

Examen: n°475985 "Validation des acquis - sécurité des applications web"

Copie n°12826521

Reference de l'examen: 251117-701-194004-475985

Exam effectué depuis l'adresse IP 176.165.222.40 en utilisant le login OTP matthieu42 / 9567

Commencé le 2025-11-17 16:34:22 et terminé le 2025-11-17 16:46:40

Note : 19/20 (19 points / 20) - 20 questions

Barème: (Barème 1) Demi-point attribué si au moins la moitié des bonnes réponses sont cochées

(Examen ouvert le 2025-11-07 15:30:00)

Légende

✔ Correct

⚠ Devait être coché

✖ Faux

1 Qu'appelle t'on le hachage d'un mot de passe ?

- A ☐ Technique qui consiste à crypter un mot de passe avec une clé. Pour décrypter le mot de passe on utilise cette même clé.
- B ☒ Technique qui consiste à transformer une chaîne de caractères de manière non réversible. On ne peut pas "dé-hacher" un mot de passe haché.

(1 point / 1) Question à choix multiple

2 Qu'appelle t'on le salage dans le hachage d'un mot de passe ?

- A ☐ Technique qui consiste à crypter le mot de passe
- B ☐ Technique à double sécurité qui consiste à crypter le mot de passe une fois haché
- C ☒ Technique qui consiste à ajouter au mot de passe une chaîne de caractères avant de le hacher

(1 point / 1) Question à choix multiple

3 Quel est l'algorithme de hachage recommandé actuellement parmi les 3 suivants ?

- A ☐ sha-256
- B ☐ BCrypt
- C ☒ Argon2

(1 point / 1) Question à choix multiple

4 Qu'est-ce qu'une injection SQL ?

- A ☒ Une technique qui consiste à insérer du code SQL malveillant dans une requête afin de manipuler la base de données de façon non autorisée.
- B ☐ Un type d'attaque où l'on intercepte les communications réseau pour voler des identifiants de connexion.
- C ☐ Une méthode pour saturer un serveur avec un grand nombre de requêtes afin de le rendre indisponible.

(1 point / 1) Question à choix multiple

5 Comment se prémunir effectivement contre les attaques par injection SQL ?

- A ☒ Valider et nettoyer les entrées utilisateurs avant utilisation dans les requêtes SQL.
- B ☒ Utiliser des requêtes préparées (PreparedStatement) avec des paramètres liés.
- C ☒ Utiliser un ORM comme Hibernate qui gère la construction sécurisée des requêtes.
- D ☐ Construire les requêtes SQL en concaténant les entrées utilisateur sans filtre.

(0 point / 1) Question à choix multiple

6 Qu'est-ce qu'une attaque XSS ?

- A ☐ Une méthode qui exploite une faille dans les systèmes de chiffrement pour déchiffrer les communications sécurisées.
- B ☐ Une attaque visant à saturer un site web avec un grand nombre de connexions simultanées pour le rendre indisponible.
- C ☒ Une attaque qui injecte du code JavaScript malveillant dans une page web consultée par d'autres utilisateurs, permettant par exemple de voler des cookies ou manipuler le contenu affiché.

(1 point / 1) Question à choix multiple

7 Parmi les attaques suivantes, lesquelles sont des attaques XSS ?

- A ☒ Injection de code JavaScript malveillant dans un champ de formulaire pour voler des cookies utilisateur.
- B ☐ Envoi massif de requêtes pour saturer un serveur (attaque DDoS).
- C ☒ Injection de script malveillant dans une URL affichée sur une page web.
- D ☐ Exploitation d'une faille dans un protocole pour intercepter des données chiffrées.
- E ☐ Vol d'identifiants via phishing par email.

(1 point / 1) Question à choix multiple

8 Parmi les propositions suivantes, quelles sont celles à mettre en place pour prévenir des attaques XSS ?

- A ☒ Valider et filtrer systématiquement les entrées utilisateurs avant de les afficher.
- B ☐ Utiliser HTTPS pour chiffrer les données échangées entre le client et le serveur.
- C ☐

- ☐ Éviter de stocker des mots de passe en clair dans la base de données.
- ☒ Mettre en place une CSP côté serveur (Content Security Policy).
- ☐ Limiter le nombre de requêtes par seconde pour éviter les attaques par déni de service.

(1 point / 1) Question à choix multiple

9 Qu'est-ce qu'un cookie de session ?

- ☐ Un type de virus informatique qui infecte les cookies du navigateur.
- ☒ Un fichier stocké temporairement sur le navigateur qui permet d'identifier un utilisateur pendant une session de navigation.
- ☐ Un protocole de sécurité utilisé pour chiffrer les communications entre un navigateur et un serveur.

(1 point / 1) Question à choix multiple

10 A quoi sert un algorithme de cryptage ?

- ☒ À transformer des données en une forme illisible pour protéger leur confidentialité.
- ☐ À compresser des fichiers pour réduire leur taille.
- ☐ À accélérer l'exécution des programmes informatiques.

(1 point / 1) Question à choix multiple

11 Un algorithme de cryptage tel que AES est-il réversible ou non ?

- ☒ Oui
- ☐ Non

(1 point / 1) Question à choix multiple

12 Où est-il recommandé de stocker une clé de cryptage ?

- ☐ Dans le code source de l'application.
- ☒ Dans un module matériel sécurisé (HSM) ou un coffre-fort matériel.
- ☐ Dans un fichier de propriétés utilisé par l'application au démarrage.
- ☒ Dans une variable d'environnement du serveur.

(1 point / 1) Question à choix multiple

13 Qu'est-ce qu'un algorithme de cryptage asymétrique ?

- ☐ Un algorithme qui compresse les données sans perte d'information.
- ☐ Un algorithme qui chiffre les données avec une seule clé partagée entre l'émetteur et le destinataire.
- ☒ Un algorithme qui utilise une paire de clés, une publique pour chiffrer et une privée pour déchiffrer les données.

(1 point / 1) Question à choix multiple

14 Quelle est la différence entre cryptage et hachage ?

- ☐ Le cryptage est utilisé uniquement pour compresser des données, alors que le hachage sert à les chiffrer.
- ☐ Le cryptage transforme les données en clair, tandis que le hachage déchiffre les données cryptées.
- ☒ Le cryptage permet de chiffrer des données de manière réversible, tandis que le hachage produit une empreinte unique non réversible.

(1 point / 1) Question à choix multiple

15 Qu'est-ce qu'une table arc-en-ciel ?

- ☐ Un tableau de données coloré utilisé pour visualiser des statistiques en cybersécurité.
- ☐ Un type de base de données spécialement conçu pour stocker des informations chiffrées.
- ☒ Une table pré-calculée utilisée pour retrouver rapidement des mots de passe à partir de leurs valeurs hachées.
- ☐ Un algorithme de chiffrement symétrique très performant.

(1 point / 1) Question à choix multiple

16 Qu'est-ce qu'une attaque de type session fixation ?

- ☐ Une attaque visant à saturer le serveur en multipliant les requêtes de connexion.
- ☒ Une attaque où un pirate force un utilisateur à utiliser un identifiant de session connu pour prendre le contrôle de sa session.
- ☐ Une technique consistant à intercepter les données chiffrées lors d'une communication.

(1 point / 1) Question à choix multiple

17 Qu'est-ce qui est important dans la mise en place d'une stratégie de sécurité globale ?

- ☐ Tout mettre en place pour éviter les attaques.
- ☒ Mettre en balance le coût d'une politique de sécurité maximale avec le coût d'une attaque

(1 point / 1) Question à choix multiple

18 Parmi les méthodes suivantes, laquelle est une méthode d'évaluation des risques ?

- ☒ Octave.
- ☐ BIOS
- ☐ CNIL

(1 point / 1) Question à choix multiple

19 Qu'est-ce que la CNIL ?

- A ☒ La Commission Nationale de l'Informatique et des Libertés, l'autorité française chargée de protéger les données personnelles.
- B ☐ La Commission Nationale de l'Informatique et des Libertés, chargée de la cybersécurité mondiale.
- C ☐ Une entreprise spécialisée dans la sécurité informatique.

(1 point / 1) Question à choix multiple

20 Quelles sont les recommandations de la CNIL en termes de structure d'un mot de passe ?

- A ☐ Imposer systématiquement des mots de passe avec au moins une majuscule, une minuscule, un chiffre et un caractère spécial.
- B ☐ Autoriser uniquement des mots de passe composés de chiffres pour simplifier la saisie.
- C ☒ Favoriser la longueur (au moins 12 caractères) et la complexité, mais privilégier la longueur plutôt que la complexité excessive (types de caractères).
- D ☐ Changer le mot de passe tous les mois, quel que soit le contexte.

(1 point / 1) Question à choix multiple