

# Les guides de tests

# Table des matières

<b>I. Contexte</b>	<b>3</b>
<b>II. Introduction à la veille technologique en développement</b>	<b>3</b>
A. Introduction à l'importance des guides de tests dans la sécurité des applications web.....	3
B. Présentation de l'OWASP (Open Web Application Security Project) .....	3
C. Rôle de l'OWASP Testing Guide .....	4
D. Avantages de l'utilisation d'un guide de tests reconnu.....	4
E. Exercice : Quiz .....	5
<b>III. Les différentes catégories de tests</b>	<b>6</b>
A. Tests de sécurité .....	6
B. Tests de vulnérabilité .....	7
C. Tests fonctionnels .....	8
D. Exercice : Quiz.....	8
<b>IV. L'essentiel</b>	<b>10</b>
<b>V. Auto-évaluation</b>	<b>11</b>
A. Exercice .....	11
B. Test.....	11
<b>Solutions des exercices</b>	<b>12</b>

## I. Contexte

**Durée : 1 H**

**Prérequis : notions élémentaires en développement logiciel**

**Environnement de travail : navigateur web**

### Contexte

Les guides de tests jouent un rôle crucial dans le domaine de la sécurité des applications web. Pour un développeur, il est essentiel de comprendre l'importance de ces guides et de savoir comment les utiliser afin d'assurer la fiabilité et la sécurité des applications développées.

Lors du processus de développement d'une application web, la sécurité est un aspect fondamental à prendre en considération. En raison de la fréquence croissante et de la sophistication des attaques informatiques, il est impératif de mettre en œuvre des tests de sécurité rigoureux afin de détecter et de corriger les potentielles vulnérabilités.

Ce cours spécialisé dans les guides de tests permet d'améliorer ses compétences en matière de tests de sécurité, offrant ainsi l'opportunité d'optimiser la qualité et la sécurité des applications web.

## II. Introduction à la veille technologique en développement

### A. Introduction à l'importance des guides de tests dans la sécurité des applications web

#### Présentation de l'importance des guides de tests dans le domaine de la sécurité des applications web

Au fur et à mesure que le paysage numérique évolue, les applications web sont devenues un élément central des opérations commerciales, de l'engagement client et du stockage d'informations.

Tandis que ces applications offrent des avantages substantiels en termes d'efficacité et de connectivité, elles introduisent également une série de vulnérabilités qui, si elles ne sont pas correctement gérées, peuvent exposer des organisations à des risques considérables. C'est là qu'intervient l'importance des guides de tests.

Ces guides fournissent une méthodologie structurée pour évaluer, identifier et rectifier les vulnérabilités potentielles dans les applications web, garantissant ainsi leur sécurité et leur fiabilité.

### Rappel Importance de la sécurité dans le développement web

Dans le passé, le développement web était davantage axé sur les fonctionnalités et la performance. Cependant, avec l'augmentation des cyberattaques, la sécurité est devenue un élément incontournable du processus de développement.

Aujourd'hui, ignorer la sécurité revient à inviter activement les cybercriminels à exploiter votre application, mettant en péril non seulement les données de votre organisation, mais aussi la confiance des utilisateurs et votre réputation.

Voici un lien vers un article de l'ANSSI sur les bonnes pratiques pour sécuriser un site web : ANSSI<sup>1</sup>

### B. Présentation de l'OWASP (Open Web Application Security Project)

#### Présentation de l'OWASP en tant qu'organisation reconnue dans le domaine de la sécurité des applications web

L'OWASP, ou Open Web Application Security Project, est une organisation à but non lucratif qui œuvre pour améliorer la sécurité des logiciels à travers le monde.

---

<sup>1</sup> <https://www.ssi.gouv.fr/guide/recommandations-pour-la-securisation-des-sites-web/>

Fondée en 2001, cette entité se distingue par son approche collaborative, rassemblant des professionnels, des chercheurs, des éducateurs et des experts en sécurité du monde entier.

L'OWASP est reconnue pour son objectivité, son engagement à créer des outils et des ressources ouverts et gratuits, et sa détermination à éduquer les organisations et les individus sur les meilleures pratiques de sécurité des applications web.

Lien : OWASP<sup>1</sup>

#### **Rappel** Rôle de l'OWASP dans la sensibilisation à la sécurité des applications web

L'importance de l'OWASP dans le monde de la cybersécurité ne peut être sous-estimée. Au-delà de son rôle de fournisseur d'outils et de ressources, l'organisation joue un rôle majeur dans la sensibilisation à la sécurité des applications web.

Parmi ses contributions les plus notables, citons le célèbre « *OWASP Top Ten* », une liste régulièrement mise à jour des dix principales vulnérabilités des applications web.

Ce document est largement reconnu comme une référence incontournable pour les développeurs et les professionnels de la sécurité afin de comprendre et de prévenir les menaces les plus courantes.

### **C. Rôle de l'OWASP Testing Guide**

#### **Explication du rôle de l'OWASP Testing Guide en tant que référence pour les tests de sécurité des applications web**

Parmi les nombreuses initiatives de l'OWASP, leur Testing Guide se distingue comme une référence essentielle pour quiconque cherche à comprendre et à mettre en œuvre des tests de sécurité pour des applications web.

Ce guide offre un cadre détaillé et structuré pour la réalisation de tests de sécurité, englobant des techniques, des outils, et des meilleures pratiques. Il couvre un large éventail de scénarios de menaces potentielles et fournit des directives sur la manière de les identifier et de les atténuer.

#### **Définition** Définition de l'OWASP Testing Guide et son importance dans l'industrie de la sécurité des applications web

L'**OWASP Testing Guide** est un document structuré et complet créé par l'OWASP pour fournir une référence claire sur le test de sécurité des applications web. Il est organisé en plusieurs sections, chacune axée sur une catégorie spécifique de tests, tels que les tests d'authentification, les tests de session management, etc.

Le guide est conçu pour être utilisé à la fois par les débutants dans le domaine de la sécurité et par les experts, afin de garantir une approche uniforme et exhaustive du test de sécurité.

Lien : [owasp.org](https://owasp.org)<sup>2</sup>

### **D. Avantages de l'utilisation d'un guide de tests reconnu**

#### **Présentation des avantages de l'utilisation d'un guide de tests reconnu pour garantir la fiabilité et la sécurité d'une application web.**

L'utilisation d'un guide de tests reconnu, comme l'OWASP Testing Guide, apporte de multiples avantages à toute équipe de développement ou de sécurité.

Un tel guide fournit une méthodologie structurée et éprouvée qui élimine les approximations et assure une couverture complète des différents scénarios de vulnérabilités.

<sup>1</sup> <https://owasp.org>

<sup>2</sup> [https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP\\_Testing\\_Guide\\_v4.pdf](https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf)

Grâce à cela, les équipes peuvent identifier de manière proactive et systématique les éventuelles faiblesses de l'application avant qu'elles ne soient exploitées par des acteurs malveillants.

- **Couverture complète** : les guides reconnus offrent une vue d'ensemble exhaustive des tests de sécurité nécessaires, assurant ainsi qu'aucun aspect crucial n'est négligé.
- **Standardisation** : en suivant un guide standardisé, les équipes peuvent assurer une cohérence dans le processus de test, rendant les résultats comparables et mesurables au fil du temps.
- **Mise à jour régulière** : les guides reconnus, en particulier ceux gérés par des organisations renommées comme l'OWASP, sont fréquemment mis à jour pour refléter le paysage changeant des menaces.
- **Gagner la confiance** : utiliser un guide de tests reconnu peut augmenter la confiance des parties prenantes, des clients et des utilisateurs, sachant que l'application a été testée selon une norme industrielle.
- **Économie de temps** : plutôt que de réinventer la roue ou de passer du temps à chercher comment effectuer certains tests, les équipes peuvent se référer directement au guide pour obtenir des instructions claires et précises.
- **Réduction des risques** : en identifiant et en traitant les vulnérabilités de manière proactive, les entreprises peuvent éviter d'éventuelles violations de données coûteuses et préserver leur réputation.

#### **Conseil** L'importance de suivre un guide de tests reconnu pour améliorer la sécurité des applications web

Lors de l'adoption d'un guide de tests, il est crucial de l'intégrer pleinement dans les workflows de l'équipe et de s'assurer que tous les membres comprennent son importance. Des sessions de formation régulières et des ateliers peuvent aider à familiariser l'équipe avec le guide et à renforcer l'importance de chaque test.

En outre, il est conseillé de revoir et de mettre à jour régulièrement les pratiques de test à mesure que le guide évolue, afin de s'assurer que l'équipe est toujours à jour avec les dernières techniques et recommandations.

Suivre un guide de tests reconnu est une étape essentielle vers la création d'applications sécurisées et robustes. En mettant l'accent sur la sécurité dès le début, les entreprises peuvent non seulement protéger leurs actifs et leurs utilisateurs, mais aussi établir une position de leader en matière de sécurité dans leur secteur.

### **E. Exercice : Quiz**

[solution n°1 p.13]

#### Question 1

Pourquoi est-il essentiel de se référer à un guide de tests reconnu lors de la sécurité d'une application web ?

- ☐ Pour garantir une esthétique cohérente de l'application
- ☐ Pour assurer une méthodologie de test structurée et complète
- ☐ Pour réduire le temps de développement de l'application

#### Question 2

Quelle organisation est reconnue pour ses contributions majeures dans la sensibilisation à la sécurité des applications web ?

- ☐ Microsoft
- ☐ Google
- ☐ OWASP

#### Question 3

Quel est le rôle principal de l'OWASP Testing Guide ?

- ☐ Fournir un tutoriel sur le développement web
- ☐ Servir de référence pour les tests de sécurité des applications web
- ☐ Présenter les meilleures pratiques de conception d'interface utilisateur

Question 4

Quel avantage l'utilisation d'un guide de tests reconnu n'offre-t-il **PAS** ?

- ☐ Gagner la confiance des utilisateurs
- ☐ Faire une promotion pour l'application
- ☐ Réduire les risques liés à la sécurité

Question 5

En suivant un guide de tests reconnu, quel est l'un des principaux avantages pour une entreprise ?

- ☐ Augmenter ses ventes directement
- ☐ Éviter d'éventuelles violations de données coûteuses
- ☐ Diminuer la nécessité d'une équipe de développement compétente

### III. Les différentes catégories de tests

#### A. Tests de sécurité

**Présentation des tests de sécurité couramment utilisés, tels que les tests d'injection (SQL, XSS), les tests d'authentification et d'autorisation, les tests de configuration, etc.**

Les tests de sécurité sont essentiels pour s'assurer que les applications web sont résistantes contre les diverses menaces qui prévalent sur Internet. Ces tests consistent à évaluer systématiquement l'application pour détecter d'éventuelles vulnérabilités, garantissant ainsi la protection des données de l'utilisateur et la fonctionnalité intégrale du système.

**Types courants de tests de sécurité :**

1. **Tests d'injection** : ces tests vérifient les vulnérabilités qui peuvent permettre à un attaquant d'insérer ou « injecter » un code malveillant dans l'application. Les plus courants sont l'injection SQL (où des requêtes malveillantes sont insérées dans une entrée qui est ensuite traitée par la base de données) et l'injection XSS (où des scripts malveillants sont injectés dans des pages web et exécutés par d'autres utilisateurs).
2. **Tests d'authentification et d'autorisation** : ces tests vérifient comment l'application gère les droits d'accès pour différents utilisateurs. Il s'agit de s'assurer que seuls les utilisateurs autorisés ont accès aux fonctionnalités ou aux données appropriées.
3. **Tests de configuration** : ils évaluent la sécurité des configurations du serveur, de la base de données et des autres composants de l'application pour s'assurer qu'il n'y a pas de failles permettant des accès non autorisés.

#### **Exemple** Illustration d'un scénario de test d'injection SQL et de ses conséquences

##### **Scénario de test d'injection SQL :**

- **Description** : un site de commerce électronique permet aux utilisateurs de rechercher des produits en entrant un mot-clé dans une barre de recherche.
- **Test** : au lieu d'un mot-clé produit, un code SQL est entré : `OR « 1' = » 1``. Si la barre de recherche est vulnérable à une injection SQL, cette entrée pourrait retourner tous les produits de la base de données.

- **Conséquences** : si un attaquant est capable de manipuler la base de données de cette manière, il pourrait potentiellement accéder à des informations sensibles, telles que les détails des utilisateurs, voire modifier ou supprimer des données. Cela peut entraîner des pertes financières pour l'entreprise, une violation de la confidentialité des utilisateurs et une perte de confiance dans le service.

L'importance des tests de sécurité ne peut être sous-estimée. Avec la montée des cyberattaques et les exigences réglementaires croissantes en matière de protection des données, il est essentiel que toutes les applications web soient testées régulièrement et minutieusement pour garantir leur résilience face aux menaces.

## B. Tests de vulnérabilité

### Présentation des tests de vulnérabilité, tels que les tests de détection de vulnérabilités connues, les tests de gestion des erreurs, etc.

Les tests de vulnérabilité jouent un rôle crucial pour identifier et corriger les points faibles potentiels d'une application ou d'un système. Ces tests visent à déceler les vulnérabilités avant qu'elles ne soient exploitées par des cybercriminels, garantissant ainsi l'intégrité, la disponibilité et la confidentialité des données et des systèmes.

Contrairement aux tests de pénétration qui simulent des attaques réelles, les tests de vulnérabilité se concentrent sur la détection des failles sans nécessairement les exploiter.

#### Types courants de tests de vulnérabilité :

1. **Tests de détection de vulnérabilités connues** : ces tests exploitent des bases de données de vulnérabilités connues pour identifier les failles dans le système. Des outils comme Nessus ou OpenVAS peuvent être utilisés pour cela.
2. **Tests de gestion des erreurs** : ces tests examinent comment l'application ou le système gère les erreurs. Une mauvaise gestion des erreurs peut révéler des informations sensibles à un attaquant, comme des détails de configuration ou même des données utilisateur.
3. **Tests de patches et de mises à jour** : ils évaluent si tous les composants du système sont à jour et patchés contre les vulnérabilités connues. Les systèmes obsolètes ou non patchés peuvent offrir une porte d'entrée facile pour les attaquants.

#### Exemple Exemple de vulnérabilité de gestion des erreurs et son impact sur la sécurité

##### Scénario de vulnérabilité de gestion des erreurs :

- **Description** : supposons qu'un utilisateur tente de se connecter à une application web avec des informations d'identification incorrectes.
- **Comportement attendu** : l'application devrait renvoyer un message d'erreur générique comme « *Identifiant ou mot de passe incorrect* ».
- **Comportement observé** : au lieu de cela, l'application renvoie « *Identifiant incorrect* ». Dans une autre tentative avec un bon identifiant mais un mauvais mot de passe, l'application renvoie « *Mot de passe incorrect pour cet utilisateur* ».
- **Impact sur la sécurité** : cette mauvaise gestion des erreurs fournit un indice à un attaquant sur la validité de l'identifiant. Un attaquant peut ainsi savoir si un identifiant particulier existe, ce qui peut faciliter d'autres types d'attaques, comme le brute-forcing.

La détection et la correction des vulnérabilités est une étape essentielle du cycle de vie du développement. La prise de conscience et l'attention portée à ces vulnérabilités permettent non seulement d'améliorer la sécurité, mais aussi de renforcer la confiance des utilisateurs dans l'application ou le système.

## C. Tests fonctionnels

### Présentation des tests fonctionnels visant à vérifier le bon fonctionnement de l'application web

Les tests fonctionnels jouent un rôle essentiel dans le processus de développement des applications web. Ils ont pour but principal de s'assurer que l'application fonctionne comme elle est censée le faire, selon les exigences définies et les spécifications.

Plutôt que de se concentrer sur les aspects techniques sous-jacents, les tests fonctionnels vérifient le comportement de l'application du point de vue de l'utilisateur.

#### Principaux objectifs des tests fonctionnels :

1. **Valider les fonctionnalités** : assurez-vous que toutes les fonctionnalités de l'application fonctionnent comme prévu.
2. **Tester les interfaces utilisateur** : valider que l'interface utilisateur fonctionne correctement et est intuitive pour les utilisateurs.
3. **Examiner les interactions de base de données** : vérifier que les données sont correctement interrogées, stockées, mises à jour et effacées.
4. **Tester les scénarios d'utilisation** : simuler des scénarios d'utilisation réelle pour garantir que l'application se comporte de manière appropriée.

#### Méthode Méthodes et outils couramment utilisés pour réaliser des tests fonctionnels

Réaliser des tests fonctionnels requiert une méthodologie précise, ainsi que l'utilisation d'outils adaptés pour automatiser et faciliter ces tests.

##### Étapes courantes pour les tests fonctionnels :

1. **Définition des exigences** : établissez clairement les fonctionnalités que l'application est censée fournir et les résultats attendus.
2. **Création des scénarios de test** : sur la base des exigences, élaborer des scénarios ou des cas de test pour vérifier chaque fonctionnalité.
3. **Préparation des données de test** : identifiez et préparez les données nécessaires pour exécuter vos scénarios de test.
4. **Exécution des tests** : utilisez des outils de test fonctionnels pour exécuter les scénarios, soit manuellement, soit de manière automatisée.
5. **Analyse des résultats** : examinez les résultats pour identifier les échecs ou les écarts par rapport aux attentes.

##### Outils couramment utilisés pour les tests fonctionnels :

- **Selenium** : un outil d'automatisation de navigateur populaire qui permet d'écrire des scripts pour tester des applications web à travers différents navigateurs.
- **JUnit** : utilisé pour les tests unitaires en Java, il peut également être utilisé pour des tests fonctionnels.
- **TestNG** : inspiré de JUnit, il offre des fonctionnalités supplémentaires adaptées aux tests fonctionnels.
- **QTP/UFT** : outil commercial de Hewlett-Packard pour l'automatisation des tests.

En utilisant une combinaison de tests manuels et automatisés, les tests fonctionnels garantissent que les utilisateurs finaux obtiennent une application stable, fiable et fonctionnelle.

## D. Exercice : Quiz

[solution n°2 p.14]

### Question 1



Quel type de tests se concentre principalement sur la détection des vulnérabilités qui pourraient être exploitées par des attaquants ?

- ☐ Tests de charge
- ☐ Tests fonctionnels
- ☐ Tests d'interface utilisateur
- ☐ Tests de sécurité

Question 2

Lequel des tests suivants assure que l'application fonctionne correctement et conformément aux spécifications ?

- ☐ Tests fonctionnels
- ☐ Tests de performance
- ☐ Tests de vulnérabilité

Question 3

Dans quel type de tests serait-on principalement concerné par la façon dont l'application gère un grand nombre de requêtes sur une longue période ?

- ☐ Tests de charge
- ☐ Tests d'endurance
- ☐ Tests de sécurité
- ☐ Tests fonctionnels

Question 4

Lesquels des tests suivants se focalisent sur la détection des faiblesses d'une application, notamment en ce qui concerne les erreurs de gestion ?

- ☐ Tests d'interface utilisateur
- ☐ Tests fonctionnels
- ☐ Tests de vulnérabilité
- ☐ Tests de performance

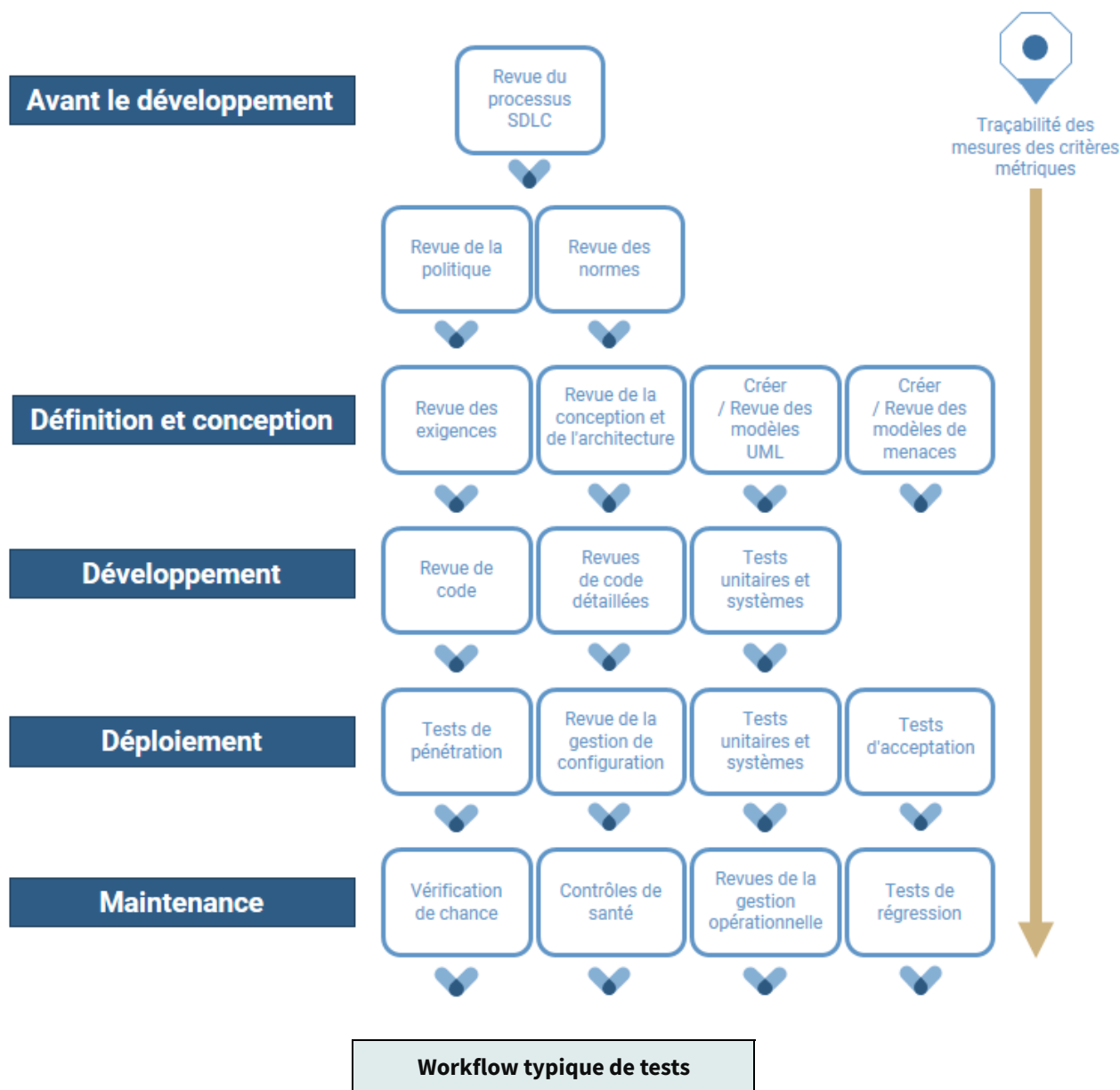
Question 5

Quel type de tests aiderait principalement à s'assurer que l'interface utilisateur de l'application est intuitive et répond aux attentes de l'utilisateur ?

- ☐ Tests de charge
- ☐ Tests de sécurité
- ☐ Tests d'interface utilisateur
- ☐ Tests fonctionnels

## IV. L'essentiel

Les tests sont conçus pour garantir la robustesse, l'efficacité et la sécurité des applications. Les tests de sécurité, notamment, sont essentiels pour déceler et prévenir des menaces courantes telles que les injections SQL et les failles XSS. Les tests de vulnérabilité, de leur côté, ciblent la détection de points faibles connus dans le système, permettant une correction proactive. Enfin, les tests fonctionnels s'assurent que chaque composant de l'application fonctionne comme prévu, assurant une expérience utilisateur optimale. En somme, l'intégration rigoureuse de ces tests dans le développement d'applications web est non seulement recommandée, mais elle est devenue une norme industrielle pour garantir la qualité et la sécurité des produits.



(Source : [owasp.org](https://owasp.org/)<sup>1</sup>)

<sup>1</sup> <https://owasp.org/>

## V. Auto-évaluation

### A. Exercice

Dans cet exercice, vous serez confronté à plusieurs scénarios de développement d'applications web. Votre mission sera d'identifier les différentes catégories de tests appropriées pour chaque scénario.

Après avoir identifié les catégories de tests pour chaque scénario, expliquez brièvement pourquoi vous avez choisi cette catégorie et comment vous procéderiez à la mise en œuvre des tests.

#### Question 1

[solution n°3 p.15]

Vous êtes en train de développer une application e-commerce et souhaitez garantir que chaque fonctionnalité, de l'ajout d'un produit au panier à la finalisation de l'achat, fonctionne comme prévu.

#### Question 2

[solution n°4 p.15]

Votre équipe vient d'introduire une nouvelle fonctionnalité qui permet aux utilisateurs de se connecter via un réseau social. Vous souhaitez vous assurer qu'aucune donnée sensible n'est exposée lors de ce processus.

#### Question 3

[solution n°5 p.16]

Vous avez reçu des rapports indiquant que votre application pourrait être vulnérable à des attaques par injection SQL. Vous souhaitez vérifier et corriger cela.

#### Question 4

[solution n°6 p.16]

Votre application contient une fonctionnalité qui permet aux utilisateurs de télécharger et de partager des documents. Vous voulez vous assurer que les utilisateurs ne peuvent télécharger que les types de fichiers autorisés et qu'aucun malware ne peut être introduit via cette fonctionnalité.

### B. Test

#### Exercice 1 : Quiz

[solution n°7 p.16]

##### Question 1

Quelle organisation est particulièrement reconnue pour sa contribution majeure à la sensibilisation à la sécurité des applications web ?

- ☐ Microsoft
- ☐ Google
- ☐ OWASP
- ☐ Apple

##### Question 2

Quelle est la principale différence entre les tests de vulnérabilité et les tests de pénétration ?

- ☐ Les tests de vulnérabilité sont réalisés après les tests de pénétration
- ☐ Les tests de pénétration simulent des attaques réelles, tandis que les tests de vulnérabilité se concentrent sur la détection des failles
- ☐ Il n'y a aucune différence ; les termes sont interchangeables
- ☐ Les tests de vulnérabilité sont toujours automatisés, tandis que les tests de pénétration sont manuels

##### Question 3

Quel type de tests est essentiel pour s'assurer que les applications web sont résistantes aux menaces courantes sur Internet ?

- ☐ Tests de charge
- ☐ Tests d'interface utilisateur
- ☐ Tests fonctionnels
- ☐ Tests de sécurité

#### Question 4

Lors de la réalisation d'un test d'injection SQL, quel type de code un testeur pourrait-il entrer pour vérifier la vulnérabilité ?

- ☐ ``<script>alert(« Hacked! »);</script>``
- ☐ `« OR « 1' = » 1``
- ☐ ``SELECT * FROM users WHERE username = »``
- ☐ ``#include <stdio.h>``

#### Question 5


Quel avantage l'utilisation d'un guide de tests reconnu, comme l'OWASP Testing Guide, n'offre-t-il **PAS** ?

- ☐ Augmentation directe des ventes
- ☐ Méthodologie de test structurée et complète
- ☐ Réduction des risques liés à la sécurité
- ☐ Standardisation du processus de test

## Solutions des exercices


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

Pourquoi est-il essentiel de se référer à un guide de tests reconnu lors de la sécurité d'une application web ?

- ☐ Pour garantir une esthétique cohérente de l'application
- ☒ Pour assurer une méthodologie de test structurée et complète
- ☐ Pour réduire le temps de développement de l'application
-  Utiliser un guide de tests reconnu assure une méthodologie de test structurée et complète, garantissant que tous les aspects cruciaux de la sécurité sont pris en compte.


**Question 2**

Quelle organisation est reconnue pour ses contributions majeures dans la sensibilisation à la sécurité des applications web ?

- ☐ Microsoft
- ☐ Google
- ☒ OWASP
-  L'OWASP (Open Web Application Security Project) est une organisation mondialement reconnue pour sa contribution à la sensibilisation à la sécurité des applications web.


**Question 3**

Quel est le rôle principal de l'OWASP Testing Guide ?

- ☐ Fournir un tutoriel sur le développement web
- ☒ Servir de référence pour les tests de sécurité des applications web
- ☐ Présenter les meilleures pratiques de conception d'interface utilisateur
-  L'OWASP Testing Guide est principalement utilisé comme une référence pour effectuer des tests de sécurité des applications web, garantissant une couverture complète des potentiels scénarios de vulnérabilité.


**Question 4**

Quel avantage l'utilisation d'un guide de tests reconnu n'offre-t-il **PAS** ?

- ☐ Gagner la confiance des utilisateurs
- ☒ Faire une promotion pour l'application
- ☐ Réduire les risques liés à la sécurité
-  Bien que suivre un guide de tests reconnu puisse indirectement augmenter la réputation de l'application en raison de normes de sécurité élevées, sa fonction principale n'est pas la promotion de l'application.

**Question 5**


En suivant un guide de tests reconnu, quel est l'un des principaux avantages pour une entreprise ?

- ☐ Augmenter ses ventes directement
- ☒ Éviter d'éventuelles violations de données coûteuses
- ☐ Diminuer la nécessité d'une équipe de développement compétente
-  L'un des avantages majeurs d'utiliser un guide de tests reconnu est de minimiser les vulnérabilités et d'éviter ainsi des violations de données qui peuvent être coûteuses en termes financiers et de réputation.

## Exercice p. 8 Solution n°2


### Question 1

Quel type de tests se concentre principalement sur la détection des vulnérabilités qui pourraient être exploitées par des attaquants ?

- ☐ Tests de charge
- ☐ Tests fonctionnels
- ☐ Tests d'interface utilisateur
- ☒ Tests de sécurité
-  Les tests de sécurité sont conçus pour identifier et prévenir les vulnérabilités qui pourraient être exploitées par des attaquants, compromettant ainsi la sécurité de l'application.


### Question 2

Lequel des tests suivants assure que l'application fonctionne correctement et conformément aux spécifications ?

- ☒ Tests fonctionnels
- ☐ Tests de performance
- ☐ Tests de vulnérabilité
-  Les tests fonctionnels se concentrent sur le comportement de l'application, s'assurant que toutes les fonctionnalités offrent les résultats attendus pour l'utilisateur final.

### Question 3


Dans quel type de tests serait-on principalement concerné par la façon dont l'application gère un grand nombre de requêtes sur une longue période ?

- ☐ Tests de charge
- ☒ Tests d'endurance
- ☐ Tests de sécurité
- ☐ Tests fonctionnels
-  Les tests d'endurance examinent la capacité de l'application à gérer une charge continue sur une longue période sans dégradation des performances.

### Question 4

Lesquels des tests suivants se focalisent sur la détection des faiblesses d'une application, notamment en ce qui concerne les erreurs de gestion ?


- ☐ Tests d'interface utilisateur
- ☐ Tests fonctionnels
- ☒ Tests de vulnérabilité
- ☐ Tests de performance

 Les tests de vulnérabilité se concentrent sur la détection des points faibles ou des vulnérabilités d'une application, y compris les erreurs de gestion qui pourraient exposer des informations sensibles.

### Question 5

Quel type de tests aiderait principalement à s'assurer que l'interface utilisateur de l'application est intuitive et répond aux attentes de l'utilisateur ?

- ☐ Tests de charge
- ☐ Tests de sécurité
- ☒ Tests d'interface utilisateur
- ☐ Tests fonctionnels

 Les tests d'interface utilisateur évaluent l'ergonomie, la convivialité et la réactivité de l'interface utilisateur, garantissant ainsi une expérience utilisateur positive.

### p. 11 Solution n°3

Catégorie de tests : tests fonctionnels.

Explication : les tests fonctionnels permettent de s'assurer que chaque fonctionnalité de l'application fonctionne comme prévu, garantissant ainsi une expérience utilisateur optimale. Dans le contexte d'une application e-commerce, cela implique de vérifier que tous les processus, de l'ajout d'un produit au panier à la finalisation de l'achat, se déroulent sans accroc.

Mise en œuvre des tests : pour mettre en œuvre les tests fonctionnels, je commencerais par créer des cas de test pour chaque fonctionnalité de l'application e-commerce. J'utiliserais un outil de test automatisé pour simuler l'ajout d'un produit au panier, la navigation à travers le processus de paiement, et la finalisation de l'achat. Chaque étape serait vérifiée pour s'assurer qu'elle se déroule comme prévu.

### p. 11 Solution n°4

Catégorie de test : tests d'authentification et d'autorisation.

Explication : l'intégration d'une nouvelle fonctionnalité de connexion via un réseau social nécessite de vérifier que l'authentification et l'autorisation se font correctement, sans exposer de données sensibles. Il est essentiel de s'assurer que seuls les utilisateurs autorisés ont accès aux fonctionnalités ou aux données appropriées.

Mise en œuvre des tests : pour tester l'authentification via un réseau social, je mettrais en place des tests automatisés qui tentent de se connecter avec différents scénarios d'utilisateurs (utilisateur valide, utilisateur invalide, etc.). Je vérifierais également que les données sensibles ne sont pas exposées pendant le processus.

**p. 11 Solution n°5**

Catégorie de test : tests de sécurité (spécifiquement tests d'injection).

Explication : les tests d'injection, en particulier l'injection SQL, visent à vérifier la vulnérabilité de l'application face aux tentatives d'insertion de requêtes malveillantes dans la base de données. Si l'application est vulnérable, des mesures doivent être prises pour rectifier cette faille.

Mise en œuvre des tests : pour tester la vulnérabilité à l'injection SQL, j'utiliserais des outils spécifiques d'évaluation de la sécurité et je tenterais d'injecter des requêtes SQL malveillantes dans les champs d'entrée de l'application. Si une injection réussit, je prendrais note de la vulnérabilité pour la corriger.

**p. 11 Solution n°6**

Catégorie de test : tests de sécurité et tests fonctionnels.

Explication : les tests de sécurité vérifient que seuls les types de fichiers autorisés peuvent être téléchargés, évitant ainsi la possibilité d'introduire des malwares. Les tests fonctionnels, quant à eux, s'assurent que la fonctionnalité de téléchargement fonctionne correctement du point de vue de l'utilisateur.


Mise en œuvre des tests : je commencerais par définir une liste blanche des types de fichiers autorisés et mettrais en place des tests automatisés pour tenter de télécharger des types de fichiers non autorisés. De plus, j'utiliserais des outils de détection de malwares pour scanner les fichiers téléchargés et m'assurer qu'aucun malware n'est introduit via cette fonctionnalité.

**Exercice p. 11 Solution n°7**

**Question 1**


Quelle organisation est particulièrement reconnue pour sa contribution majeure à la sensibilisation à la sécurité des applications web ?

- ☐ Microsoft
- ☐ Google
- ☒ OWASP
- ☐ Apple

 L'OWASP (Open Web Application Security Project) est une organisation mondiale non lucrative qui vise à améliorer la sécurité des logiciels.

**Question 2**

Quelle est la principale différence entre les tests de vulnérabilité et les tests de pénétration ?


- ☐ Les tests de vulnérabilité sont réalisés après les tests de pénétration
  - ☒ Les tests de pénétration simulent des attaques réelles, tandis que les tests de vulnérabilité se concentrent sur la détection des failles
  - ☐ Il n'y a aucune différence ; les termes sont interchangeables
  - ☐ Les tests de vulnérabilité sont toujours automatisés, tandis que les tests de pénétration sont manuels
-  Les tests de pénétration cherchent à exploiter les vulnérabilités, tandis que les tests de vulnérabilité identifient et évaluent les failles sans nécessairement les exploiter.



### Question 3

Quel type de tests est essentiel pour s'assurer que les applications web sont résistantes aux menaces courantes sur Internet ?


- ☐ Tests de charge
- ☐ Tests d'interface utilisateur
- ☐ Tests fonctionnels
- ☒ Tests de sécurité

 Les tests de sécurité évaluent les applications pour détecter d'éventuelles vulnérabilités, garantissant ainsi la protection des données des utilisateurs et la fonctionnalité intégrale du système.

### Question 4

Lors de la réalisation d'un test d'injection SQL, quel type de code un testeur pourrait-il entrer pour vérifier la vulnérabilité ?


- ☐ ``<script>alert(« Hacked! »);</script>``
- ☒ `« OR « 1'= » 1``
- ☐ ``SELECT * FROM users WHERE username = »``
- ☐ ``#include <stdio.h>``

 Cette entrée est un exemple classique d'une tentative d'injection SQL, qui pourrait potentiellement retourner toutes les entrées d'une base de données si elle est vulnérable.

### Question 5

Quel avantage l'utilisation d'un guide de tests reconnu, comme l'OWASP Testing Guide, n'offre-t-il **PAS** ?

- ☒ Augmentation directe des ventes
- ☐ Méthodologie de test structurée et complète
- ☐ Réduction des risques liés à la sécurité
- ☐ Standardisation du processus de test

 Bien que l'utilisation d'un guide de tests reconnu puisse indirectement améliorer la réputation d'une application en raison de normes de sécurité élevées, sa fonction principale n'est pas de promouvoir directement les ventes.