OWASP (Open Web Application Security Project)

L'OWASP (Open Web Application Security Project) est une organisation mondiale à but non lucratif qui se consacre à la sécurité des applications logicielles. Depuis sa création en 2001, l'OWASP se concentre sur l'amélioration de la sécurité des logiciels grâce à des projets collaboratifs, des outils gratuits, des documents de formation, des forums et des conférences. Voici une vue d'ensemble des principaux aspects de l'OWASP :

1. Projets OWASP

L'OWASP développe une multitude de projets visant à améliorer la sécurité des applications. Les plus connus incluent :

- **OWASP Top Ten** : Une liste des dix vulnérabilités les plus critiques dans les applications web. Elle est mise à jour régulièrement pour refléter les menaces actuelles et est largement utilisée par les développeurs et les professionnels de la sécurité pour orienter leurs efforts de sécurisation.
- **OWASP SAMM (Software Assurance Maturity Model)** : Un cadre permettant aux organisations de formuler et de mettre en œuvre une stratégie de sécurité logicielle adaptée à leurs risques spécifiques.
- **OWASP ASVS (Application Security Verification Standard)** : Un cadre de vérification de la sécurité des applications qui fournit un guide pour tester la sécurité des applications web.
- **OWASP ZAP (Zed Attack Proxy)** : Un outil de test de sécurité des applications web, très utilisé pour identifier les vulnérabilités dans les applications.

2. OWASP Top Ten

L'OWASP Top Ten est l'un des documents les plus influents et les plus consultés. Voici les catégories de vulnérabilités qui sont souvent présentes dans le Top Ten :

1. **Injection** : Problèmes où des données non fiables sont envoyées à un interpréteur en tant que partie d'une commande ou d'une requête. Les injections SQL, OS et LDAP sont des exemples courants.
2. **Violation de la gestion de l'authentification et des sessions** : Problèmes où des attaquants peuvent exploiter des faiblesses dans l'authentification ou la gestion des sessions pour usurper l'identité d'un utilisateur.
3. **Exposition de données sensibles** : Problèmes où des informations sensibles sont exposées aux utilisateurs ou aux attaquants, souvent à cause de l'absence de chiffrement approprié.
4. **XML External Entities (XXE)** : Vulnérabilités liées à l'analyse de XML où des entités externes peuvent être utilisées pour divulguer des données internes.
5. **Contrôle d'accès insuffisant** : Problèmes où les utilisateurs peuvent accéder à des fonctions ou à des données pour lesquelles ils n'ont pas les autorisations appropriées.
6. **Mauvaise configuration de sécurité** : Problèmes dus à des configurations incorrectes ou insuffisantes des applications ou des serveurs, exposant ainsi les systèmes à des vulnérabilités.

7. **Cross-Site Scripting (XSS)** : Problèmes où les scripts malveillants peuvent être injectés dans des sites web et exécutés dans le navigateur des utilisateurs.
8. **Désérialisation non sécurisée** : Problèmes où des objets non fiables peuvent être désérialisés, conduisant à une exécution de code arbitraire ou à d'autres attaques.
9. **Utilisation de composants avec des vulnérabilités connues** : Problèmes dus à l'utilisation de bibliothèques, frameworks ou autres modules avec des vulnérabilités connues.
10. **Journalisation et surveillance insuffisantes** : Problèmes où des attaques ne sont pas détectées ou enregistrées, retardant ainsi les réponses et les remédiations.

3. Ressources et formations

L'OWASP offre une variété de ressources éducatives pour aider les développeurs et les professionnels de la sécurité à comprendre et à résoudre les problèmes de sécurité :

- **Guides de développement sécurisé** : Fournissent des pratiques exemplaires pour écrire du code sécurisé.
- **Formation et ateliers** : L'OWASP organise des sessions de formation et des ateliers lors de conférences et d'événements.
- **Cheatsheets** : Des résumés concis et pratiques des meilleures pratiques de sécurité pour diverses technologies et situations.

4. Communauté et événements

L'OWASP est également connue pour sa communauté dynamique et ses événements réguliers, tels que les Global AppSec conferences, les meetups locaux et les événements de capture the flag (CTF). Ces événements rassemblent des professionnels de la sécurité, des développeurs et des chercheurs pour partager des connaissances, des techniques et des expériences.