

# Sécuriser la publication d'une application web

# Table des matières

<b>I. Contexte</b>	<b>3</b>
<b>II. Introduction à la sécurité de la publication d'une application web</b>	<b>3</b>
A. Importance de la sécurité lors de la publication d'une application web.....	3
B. Risques associés à une publication non sécurisée.....	4
C. Mesures de sécurité pour une publication sécurisée d'une application web .....	4
D. Exercice : Quiz.....	5
<b>III. Protocoles et outils de publication sécurisée</b>	<b>6</b>
A. Présentation des protocoles de publication sécurisée : SCP (Secure Copy Protocol) et SSH (Secure Shell).....	6
B. Présentation d'outils simples tels que FileZilla pour la publication sécurisée .....	6
C. Exercice : Quiz.....	7
<b>IV. Bonnes pratiques et vérifications de sécurité</b>	<b>8</b>
A. Présentation des bonnes pratiques pour une publication sécurisée .....	8
B. Vérification de l'intégrité des fichiers publiés.....	9
C. Sensibilisation à la mise à jour régulière des applications et des systèmes .....	9
D. Exercice : Quiz.....	9
<b>V. L'essentiel</b>	<b>10</b>
<b>VI. Auto-évaluation</b>	<b>11</b>
A. Exercice .....	11
B. Test.....	11
<b>Solutions des exercices</b>	<b>12</b>

## I. Contexte

### Contexte

La publication d'une application web est une étape cruciale dans le processus de développement, permettant de rendre une application accessible en ligne. Cependant, cette étape expose l'application à des risques potentiels en termes de sécurité.

Les attaques informatiques sont de plus en plus fréquentes et sophistiquées, ce qui nécessite une attention particulière pour garantir la sécurité lors de la publication. Ce cours se concentre sur les mesures de sécurité essentielles à prendre lors de la publication d'une application web, afin de minimiser les vulnérabilités et de protéger les données sensibles.

La sécurité est une préoccupation constante dans l'environnement en ligne en constante évolution, et il est impératif de rester informé des meilleures pratiques et des mesures de sécurité les plus récentes. Ce cours fournit les bases nécessaires pour s'engager dans un processus de publication sécurisée, en protégeant les utilisateurs finaux et en préservant la réputation et la confidentialité des données de l'application web.

## II. Introduction à la sécurité de la publication d'une application web

### A. Importance de la sécurité lors de la publication d'une application web

#### Rappel

#### L'importance de la sécurité lors de la publication d'une application web

L'importance de la sécurité lors de la publication d'une application web est primordiale pour plusieurs raisons :

1. **Protection des données** : une application web, qu'elle soit commerciale, institutionnelle ou autre, manipule souvent des données, certaines pouvant être extrêmement sensibles. Il peut s'agir d'informations personnelles, financières ou stratégiques. Une faille de sécurité pourrait exposer ces données, menaçant la vie privée des utilisateurs et l'intégrité de l'entreprise.
2. **Réputation** : une violation de la sécurité peut ternir considérablement la réputation d'une organisation. Les utilisateurs perdent leur confiance, et il est souvent difficile de la regagner. Une entreprise dont l'application a été compromise pourrait également subir des pertes financières conséquentes, non seulement en termes de ventes perdues mais aussi en raison d'éventuelles sanctions ou actions en justice.
3. **Continuité des affaires** : un incident de sécurité peut entraîner des temps d'arrêt ou des perturbations dans le service, affectant ainsi la continuité des affaires. Pour certaines entreprises, même une courte période d'indisponibilité peut entraîner des pertes financières significatives.
4. **Exigences réglementaires** : de nombreuses industries sont soumises à des réglementations strictes en matière de cybersécurité. La non-conformité à ces réglementations lors de la publication d'une application web peut entraîner des amendes, des sanctions et d'autres conséquences juridiques.

Il est donc essentiel de comprendre que la publication d'une application web n'est pas simplement un acte technique. C'est un événement qui, s'il n'est pas géré avec la prudence et l'attention requises en matière de sécurité, peut avoir des répercussions majeures pour une organisation. La préparation, la validation et la vigilance sont les clés pour garantir que la transition de l'application vers un environnement de production se fasse sans encombre.

## B. Risques associés à une publication non sécurisée

### Les risques associés à une publication non sécurisée

Le processus de publication d'une application web est une étape cruciale qui, si elle n'est pas effectuée en toute sécurité, peut exposer l'application à des menaces supplémentaires. Les risques associés à un processus de publication non sécurisé incluent :

1. **Publication d'une version incorrecte** : sans un processus sécurisé, il y a un risque de déployer accidentellement une version de l'application contenant des bugs, des fonctions incomplètes ou des fonctionnalités non sécurisées.
2. **Exposition des paramètres de configuration** : lors de la publication, des informations sensibles, telles que des clés API, des mots de passe ou d'autres paramètres, pourraient être accidentellement incluses dans la version publique, offrant ainsi un point d'entrée pour les attaquants.
3. **Manipulation des fichiers lors du transfert** : sans un transfert sécurisé, les fichiers de l'application peuvent être interceptés, modifiés ou corrompus en cours de route vers le serveur de production.
4. **Non-révocation d'accès temporaire** : pour faciliter la publication, il peut être courant d'accorder des droits d'accès temporaires. Si ces droits ne sont pas révoqués après la publication, cela pourrait laisser des ouvertures pour une intrusion malveillante.
5. **Absence de sauvegarde avant publication** : ne pas effectuer de sauvegardes avant une mise à jour peut rendre difficile, voire impossible, le retour à une version précédente en cas de problème.
6. **Publication non autorisée** : un processus non sécurisé pourrait permettre à des personnes non autorisées de publier des versions malveillantes de l'application ou de la mettre hors ligne.
7. **Réutilisation d'anciens composants** : sans un contrôle adéquat, il est possible de réutiliser accidentellement d'anciens composants ou bibliothèques avec des vulnérabilités connues lors de la publication.

Le processus de publication d'une application est tout aussi essentiel que le développement de l'application elle-même. Si cette étape n'est pas traitée avec les précautions nécessaires, elle pourrait annuler tous les efforts antérieurs consacrés à la sécurisation de l'application. Il est donc essentiel de s'assurer que le processus de publication est sécurisé pour garantir l'intégrité de l'application et la confiance des utilisateurs.

## C. Mesures de sécurité pour une publication sécurisée d'une application web

### Les mesures de sécurité à prendre lors de la publication d'une application web

Lorsqu'il s'agit de mettre en ligne une application web, la sécurité doit être au cœur de chaque décision. Le protocole de transfert joue un rôle primordial. Au lieu de recourir à des méthodes traditionnelles, **privilégiez des protocoles de transfert sécurisés comme le SFTP ou le SCP**. Ces derniers chiffrent les données lors du transfert, rendant toute interception presque impossible.

Mais ce n'est que le début. Avant même de penser à mettre en ligne, **chaque ligne de code** doit être scrupuleusement **vérifiée**. C'est crucial pour s'assurer qu'aucune information sensible, telle que des mots de passe ou des clés API, ne soit exposée accidentellement.

**L'utilisation d'environnements de préproduction**, communément appelés « *staging* », s'avère être une étape intermédiaire précieuse. Dans cet espace, la version finale de l'application est testée en conditions réelles, sans toutefois toucher le grand public. Cela évite des surprises désagréables une fois en ligne.

Mais même avec des précautions, les choses peuvent mal tourner. D'où l'importance de toujours avoir une **sauvegarde complète** de votre application. En cas d'échec ou de problème, une restauration rapide est alors à portée de main.

La sécurité concerne aussi les personnes. **L'accès au serveur de production** doit être soigneusement **contrôlé**. Dans l'idéal, seules quelques personnes clés devraient avoir ce privilège, et uniquement pour la durée nécessaire.

Une fois en ligne, le travail ne s'arrête pas. **La surveillance continue** est essentielle pour s'assurer que tout fonctionne comme prévu. Toute activité suspecte doit être immédiatement signalée et traitée. En outre, il est essentiel d'avoir un plan d'action solide en cas d'incident de sécurité.

En fin de compte, la mise en ligne sécurisée d'une application web est un processus continu, combinant **prévention, surveillance et intervention**. C'est un investissement nécessaire pour garantir la confiance des utilisateurs et la réputation de votre application sur le long terme.

## D. Exercice : Quiz

[solution n°1 p.13]

### Question 1

Pourquoi le SFTP est-il recommandé lors du transfert de fichiers pour la mise en ligne d'une application web ?

- ☐ Il est plus rapide que le FTP
- ☐ Il chiffre les données lors du transfert
- ☐ Il prend en charge les fichiers volumineux

### Question 2

Quelle est la principale raison d'utiliser un environnement de préproduction ou « *staging* » avant de mettre une application en ligne ?

- ☐ Pour augmenter la capacité de stockage de l'application
- ☐ Pour tester l'application dans des conditions réelles sans toucher au grand public
- ☐ Pour accélérer la vitesse de l'application

### Question 3

Pourquoi est-il essentiel de vérifier le code avant la mise en ligne de l'application ?

- ☐ Pour s'assurer qu'il n'y a pas de fautes d'orthographe
- ☐ Pour garantir que l'application est visuellement attrayante
- ☐ Pour s'assurer qu'aucune information sensible n'est exposée accidentellement

### Question 4

Quelle est l'une des principales raisons pour limiter l'accès au serveur de production lors de la publication d'une application web ?

- ☐ Pour réduire la charge sur le serveur
- ☐ Pour éviter les conflits de version entre les développeurs
- ☐ Pour minimiser les risques de brèches de sécurité ou d'erreurs humaines

### Question 5

Pourquoi est-il important de continuer à surveiller une application web même après sa mise en ligne ?

- ☐ Pour s'assurer que l'application attire plus de visiteurs
- ☐ Pour surveiller l'espace de stockage de l'application
- ☐ Pour détecter et répondre rapidement à toute activité suspecte ou à tout problème de sécurité

### III. Protocoles et outils de publication sécurisée

#### A. Présentation des protocoles de publication sécurisée : SCP (Secure Copy Protocol) et SSH (Secure Shell)

##### Les protocoles de publication sécurisée tels que SCP et SSH

La publication sécurisée est cruciale pour garantir que les données transférées restent confidentielles et intègres. Parmi les méthodes de transfert de données les plus sécurisées, SCP et SSH sont largement reconnus pour leur robustesse et leur efficacité.

- **SCP (Secure Copy Protocol) :**

SCP est un protocole qui permet le transfert sécurisé de fichiers entre un ordinateur local et un ordinateur distant, ou entre deux ordinateurs distants, en utilisant le protocole SSH pour assurer la sécurité du transfert. Les principales caractéristiques de SCP incluent :

- **Sécurité** : tout comme SSH, SCP offre un transfert de fichiers chiffré, garantissant que les données restent privées pendant le transfert.
- **Intégrité** : avec SCP, il y a une assurance que les fichiers transférés ne sont pas altérés ou corrompus pendant le processus.
- **Authentification** : SCP utilise une authentification basée sur une clé publique ou un mot de passe pour garantir que seules les personnes autorisées peuvent transférer ou accéder aux fichiers.

- **SSH (Secure Shell) :**

SSH est un protocole permettant de se connecter de manière sécurisée à un serveur distant. Il offre des fonctionnalités au-delà du simple transfert de fichiers, notamment :

- **Connexion sécurisée** : SSH chiffre la session, empêchant l'écoute clandestine et garantissant que les données sensibles, comme les mots de passe, ne sont pas exposées.
- **Tunnélisation** : SSH peut encapsuler d'autres protocoles (comme FTP) pour offrir une couche supplémentaire de sécurité pendant le transfert.
- **Authentification** : tout comme SCP, SSH utilise une authentification basée sur une clé publique ou un mot de passe.

Fondamental	Les avantages et les fonctionnalités de chaque protocole
-------------	--

Les protocoles SCP et SSH offrent un moyen fiable et sécurisé de transférer et d'accéder aux données. Leur capacité à chiffrer les données pendant le transfert est essentielle pour garantir la confidentialité et l'intégrité des informations.

En utilisant SCP ou SSH lors de la publication d'une application web, les développeurs et administrateurs peuvent avoir confiance dans le fait que les données et les codes sources sont protégés contre les interceptions malveillantes.

#### B. Présentation d'outils simples tels que FileZilla pour la publication sécurisée

##### Des outils simples tels que FileZilla pour faciliter la publication sécurisée d'une application web

La publication sécurisée d'une application web nécessite souvent l'utilisation d'outils qui simplifient le processus tout en garantissant que la sécurité n'est pas compromise. FileZilla est l'un de ces outils, largement adopté par la communauté, qui offre une interface conviviale pour la gestion des transferts de fichiers sécurisés.

**FileZilla :**

FileZilla est un client FTP, FTPS (FTP over SSL/TLS) et SFTP (SSH File Transfer Protocol) gratuit et open source, disponible pour Windows, Linux et macOS. Il est apprécié pour sa simplicité d'utilisation et ses riches fonctionnalités. Voici quelques-uns des avantages et caractéristiques de FileZilla en matière de publication sécurisée :

- **Support de multiples protocoles** : FileZilla prend en charge FTP, qui est un protocole standard pour le transfert de fichiers, ainsi que FTPS et SFTP, qui ajoutent des couches de sécurité au transfert.
- **Interface graphique conviviale** : FileZilla offre une interface graphique intuitive qui facilite la navigation, le glisser-déposer des fichiers, et la gestion des transferts en cours.
- **Gestion des connexions sécurisées** : FileZilla permet d'enregistrer les paramètres de connexion sécurisée, y compris les clés privées pour SFTP, dans son gestionnaire de sites. Ceci accélère les connexions ultérieures aux mêmes serveurs.
- **Transferts simultanés** : FileZilla est capable de gérer plusieurs transferts de fichiers en parallèle, ce qui peut accélérer le processus de publication.
- **Reprise des transferts interrompus** : dans le cas où un transfert est interrompu, FileZilla peut le reprendre là où il s'était arrêté, garantissant ainsi que les gros fichiers ou les longues listes de fichiers sont complètement transférés même en cas d'interruption.

En utilisant un outil comme FileZilla, les développeurs et les administrateurs peuvent gagner du temps et réduire les erreurs courantes associées au transfert manuel de fichiers. Tout en bénéficiant des garanties de sécurité des protocoles FTPS et SFTP, ils peuvent ainsi se concentrer davantage sur d'autres aspects de la publication et du déploiement de leurs applications web.

**C. Exercice : Quiz**

[solution n°2 p.14]

## Question 1

Lequel des protocoles suivants est considéré comme une version sécurisée du FTP qui utilise le protocole SSH ?

- ☐ FTPS
- ☐ HTTPS
- ☐ SCP
- ☐ SFTP

## Question 2

Pourquoi FileZilla est-il populaire pour la publication sécurisée d'une application web ?

- ☐ Il prend uniquement en charge le protocole FTP
- ☐ Il propose une interface graphique conviviale
- ☐ Il ne permet pas de reprendre les transferts interrompus
- ☐ Il est payant

## Question 3

Quel protocole utilise une couche de sécurité SSL/TLS pour encrypter le transfert de fichiers ?

- ☐ HTTPS
- ☐ FTPS
- ☐ SFTP
- ☐ SCP

Question 4

Quelle affirmation concernant SCP est vraie ?

- ☐ SCP ne prend en charge que le transfert de texte
- ☐ SCP est basé sur le protocole SSH
- ☐ SCP est moins sécurisé que FTP
- ☐ SCP est principalement utilisé pour le transfert de pages web

Question 5

Dans FileZilla, quelle fonctionnalité permet de gagner du temps lors de connexions ultérieures aux mêmes serveurs ?

- ☐ L'interface de glisser-déposer
- ☐ Le support des transferts simultanés
- ☐ Le gestionnaire de sites
- ☐ Le répertoire de fichiers distants

## IV. Bonnes pratiques et vérifications de sécurité

### A. Présentation des bonnes pratiques pour une publication sécurisée

#### Les bonnes pratiques à suivre pour assurer une publication sécurisée

La publication sécurisée d'une application web ne se limite pas simplement à l'utilisation de protocoles et d'outils sécurisés. Elle s'appuie également sur une série de bonnes pratiques qui doivent être suivies avant, pendant et après la publication pour garantir l'intégrité et la sécurité de l'application.

#### Méthode

#### La gestion des autorisations des fichiers et des dossiers, la mise en place de règles de pare-feu pour renforcer la sécurité et le contrôle des accès et des autorisations

- **Gestion des autorisations des fichiers et des dossiers** : avant de publier une application web, il est essentiel de vérifier les autorisations de tous les fichiers et dossiers pour s'assurer qu'ils ne sont accessibles qu'aux utilisateurs appropriés. Les fichiers sensibles, comme les fichiers de configuration contenant des identifiants, doivent être particulièrement protégés et restreints pour éviter tout accès non autorisé.
- **Mise en place de règles de pare-feu** : un pare-feu joue un rôle crucial pour surveiller et contrôler le trafic réseau entrant et sortant d'une application ou d'un serveur. Pour une publication sécurisée, il est crucial d'établir des règles précises permettant uniquement le trafic nécessaire et bloquant tout autre trafic potentiellement malveillant.



- **Contrôle des accès et des autorisations** : la gestion des accès est centrale dans la sécurisation de la publication. Il s'agit de s'assurer que seules les personnes appropriées ont les droits nécessaires pour accéder, modifier ou gérer l'application. Cela implique l'utilisation d'authentification forte, la gestion rigoureuse des comptes d'utilisateur et la mise en œuvre de principes tels que le moindre privilège, où les utilisateurs n'ont que les droits strictement nécessaires pour effectuer leurs tâches.

Enfin, la publication sécurisée nécessite une vigilance constante et une réévaluation régulière des mesures de sécurité en place. Avec l'évolution constante des menaces et des technologies, il est impératif de rester informé et prêt à adapter et améliorer les mesures de sécurité pour garantir la sécurité continue de l'application web.

## B. Vérification de l'intégrité des fichiers publiés

Méthode	Comment vérifier l'intégrité des fichiers publiés
---------	---

Lors de la publication d'une application web, il est essentiel de garantir l'intégrité des fichiers publiés. Cela implique de s'assurer que les fichiers n'ont pas été altérés, corrompus ou remplacés par des versions malveillantes durant leur transfert ou leur stockage.

Pour vérifier l'intégrité, on utilise couramment des sommes de contrôle (ou « *hashes* »). Ces sommes représentent une valeur fixe pour un fichier donné, basée sur son contenu. Avant la publication, on génère la somme de contrôle du fichier original et, une fois le fichier publié ou transféré, on génère à nouveau sa somme de contrôle pour s'assurer qu'elle correspond à l'originale. Les outils comme SHA-256 ou MD5 sont couramment utilisés à cette fin, bien que SHA-256 soit préférable pour sa robustesse.

## C. Sensibilisation à la mise à jour régulière des applications et des systèmes

### Importance de la mise à jour régulière des applications et des systèmes pour maintenir la sécurité de la publication

La mise à jour régulière des applications et des systèmes est une composante fondamentale de la sécurité d'une publication web. En effet, les cyberattaquants sont constamment à la recherche de vulnérabilités dans les logiciels et systèmes obsolètes pour les exploiter.

Avec chaque mise à jour, les éditeurs de logiciels corrigent des bugs, comblent des vulnérabilités et améliorent les performances générales de leurs produits. En négligeant ces mises à jour, on expose non seulement l'application à des risques potentiels, mais on compromet également la sécurité des utilisateurs et des données.

Il est donc crucial de mettre en place une routine de mise à jour régulière et d'être informé des dernières versions disponibles pour tous les éléments de l'infrastructure de publication : système d'exploitation, serveurs, bases de données, frameworks, plugins, etc. Cette démarche proactive garantit une sécurité renforcée et offre une meilleure expérience pour les utilisateurs, tout en préservant la réputation de l'entreprise ou de l'organisation en charge de la publication.

## D. Exercice : Quiz

[solution n°3 p.15]

### Question 1

Pourquoi est-il essentiel de garantir l'intégrité des fichiers lors de leur publication sur le web ?

- ☐ Pour éviter une consommation excessive de bande passante
- ☐ Pour s'assurer que les fichiers n'ont pas été altérés ou remplacés par des versions malveillantes
- ☐ Pour réduire la taille des fichiers
- ☐ Pour garantir une bonne expérience utilisateur

### Question 2

Quel est un outil couramment utilisé pour vérifier l'intégrité des fichiers ?

- ☐ FTP
- ☐ MD5
- ☐ HTML5
- ☐ CSS3

Question 3

Pourquoi est-il vital de mettre à jour régulièrement les applications et les systèmes ?

- ☐ Pour obtenir de nouvelles fonctionnalités uniquement
- ☐ Pour corriger des bugs et combler des vulnérabilités
- ☐ Pour changer l'apparence de l'application
- ☐ Pour augmenter le coût de maintenance

Question 4

Quel risque encourt une entreprise qui néglige la mise à jour régulière de ses systèmes et applications ?

- ☐ Une baisse des ventes
- ☐ Une diminution des visites sur son site web
- ☐ La compromission de la sécurité des utilisateurs et des données
- ☐ Une meilleure réputation

Question 5

Quelle démarche doit être adoptée pour assurer une publication sécurisée d'une application web ?

- ☐ Ignorer toutes les mises à jour
- ☐ Publier l'application le plus rapidement possible
- ☐ Suivre les bonnes pratiques, vérifier l'intégrité des fichiers et mettre à jour régulièrement
- ☐ Se fier uniquement aux retours des utilisateurs pour identifier les problèmes

## V. L'essentiel

La sécurisation de la publication d'une application web est une étape cruciale dans le développement et le déploiement d'une application. Il a été souligné qu'une publication non sécurisée expose l'application à des risques variés, allant de la corruption de fichiers à la mise en danger des données sensibles des utilisateurs.

En utilisant des protocoles sécurisés comme SCP et SSH, combinés à des outils tels que FileZilla, les développeurs peuvent garantir une transmission sécurisée de leurs applications.

Toutefois, la publication ne se termine pas une fois l'application mise en ligne : une attention particulière doit être accordée à la vérification de l'intégrité des fichiers et à la mise à jour régulière des systèmes et des applications pour répondre aux nouvelles menaces. Dans un environnement professionnel, négliger ces étapes peut entraîner des conséquences financières, juridiques et de réputation.

En somme, la sécurité lors de la publication d'une application web n'est pas seulement une étape technique, mais une composante essentielle de la stratégie globale de cybersécurité d'une entreprise.

## VI. Auto-évaluation

### A. Exercice

Vous êtes un développeur junior au sein de la société WebSafe Inc. L'équipe vient de terminer le développement d'une nouvelle application web et il est maintenant temps de la publier. Cependant, le chef de projet a insisté sur l'importance de la sécurité pendant le processus de publication. Votre tâche est d'assurer une publication sécurisée de l'application.

#### Question 1

[solution n°4 p.16]

Quels sont les deux protocoles sécurisés que vous pourriez utiliser pour transférer les fichiers de l'application vers le serveur de production ?

#### Question 2

[solution n°5 p.16]

Vous choisissez d'utiliser FileZilla pour le transfert des fichiers. Comment garantissez-vous que le transfert est sécurisé ?

#### Question 3

[solution n°6 p.16]

Avant la publication, vous souhaitez vérifier l'intégrité de vos fichiers. Quelle technique pouvez-vous utiliser pour vous assurer qu'ils n'ont pas été altérés depuis leur dernière mise à jour ?

#### Question 4

[solution n°7 p.17]

Votre chef de projet vous a demandé de restreindre l'accès à certaines parties de l'application web. Comment pouvez-vous gérer efficacement les droits d'accès pour différents utilisateurs ou groupes d'utilisateurs ?

### B. Test

#### Exercice 1 : Quiz

[solution n°8 p.17]

Question 1

Pourquoi est-il important de sécuriser la publication d'une application web ?

- ☐ Pour augmenter la vitesse de publication
- ☐ Pour assurer la confidentialité, l'intégrité et la disponibilité des données
- ☐ Pour avoir une belle interface utilisateur

Question 2

Quel outil peut être utilisé pour une publication sécurisée ?

- ☐ WinRAR
- ☐ FileZilla avec SFTP
- ☐ Paint

Question 3

Qu'est-ce que SCP ?

- ☐ Secure Control Protocol
- ☐ System Copy Protocol
- ☐ Secure Copy Protocol

Question 4

Quelle est l'une des bonnes pratiques à suivre pour garantir la sécurité lors de la publication ?

- ☐ Utiliser le même mot de passe pour tous les comptes
- ☐ Ignorer les mises à jour du système
- ☐ Gérer les autorisations des fichiers et des dossiers

Question 5


Pourquoi est-il important de vérifier l'intégrité des fichiers publiés ?

- ☐ Pour garantir que les fichiers n'ont pas été altérés ou corrompus pendant le transfert
- ☐ Pour rendre le site web plus attractif
- ☐ Pour réduire la taille des fichiers

## Solutions des exercices


**Exercice p. 5 Solution n°1****Question 1**

Pourquoi le SFTP est-il recommandé lors du transfert de fichiers pour la mise en ligne d'une application web ?

- ☐ Il est plus rapide que le FTP
- ☒ Il chiffre les données lors du transfert
- ☐ Il prend en charge les fichiers volumineux
-  Le SFTP (Secure File Transfer Protocol) est préféré, car il chiffre les données lors du transfert, offrant une sécurité accrue contre les interceptions.


**Question 2**

Quelle est la principale raison d'utiliser un environnement de préproduction ou « *staging* » avant de mettre une application en ligne ?

- ☐ Pour augmenter la capacité de stockage de l'application
- ☒ Pour tester l'application dans des conditions réelles sans toucher au grand public
- ☐ Pour accélérer la vitesse de l'application
-  L'environnement de préproduction permet de tester l'application en conditions réelles, repérant ainsi d'éventuels problèmes sans impacter les utilisateurs finaux.


**Question 3**

Pourquoi est-il essentiel de vérifier le code avant la mise en ligne de l'application ?

- ☐ Pour s'assurer qu'il n'y a pas de fautes d'orthographe
- ☐ Pour garantir que l'application est visuellement attrayante
- ☒ Pour s'assurer qu'aucune information sensible n'est exposée accidentellement
-  Vérifier le code est crucial pour s'assurer qu'aucune donnée ou information sensible ne soit accidentellement incluse ou exposée lors de la mise en ligne.


**Question 4**

Quelle est l'une des principales raisons pour limiter l'accès au serveur de production lors de la publication d'une application web ?

- ☐ Pour réduire la charge sur le serveur
- ☐ Pour éviter les conflits de version entre les développeurs
- ☒ Pour minimiser les risques de brèches de sécurité ou d'erreurs humaines
-  En limitant l'accès au serveur de production, on minimise les risques associés aux erreurs humaines et aux menaces potentielles qui pourraient compromettre la sécurité de l'application.

**Question 5**


Pourquoi est-il important de continuer à surveiller une application web même après sa mise en ligne ?

- ☐ Pour s'assurer que l'application attire plus de visiteurs
- ☐ Pour surveiller l'espace de stockage de l'application
- ☒ Pour détecter et répondre rapidement à toute activité suspecte ou à tout problème de sécurité
-  Une surveillance continue est essentielle pour garantir la sécurité et l'intégrité de l'application, permettant une détection et une intervention rapides en cas de problèmes ou d'activités suspectes.

### Exercice p. 7 Solution n°2


#### Question 1

Lequel des protocoles suivants est considéré comme une version sécurisée du FTP qui utilise le protocole SSH ?

- ☐ FTPS
- ☐ HTTPS
- ☐ SCP
- ☒ SFTP
-  SFTP (SSH File Transfer Protocol) est une version sécurisée de FTP qui utilise le protocole SSH pour encrypter le transfert de données. Ce n'est pas la même chose que FTPS, qui est FTP sécurisé avec SSL/TLS.


#### Question 2

Pourquoi FileZilla est-il populaire pour la publication sécurisée d'une application web ?

- ☐ Il prend uniquement en charge le protocole FTP
- ☒ Il propose une interface graphique conviviale
- ☐ Il ne permet pas de reprendre les transferts interrompus
- ☐ Il est payant
-  FileZilla est apprécié pour sa simplicité d'utilisation, son interface conviviale et sa prise en charge des protocoles sécurisés comme FTPS et SFTP, en plus de nombreuses autres fonctionnalités.


#### Question 3

Quel protocole utilise une couche de sécurité SSL/TLS pour encrypter le transfert de fichiers ?

- ☐ HTTPS
- ☒ FTPS
- ☐ SFTP
- ☐ SCP
-  FTPS (FTP Secure) est une extension du FTP qui ajoute le support de la sécurité SSL/TLS pour encrypter le transfert de fichiers.


#### Question 4

Quelle affirmation concernant SCP est vraie ?

- ☐ SCP ne prend en charge que le transfert de texte
- ☒ SCP est basé sur le protocole SSH
- ☐ SCP est moins sécurisé que FTP
- ☐ SCP est principalement utilisé pour le transfert de pages web
-  SCP (Secure Copy Protocol) est basé sur le protocole SSH, ce qui le rend sécurisé pour le transfert de fichiers. Il n'est pas limité au transfert de texte et est généralement plus sécurisé que FTP simple.

#### Question 5


Dans FileZilla, quelle fonctionnalité permet de gagner du temps lors de connexions ultérieures aux mêmes serveurs ?

- ☐ L'interface de glisser-déposer
- ☐ Le support des transferts simultanés
- ☒ Le gestionnaire de sites
- ☐ Le répertoire de fichiers distants
-  Le gestionnaire de sites de FileZilla permet d'enregistrer les paramètres de connexion, y compris les clés privées pour SFTP, ce qui accélère les connexions ultérieures aux mêmes serveurs.

### Exercice p. 9 Solution n°3


#### Question 1

Pourquoi est-il essentiel de garantir l'intégrité des fichiers lors de leur publication sur le web ?

- ☐ Pour éviter une consommation excessive de bande passante
- ☒ Pour s'assurer que les fichiers n'ont pas été altérés ou remplacés par des versions malveillantes
- ☐ Pour réduire la taille des fichiers
- ☐ Pour garantir une bonne expérience utilisateur
-  La vérification de l'intégrité s'assure que le fichier n'a pas été modifié de manière non autorisée, évitant ainsi la mise en ligne de versions corrompues ou malveillantes.


#### Question 2

Quel est un outil couramment utilisé pour vérifier l'intégrité des fichiers ?

- ☐ FTP
- ☒ MD5
- ☐ HTML5
- ☐ CSS3
-  MD5 est un algorithme couramment utilisé pour générer une somme de contrôle (ou « hash ») pour un fichier afin de vérifier son intégrité.


#### Question 3

Pourquoi est-il vital de mettre à jour régulièrement les applications et les systèmes ?

- ☐ Pour obtenir de nouvelles fonctionnalités uniquement
- ☒ Pour corriger des bugs et combler des vulnérabilités
- ☐ Pour changer l'apparence de l'application
- ☐ Pour augmenter le coût de maintenance
-  Les mises à jour sont souvent fournies pour corriger des bugs, combler des vulnérabilités et améliorer les performances. Négliger ces mises à jour expose l'application à des risques potentiels.


#### Question 4

Quel risque encourt une entreprise qui néglige la mise à jour régulière de ses systèmes et applications ?

- ☐ Une baisse des ventes
- ☐ Une diminution des visites sur son site web
- ☒ La compromission de la sécurité des utilisateurs et des données
- ☐ Une meilleure réputation
-  Négliger les mises à jour peut exposer l'entreprise à des vulnérabilités qui, une fois exploitées, peuvent compromettre la sécurité des utilisateurs et des données.

#### Question 5

Quelle démarche doit être adoptée pour assurer une publication sécurisée d'une application web ?

- ☐ Ignorer toutes les mises à jour
- ☐ Publier l'application le plus rapidement possible
- ☒ Suivre les bonnes pratiques, vérifier l'intégrité des fichiers et mettre à jour régulièrement
- ☐ Se fier uniquement aux retours des utilisateurs pour identifier les problèmes
-  Pour assurer une publication sécurisée, il est essentiel de suivre les bonnes pratiques, de garantir l'intégrité des fichiers et de s'engager dans une routine de mise à jour régulière.

#### p. 11 Solution n°4

SCP (Secure Copy Protocol) et SSH (Secure Shell).

#### p. 11 Solution n°5

En utilisant SFTP (Secure File Transfer Protocol) avec FileZilla et en vérifiant l'authenticité du serveur avant d'établir la connexion.

#### p. 11 Solution n°6

L'utilisation de hachages, comme SHA-256, pour générer une empreinte digitale (ou hash) du fichier. En comparant le hash avant et après le transfert, vous pouvez vérifier si le fichier a été modifié ou non.




**p. 11 Solution n°7**

Utiliser un système de gestion des droits d'accès basé sur des rôles (RBAC, Role-Based Access Control). Avec RBAC, on attribue des droits à des rôles spécifiques plutôt qu'à des utilisateurs individuels. Ensuite, on assigne ces rôles aux utilisateurs, garantissant ainsi que chaque utilisateur a uniquement les permissions nécessaires pour effectuer ses tâches.


**Exercice p. 11 Solution n°8****Question 1**

Pourquoi est-il important de sécuriser la publication d'une application web ?

- ☐ Pour augmenter la vitesse de publication
- ☒ Pour assurer la confidentialité, l'intégrité et la disponibilité des données
- ☐ Pour avoir une belle interface utilisateur
-  La sécurisation de la publication est cruciale pour protéger l'application contre d'éventuelles menaces et garantir que les données restent confidentielles, intègres et disponibles.


**Question 2**

Quel outil peut être utilisé pour une publication sécurisée ?

- ☐ WinRAR
- ☒ FileZilla avec SFTP
- ☐ Paint
-  FileZilla, lorsqu'il est utilisé avec SFTP, garantit un transfert sécurisé des fichiers.


**Question 3**

Qu'est-ce que SCP ?

- ☐ Secure Control Protocol
- ☐ System Copy Protocol
- ☒ Secure Copy Protocol
-  SCP signifie Secure Copy Protocol.

**Question 4**

Quelle est l'une des bonnes pratiques à suivre pour garantir la sécurité lors de la publication ?

- ☐ Utiliser le même mot de passe pour tous les comptes
- ☐ Ignorer les mises à jour du système
- ☒ Gérer les autorisations des fichiers et des dossiers
-  La gestion des autorisations garantit que seules les personnes autorisées ont accès à des informations spécifiques.

**Question 5**

---

Pourquoi est-il important de vérifier l'intégrité des fichiers publiés ?

- ☒ Pour garantir que les fichiers n'ont pas été altérés ou corrompus pendant le transfert
- ☐ Pour rendre le site web plus attractif
- ☐ Pour réduire la taille des fichiers
- ☐ Vérifier l'intégrité des fichiers assure qu'ils n'ont pas été modifiés de manière malveillante ou accidentelle pendant le transfert.