Veille Technologique : La sécurisation des sites web

1. Description du thème choisi : La sécurisation des sites web

La sécurisation des sites web regroupe l'ensemble des pratiques, technologies et protocoles visant à protéger les sites internet contre les cyberattaques, les vulnérabilités logicielles et les risques liés à l'utilisation malveillante des données. Elle inclut la gestion des accès, la protection des données sensibles, et la prévention contre des attaques telles que les injections SQL, les attaques DDoS, ou encore les failles de configuration. En 2023, plus de 330 000 cyberattaques ont été réalisées et réussi sur des PME ou de plus grosses entreprises..

Avec l'explosion des services en ligne et du e-commerce, la sécurité des sites web est devenue une préoccupation majeure pour les entreprises, les développeurs et les utilisateurs. En 2021, plus de 3.5 millions de postes dans la cybersécurité étaient à pourvoir dans le monde. Le marché des cyberattaques malveillantes ne fait que s'accroître au fur et à mesure des années..

2. Pourquoi ce choix ?

J'ai choisi ce thème par rapport à :

L'importance croissante des sites web
Aujourd'hui, la sécurisation des sites devient de plus en plus cruciale pour une confiance optimale des utilisateurs et des clients. Chaque année un grand nombre d'entreprises arrivent sur ce marché faisant de nombreux nouveaux postes dans la cybersécurité.

Un domaine en constante évolution
Les menaces et les technologies de sécurisation des sites web progresse à une grande vitesse rendant nécessaire une vieille informatique active, avec des mises à jour hebdomadaires, voire quotidiennes.

Impact personnel et professionnel
Ce thème est pertinent pour les professionnels du numérique et les développeurs, car la sécurité est au cœur de la conception web.

J'ai fait ce choix du fait que je veux m'orienter dans ce domaine. Le fait que la sécurité est au cœur de la conception web me fascine, car réaliser un site web est une chose mais le protéger de manière professionnelle et sûre tous les jours en est une autre.

3. Mise en œuvre de la veille technologique

Pour réaliser cette veille technologique, plusieurs étapes et outils ont été mobilisés :

Sources utilisées :

- ★ **Sites spécialisés dans la cybersécurité** :
  - *L'ANSSI*
  - *Zataz.com*
  - *Silicon.fr*
  - *Infosécurité*
  - *Sécurité Weekly*
  - *L'usine Digitale*
  - *NextGov*
  - *Dark reading*
- ★ **Forums et communautés** :
  - Root Me
  - Reddit
  - Hack Forums

Outils et méthodes utilisés :

- ★ **Alertes Google** : Mise en place d'alertes avec des mots-clés comme "sécurisation site web", "cyberattaque web", "nouvelles failles web".
- ★ **Réseaux sociaux** : Twitter pour suivre des comptes influents dans le domaine de la cybersécurité.

4. Premiers éléments recueillis issus de la veille

Voici quelques résultats préliminaires obtenus :

Importance des certificats HTTPS :

> Beaucoup de sites utilisent encore HTTP, qui n'est pas sécurisé. Passer à HTTPS avec des certificats SSL gratuits, comme ceux offerts par Let's Encrypt, est une solution facile pour sécuriser les échanges entre les utilisateurs et le site.

Protéger les mots de passe :

> Il est recommandé de ne jamais stocker les mots de passe en clair dans les bases de données. Utiliser un algorithme de hachage, comme bcrypt, est une bonne pratique simple à mettre en place. D'autres algorithmes de hachage existent bien entendu mais certains ne sont pas assez sécurisés.

Mettre à jour régulièrement les logiciels :

> Les CMS comme WordPress et leurs extensions doivent être mis à jour fréquemment pour éviter d'être exposés à des failles connues.

Validation des formulaires utilisateur :

Une validation des données saisies par les utilisateurs permet d'éviter des attaques courantes comme l'injection SQL ou le XSS. C'est une mesure basique mais très efficace.

Créer des sauvegardes :

Toujours garder une copie de sauvegarde du site et de sa base de données. En cas d'attaque, cela permet de restaurer le site rapidement. De ce fait, la sauvegarde doit être faite de manière régulière, voire même plusieurs fois au cas ou.

Montée en puissance des attaques DDoS :

De nombreux sites et forums ont rapporté que les attaques DDOS ne font qu'augmenter, rendant aux entreprises l'obligation de se protéger et de modifier leurs protection.

Conclusion

Cette veille technologique souligne l'importance grandissante de sécuriser les sites web dans un environnement numérique de plus en plus vulnérable. Les premières observations indiquent que pour assurer une protection maximale,l'intégration des nouvelles technologies de sécurité ainsi que la formation des développeurs et la sensibilisation des utilisateurs sont essentielles.

La veille se poursuivra en explorant davantage les tendances émergentes que ce soit dans la sécurisation des API ou dans les technologies d'intelligence artificielle employées pour repérer les intrusions.