**Web Application Security**

1. Which of the Your application is created using a language that does not support a clear distinction between code and data. Which vulnerability is most likely to occur in your application?
   1. Spoofing
   2. Cross-site request forgery
   3. Denial of service
   4. Insecure direct object references.
2. Your application is created using a language that does not support a clear distinction between code and data. Which vulnerability is most likely to occur in your application?
3. Injection
4. Insecure direct object references
5. Failure to restrict URL access
6. Insufficient transport layer protection
7. Which of the following scenarios is most likely to cause an injection attack?
8. Invalidated input is embedded in an instruction stream.
9. Invalidated input can be distinguished from valid instructions.
10. A Web application does not validate a client’s access to a resource.
11. A Web action performs an operation on behalf of the user without checking a shared secret.
12. A user is able to pass malicious input that invokes control codes in your Web application. Which vulnerability is most likely to occur in your Web application?
13. Injection
14. Insecure direct object references
15. Failure to restrict URL access
16. Insufficient transport layer protection
17. Which of the following is the best way to protect against injection attacks?
18. SQL queries based on user input
19. Input validation using an allow list
20. Memory size checks
21. Validate integer values before referencing arrays

**Answers**

1. C
2. A
3. A
4. A
5. B