



Rapport de stage

Hadjab Zineddine

Du 13 Mai au 14 Juin 2024

Tuteur de Stage : Monsieur Benezzine

Etablissement / Formation :

Pôle Supérieur Saint Paul Bourdon Blanc – BTS SIO (Services Informatiques aux Organisations) 1ère année option SISR (Solutions Infrastructures Systèmes Réseaux)

Entreprise : Logic4com – 33 rue Camille Claudel, 45000 Orléans

Sommaire :

I - Introduction

II - Présentation de l'entreprise

III - Présentation de mes compétences

IV - Les missions souhaitées

V - Présentation d'un site web à partir de la plateforme WordPress avec les plugins et modules nécessaires.

VI – Mise en place de processus de sécurité pour le site web

I – Introduction

J'ai voulu faire ce stage car, étant en BTS SIO 1ère année option SISR, l'exécution de ce stage est crucial non seulement pour la validation de ma 1ère année de BTS mais également afin d'enrichir mes compétences en informatique.

Les objectifs et attendus durant ce stage sont les suivants :

- Appréhender les caractéristiques (économiques, juridiques, organisationnelles et technologiques) des situations rencontrées et en percevoir les enjeux.
- Se situer dans un environnement organisationnel réel et de s'immerger dans des contextes professionnels variés.
- Construire une représentation des métiers d'un prestataire informatique dans toutes leurs dimensions : production et fourniture de services, conception et maintenance de solutions techniques, relations avec les parties prenantes, conseil et assistance aux utilisateurs, veille technologique, etc.
- Acquérir et de développer des attitudes et des comportements professionnels adaptés, en prenant en compte les contraintes s'exerçant dans chacune des activités réalisées.

II - Présentation de l'entreprise

L'entreprise Logic4com est une entreprise de graphisme, webdesign, développement et consulting veillant à accompagner et conseiller les clients en fonction de leurs besoins.

Cette entreprise est composée de graphistes, webdesigners, développeurs et monteurs vidéo indépendants ayant réalisé 950 projets ayant satisfait 868 clients en 20550 heures de travail à ce jour.

Leurs projets sont axés sur la réalisation de sites web vitrine et e-commerce ; le développement de logiciels sur mesure ; la réalisation de logos, catalogues, flyers, affiches ; la mise en place de vidéos promotionnelles et explicative ainsi que des conseils personnalisés en stratégie de communication.

Tous ces projets sont synthétisés en un portfolio disponible sur leur site (<https://logic4com.fr/>).

III - Présentation de mes compétences

Mon domaine de compétences s'étend sur :

- L'installation, l'intégration, l'administration, la sécurisation des équipements et des services.
- L'exploitation, la supervision et la maintenance d'une infrastructure.
- La définition et la configuration des postes clients, des serveurs et des équipements d'interconnexion, leur déploiement et leur maintenance.
- La gestion des actifs de l'infrastructure.
- La recherche de réponses adaptées à des besoins d'évolution de l'infrastructure ou à des problèmes liés à la mise à disposition des services informatiques.
- La résolution des incidents et l'assistance des utilisateurs.
- Le maintien de la qualité des services informatiques.
- L'étude et la caractérisation de solutions d'évolution ou d'optimisation d'une infrastructure.
- La mesure des performances d'une infrastructure, des équipements ou des services informatiques.

Mes domaines de prédilection sont au niveau de l'installation, de l'intégration, de l'administration et de la sécurisation des équipements et des services et de la configuration des serveurs, des équipements d'interconnexion et des postes clients.

Mes axes et points d'amélioration en revanche sont au niveau de l'étude et la caractérisation de solutions d'évolution ou d'optimisation d'une infrastructure et la recherche de réponses adaptées à des besoins d'évolution de l'infrastructure ou à des problèmes liés à la mise à disposition des services informatiques.

IV – Les missions souhaitées

Les missions que je souhaite réaliser peuvent être de créer puis implémenter des serveurs bénéficiant de services (DHCP ou DNS par exemple) ou encore configurer des équipements réseau (comme des commutateurs ou des routeurs par exemple) mais je suis également ouvert à des missions dans le domaine SLAM (Solutions Logicielles Application Métier) tel que l'élaboration de sites web par exemple afin de pouvoir élargir mon champ de compétences orienté réseau à une autre spécialité.

V - Présentation d'un site web à partir de la plateforme WordPress avec les plugins et modules nécessaires.

Tout d'abord, WordPress est un système de gestion de contenu utilisé principalement pour créer des sites web de toute sorte comme des forums, des blogs ou des boutiques en ligne par exemple.

Dans le cadre de mes missions, il m'a été demandé de créer un site web à partir de la plateforme WordPress dont l'URL est (<https://sitestageseo.wordpress.com/>).

Ce site web étant désormais créé, il faut y intégrer des plugins afin de pouvoir avoir des fonctionnalités supplémentaires comme une sécurité renforcée par exemple.

Un plugin est un module servant à ajouter ou améliorer des fonctionnalités d'un site web sans modifier le code du site.

Ces plugins feront ensuite l'objet d'une analyse SWOT (analyse portant sur les forces et les faiblesses d'un produit, une entreprise ou une situation spécifique) afin de juger quels plugins seraient les plus adéquats pour notre site.

Dans le cas de notre site web, il faut tout d'abord le sauvegarder afin de pouvoir le restaurer en cas d'attaques entraînant une perte de données.

Pour cela, des plugins de sauvegarde tels que UpdraftPlus ou Jetpack VaultPress Backup sont préférables afin de pouvoir effectuer des sauvegardes efficaces.

En effet, UpdraftPlus est un plugin de sauvegarde très populaire sur WordPress permettant de sauvegarder ou restaurer un site via de nombreux services de stockage cloud comme Google Drive, FTP ou encore Microsoft OneDrive.

Le seul inconvénient est que certaines fonctionnalités sont payantes mais la majorité sont gratuites à condition de bénéficier de la mise à niveau du plan Creator (40€/mois).



UpdraftPlus : Extension WordPress de sauvegarde et migration

Par [UpdraftPlus.Com](https://updraftplus.com), [DavidAnderson](#)

backup cloud backup database backup

Backup, restoration and migration - world's most popular backup tool. Backup to the cloud - schedule backups or backup manually.

Évaluations
★★★★★ 4.8

Version
1.24.3

Mis à jour récemment
30 avril 2024

Installations actives
3M

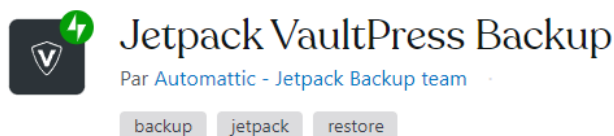
Gratuit sur le plan Creator

Mettre à niveau et activer

Jetpack VaultPress Backup quant à lui est un service de sauvegarde mais aussi de sécurité pour les sites WordPress intégré au plugin Jetpack.

Les sauvegardes sont effectuées en temps réel et stocké dans le cloud ainsi que leur sécurisation contre les menaces pouvant survenir en ligne.

Cependant, de même que pour UpdraftPlus, les fonctionnalités de sauvegarde avancées nécessitent un plan premium payant mais le service reste gratuit.



Save each change and get back online fast with one-click restores.
The most proven WordPress backup plugin with over 270 million backups.

Évaluations
★★★★☆ 4.6

Mis à jour récemment
9 mai 2024

Version
2.6

Installations actives
9K

Gratuit sur le plan Creator

Mettre à niveau et activer

La menace des cyberattaques est de plus en plus fréquente notamment par le piratage de sites web.

Pour cela, il faut des plugins de sécurité afin de s'en protéger.

Wordfence Login Security ou encore All-In-One-Security (AIOS) en sont des exemples.

Wordfence Login Security est un plugin de sécurité permettant de protéger les sites contre les attaques par force brute entraînant le blocage temporaire des adresses IP lorsqu'il y a plusieurs tentatives de connexion infructueuses, l'authentification à 2 facteurs et une protection XML-RPC (protocole étant la plus grosse cible des attaques des sites WordPress).

L'inconvénient est que les adresses IP peuvent être bloquées accidentellement si elles mettent des identifiants incorrects plusieurs fois mais aussi qu'une configuration appropriée est nécessaire afin de bénéficier de toute la protection qu'offre ce plugin.



Wordfence Login Security

Par Wordfence

2FA

captcha

login security

Secure your website with Wordfence Login Security, providing two-factor authentication, login and registration CAPTCHA, and XML-RPC protection.

Évaluations

★★★★☆ 4.1

Mis à jour récemment

3 avril 2024

Version

1.1.11

Installations actives

60K

Gratuit

sur le plan Creator

Mettre à niveau et activer

All-In-One-Security (AIOS) est un plugin de sécurité faisant office de pare-feu afin de bloquer les potentielles attaques par injection SQL ou tentatives d'intrusion.

Il protège également le fichier de modifications (.htaccess) afin d'empêcher les modifications non autorisées.

Il permet aussi, comme Wordfence Login Security, d'empêcher les attaques par force brute.

Cependant, toutes ces fonctionnalités peuvent avoir un impact sur les performances du site, ralentissant le chargement des pages.



All-In-One Security (AIOS) – Security and Firewall

Par All In One WP Security & Firewall Team

firewall login security Malware Scanning

Protect your website investment with All-In-One Security (AIOS) – a comprehensive and easy to use security plugin designed especially for WordPress.

Évaluations
★★★★☆ 4.7

Mis à jour récemment
1 mai 2024

Version
5.3.0

Installations actives
1M

Gratuit sur le plan Creator

Mettre à niveau et activer

Enfin, il faut pouvoir le référencer afin qu'il puisse apparaître lorsque l'on effectue une recherche sur google avec le mot-clé correspondant et qu'on puisse le visiter.

Pour cela, un plugin SEO est nécessaire.

Yoast SEO est un exemple de plugin SEO prisé sur WordPress.

En effet, Yoast SEO permet une optimisation du contenu, un plan de site XML et fichier robots.txt généré automatiquement par le plugin pour aider les moteurs de recherche à indexer le site, évalue la lisibilité du contenu du site en effectuant des recommandations par la suite et l'affichage d'un aperçu sur comment le contenu va apparaître lorsque l'on effectuera une recherche.

Cependant, ce plugin est assez compliqué à prendre en main lorsque l'on est un utilisateur novice et impacte les performances sur le site ainsi que l'ajout d'une version premium payante plus performante que celle gratuite.



The screenshot shows the official WordPress plugin page for Yoast SEO. It features the Yoast logo (a stylized 'y' with a green leaf) and the text 'Yoast SEO' followed by 'Par Team Yoast'. Below this are three tabs: 'Content analysis', 'Readability', and 'schema'. A descriptive paragraph states: 'Améliorez votre SEO avec WordPress : rédigez de meilleurs contenus et obtenez un site WordPress optimisé en utilisant l'extension Yoast SEO.' At the bottom, there are two columns of information: 'Évaluations' with a 4.8 star rating and 'Version 22.7' on the left, and 'Mis à jour récemment 14 mai 2024' and 'Installations actives 5M' on the right.

Yoast SEO
Par Team Yoast

Content analysis Readability schema

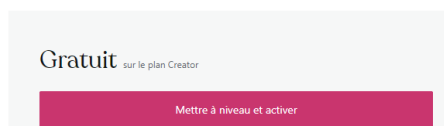
Améliorez votre SEO avec WordPress : rédigez de meilleurs contenus et obtenez un site WordPress optimisé en utilisant l'extension Yoast SEO.

Évaluations
★★★★★ 4.8

Version
22.7

Mis à jour récemment
14 mai 2024

Installations actives
5M



This is a small badge for the free version of Yoast SEO. It has a light gray background. On the left, the word 'Gratuit' is written in a large, bold, black font. To its right, in a smaller font, is 'sur le plan Creator'. Below this text is a solid magenta rectangular button with the white text 'Mettre à niveau et activer'.

Gratuit sur le plan Creator

Mettre à niveau et activer

Les conséquences de la non-mise en place des plugins de sécurité peuvent entraîner une exposition forte aux malwares pouvant voler les données à caractère personnel présents sur le site (ce qui est contraire au Règlement Général sur la Protection des Données ou RGPD et pouvant être une cause de sanctions légales et d'amendes) ou l'endommager, un piratage du site et l'utilisation de celui-ci à des fins illégales et subir des attaques de type DDoS (attaques par déni de service).

D'un point de vue des sauvegardes, s'il n'y a pas de plugins de sauvegarde, si une attaque de type ransomware (rançongiciel) survient, chiffrant ainsi toutes les données présentes sur le site, il sera presque impossible de pouvoir les récupérer sans la clé de déchiffrement détenue par l'attaquant.

Dans le cadre du SEO, si le site s'est fait attaquer, il y aura une dégradation de la réputation et donc une diminution du trafic car il y aura une perte de confiance de la part des clients mais aussi des pénalités de la part des moteurs de recherche qui vont faire baisser de façon significative le classement du site et du trafic.

VI – Mise en place de processus de sécurité pour le site web

Suite à la mise en place de mon site web et des plugins intégrés au site, l'entreprise m'a demandé de recenser les attaques de site web les plus fréquentes et d'effectuer un processus de sécurité afin de parer ces attaques.

Tout d'abord, les attaques les plus fréquentes sont :

- Les attaques de type DoS ou DDoS (Déni de service ou Déni de service distribué)
- Les attaques par Injection SQL (Structured Query Language)
- Le Cross-Site Scripting (XSS)
- Le phishing

Une attaque de type DoS est une attaque qui vise à rendre un site web ou un service en ligne indisponible pour ses utilisateurs légitimes.

Cela est accompli en submergeant le système cible avec un flux massif de requêtes ou de trafic, épuisant ses ressources (comme la mémoire, la bande passante, ou la puissance de calcul) au point où il ne peut plus répondre ou fonctionner correctement.

Une attaque de type DDoS est une attaque de type DoS dont la seule différence est que l'attaque provient de multiples machines situées à divers endroits. Ces machines sont souvent des ordinateurs compromis, formant un réseau de "zombies" ou de "botnets" contrôlé par l'attaquant.

L'injection SQL est une technique d'attaque dans laquelle un attaquant insère des requêtes SQL malveillantes dans un champ d'entrée destiné à des commandes SQL légitimes. Cette injection permet à l'attaquant d'accéder, modifier, ou supprimer des données de la base de données, contourner l'authentification, ou même obtenir des commandes administratives.

Le Cross-Site Scripting (XSS) est une attaque survenant en exploitant une vulnérabilité de sécurité sur le web permettant à un attaquant d'injecter des scripts malveillants dans le contenu d'un site web vu par d'autres utilisateurs. Ces scripts peuvent être utilisés pour voler des informations sensibles, usurper l'identité de l'utilisateur, ou effectuer des actions non autorisées en son nom.

Le phishing est une technique d'attaque où des attaquants se font passer pour une entité de confiance afin de tromper les utilisateurs et les inciter à divulguer des informations personnelles sensibles telles que des identifiants de connexion, des numéros de carte de crédit, ou des informations bancaires.

Les attaques de phishing se présentent généralement sous la forme de messages électroniques, de sites web frauduleux, ou d'autres communications électroniques.

Les sanctions légales soumises au RGPD (Règlement Général sur la Protection des Données) pour des manquements au niveau de la sécurité du propriétaire du site et au Code Pénal pour l'attaque commise sont :

Attaquant : 3 ans de prison et 100.000 € d'amende (Article 323-1 du Code Pénal)

Propriétaire du site : Jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires annuel (article 32 du RGPD).

Ces attaques font préjudice aux clients car ces attaques de sites web entraînent une indisponibilité des sites web, l'accès, la modification, la suppression des données de la base de données du site ou encore la divulgation d'informations à caractère personnel (identifiants de connexion, des numéros de carte de crédit, ou des informations bancaires, ...).

C'est pour cela que des protocoles de protection, de prévention et de réponse à incident seront établis sous forme de logigramme afin de parer toutes ces attaques et ainsi protéger les utilisateurs :

