QCM – OWASP Top 10

20 questions avec choix multiples

1. Que signifie OWASP ?

   a) Online Web Application Security Platform
   b) Open Worldwide Application Security Project
   c) Open Web Application Security Project
   d) Operational Web Assessment Security Program

2. Quel est l'objectif de l'OWASP Top 10 ?

   a) Fournir un antivirus
   b) Lister les 10 vulnérabilités les plus critiques
   c) Donner les meilleurs frameworks frontend
   d) Simplifier la configuration réseau

3. Quel type d'attaque correspond à ' OR 1=1 -- ?

   a) XSS
   b) CSRF
   c) SQL Injection
   d) SSRF

4. Quel mécanisme empêche un script injecté d'être exécuté ?

   a) CSP
   b) DNSSEC
   c) ARP
   d) SSL

5. Comment doivent être stockés les mots de passe ?

   a) En clair
   b) En base64
   c) Hashés (bcrypt/Argon2)
   d) En MD5 simple

6. Quelle vulnérabilité apparaît lorsqu'un user accède à /admin ?

   a) Security Misconfiguration
   b) Broken Access Control
   c) Injection
   d) Software Integrity Failure

7. Quel header empêche l'affichage de ton site dans un iframe ?

   a) X-Frame-Options
   b) X-Token
   c) X-Access
   d) Content-Type

8. Quel risque implique un package obsolète ?

a) Plus de rapidité
b) Vulnérabilités connues
c) Plus de fonctionnalités
d) Meilleure compatibilité

9. Une attaque XSS permet :

a) D’injecter du SQL
b) De voler des sessions utilisateur
c) De désactiver le serveur
d) De scanner les ports

10. Quelle mesure protège d’un brute-force ?

a) Timeout session
b) Contrôle RBAC
c) Captcha / blocage après X essais
d) Logs horodatés

11. Que signifie SSRF ?

a) Server-Side Request Forgery
b) Secure Script Request Function
c) System Security Recovery Failure
d) Server Safe Routing Firewall

12. Qu’est-ce qu’une requête préparée ?

a) Une requête plus rapide
b) Empêche l’injection SQL
c) Chiffre les données
d) Une requête en cache

13. Quel drapeau de cookie empêche l’accès via JavaScript ?

a) Secure
b) HttpOnly
c) Path
d) SameSite

14. Une mauvaise configuration inclut :

a) Code trop bien organisé
b) Port ouvert inutile
c) Trop de chiffrage
d) Trop de logs

15. Quel outil détecte les vulnérabilités automatiquement ?

a) Photoshop
b) ZAP
c) Excel

d) Postman

16. Quelle vulnérabilité fait appeler une URL par le serveur ?

a) XSS
b) CSRF
c) SSRF
d) RCE

17. Ne jamais loguer :

a) Date
b) Utilisateur
c) Mot de passe
d) Action

18. Protection XSS ?

a) Minifier le code
b) htmlspecialchars()
c) Utiliser HTTP
d) Cacher le HTML

19. Pourquoi appliquer un CSP ?

a) Accélérer
b) Empêcher scripts non autorisés
c) Faire un backup
d) Changer le style

20. Score minimal requis ?

a) 20%
b) 40%
c) 70%
d) 95%

Correction du QCM

1-c, 2-b, 3-c, 4-a, 5-c, 6-b, 7-a, 8-b, 9-b, 10-c, 11-a, 12-b, 13-b, 14-b, 15-b, 16-c, 17-c, 18-b, 19-b, 20-c