1. Which vulnerability is being exploited in an OS Command Injection attack? **1 point**

- ○ Improperly configured security settings in the MySQL database.
- ◉ Poor user input sanitation and unsafe execution of OS commands.
- ○ Vulnerabilities in the operating system shell interpreter.
- ○ Vulnerabilities in the operating system kernel.

2. What is a simple but effective way to protect against DLL hijacking? **1 point**

- ○ Write-protect the folders that contain your libraries.
- ○ Avoid using DLL libraries in commercial applications where security is a concern.
- ◉ Always use explicit paths to the commands or library applications.
- ○ Use only hijack resistant open-source libraries whenever possible.

3. True or False: Safe coding practice runs code with the least possible privilege. **1 point**

- ◉ True
- ○ False

4. True or False: Safe coding practice always specifies relative paths when running applications or using shared libraries. **1 point**

- ○ True
- ◉ False

5. True or False: Safe coding practice does not let user input reach an OS command unchanged. **1 point**

- ◉ True
- ○ False

6. A hacker exfiltrating data by injecting an HTTPrequest command is an example of which type of SQL Injection attack? **1 point**

- ◉ Out of Band
- ○ Error-based
- ○ UNION-based
- ○ Blind injection

7. Protecting against SQL Injection attacks by sanitizing user input can be accomplished by which two (2) of the following techniques? **1 point**

- ☐ Use of blacklists.
- ☑ Use of mapping tables.
- ☐ Use of an SQL command interpreter to precompile user input.
- ☑ Use of whitelists.

8. True or False: Limiting database user permissions is an ineffective strategy in preventing SQL Injection attacks since the injected code will run directly against the database regardless of the permission levels that have been set. **1 point**

- ○ True
- ◉ False

9. Which of the following will help reduce the SQL Injection attack surface? **1 point**

- ○ Direct SQL execution from user input values.
- ○ Showing users the exact nature of database input errors.
- ◉ Use of stored procedures.
- ○ Direct use of native operating system commands.

10. When developing an application, using NoSQL instead of MySQL will have what effect on the applications susceptibility to SQL Injection attacks? **1 point**

- ○ It will eliminate the injection attack surface.
- ◉ It will reduce, but not eliminate, the injection attack surface.
- ○ It will have no impact on the risk of an injection attack.
- ○ It will increase the risk of an injection attack.

11. You work at a software development company. The development team incorporates security checks throughout software development, and all their code passes them. But you want extra assurance that the applications that they develop can withstand real-world cyberattacks. You want to simulate real hacking techniques to identify any remaining vulnerabilities. What cyberdefense method should you use? **1 point**

- ○ Dynamic application security testing
- ○ Security monitoring
- ◉ Penetration testing
- ○ System information event management

12. How can you view a complete list of all vulnerabilities that OWASP ZAP detected while scanning an application? **1 point**

- ◉ Click the **Alerts** tab in the Information window.
- ○ Click the **Request** tab in the Workspace window.
- ○ Expand **Sites** in the Tree window.
- ○ Select **Protected Mode** from the list of modes.

13. You find a public GitHub repository for an application and would like to use and modify the application's code for your own project. However, you need to do so without impacting the current repository. What should you do? **1 point**

- ◉ Access the repository's web page, and then click **Fork**.
- ○ Access your list of GitHub repositories, and then click **Sort**.
- ○ Access your list of GitHub repositories, and then click **Projects**.
- ○ Access the repository's web page, and then click **Pull requests**.

14. You're the project manager for a development team working on code in a GitHub repository. You use Snyk to scan the repository for vulnerabilities. Snyk identifies only one vulnerability, "Container has no CPU limit", and marks the vulnerability as low severity. The fix for this issue is currently in development, but you don't know when it will be ready. What should you do next on the file's Overview page? **1 point**

- ○ Click **Ignore**, click **Ignore permanently**, and then click **Save**.
- ◉ Click **Ignore**, click **Ignore temporarily**, select the **Until fix is available** checkbox, and then click **Save**.
- ○ Click **Ignore**, click **Not vulnerable**, and then click **Save**.
- ○ Click **Ignore**, click **Not vulnerable**, type a comment in the comment field, and then click **Save**.

Coursera Honor Code Learn more

☑ I, **Giang Pham**, understand that submitting work that isn't my own may result in permanent failure of this course or deactivation of my Coursera account.

Submit **Save draft**