La sécurité des sites web est toujours d’actualité. Les menaces et les attaques sur les sites Web augmentent considérablement.

Étapes à suivre pour sécuriser votre site internet

Injections SQL

Les injections SQL sont très dangereuses, si un pirate parvient à les injecter dans notre site. Ces injections se déroulent à travers les formulaires Web que vous utilisez pour recueillir des informations auprès des visiteurs de votre site. Si vous ne soumettez pas les contraintes nécessaires à tous les champs d'un formulaire Web, les pirates informatisés pourront y insérer un code qui, à leur tour, leur permet de pirater notre base de données et de voler toute information confidentielle disponible.

Afin de protéger votre site web contre ces injections, il suffit d’utiliser en permanence des requêtes paramétrées. votre site Internet aura ainsi des paramètres spécifiques pour empêcher les pirates d’avoir accès à vos données et entrer leur code malveillant.

Les attaques XSS

Ces attaques sont similaires aux injections de SQL dans la mesure où les pirates utilisent des champs de formulaire Web des codes HTML pour y accéder. Cependant, ils sont beaucoup plus dangereux que les injections SQL. Les attaques XSS font référence à l'insertion de balises de script malveillantes et de JavaScript dans votre site Web, ce qui peut se propager sur les comptes de tous les visiteurs qui affichent la page sur laquelle il a été inséré.

Pour prévenir les attaques XSS, assurez-vous que les visiteurs n'ont pas les privilèges (ou opportunité) d'insérer des tags JavaScript ou script n'importe où sur notre site.

Mots de passe et protection

Il est préférable d'utiliser des mots de passe toujours plus complexes, mêlant lettres minuscules, majuscules, chiffres, et caractères spéciaux pour tous vos comptes et surtout pour le compte administrateur de votre site. N’utilisez jamais des mots de passe simples. N'utilisez pas de mots de passe tels que le nom de votre enfant ou votre date d’anniversaire, car les pirates informatiques peuvent habituellement accéder facilement à cette information.

De plus, assurez-vous que tous ceux qui ont accès à votre site Web utilisent un mot de passe sécurisé et impossible à deviner. L'utilisation d'un mot de passe faible par un utilisateur pourrait mettre en danger tout votre site Internet et tous les comptes visiteurs.

Utilisez HTTPS

En plus d'utiliser des plugins de sécurité, vous devriez également envisager de passer à HTTPS « protocole de transfert hypertexte sécurisé » pour renforcer davantage la sécurité de votre site. Les sites Web utilisant le protocole standard pour le transfert de données entre le serveur et le navigateur du client, HTTP ou protocole de transfert hypertexte sont susceptibles d'intercepter les données et de les utiliser de façon malveillante. HTTPS rend l'échange d'informations via votre site Web plus sécurisé et impénétrable.

L'utilisation de HTTPS est fortement conseillée pour un site e-commerce, ou un site traitant des informations confidentielles et privées sur des clients.

Choisissez le bon hébergeur

Vous pourrez, bien entendu, choisir votre hébergement en vous basant sur des offres très bon marché. Toutefois, vous risquez d'être exposé à des cybattaques. C'est pourquoi, il est raisonnable de trouver des fournisseurs d'hébergement Web réputés qui offrent des fonctionnalités telles qu'un serveur SSL sécurité (requis pour HTTPS), SSH Secure Shell Access, un support sécurisé par courrier électronique, une base de données sécurisée, des sauvegardes régulières, etc. Si vous avez des doutes concernant la sécurité d'hébergement des données, tentez de vous faire recommander un fournisseur. Venture Harbour a effectué des recherches et a comparé 53 fournisseurs différents d'hébergement Web pour ensuite, sélectionner les meilleurs d'entre eux.

Effectuer des mises à jour régulières

Cela peut sembler assez évident, mais c'est l'une des étapes les plus fondamentales et les plus importantes. Il est important de faire des mises à jour dès que possible à la sortie d'une nouvelle version de WordPress, en particulier les scripts ou les plugins. Beaucoup d'entre eux sont open-source, ce qui signifie que tout le monde peut analyser leur code source et découvrir les failles. Ces failles de sécurité sont l'une des façons les plus courantes pour les pirates d'accéder à votre site internet.

Pour sécuriser votre site Web de ces attaques, il est vivement recommandé de mettre à jour vos plugin, scripts et plateformes (comme WordPress)

Plugins de sécurité

WordPress (WP) est la plateforme de site web la plus utilisée. En plus de mettre à jour tous les logiciels, il est crucial pour un site WordPress d'utiliser des plugins de sécurité et lui garantir une sécurité maximale. Il existe de nombreux plugins de sécurité, gratuits et payants, pour garder votre site sécurisé.

Certains sont plus populaires que d’autres et incluent des plugins de sécurité. Ces plugins offrent des fonctionnalités supplémentaires pour rendre votre site WordPress sécurisé et réduire les risques de piratage.