OWASP Proactive Controls

Chapter 2 - Controls 6-10

WORKBOOK

Questions and Answers

Review Questions:

1. Implement Appropriate Access Controls addresses which of the following OWASP Top 10 Risks? (Choose all that apply)
    A. A5 - Security Misconfiguration
    B. A7 - Missing Function-level Access Control
    C. A4 - Insecure Direct Object References
    D. A6 - Sensitive Data Exposure

2. What does the STS in HSTS stand for?
    A. Strict Transport Security
    B. Sensitive Transport Security
    C. Sensitive Transit Security
    D. Strict Transit Security

3. What is Apache's logging framework called?
    A. AppLog4j2
    B. Log4j2
    C. ALF4J2
    D. SLF4J2

4. True or False: It's best to start from scratch when implementing security.
    A. True
    B. False

5. True or False: Authentication is a process where requests to access a feature or resource are granted or denied.
    A. True
    B. False

6. One of the first principles of access control is that you should _____ by default.
    A. Question
    B. Allow
    C. Deny
    D. Alert

7. True or False: Lack of centralized access control logic is an example of an access control anti-pattern.
    A. True
    B. False

8. Apache _____ is a Java library that supports permission-based access control.
    A. Weiss
    B. Safed
    C. Blanco
    D. Shiro

9. Protect Data addresses which of the following OWASP Top 10 Risks?
    A. A5 - Security Misconfiguration
    B. A6 - Sensitive Data Exposure
    C. A4 - Insecure Direct Object References
    D. A7 - Missing Function-level Access Control

10. True or False: Certificate pinning is a key continuity scheme that detects when an imposter with an un-validated certificate attempts to act like the real server.
    A. True
    B. False

11. True or False: With perfect forward secrecy, ciphertext traffic doesn't help an attacker even if the private server key is stolen.
    A. True
    B. False

12. What does TOFU stand for?
    A. Transport on First Use
    B. Transport on Free Use
    C. Trust on First Use
    D. Trust on Free Use

13. True or False: HSTS forces the browser to only make HTTPS connections to servers.
    A. True
    B. False

14. True or False: Implementing logging and intrusion detection addresses all of both the OWASP Top 10 2013 and the OWASP Mobile Top 10 2014.
    A. True
    B. False

15. The _____ OWASP project is a useful resource for intrusion detection.
    A. SenseLogger
    B. AppSensor
    C. LogSensor
    D. AppLogger

16. True or False: You should choose a security framework with integrated cross-site request forgery protection.
    A. True
    B. False

17. You should manage exceptions in a _____ manner to avoid duplicated try/catch blocks in code.
    A. Case-by-case
    B. Minimal
    C. Dispersed
    D. Centralized

Answer Key:

1. B, C
   Implement Appropriate Access Controls addresses missing function-level access control and insecure direct object references.

2. A
   The STS in HSTS stands for Strict Transport Security.

3. B
   Apache's logging framework is called Log4j2.

4. B
   This statement is false.

5. B
   This statement is false.

6. C
   One of the first principles of access control is that you should deny by default.

7. A
   True. Lack of centralized access control logic is an example of an access control anti-pattern.

8. D
   Apache Shiro is a Java library that supports permission-based access control.

9. B
   Protect Data addresses sensitive data exposure (A6).

10. B
    This statement is false.

11. A
    True. With perfect forward secrecy, ciphertext traffic doesn't help an attacker even if the private server key is stolen.

12. C
    TOFU stands for Trust on First Use.

13. A
    True. HSTS forces the browser to only make HTTPS connections to servers.

14. A
    True. Implementing logging and intrusion detection addresses all of both the OWASP Top 10 2013 and the OWASP Mobile Top 10 2014.

15. B
    The AppSensor OWASP project is a useful resource for intrusion detection.

16. A
    True. You should choose a security framework with integrated cross-site request forgery protection.

17. D
    You should manage exceptions in a centralized manner to avoid duplicated try/catch blocks in code.