OWASP Proactive Controls

Chapter 1 - Controls 1-5

WORKBOOK

Questions

and

Answers

Review Questions:

1. True or False: The OWASP Top 10 Proactive Controls are listed in order of importance.
   A. True
   B. False

2. True or False: DevOps is a continuous delivery pipeline.
   A. True
   B. False

3. True or False: SQL injection attacks occur when executable code is passed to a concatenated SQL query.
   A. True
   B. False

4. Microsoft _______ and AntiXSS library is a native .NET library that encodes data to protect against cross-site scripting.
   A. Enveloper
   B. Eraser
   C. Enabler
   D. Encoder

5. Which of the following are considered inputs when it comes to the internet? (Choose all that apply)
   A. HTTP headers
   B. Cookies
   C. GET parameters
   D. POST parameters

6. What's the minimum size a salt should be in order to keep passwords secure?
   A. 16 characters
   B. 8 characters
   C. 32 characters
   D. 64 characters

7. Security controls help _______ security risks. (Choose all that apply)
    A. Detect
    B. Counteract
    C. Avoid
    D. Minimize

8. The 2016 edition of OWASP Top 10 Proactive Controls is what version of the list?
    A. 1.5
    B. 1.0
    C. 2.5
    D. 2.0

9. What does ASVS stand for?
    A. Application Security Verification System
    B. Assured Security Verification Software
    C. Assured Security Verification System
    D. Application Security Verification Software

10. True or False: BDD uses a natural-language If, Then, and Else format to describe security requirements.
    A. True
    B. False

11. What character is used to represent a parameter in a parameterized query?
    A. Question mark (?)
    B. Exclamation point (!)
    C. Percent Sign (%)
    D. Ampersand (&)

12. Parameterize Queries addresses which of the following risks from OWASP Mobile Top 10 2014?
    A. M4 - Unintended Data Leakage
    B. M3 - Insufficient Transport Layer Protection
    C. M1 - Weak Server Side Controls
    D. M2 - Insecure Data Storage

13. True or False: No third-party libraries or configuration is necessary to use the OWASP Java Encoder Project.
    A. True
    B. False

14. True or False: All inputs from outside applications should be considered untrusted.
    A. True
    B. False

15. The OWASP HTML Sanitizer Project is written in what language?
    A. Python
    B. C++
    C. C#
    D. Java

16. True or False: For security purposes, you should avoid renaming files that have been uploaded.
    A. True
    B. False

17. True or False: HashCat is an example of a password-cracking application.
    A. True
    B. False

Answer Key:

1. A
   True. The OWASP Top 10 Proactive Controls are listed in order of importance.

2. A
   True. DevOps is a continuous delivery pipeline.

3. A
   True. SQL injection attacks occur when executable code is passed to a concatenated SQL query.

4. D
   Microsoft Encoder and AntiXSS library is a native .NET library that encodes data to protect against cross-site scripting.

5. A, B, C, D
   All of these are considered inputs when it comes to the internet.

6. C
   32 characters is the minimum size a salt should be in order to keep passwords secure.

7. A, B, C, D
   Security controls help detect, counteract, avoid, and minimize security risks.

8. D
   The 2016 edition of OWASP Top 10 Proactive Controls is version 2.0 of the list.

9. A
   ASVS stands for Application Security Verification System.

10. B
    This statement is false.

11. A
    The question mark (?) is used to represent a parameter in a parameterized query.

12. C
Parameterize Queries addresses weak server side controls (M1).

13. A
True. No third-party libraries or configuration is necessary to use the OWASP Java Encoder Project.

14. A
True. All inputs from outside applications should be considered untrusted.

15. D
The OWASP HTML Sanitizer Project is written in Java.

16. B
This statement is false.

17. A
True. HashCat is an example of a password-cracking application.