

# Secure Coding Assessment

\* Indicates required question

---

1. Please fill you name & HR ID: \*

---

## Quiz Questions:

### Part One:

2. What is meant by the term "Security By-Design"? \*

1 point

*Mark only one oval.*

- ☐ Request the analysis of the safety requirements to third parties with respect to those who draw up the functional requirements
- ☐ Think about security checks right from the software design stage
- ☐ Implement security checks after software validation test

3. Which of these is not a binding regulation (a legal obligation)? \*

1 point

*Mark only one oval.*

- ☐ The GDPR
- ☐ The ISO27001
- ☐ The NIS directive

4. **On a statistical level, which of these consequences are the most frequent in security incidents?**

\* 1 point

*Mark only one oval.*

- ☐ Access to user accounts
- ☐ Access to financial accounts
- ☐ Identity data theft

5. **What does the Threat Modeling methodology consist of? \***

1 point

*Mark only one oval.*

- ☐ In trying to identify the causes of a security incident
- ☐ In identifying possible threats during the software design phase
- ☐ In restoring business continuity after a data breach

6. **Which of the following is not part of a risk management strategy? \***

1 point

*Mark only one oval.*

- ☐ Risk avoidance
- ☐ Risk transfer
- ☐ Risk reduction
- ☐ Risk denial
- ☐ Risk acceptance

7. **Which of the following projects of the Owasp community deals with methodologies for code inspection?** \* 1 point

*Mark only one oval.*

- ☐ Owasp Testing guide
- ☐ Owasp Secure Coding practices
- ☐ Owasp Top 10 web security risks
- ☐ Owasp code review

8. **What is made available on the Carnegie Mellon University SEI (Software Engineering Institute) wiki site?** \* 1 point

*Mark only one oval.*

- ☐ Secure development guidelines for various programming languages, including Java, C / C ++, Android.
- ☐ Best practices on how to carry out Vulnerability Assessment and Penetration Test activities
- ☐ Tools for static analysis of web application code

**Part Two:**

9. **What is the difference between the HTTP GET method and the HTTP POST method?** \* 1 point

*Mark only one oval.*

- ☐ The GET method passes the parameters sent to the server in the URL, while the POST passes them in the body
- ☐ The GET method cannot pass parameters with the request, while POST can do it
- ☐ The GET method passes the parameters sent to the server in the body of the HTTP request, while the POST passes them in the header

10. **Where you can find the following line of instructions concerning the HTTP protocol:** \* 1 point

**Set-Cookie: <cookie-name> = <cookie-value>; Domain = <domain-value>; Secure; HttpOnly**

*Mark only one oval.*

- ☐ In the header of an HTTP request, it is used to send a cookie to the web server
- ☐ In the body of an HTTP response, it is used to send a cookie to the client user agent
- ☐ In the header of an HTTP response, it is used to send a cookie to the client user agent so that it can subsequently send it again with a request

11. **What function does the HttpOnly attribute set (to true) have in the cookie?** \* 1 point

**Set-Cookie: <cookie-name> = <cookie-value>; Domain = <domain-value>; Secure; HttpOnly**

*Mark only one oval.*

- ☐ Force the transmission of the cookie only on the Https channel
- ☐ It prevents Javascript code from reading the contents of the cookie
- ☐ Blocks the ability to request content other than static html from the server

12. **. For what type of activity can you draw inspiration from the Owasp Web Security Testing guide as a methodological reference?** \* 1 point

*Mark only one oval.*

- ☐ For code review activities of web application code
- ☐ For threat modeling activities in the web application design phase
- ☐ For carrying out vulnerability assessment and penetration tests of web applications

13. **What role can proxies (like Fiddler, WebScarab, etc) play in the testing of web applications?** \* 1 point

*Mark only one oval.*

- ☐ Detect exploit the possibility of exploiting vulnerabilities present in web applications
- ☐ Stand between the client and the server and allow to bypass the client side validation, checking if the server side applications implement a further validation of the user inputs
- ☐ Allow you to do a static analysis of the code of web applications

14. **The cross-site scripting vulnerability results from:** \* 1 point

*Mark only one oval.*

- ☐ Incorrect coding of the authentication logic of a web application
- ☐ Incorrect implementation of web session management logic
- ☐ Incorrect coding of the input validation logic of a web application
- ☐ Lack of checks for possible memory overflows on the web server

15. **What control must be done on a request in order not to generate a possible vulnerability related to an insecure upload of files to the webserver?** \* 1 point

*Mark only one oval.*

- ☐ Just check only the extension of the file being uploaded
- ☐ Just check only the Mime type of the file that is uploaded
- ☐ At least the so-called magic number of the file (contained in the header of the file itself) must be checked

**Part Three:**

16. **How does basic authentication that can be set at the web server level work?** \* 1 point

*Mark only one oval.*

- ☐ Authentication is requested by the web server at the application level, therefore it must be implemented by the developer
- ☐ The server asks the user for the login / password pair (challenge) before authorizing access to resources
- ☐ The web server allows access to resources, whether reserved or not, to all users, without requiring authentication

17. **It should be possible to change passwords only after a given settable period (typically one day) from the last change made.** \* 1 point

*Mark only one oval.*

- ☐ False
- ☐ True

18. **Which of the following does not fit into a type of man-in-the-middle attack on authentication?** \* 1 point

*Mark only one oval.*

- ☐ ARP Poisoning
- ☐ DHCP Rogue Server
- ☐ DNS Spoofing
- ☐ Pass-the-hash

19. **How long do web application session cookies expire? \***

1 point

*Mark only one oval.*

- ☐ It depends on the presence of an expires attribute, which determines its expiration date
- ☐ The deadline is settable but cannot be longer than one month
- ☐ It cannot be set, the duration is predefined and depends on the type of webserver

20. **Why must the SessionID of an unauthenticated user of a web application be changed by the server when the user authenticates successfully?**

\* 1 point

*Mark only one oval.*

- ☐ It's not mandatory
- ☐ To avoid opening up to Session Fixation vulnerabilities and attacks
- ☐ To make the session management mechanism more efficient and performing

21. **Which of the following is not directly a technique for mitigating XSRF (Cross-site Request Forgery) attacks**

\* 1 point

*Mark only one oval.*

- ☐ Programmatically set the use of anti-forgery tokens in the data submission forms related to critical operations
- ☐ Request the user, even if already authenticated, in the processing of critical requests to pass an additional authentication factor
- ☐ Enable the HttpOnly attribute for session cookies

22. **Which of the following is not a symmetric or private key encryption algorithm?** \* 1 point

*Mark only one oval.*

- ☐ DES
- ☐ ECC
- ☐ AES
- ☐ RC5

23. **What does the recipient of a data encrypted with asymmetric encryption, necessarily need, in order to decrypt the data received?** \* 1 point

*Mark only one oval.*

- ☐ His private key
- ☐ His public key
- ☐ The public key of the sender
- ☐ The private key of the sender

24. **What is the problem of collisions in hashing algorithms?** \* 1 point

*Mark only one oval.*

- ☐ The fact that two different data files input to a hashing algorithm can generate the same hash-code
- ☐ The fact that the same file can generate the same digest with two different hashing algorithms
- ☐ The fact that for some types of data supplied as input to a hashing algorithm, it can generate calculation errors (anomalous digest)



# Google Forms

