacks?   1. Heap and stack 2. Heap and overflow 3. Stack and memory allocation 4. Injection and heap | [Heap and stack are the two types of buffer overflows.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N296) |
| **12.** | Variables that are gathered from a user input field in a web application for later execution by the web application are known as \_\_\_\_\_\_\_\_\_\_\_.   1. Delayed execution 2. Dynamic strings 3. Static variables 4. Automatic functions | [Dynamic strings are user input fields stored for later execution by the application.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N321) |
| **13.** | What is one purpose of SQL injection attacks?   1. To create heap-based buffer overflows 2. To create stack-based buffer overflows 3. To perform NOP execution 4. To identify vulnerable parameters | [One purpose of attacking a SQL database based application is to identify user input parameters susceptible to SQL injection attacks.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N346) |
| **14.** | Which application will help identify whether a website is vulnerable to SQL injection attacks?   1. BlackWidow 2. Metasploit 3. Scrawlr 4. SQL Block | [HP's Scrawlr will scan a web URL to determine if the site is vulnerable to SQL injection attacks.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N371) |
| **15.** | A countermeasure to buffer overflows is to use the \_\_\_\_\_\_\_\_\_\_\_ programming language because it is not susceptible to buffer overflow attacks.   1. Java 2. Netscape 3. Oracle 4. ASP | [A recommended countermeasure to buffer overflow attacks is to use Java-based applications, which are not susceptible to buffer overflow attacks.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N396) |
| **16.** | You are a programmer analyzing the code of an application running on your organization's servers. There are an excessive number of fgets () commands. These are C++ functions that do not perform bounds checking. What kind of attack is this program susceptible to?   1. Buffer overflow 2. Denial of service 3. SQL injection 4. Password cracking | [Applications that do not perform bounds checking on user input fields are susceptible to buffer overflow attacks.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N421) |
| **17.** | Which of the following are countermeasures to SQL injection attacks? (Choose two.)   1. Rejecting known bad input 2. Sanitizing and validating input field 3. Performing user validation 4. Ensuring all user input is a variable | [Rejecting known bad input and sanitizing and validating user input prior to sending the command to the SQL database is a countermeasure to SQL injection attacks.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N450) |
| **18.** | An ethical hacker is performing a penetration test on a web application. The hacker finds a user input field on a web form and enters a single quotation mark. The website responds with a server error. What does the error indicate?   1. The web application is susceptible to SQL injection attacks. 2. The web application is not susceptible to SQL injection attacks. 3. The server is experiencing a denial of service. 4. The web application has crashed. | [A server error in response to a single quotation mark in a web application user input field indicates the application is not sanitizing the user data and is therefore susceptible to SQL injection attacks.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N475) |
| **19.** | SQL statements that vary from execution to execution are known as \_\_\_\_\_\_\_\_\_\_\_\_\_\_ strings.   1. Variable 2. Dynamic 3. Application-based 4. Static | [Dynamic strings are built on the fly from user input and will vary each time the command is executed.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N500) |
| **20.** | When is a No Operation (NOP) instruction added to a string?   1. After the malicious code is executed 2. Before the malicious code is executed 3. At exactly the same time the malicious code is executed 4. During the time the malicious code is executed | [A NOP instruction is added to a string just before the malicious code is to be executed.](http://www.books24x7.com/assetviewer.aspx?bookid=31967&chunkid=230390684&rowid=333&noteMenuToggle=0&leftMenuState=1#answer.N525) |

**Answers**

|  |  |
| --- | --- |
| **1.** | Use of a single quote indicates a SQL injection attack. |
| **2.** | The purpose of mutating a buffer overflow by replacing NOP instructions is to bypass an IDS. |
| **3.** | A heap is using to store dynamic variables. |
| **4.** | The first step in a SQL injection attack is to locate a user input field on a web page using a web browser. |
| **5.** | The command to retrieve information from a SQL database is SELECT. |
| **6.** | Performing bounds checking is a countermeasure for buffer overflow attacks. |
| **7.** | NOP is an acronym for No Operation. |
| **8.** | All a hacker needs to be able to do to launch a buffer overflow attack is to identify a target system. A hacker can run a prewritten exploit to launch a buffer overflow. |
| **9.** | Programs can be exploited because they're written quickly and poorly. |
| **10.** | The command Blah';exec master..xp\_cmdshell “dir c:\\*.\* /s >c:\directory.txt”— obtains a directory listing utilizing SQL injection. |
| **11.** | Heap and stack are the two types of buffer overflows. |
| **12.** | Dynamic strings are user input fields stored for later execution by the application. |
| **13.** | One purpose of attacking a SQL database–based application is to identify user input parameters susceptible to SQL injection attacks. |
| **14.** | HP's Scrawlr will scan a web URL to determine if the site is vulnerable to SQL injection attacks. |
| **15.** | A recommended countermeasure to buffer overflow attacks is to use Java-based applications, which are not susceptible to buffer overflow attacks. |
| **16.** | Applications that do not perform bounds checking on user input fields are susceptible to buffer overflow attacks. |
| **17.** | Rejecting known bad input and sanitizing and validating user input prior to sending the command to the SQL database is a countermeasure to SQL injection attacks. |
| **18.** | A server error in response to a single quotation mark in a web application user input field indicates the application is not sanitizing the user data and is therefore susceptible to SQL injection attacks. |
| **19.** | Dynamic strings are built on the fly from user input and will vary each time the command is executed. |
| **20.** | A NOP instruction is added to a string just before the malicious code is to be executed. |