Commencé le	lundi 22 avril 2024, 09:30
État	Terminé
Terminé le	lundi 22 avril 2024, 09:32
Temps mis	2 min 49 s
Points	18,00/18,00
Note	**10,00** sur 10,00 (**100**%)

Question 1

Correct

Note de 1,00 sur 1,00

Comment l'utilisation de certificats permet l'authentification des sites web ?

Veuillez choisir une réponse.

- a. La signature numérique du certificat valide le champ CN (l'adresse du site) ✓
- b. Le certificat permet l'utilisation d'un algorithme à clé publique
- c. Il est très difficile pour un pirate d'avoir accès au certificat
- d. Le protocole SSL/TLS assure la confidentialité des informations
- e. L'utilisation de certificat n'a rien à voir avec l'authentification

Votre réponse est correcte.

La réponse correcte est : La signature numérique du certificat valide le champ CN (l'adresse du site)

Question 2

Correct

Note de 1,00 sur 1,00

Laquelle de ces méthodes d'authentification sur une application Web représente le risque le plus élevé en terme d'exposition à un scénario de piratage de l'externe (via Internet).

Veuillez choisir une réponse.

a. Le code usager et le mot de passe sont vérifiés par le serveur Web en accédant à une base de données de hachés cryptographiques d'usagers stockée sur la BD relationnelle de l'application Web

b. Le code usager et mot de passe sont vérifiés par le serveur Web en utilisant le fichier /etc/shadow stocké sur le serveur Web

c. Le code usager et le mot de passe sont envoyés à un serveur d'authentification qui répond avec un identificateur de session unique (« session ID ») s'ils sont valides

d. Le code usager et mot de passe sont envoyés tels quels au serveur de BD relationnelle pour ouvrir une session SQL ✓

Votre réponse est correcte.

La réponse correcte est : Le code usager et mot de passe sont envoyés tels quels au serveur de BD relationnelle pour ouvrir une session SQL

Question 3

Correct

Note de 1,00 sur 1,00

Laquelle de ces méthodes ne constitue pas une méthode de prévention des erreurs d'injection de SQL

Veuillez choisir une réponse.

a. L'utilisation d'instructions GRANT et REVOKE pour contrôler l'accès à la base de données ✓

b. L'utilisation de méthodes ou fonctions de filtrage des entrées venant des usagers

c. L'utilisation de méthodes et fonctions directement implémentés sur le serveur de BD (« stored procedures »)

d. L'utilisation d'un détecteur d'intrusion pouvant détecter les chaînes susceptibles d'être utilisés par une attaque d'injection de SQL

Votre réponse est correcte.

La réponse correcte est : L'utilisation d'instructions GRANT et REVOKE pour contrôler l'accès à la base de données

Question 4

Correct

Note de 1,00 sur 1,00

Laquelle de ces méthodes de générations de jeton de session (« session ID ») est préférable en terme de sécurité

Veuillez choisir une réponse.

a. Un jeton de 10 caractères imprimables, choisis au hasard parmi les lettres majuscules et minuscules sans accent et des chiffres de 0 à 9.

b. Un nombre choisi au hasard entre 1 et 100 milliards, codé avec un caractère ASCII pour chaque chiffre (0 à 9).

c. Une chaine de 64 bits aléatoires codées avec des 0 et des 1 (en ASCII)

d. Une chaine de 5 mots de la langue anglaise, choisis au hasard dans un dictionnaire de 100 000 mots et séparé par un caractère spécial. ✓

Votre réponse est correcte.

La réponse correcte est : Une chaine de 5 mots de la langue anglaise, choisis au hasard dans un dictionnaire de 100 000 mots et séparé par un caractère spécial.

Question 5

Correct

Note de 1,00 sur 1,00

Quel type d'attaque XSS (cross-site scripting) est la plus dangereuse et pourquoi ?

Veuillez choisir une réponse.

a. XSS non-persistent parce qu'on peut faire activer l'attaque par de l'ingénierie sociale.

b. XSS persistent puisqu'aucune interaction de l'usager n'est requise. ✓

c. XSS persistent parce qu'on peut faire activer l'attaque par de l'ingénierie sociale.

d. XSS non-persistent puisqu'aucune interaction de l'usager n'est requise.

Votre réponse est correcte.

La réponse correcte est : XSS persistent puisqu'aucune interaction de l'usager n'est requise.

Question 6

Correct

Note de 1,00 sur 1,00

Lequel de ces systèmes n'utilise pas de l'authentification à deux facteurs :

Veuillez choisir une réponse.

- a. Un site Web qui demande le nom d'usager et le mot de passe, et ensuite de répondre à une question de sécurité ✓
- b. Un ordinateur de bureau qui se débloque seulement lorsqu'on insère une carte à puce et lorsqu'on introduit le bon code usager et mot de passe
- c. Un ordinateur portable qui se débloque lorsqu'on passe son doigt sur le lecteur d'empreinte digitale **et** qui nécessite l'introduction d'un mot de passe au démarrage
- d. Un site Web qui détecte et reconnait le rythme de frappe au clavier de l'usager (à travers une applet Java sur le fureteur) et qui demande un code à usage unique (« one-time password ») généré sur un téléphone intelligent

Votre réponse est correcte.

La réponse correcte est : Un site Web qui demande le nom d'usager et le mot de passe, et ensuite de répondre à une question de sécurité

Question 7

Correct

Note de 1,00 sur 1,00

Quelle est l'utilité de faire de la validation des données saisies sur le client ?

Veuillez choisir une réponse.

- a. Permet de détecter des exploits (« shell code ») qui aurait pu être insérés dans les inputs d'usagers
- b. Permet de filtrer les injections SQL et les attaques XSS (cross-site scripting). ✓
- c. Permet d'améliorer la performance et l'expérience usager pour les usagers non-malveillants.
- d. Aucune utilité.

Votre réponse est correcte.

La réponse correcte est : Permet de filtrer les injections SQL et les attaques XSS (cross-site scripting).

Question 8

Correct

Note de 1,00 sur 1,00

Laquelle de ces mesures de remédiation ne permet pas d'empêcher les injections SQL ?

Veuillez choisir une réponse.

a. L'utilisation de pare-feu applicatif spécialisé en application web.

b. L'utilisation de procédures stockées (« stored procedures »).

c. Le filtrage des caractères spéciaux.

d. La limitation des droits de l'application dans la base de données. ✓

e. Le ré-encodage des caractères spéciaux.

Votre réponse est correcte.

La réponse correcte est : La limitation des droits de l'application dans la base de données.

Question 9

Correct

Note de 1,00 sur 1,00

Pourquoi est-il nécessaire de chiffrer les communications d'un site web après l'authentification, même si le contenu du site ne nécessite aucune confidentialité

Veuillez choisir une réponse.

a. Pour préserver la vie privée.

b. Pour garantir la disponibilité.

c. Parce que l'utilisation de SSL/TLS est sécuritaire.

d. Pour éviter l'utilisation de cookies.

e. Certaines informations systèmes comme l'identificateur de session sont sensibles et peuvent transiter dans la communication. ✓

Votre réponse est correcte.

La réponse correcte est : Certaines informations systèmes comme l'identificateur de session sont sensibles et peuvent transiter dans la communication.

Question 10

Correct

Note de 1,00 sur 1,00

Pourquoi est-il nécessaire d'utiliser une forme de XSS (cross-site scripting) pour voler un cookie ?

Veuillez choisir une réponse.

a. Pour que la requête s'exécute dans le contexte du site web attaquant.

b. Pour que la requête s'exécute dans le contexte du site web à qui appartient le cookie. ✓

c. Pour faciliter l'ingénierie sociale.

d. Pour permettre à l'attaque de faire une attaque d'homme au milieu (man-in-the-middle).

e. Pour outrepasser le chiffrement.

Votre réponse est correcte.

La réponse correcte est : Pour que la requête s'exécute dans le contexte du site web à qui appartient le cookie.

Question 11

Correct

Note de 1,00 sur 1,00

Laquelle de ces méthodes est la plus efficace pour détecter les failles de logique applicatives dans les applications web ?

Veuillez choisir une réponse.

a. L'utilisation de pare-feu applicatif spécialisé en application web.

b. La revue manuelle de code. ✓

c. Le filtrage des caractères spéciaux.

d. La limitation des droits de l'application dans la base de données.

e. Le ré-encodage des caractères spéciaux.

Votre réponse est correcte.

La réponse correcte est : La revue manuelle de code.

Question 12

Correct

Note de 1,00 sur 1,00

Lequel de ces moyens n'est pas adéquat pour implémenter la logique du mécanisme de contrôle d'accès dans une application Web :

Veuillez choisir une réponse.

a. Les commandes grant et revoke sur le serveur de base de données

b. Les permissions d'accès des fichiers HTML sur les répertoires du serveur Web

c. Le code javascript exécuté sur le fureteur du client Web ✓

d. Le code qui s'exécute sur un serveur d'application entre le serveur Web et le serveur de base de données

Votre réponse est correcte.

La réponse correcte est : Le code javascript exécuté sur le fureteur du client Web

Question 13

Correct

Note de 1,00 sur 1,00

Un hacker souhaite frauder un service Web. Une transaction sur ce site suit le format suivant

GET www.banqueacme.com/transactions/DO?sessionID=8734521203&trans_id=6&value=1000

où la sessionID est le jeton de session qui est inclus dans le cookie du site. Il est possible de changer le paramètre "value" pour payer un montant moins élevé que le montant prévu par l'application. De quel type d'attaque s'agit-il ?

Veuillez choisir une réponse.

a. XSS persistent

b. XSS non persistent

c. Injection SQL

d. CSRF

e. Logique de l'application ✓

Votre réponse est correcte.

La réponse correcte est : Logique de l'application

Question 14

Correct

Note de 1,00 sur 1,00

Les vulnérabilités d'injection de code SQL dans les applications Web sont un exemple de vulnérabilités du au filtrage déficient des entrées d'usager

Veuillez choisir une réponse.

- Vrai ✓
- Faux

La réponse correcte est « Vrai ».

Question 15

Correct

Note de 1,00 sur 1,00

L'injection SQL n'est pas un problème si votre mode d'authentification n'utilise pas des requêtes de base de données

Veuillez choisir une réponse.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 16

Correct

Note de 1,00 sur 1,00

Les vulnérabilités de cross-site scripting (XSS) sont un exemple de vulnérabilités du au filtrage déficient des entrées d'usager

Veuillez choisir une réponse.

- Vrai ✓
- Faux

La réponse correcte est « Vrai ».

Question 17

Correct

Note de 1,00 sur 1,00

L'utilisation de fonctions stockées (« stored procedures ») sur un moteur de base de données peut constituer une contremesure efficace contre les vulnérabilités d'injection de SQL.

Veuillez choisir une réponse.

- Vrai ✓
- Faux

La réponse correcte est « Vrai ».

Question 18

Correct

Note de 1,00 sur 1,00

Le modèle de sécurité basée sur l'origine de HTTP (« same domain policy ») permet de prévenir le vol de cookie par XSS

Veuillez choisir une réponse.

- Vrai ✓
- Faux

La réponse correcte est « Vrai ».