BTS SIO SESSION 2020/2021

FICHE technique épreuve E6

Sécuriser son site WordPress.

Tables des matières

La table des matières permettra d'ordonnée mon travail.

Présentation de l'entreprise :

Dans le cadre de mon stage de deuxième année j'ai effectué un stage au sein de l'entreprise YggVal à Molsheim.

Cette société emploie une cinquantaine de salariés, qui sont divisés en 4 départements :

- Validation
- Infogérance
- Développement
- Formation

Le service principal est celui de la validation, c'est le cœur du métier de la société. La validation consiste à vérifier qu'un produit répond à un cahier des charges donné. Le produit soumis à validation peut être de tout type, équipement domotique, électroménager, téléphonique, etc. De ce fait, des connaissances dans de multiple domaines sont nécessaires, et YggVal dispose des ressources internes pour subvenir à ces besoins.

YggVal peut ainsi se charger du développement d'un logiciel, d'un site web, mais également de l'infrastructure réseau et informatique de ses clients. Afin de maintenir leurs compétences en développement et répondre à des demandes ponctuelles, YggVal a choisi de développer sa propre application : TilaMobile.

Celle-ci est un ERP entièrement personnalisable, accessible par internet permettant de consulter ses données et ses fichiers à distance. Cette application est utilisée par YggVal pour sa propre gestion, mais aussi, l'entreprise propose de la louer.
Au cours de ce stage, j'ai été affecté au département développement, cependant je n'ai pas travaillé sur TilaMobile mais sur un nouveau projet à part.

Ma mission a été de réaliser un site internet pour un Syndicat des eaux à l'aide du système de gestion de contenus, WordPress, tout en suivant le cahier des charges, et en prenant en compte les évolutions des besoins du client. J'ai donc eu à créer toutes les pages ainsi que leurs contenus. Afin de rendre un produit complet il est nécessaire de sécuriser le site. WordPress est un gestionnaire de contenue très populaire, ainsi énormément de personnes qui ne connaissent pas les dangers su web, créés leurs sites sans protection. Les pirates ne se privent pas et plusieurs sites WordPress se font pirater chaque jour.

Nom d'utilisateur

Lord de l'installation de WordPress l'administrateur, par défaut, a pour nom d'utilisateur "admin". Cependant, c'est le nom d'utilisateur qu'une personne mal intentionné utilise en premier lorsqu'il tente de s'introduire dans un site web sous WordPress.
Pour modifier cela il faut de connecter au tableau de bord WordPress et créer un nouvel utilisateur. C'est là qu'il faudra choisir un nouveau nom d'utilisateur. Une fois les champs remplient, il est très important de définir le rôle de cet utilisateur en tant Administrateur. Il faut penser à récupérer le mot de passe, pour cela cliquer sur Afficher le mot de passe et copier. Il faut se déconnecter et se connecter avec le nouvel utilisateur. Maintenant dans Utilisateurs > Tous les utilisateurs il faut supprimer l'ancien compte administrateur.

Mot de passe

Tous comme le nom d'utilisateur il est évident qu'un mot de passe fort est une bonne pratique. Un mot de passe long mêlant majuscules, minuscules, chiffres et symboles est recommandé. Pour modifier votre mot de passe d'administrateur de votre site WordPress, depuis la colonne de gauche de votre console d'administration, rendez-vous sur :
Utilisateurs > tous les utilisateurs, ensuite cliquer sur Modifier, sur l'utilisateur en question.

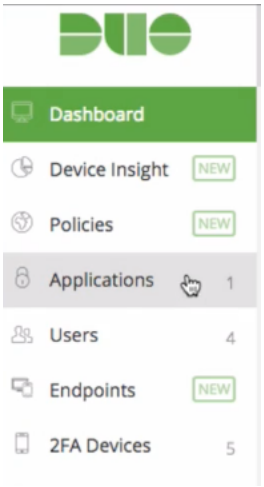
Puis, dans la section Gestion de compte, cliquer sur le bouton Générer un mot de passe, et saisir un mot de passe fort, finalement cliquer sur Mettre à jour le profil.

A2F

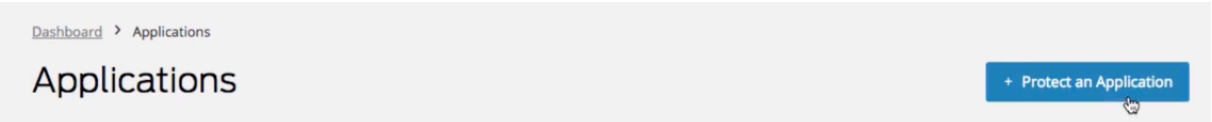
Afin de sécuriser au mieux l'accès au compte administrateur il est fréquent d'utiliser l'authentification à deux facteurs (A2F). Cela renforce la sécurité quel que soit la plateforme internet. Elle implique un processus de connexion en 2 étapes, entrer le bon mot de passe correspondant au compte. Mais aussi la validation de l'accès via un code envoyer par SMS ou un appel téléphonique.
Dans la plupart des cas, c'est 100 % efficace pour empêcher les attaques par force brute sur un site WordPress, car il faut avoir accès à votre téléphone portable.
Pour mettre en place cette authentification à deux facteurs il y a deux possibilités principales. Passer par l'hébergeur web qui peut offrir cette fonctionnalité. Ou bien utiliser une extension WordPress comme Duo Two-Factor Authentification, Google Authentification.

Installation de Duo Two-Factor.

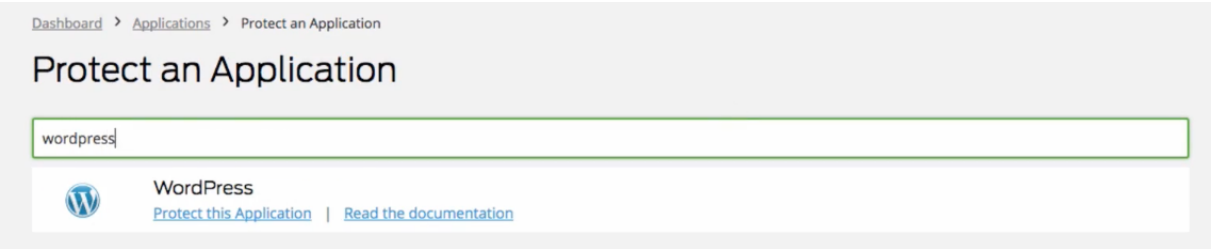
-Première étape créer un compte sur duo.com. DUO est l'entreprise qui a créé le plugin.
-Sur le Tableau de bord aller dans Applications.



-Sur cette page il faudra cliquer sur le bouton « protéger une application ».



-Chercher WordPress dans la barre de recherche et cliquer sur « protéger cette application ».

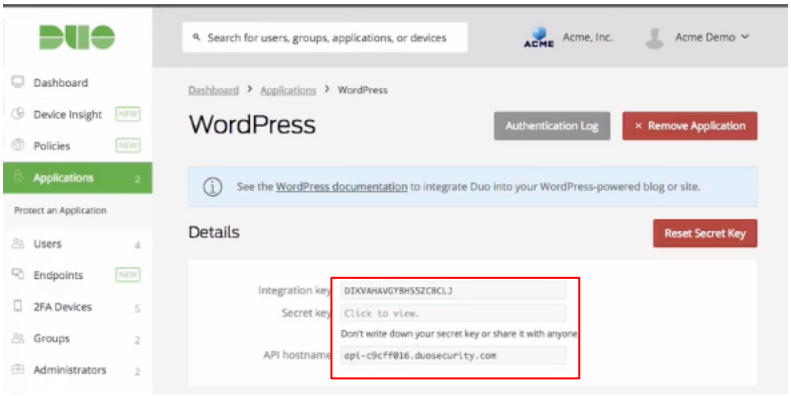


-Rendez-vous sur la documentation WordPress concernant DUO pour l'intégrer.

-Sur votre WordPress installer l'extension « Duo Two-Factor Authentification" dans l'onglet Extensions de votre tableau de bord WordPress.

-Une fois activé aller dans les settings.

-Un formulaire vous demandera les deux clés et le nom d'hôte qui se trouve sur la page Application de DUO.



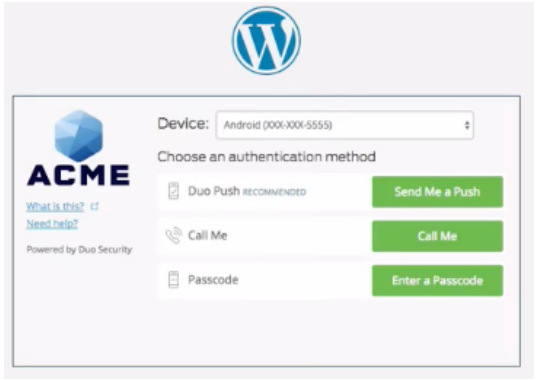
-Une fois remplit, vous pourrez choisir quel rôle aura à faire une A2F lors de sa connexion.

-Sauvegarder les changements.

-Si le rôle « Administrateur » a été choisi et que le compte WordPress est déjà lié à l'extension, le compte va être ajouter sa la base.

-Une page va s'ouvrir, elle permet de choisir de quelle manière la double authentification sera effectué.

Envoyer un push est la méthode la plus rapide. Une notification est envoyée sur votre mobile et un bouton valider l'accès et refuser l'accès sont affichés.



L'extension est installée sur WordPress.

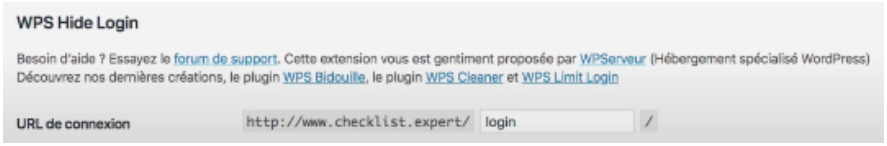
Liens

Tous les sites web WordPress ont des adresses URL semblables à :

www.votresite.com/wp-admin
www.votresite.fr/wp-login

Pour les mêmes raisons que le nom d'utilisateur "admin", il faut aussi de modifier l'URL de la page d'administration du site web de l'entreprise. Les pirates savent que l'URL par défaut se termine par "wp-admin" ou "wp-login". En changeant cela, vous gagnez facilement des points

dans vos actions pour sécuriser WordPress. La façon la plus simple consiste à utiliser une extension. De cette manière, vous personnalisez l'adresse URL de votre page de connexion.
Dans cette situation l'extensions WPS Hide Login est utilisé. Une fois installer via le menu WordPress « Extensions », il est possible d'aller dans l'onglet « Réglages » puis « Général » et en bas de la page un nouveau menu a été ajouté, « URL de connexion ». Celui-ci permet de modifier la fin de l'URL de connexion.



Par défaut, WordPress ne prend pas en compte le nombre de tentatives quand un visiteur essaie de pénétrer sur votre site avec plusieurs noms d'utilisateur et mots de passe lors de la connexion.
Des pirates utilisent des techniques avancées qui leur permettent de deviner le mot de passe en testant des millions de combinaisons de lettres et de chiffres.
Pour éviter ce type d'attaque et ajouter une couche de sécurité supplémentaire au site WordPress, il faut limitez le nombre de tentatives de connexion en utilisant une extension WordPress comme Login LockDown.
Cet outil bloque l'IP de tout pirate informatique qui tente ce type d'attaque sur votre site WordPress.
Facile à installer et configurer l'extension s'assure de limiter le nombre de tentatives de connexion incorrectes, un peu comme vous n'avez le droit qu'à 3 tentatives lors de la saisie de votre code PIN.

Https
Ne pas utiliser le protocole HTTP, toutes les informations sont transmises sur le réseau sans cryptage. Cela est le cas pour les informations d'identification, les commentaires, les numéros de carte bancaire… Et ceci depuis votre ordinateur ou ceux de vos visiteurs.

Pour pallier ce problème, l'installation d'un certificat SSL est recommandé. Ainsi, vous passez du protocole HTTP à HTTPS, le protocole le plus sécurisé qui crypte les données envoyées entre les visiteurs et le serveur hébergeant votre site web.

En plus de la sécurité obtenue, le passage à HTTPS offre de nombreux avantages, à savoir la confiance et la crédibilité de vos visiteurs ainsi que l'amélioration de référencement de votre site web. En effet, Google privilégie les sites sécurisés. OVH permet à ses utilisateurs de générer des certificat SSL gratuitement.

Sauvegarde

En cas d'attaque réussie, toutes ces techniques de sécurité ne permettent pas de restaurer votre site.

C'est pourquoi les sauvegardes régulières sont la solution ultime pour récupérer votre site web rapidement et facilement en cas d'attaque et de piratage ou de tout autre problème sur votre serveur.

Pour faire une sauvegarde complète d'un site web sous WordPress, il y a 3 solutions :

Penser à sauvegarder manuellement régulièrement,
Utiliser les outils de sauvegarde proposés par votre hébergeur web,
Utiliser des plugins comme BackupBuddy, WordPress Backup to DropBox ou VaultPress ou UpdraftPlus. C'est la solution la plus simple.
Avec ces 2 dernières solutions, vous pouvez :

Non seulement réaliser une sauvegarde sur demande, mais également planifier les sauvegardes quotidiennement. Ainsi, la sauvegarde est bien faite en temps et en heure.

Hébergeur

L'une des premières choses à faire lorsque l'on veut diffuser son site sur internet est de choisir un hébergeur. L'hébergement fait partie de zone sensible de votre site. Il est nécessaire de choisir un fournisseur de qualité à ce sujet. Celui-ci doit garantir une infrastructure robuste et sécurisée. Les serveurs doivent être régulièrement analysés en profondeur pour rechercher les éventuelles vulnérabilités et les logiciels malveillants. Le serveur doit également être configuré pour utiliser des protocoles de chiffrement de réseau et de transfert de fichiers sécurisés (tels que SFTP au lieu de FTP) afin de protéger les contenus sensibles des intrus malveillants. Enfin, tout logiciel installé sur la machine et destiné à protéger le contenu WordPress doit être compatible avec les derniers systèmes de gestion de base de données afin de maintenir des performances optimales.

Lors de mon stage nous avons choisi OVH comme hébergeur. Celui-ci met aussi à votre disposition une protection Anti-DDoS, offre un certificat SSL Let's Encrypt gratuitement, réalise de base des sauvegardes et restaurations à J-1 / J-2 / J-3 / J-7 / J-14, la protection par un pare-feu incluse. Seul point négatif le service client. En effet, réussir à avoir une personne au bout du fil peut prendre énormément de temps.

Finalement afin de protéger au mieux et complètement son site WordPress il est recommandé d'utiliser une extension de sécurité. Plusieurs extensions existent pour sécuriser son site, nous avons choisi Wordfence. Comme la plupart des extensions, les options de base sont gratuites, mais il faut payer pour accéder à la version Premium. La version gratuite permet de vérifier si un site est infecté et sécurise un site WordPress de manière générale.
L'extension envoie un avertissement si le code source du serveur est différent du code auquel l'extension se réfère. De plus, l'accès à toutes les IPs bloquées automatiquement, dont celles qui ont tenté de se connecter à votre WordPress sont disponibles. Il est possible de bloquer le nombre de tentatives ainsi que le nombre maximal de requêtes autorisées par minute.

WordPress est très ciblé par les pirates car il est très populaire. Il est donc nécessaire de faire des démarches pour protéger son site. D'autant plus que les première démarche ne sont pas longues ni compliqué.