1. Explain an SQL injection attack.
2. Explain the basic methods to maintain session state.
3. Explain by example how verbose error messages can help an attacker.
4. Explain how unlinked webpages such as
   bobadilla.engr.scu.edu\interactiveCourse\admin\addStudent.php
   get found and exploited by an attacker.
5. Explain how an XSS attack can yield a session token for the attacker.
6. Explain by example some difficulties in canonicalization and sanitization.
7. Explain why cookies are not an entirely secure authentication mechanism.
8. Explain the difference between HTTP Get and Post commands and explain whether one is more secure than the other.
9. Explain the perils of information leakage and how you test for information leakage.
10. In the olden days, cookie poisoning was used to maintain access to websites.
    How did this work? (One example suffices.)
11. What is bit flipping and why do we care?