Sécuriser un Site WEB

La sécurité des sites web est une priorité pour toutes les entreprises. Compte tenu de leur exposition publique, les sites web sont des cibles privilégiées pour les attaquants, car ils peuvent représenter des portes d'entrée vers l'ensemble de l'infrastructure. Il est donc impératif de renforcer leur sécurité face aux cyberattaques potentielles.

Menaces visant la sécurité d'un site WEB

Pour garantir la sécurité des sites web, une compréhension approfondie des risques est essentielle :

- **Les attaques par injection SQL** exploitent les failles de sécurité des formulaires web, permettant aux attaquants d'insérer du code malveillant dans la base de données du site.
- **Les attaques par brute-force** consistent à utiliser des outils automatisés pour deviner les identifiants des utilisateurs et les mots de passe associés.
- **Les attaques par déni de service (DDoS)** visent à perturber le fonctionnement normal du site en envoyant un grand nombre de requêtes simultanées.
- **Les attaques de cross-site scripting (XSS)** permettent aux hackers d'injecter du code malveillant dans les pages web pour voler des informations sensibles.
- **Les attaques de cross-site request forgery (CSRF**) tentent de tromper les utilisateurs pour qu'ils effectuent des actions non désirées sur un site web en utilisant leur compte utilisateur.
- **L'exploitation de composants tiers vulnérables**, tels que des bibliothèques, plugins ou frameworks obsolètes, accroît le risque de compromission de la sécurité d'une application.

Bonnes pratiques de protection d'un site web

Pour assurer la sécurité d'un site WEB, des mesures sont nécessaires :

- ***Au niveau du site web :***
  - **Mises à jour régulières :** Assurez-vous que votre site web, ainsi que les plugins et les frameworks, sont régulièrement mis à jour.
  - **Filtrage et Validation des Entrées** : Appliquez des filtres pour valider et nettoyer toutes les données entrantes afin de prévenir les attaques par injection de code.
  - **Gestion des accès :** Limitez l'accès au site web uniquement aux personnes autorisées. Utilisez des mots de passe forts et mettez en place une authentification multifacteur (MFA).
- ***Au niveau du serveur :***
  - **Mises à jour régulières :** Maintenez à jour le système d'exploitation, les serveurs (ex : Apache, Nginx, etc.), ainsi que tous les logiciels et bibliothèques tiers utilisés.
  - **Sauvegardes Régulières :** Effectuez des sauvegardes fréquentes des données critiques et assurez-vous qu'elles peuvent être restaurées rapidement en cas de problème.
  - **Protection anti DDoS :** Utilisez des outils de protection anti-DDoS pour réduire les risques d'indisponibilité.
  - **Utilisation de Certificats SSL :** Assurez-vous que votre site utilise le protocole HTTPS pour chiffrer les données échangées entre le navigateur et le serveur.

Ressources pertinentes mises à disposition

- Accès Web pour les tiers de la **PGSSI-S** (PDF) ;
- Fiche réflexe en cas d'intrusion web de l'**ANS** (PDF) ;
- Sécuriser un site Web de **l'ANSSI** (site Web) ;
- Protéger son site internet des cyberattaques de **l'ANSSI** (site Web) ;
- Top 10 des vulnérabilités de **l'OWASP** (site Web).