Top 10 OWASP

|  |  |
| --- | --- |
| Elément | Description |
| **Compétences** | **OO-1 : Reconnaître et pouvoir expliquer les menaces actuelles. Acquérir des informations actuelles sur ce thème (reconnaissance et contre-mesures), et pouvoir démontrer et expliquer les effets possibles.** |
| **Objectifs** | Citer les 10 risques de sécurité les plus répandus dans l’ordre de risque (top 10) |
| **Durée estimée** | 10 min |
| **Répertoire de travail** | Aucun |
| **Fichiers sources** | Aucun |
| **A produire** | Répondre aux questions directement dans ce document |
| **Moyens d’aide** | Rien |
| **Changelog** | Bulle DevOps |

# Question 1

Connecter à l’aide d’une flèche le nom du risque à sa définition.

|  |  |  |
| --- | --- | --- |
| Broken Access Control |  | Erreurs dans la mise en œuvre de mécanismes de journalisation et de surveillance appropriés, ce qui peut rendre difficile la détection rapide des incidents de sécurité ou l'analyse des activités suspectes |
| Cryptographic Failures |  | Vulnérabilités résultant de conceptions de sécurité faibles ou inexistantes au sein de l'architecture d'une application ou d'un système, ce qui rend difficile la mise en œuvre de contrôles de sécurité appropriés |
| Injection |  | Erreurs de configuration qui peuvent exposer involontairement des éléments de l'infrastructure, tels que des paramètres par défaut non sécurisés, des droits d'accès inappropriés ou des ports ouverts non nécessaires, pouvant être exploités par des attaquants. |
| Insecure Design |  | Utilisation de composants logiciels obsolètes ou vulnérables au sein d'une application, ce qui peut entraîner l'exploitation de failles de sécurité connues dans ces composants |
| Security Misconfiguration |  | Mauvaise gestion des contrôles d'accès dans une application ou un système, permettant à des utilisateurs non autorisés d'accéder à des ressources sensibles ou de modifier des données qu'ils ne sont pas autorisés à modifier. |
| Vulnerable and outdated Components |  | Vulnérabilités qui permettent à un attaquant d'injecter du code malveillant (comme du code SQL, NoSQL, OS ou LDAP) dans une application ou une base de données, pouvant entraîner l'exécution de commandes non autorisées ou la récupération de données sensible |
| Identification and Authentification Failures |  | Erreurs dans la mise en œuvre de techniques de chiffrement et de hachage, ce qui peut conduire à des fuites de données sensibles ou à des attaques de contournement du chiffrement. |
| Software and Data Integrity Failures |  | Vulnérabilités liées à l'authentification des utilisateurs, telles que la mauvaise gestion des mots de passe, la transmission non sécurisée des informations d'identification, ou la faible fiabilité des mécanismes d'authentification |
| Security Logging and Monitoring Failures |  | Vulnérabilité qui permet à un attaquant de forcer le serveur à effectuer des requêtes vers des ressources internes ou externes, pouvant entraîner l'exposition de données sensibles ou l'exploitation de services internes. |
| Server-Side Request Forgery (SSRF) |  | Vulnérabilités qui permettent à un attaquant de modifier ou de corrompre des données stockées dans une application ou un système, compromettant ainsi l'intégrité des données et pouvant entraîner des résultats indésirables ou malveillants. |

# Liens et références

<https://owasp.org/www-project-top-ten/>