DOSSIER DE PROJET PROFESSIONNEL

Alexandre DAUMAIL

Projet de refonte graphique et de création d'une section blog pour le site commercial d'une maison d'édition

TABLE DES MATIÈRES

Compétences du référentiel couvertes par le projet

Ce dossier de projet couvre plusieurs compétences, afin de les valider pour prétendre à l'obtention du titre RNCP de développeur web et web mobile. Je vais vous énumérer les différentes compétences présentes et couvertes par ce projet professionnel.

Pour l'activité 1 : *Développer la partie front-end d'une application web et web mobile en intégrant les recommandations de sécurité*

- **Maquetter une application**
    - La maquette prend en compte les spécificités fonctionnelles décrites dans les cas d'utilisation ou les scénarios utilisateur
    - Utilisation d'outils de maquettage

- **Réaliser une interface utilisateur web ou mobile statique et adaptable**
    - L'interface est conforme à la maquette de l'application
    - Les bonnes pratiques de développement sont respectées
    - Le code source des composants est documenté
    - Utilisation d'environnement de développement pour coder

- **Développer une interface utilisateur web dynamique**
    - L'interface utilisateur est dans un second temps affiné grâce à des langages de programmations dynamiques, elle est alors capable d'interagir et d'évoluer en fonction de l'utilisateur de manière la plus efficace possible
    - L'interface est sécurisée
    - Les bonnes pratiques d'accessibilité sont respectées
    - L'interface est également testée et validée par un utilisateur tiers

- **Réaliser une interface utilisateur avec une solution de gestion de contenu ou e-commerce**
    - Si nécessaire suite aux fonctionnalités décrites dans le cahier des charges, il est possible d'installer et adapter une solution préétablie de gestion de contenu ou d'e-commerce

Pour l'activité 2 : *Développer la partie back-end d'une application web ou web mobile en intégrant les recommandations de sécurité*

- **<u>Créer une base de données</u>**
    - Modélisation :
        - Le schéma entité association couvre les règles de gestion sur les données
        - Le schéma respecte le formalisme du modèle entité association
        - Le schéma physique de la base de données est normalisé
    - Conception :
        - Les scripts de génération de la base de données, les scripts de génération des jeux d'essai et les scripts de sauvegarde et de restauration de la base de données sont disponibles
        - La base de données est conforme au schéma physique
        - Les règles de nommage sont conformes aux normes qualité de l'entreprise
        - Les bonnes pratiques de sécurité pour que la base de données suive les critères DICP (Disponibilité, Intégrité, Confidentialité, Preuve) sont mises en place
        - Les droits et rôles des utilisateurs de la base de données sont gérés

- **<u>Développer les composants d'accès aux données</u>**
    - Les traitements relatifs aux manipulations des données répondent aux fonctionnalités décrites dans le dossier de conception technique
    - Connaissance du langage de requête de type SQL
    - Connaissance des principales attaques sur les bases de données (injection SQL…) et de leurs parades
    - Connaissance des règles de sécurisation des composants d'accès aux données (vérification systématique des entrées, utilisation des procédures stockées ou de requêtes paramétrées…)

- **<u>Développer la partie back-end d'une application web ou web mobile</u>**
    - Les pages web répondent aux fonctionnalités décrites dans le cahier des charges
    - L'architecture de l'application répond aux bonnes pratiques de développement d'application web
    - Le code source des composants est documenté
    - Les composants serveur contribuent à la sécurité de l'application
    - Le développement est réalisé grâce au paradigme de l'objet
    - Gérer la sécurité de l'application (authentification, permissions…) dans la partie serveur
    - Utiliser des composants d'accès aux données

- **<u>Élaborer et mettre en œuvre des composants</u>**
    - Si nécessaire suite aux fonctionnalités décrites dans le cahier des charges il est possible d'installer et adapter une solution préétablie de gestion de contenu ou d'e-commerce

Présentation de l’entreprise

L'origine des éditions Alba Capella (la petite chèvre blanche en latin) remonte à 2015 : Vincent Daumail, son créateur, suit alors à Paris le parcours qualifiant « Édition » à l'École des métiers de l'information.

Dès 2016, il rencontre les premiers auteurs, et quelques personnes décident de placer leur confiance dans ce projet audacieux. Vincent Daumail est le seul employé de cette TPE.

Depuis la création de sa maison d’édition, le catalogue Alba Capella obéit avant tout à la volonté de promouvoir de nouveaux auteurs montrant une plume prometteuse et des projets intéressants, compatibles avec la subjectivité de l'éditeur.

Le site albacapella.fr est lancé en 2021 en même temps que la première édition de la maison. Alba Capella Editions (ACE) présente et vend ses livres sur son site internet hébergé chez OVH et développé avec le CMS Prestashop.

Résumé du projet

J’ai proposé mes services de développeur web pour aider Vincent à effectuer une refonte graphique de certains éléments de son site pour le rendre plus attractif, bien qu’il soit déjà fonctionnel.

La conception graphique suit le modèle basique de Prestashop. Difficile de donner le style que l’on veut au site internet sans passer par des modules d’apparence que l’on peut acheter ou obtenir gratuitement sur la plateforme intégrée du CMS. A noter, le téléchargement de modules est une vulnérabilité car Prestashop est en open source.
Je vais devoir découvrir le système de modèles (templates) et de trames (layouts) pour pouvoir le modifier selon le design que j’aurai choisi et proposé à Vincent. Il s’agit d'un système reposant sur Symfony et Smarty.

L'interface d’ajout d’articles de blog ainsi que l’affichage des éléments sur le site internet ne conviennent pas à Vincent. Je vais donc concevoir un espace de blog avec un système d’administration d’articles et de commentaires. J’ai décidé de le faire en dehors de l’architecture de Prestashop pour éviter d’altérer la base de données. Je veillerai à ce que le design soit le même que le reste du site. Le but de ce projet est de prouver que j’ai acquis les compétences requises pour obtenir le titre de Développeur Web et Web mobile.

Cahier des charges

Contraintes de calendrier

Mémoire du stage:

Le mémoire (dossier du projet professionnel) est à soutenir lors de la présentation orale (voir ci-dessous).
Il doit être rendu le 24 juin.

Présentation orale du stage

La Plateforme doit disposer du dossier pro et du mémoire de stage pour le 24 juin (pour la reliure et l'envoi au membres du jury).
La présentation orale aura lieu entre mi-juillet et fin août.

Besoins front-end (clients ou visiteurs)

Besoins associés :

Objectifs :

- Présenter les auteurs aux visiteurs
- Présenter les actualités Alba Capella aux visiteurs
- Accéder facilement aux offres promotionnelles
- Compte à rebours sur la page d'accueil lors de promotions

1) <u>La demande graphique</u>

   a) Header et footer à revoir

- Header trop épais : hauteur à réduire
- Ajouter dans le footer les liens vers les réseaux sociaux (Page LaPetiteChevreBlanche de Facebook)

   b) Navigation

- Obtenir une fonctionnalité de blog qui respecte l'état de l'art en la matière
- Revoir le menu principal : le sous-menu Actus

   c) Lignes de force de la maquette

- Esprit : imaginaire, ludique, bienveillant, positif
- Accrocher l'œil, en tenant compte des thèmes, des activités,
- Bonne lisibilité des zones de texte

Besoins administrateur (back-end)

1) Base de données

Objectifs :

- sauvegarder la base existante ;
- comprendre le modèle de données de la base existante ;
- analyser l'impact des améliorations envisagées sur ce modèle

2) Création d'un environnement de développement PS

Objectifs :

- travailler sans risque sur des modifs, améliorations, etc. ;
- préparer une nouvelle version, la tester avant d'envisager le basculement.

Observation de départ :

La réception d'une commande nécessite des actions manuelles, chronophages, et fastidieuses, liées à la comptabilité. Le besoin se fait sentir d'analyser cette situation et trouver des moyens d'amélioration (automatisation plus ou moins poussée), sur la base de la documentation PS (maquette de factures, de bordereaux de livraison, etc.) :

- export intelligent au format Excel ou .csv ;
- récupération de cet export pour intégration au fichier de comptabilité ;
- création des enregistrements de factures du fichier de comptabilité, à partir des numéros de commande

Exemples de cas d'utilisation :

Les cas d'utilisation suivants permettent de rattacher les exigences exprimées plus haut à des situations concrètes, afin de préciser leur intérêt et de vérifier qu'il n'en manque pas.

Cas d'utilisation 1 : *Réception d'une nouvelle commande sur le site PS*

Cas d'utilisation 2 : *Bilan du mois écoulé*

Autres exigences techniques

1) Référencement naturel

Besoins identifiés :

- évaluer le score SEO du site
- décider des améliorations nécessaires => benchmark concurrence ?
- SEO : robots.txt ;
- partage sur les réseaux sociaux et liens

2) Améliorations diverses

Besoins identifiés :

- La fonctionnalité recherche d'articles du header: modifier le message d'échec

Contraintes de disponibilité et de sécurité

1) Disponibilité

Le site doit rester disponible 24 / 24.

2) Sécurité

Le site a les besoins de cybersécurité habituels dans une boutique en ligne.

Besoins identifiés :

1. Situer **albacapella.fr** et **PrestaShop** par rapport aux précautions recommandées sur le marché des boutiques en ligne
2. Vérifier les infos disponibles chez **l'hébergeur** (**OVH** cloud) : la documentation des **moyens** mis en œuvre (la gestion OVH des menaces de cybersécurité), et surtout les **exclusions** (limites contractuelles)
3. Vérifier les infos disponibles **chez PrestaShop** (la société elle-même) ou sur les **communautés** Prestashop…
4. **mise à jour de PHP** sur OVH
5. **sauvegarde BDD**

Spécifications techniques

Grâce au cahier des charges nous avons dégagé les fonctionnalités à ajouter ou les modifications à effectuer sur le site. Voici les spécifications techniques qui y sont liées car chacune de ces fonctionnalités nécessite un langage et/ou un outil particulier. Le but de cette partie est de préciser et d'expliquer notre choix pour chaque besoin.

Les spécifications techniques d'un cahier des charges sont une documentation des méthodes, procédés, et technologies sélectionnées pour faire face aux contraintes de réalisation du projet.

Choix technologiques

La refonte graphique du site est censée être légère et facile à intégrer. L'entreprise souhaite continuer d'utiliser prestashop et pouvoir ajouter du contenu facilement sans prendre de risques. Pour rester cohérent avec l'environnement existant et effectuer des tests en toute sécurité, j'ai donc installé Prestashop 1.7 en local.

Technologies utilisées pour la partie front-end :

- HTML
- CSS
- BOOTSTRAP
- Javascript
- Smarty 3 template engine (utilisation des templates Prestashop)

Technologies utilisées pour la partie back-end :

- PHP en tant que langage de script
- MySQL pour le serveur de données
- Une partie de l'application métier de Prestashop se repose sur le framework Symfony

Logiciels utilisés:

- Figma (maquettes et charte graphique)
- Visual Studio Code (IDE - environnement de développement intégré)
- WAMP (plateforme de développement web, permet de créer un serveur en local)

Accessibilité

Les sites et applications web ont des exigences d'accessibilité web fondamentales. Il faut que j'en tienne compte dans ma démarche de conseil auprès d'Alba Capella. Le site w3.org, consortium international pour développer les standards du web, a également une section WAI (Web Accessibility Initiative). Cette dernière a pour but d'aider les développeurs et utilisateurs de sites web à comprendre ou intégrer des éléments qui rendent le web plus accessible aux personnes en situation de handicap.

a) Compatibilité navigateurs

Il faut que le site fonctionne sur un maximum de navigateurs. En effet, ACE a déjà eu quelques plaintes quant à l'impossibilité de passer commande. Ca peut représenter un impact direct direct sur le taux de conversion : les clients bloqués à l'achat ou choix de livraison ne valident pas leur panier et abandonnent la commande.

b) Types d'appareils

Il en va de même concernant les appareils. Que ce soit sur tablette ou smartphone, moniteur de 11" ou 23", la navigation ne doit pas être entravée et les requêtes de l'utilisateur effectives. L'avantage de Prestashop est que l'interface est déjà adaptative grâce à certaines classes de Bootstrap. Il faut tout de même garder à l'esprit cette contrainte lors des améliorations.

c) Implémentation d'accessibilité

L'exemple le plus commun en terme de développement web, est l'utilisation de l'attribut <alt> dans une balise <img>. Il permet de lire un texte alternatif à l'image, lorsque l'utilisateur est malvoyant et utilise un lecteur d'écran. C'est aussi nécessaire dans le cas où l'image ne s'affiche pas en cas de mauvaise connexion.

Il est possible d'utiliser des outils d'évaluation pour déterminer si le site web répond un minimum aux normes d'accessibilité. J'ai pu faire une analyse rapide grâce à WAVE[1]. Cette analyse va m'inspirer lors de la création de la nouvelle charte graphique et d'autres actions comme le contrôle des bonnes pratiques sémantiques.

[1] c.f. Capture de résultats en annexe

Architecture du projet

Le site Alba Capella repose sur l'utilisation de Prestashop. Depuis sa version 1.7, cette application web open source utilise le framework Symfony dans le noyau de sa codebase. Plus concrètement, l'application métier de Prestashop se divise en 4 sous-systèmes, dont "PrestaShop Bundle" qui est le plus récent. Les templates et layouts, qui m'intéressent pour la modification de l'apparence du site, s'y trouvent.

Cette application web est construite en suivant un motif d'architecture logicielle très populaire : le MVC (Modèle-Vue-Contrôleur), composé de trois modules.

- Un modèle (Model) contient les données à afficher.
- Une vue (View) contient la présentation de l'interface graphique.
- Un contrôleur (Controller) contient la logique concernant les actions effectuées par l'utilisateur.

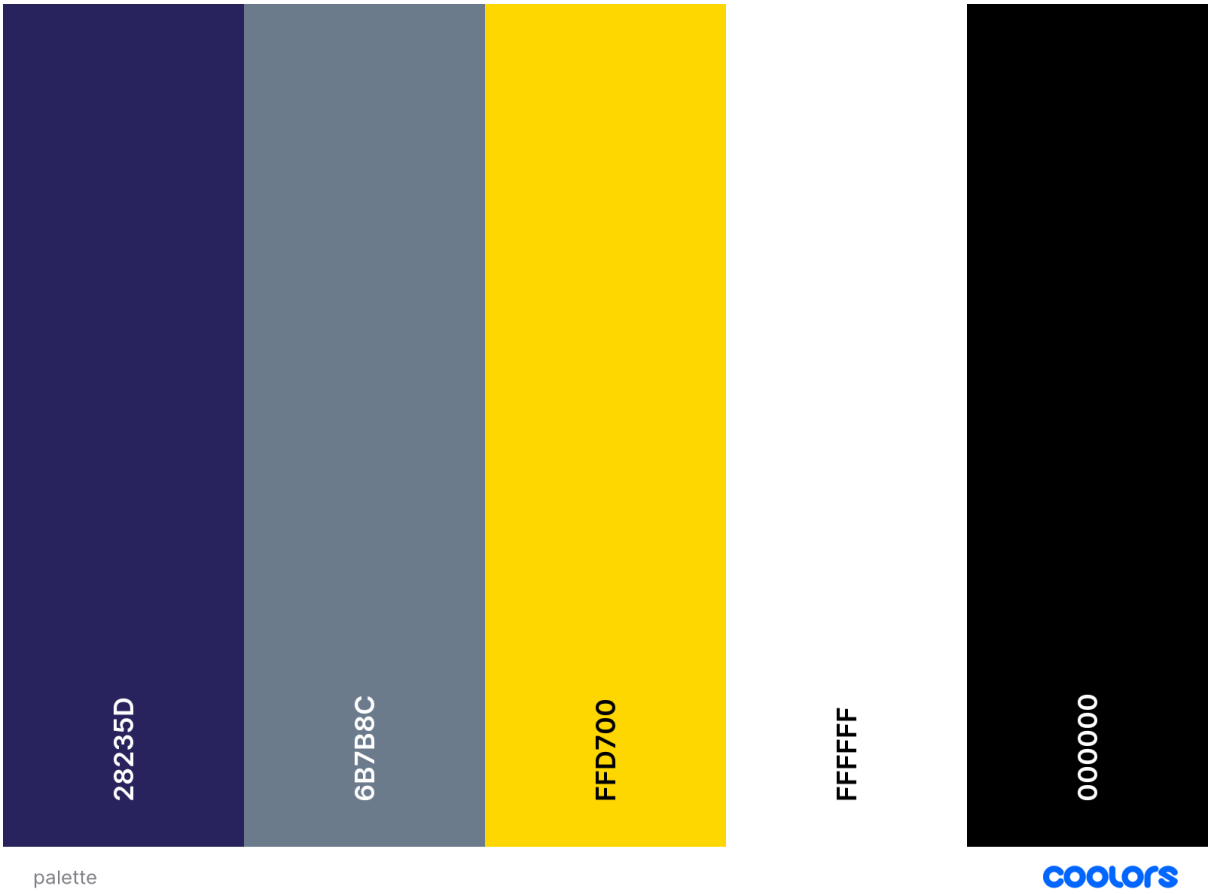
Réalisations

Charte graphique

Avant de me lancer dans la réalisation de maquettes, il faut que je définisse la charte graphique, ou cahier des normes graphiques. Pour résumer, c'est l'ensemble des règles que je vais définir pour que le site web que je vais créer ait une cohérence avec tous les outils de communication de la marque Alba Capella.

Il est important que je ne m'éloigne pas de l'identité visuelle déjà existante de la maison d'édition notamment en choisissant une palette de couleurs adaptée au domaine d'activité de l'entreprise et des valeurs qu'elle défend. Le logo, la typographie et deux couleurs ont déjà été choisies.

J'ai choisi cette palette de couleurs pour attirer le regard avec la couleur or qui peut évoquer la joie de vivre, tout en restant dans des tons sérieux avec le bleu indigo et le blanc de la petite chèvre du logo.



6B7B8c

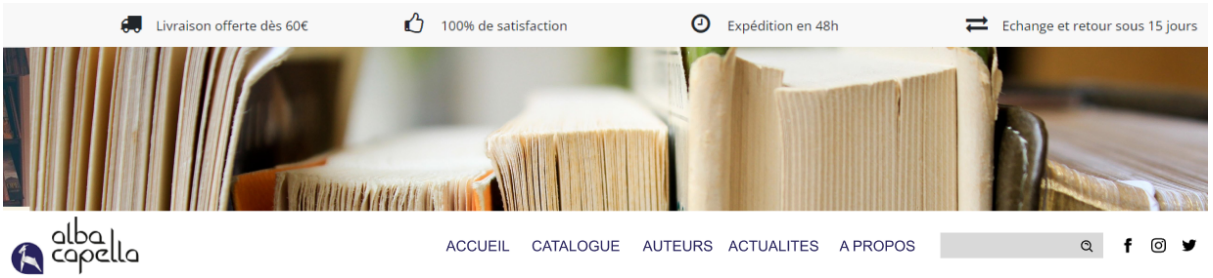
Maquette

Pour ce qui est de la maquette, j'ai consulté de nombreux sites de maisons d'édition pour être en conformité avec le domaine d'Alba Capella. C'est important que l'utilisateur trouve toutes les informations dont il a besoin à l'endroit où il s'attend à les retrouver.

C'est donc l'occasion de vérifier qu'il y ait les bons liens dans les menus, à la fois dans le header et le footer. J'aime because les pages d'accueil avec une section Hero ou Hero header : c'est un élément de web design qui permet de faire forte impression lorsqu'un visiteur atterrit par hasard sur notre site. C'est une section qui prend toute la largeur de l'écran mais il peut être de taille variable pour la hauteur. Point très important : il ne faut pas négliger son adaptabilité à tous les appareils.

Une étape cruciale en maquettage d'application web : le wireframing. Il s'agit d'une maquette fonctionnelle au graphisme simplifié. L'esthétique y est secondaire, c'est surtout important pour le parcours utilisateur comme le positionnement optimal des boutons, des menus. J'ai décidé de me passer de cette étape car le site est déjà fonctionnel.

Voici une partie de la maquette que j'ai faite sur Figma. Par soucis de compatibilité avec les templates et layouts de Prestashop, je change seulement le header et le footer en premier. Ensuite viendront différentes pages lorsque je me serai familiarisé avec l'utilisation de Smarty. Pour pouvoir présenter une nouvelle fonctionnalité du site, j'ai décidé de créer un lien externe à l'application Prestashop qui dirige vers un système de blog.



Nouveau Header

Extraits de code significatifs

Dans cette partie seront sélectionnés des morceaux de code illustrant certaines compétences acquises cette année. Ils seront argumentés pour qu'ils soient compréhensibles.

Alors que le cahier des charges était déjà établi et le projet avancé, une idée est venue à Vincent pendant une promotion qu'il proposait sur son site pour la fête des pères : mettre un compte à rebours sur la banderole de la page d'accueil de son site.

J'ai accepté car celà mettra en avant mes compétences en Javascript et en manipulation du DOM (Document Object Model). Voici la base de mon code, permettant d'afficher un compte à rebours à partir d'une date précise. Je le modifierai jusqu'à pouvoir l'intégrer au site.

Tout est écrit en anglais par soucis d'application des bonnes pratiques :

```
"use strict";

document.addEventListener("DOMContentLoaded", event => {

    // Set the date we're counting down to
    var countDownDate = new Date("Jun 23, 2022 15:37:25").getTime();

    // Update the count down every 1 second
    var x = setInterval(function () {

        // Get today's date and time
        var now = new Date().getTime();

        // Find the distance between now and the count down date
        var distance = countDownDate - now;

        // Time calculations for days, hours, minutes and seconds
        var days = Math.floor(distance / (1000 * 60 * 60 * 24));
        var hours = Math.floor((distance % (1000 * 60 * 60 * 24)) / (1000 * 60 * 60));
        var minutes = Math.floor((distance % (1000 * 60 * 60)) / (1000 * 60));
        var seconds = Math.floor((distance % (1000 * 60)) / 1000);

        // Display the result in the element with id="demo"
        document.getElementById("demo").innerHTML = days + "d " + hours + "h "
            + minutes + "m " + seconds + "s ";

        // If the count down is finished, write some text
        if (distance < 0) {
            clearInterval(x);
            document.getElementById("demo").innerHTML = "EXPIRED";
        }
    }, 1000);
})
```

Ce script est exécuté une fois le chargement de la page html à laquelle il est rattaché est terminé grâce à la ligne de code suivante :

```
document.addEventListener("DOMContentLoaded", event => {
```

Le rattachement se fait dans la page html car il est contenu dans une balise <script> elle même dans une balise <head>.

En premier lieu, la **date de départ du compte à rebours** est assignée à la variable **countDownDate**. Pour ce faire,la date voulue est entrée au format adéquat en tant que chaîne de caractères en paramètre de l'instanciation de l'**objet "Date"**. La **méthode getTime()** permet de compter l'écart entre la date du 1er Janvier 1970 et le 23 juin 2022. var countDownDate est un temps en millisecondes.

```
// Set the date we're counting down to
    var countDownDate = new Date("Jun 23, 2022
15:37:25").getTime();
```

Ensuite, la méthode setInterval prend en paramètre une fonction en rappel ("callback") et une durée en millisecondes : 1000ms pour 1 seconde.

```
// Update the count down every 1 second
    var x = setInterval(function () {
```

Après quelques calculs pour obtenir les écarts entre la date actuelle et celle de départ en jour, heures, minutes, secondes, on va afficher à l'aide du DOM le temps qui reste à s'écouler jusqu'à la date butoir, qui est celle du départ du compte à rebours.

Si le décompte est fini, la méthode clearInterval() permet d'interrompre la méthode setInterval(). Elle affiche alors "EXPIRED" dans l'élément "demo" contenu dans le document html qui charge le script JS que je viens de décrire.

```
// Display the result in the element with id="demo"
        document.getElementById("demo").innerHTML = days + "d
" + hours + "h "
            + minutes + "m " + seconds + "s ";

        // If the count down is finished, write some text
        if (distance < 0) {
            clearInterval(x);
            document.getElementById("demo").innerHTML =
"EXPIRED";
        }
```

Vulnérabilités de sécurité

Les contraintes de disponibilité et de sécurité du site web définies dans le cahier des charges sont d'une importance critique au bon fonctionnement de la boutique Alba Capella. Un site d'achat présentant des failles de sécurité ou une mise hors service a une incidence directe sur le chiffre d'affaires des ventes de livres de la maison d'édition.

Bien que Prestashop et OVH soient des sociétés de grande envergure et bénéficient de services de sécurité d'une certaine efficacité, le risque zéro n'existe pas et il est important de se tenir à la page.

Une veille technologique contre les vulnérabilités de sécurité est essentielle. Il ne s'agit pas seulement de lire des articles de temps en temps ou de faire des recherches quand on y pense. La veille requiert une certaine organisation pour être efficace.

J'ai décidé d'appliquer la méthode PDCA (ou roue de Deming) en vue d'une amélioration en continu de la sécurité du site.

P.D.C.A.

La méthode PDCA comporte 4 étapes. Le but est de mettre en place un cercle vertueux.

Chaque étape en entraîne une autre :

1) **"Plan" ou "Préparer”**

Il s’agit de définir les objectifs à atteindre, dans mon cas ce seront les points que je dégagerai après un audit de la boutique existante.

2) **"Do" ou "Développer"**

Il s’agit de tester, développer et mettre en œuvre l’organisation et le plan d’action validés.

3) **"Check" ou "Contrôler"**

Il s’agit de contrôler et vérifier si tout ce que j’ai effectué jusque-là répond aux attentes en matière d’efficacité. Pour cela, j’ai demandé l’avis à d’autres développeurs sur ce qu’ils pensent de ce que j’ai mis en place.

4) **"Act" ou "Ajuster"**

Il s’agit d’ajuster ou de réagir à la suite des retours que j’ai eus. C’est la fin de la boucle PDCA, après avoir effectué des ajustements je peux tout recommencer en fonction des nouveaux besoins.

Sans cette méthode, la veille risque de ne pas être très efficace et au bout d’un certain temps elle ne s'adaptera pas aux nouveaux besoins et objectifs.

En plus de faire preuve d’organisation, il faut analyser les informations correctement. Elles doivent m’apporter une valeur et me permettre d’agir. Pour celà, j’ai dû établir un cadre, des limites, pour mieux gérer l’ensemble des tâches à accomplir. J’ai donc dressé un état des lieux pour décider des actions à effectuer par la suite :

- test sécurité (scan) de la boutique en ligne sur immuniweb.com, spécialisé en analyse de CMS, plugins et extensions, librairies et frameworks javascript, CVE (Current Vulnerabilities Exposure - liste publique de failles de sécurité informatique en anglais).
- test sécurité du site sur SSL Server Test. Ce service gratuit en ligne effectue une analyse profonde de tout serveur web SSL.
- consultation de blogs sécurité au sujet de Prestashop, OVH, bonnes pratiques de sécurité basique sur les sites web sur différents sites tels que OWASP, …
- audit RGPD : la protection des données des utilisateurs est essentielle, je vais donc devoir m’y intéresser de prêt même si le nécessaire a probablement été fait car j’en avais discuté avec Vincent.

J’ai pu dégager les actions suivantes :

- mettre en place un Web Application Firewall sur OVH
- mettre Prestashop à jour (déjà prévu dans le cahier des charges)
- remplir check-list d’audit RGPD fournie par un élève de la promotion DPO (“Data Protection Officer”) de cette année
- Pentesting (Penetration Testing)

Mise en place de W.A.F. sur OVH

Le processus d’activation du pare-feu intégré à l’hébergeur OVH est assez simple. Lorsque que l’on dispose d’une offre d’hébergement web OVHcloud et qu’on a au moins un nom de domaine attaché à l’hébergement, il suffit de se connecter à son espace client OVHcloud.

Par la suite, dans la partie Informations générales de l’espace en question, on peut modifier la configuration actuelle en cliquant sur “...” ce qui mène vers une page qui permet de sélectionner l’activation du firewall.

M.A.J. Prestashop

Comme il n’y a pas de système de versionnage et aucun environnement de test du site, Vincent préférait éviter de mettre Prestashop à jour. D’après certains blogs tels que Mediacom87, une faille majeure de sécurité sur PrestaShop sur les versions supérieures ou égales à la version 1.7.5.

La vulnérabilité détectée est une “Blind SQLi” (injection SQL aveugle). Ce qui veut dire que l’application web est exposée aux injections SQL mais que ses réponses HTTP ne contiennent pas les résultats de la requête SQL ou détails d’erreurs de base de données. C’est presque comme une injection SQL standard, sauf que contrairement à cette dernière, les retours de requêtes SQL frauduleuses ne sont pas affichées dans l’application web et ne sont pas visibles à l’attaquant.

Ces attaques sont plus complexes et prennent plus de temps à être élaborées que les injections SQL classiques mais permettent tout de même aux personnes malveillantes d’observer le temps de réponse de la page et d’avoir un certain contrôle sur la BDD.

Il y a deux façons de corriger cette faille : soit mettre Prestashop à jour, soit installer un patch pour éviter de faire une mise à jour.

Suite à mes recherches, j’ai aussi constaté que la plupart des failles de Prestashop viennent des modules tiers. Il existe heureusement des listes des modules à risque, bien évidemment non exhaustives car il en sort très régulièrement. Il existe également des bots disponibles sur GitHub qui servent à scanner les vulnérabilités. Je préfère ne pas les utiliser car je ne connais pas leur provenance, c’est aussi s’exposer au risque que les vulnérabilités détectées soient exposées aux personnes ayant programmé ces bots.

Audit RGPD

Le RGPD est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union Européenne. Il s'adresse à toute structure privée ou publique effectuant de la collecte et/ou du traitement de données.

La CNIL délivre 4 bons réflexes pour appliquer le RGPD :

- constituer un registre des traitements de données du site web
- faire le tri dans les données (ne collecter que les données vraiment nécessaires)
- respectez le droit des personnes en matière de consultation, de rectification ou de suppression des données collectées
- sécurisez ces données.

De plus, il faut s'assurer que les partenaires et sous-traitants sont également conformes (c'est aussi important qu'en cybersécurité).Il suffit d'avoir un partenaire non conforme pour risque une sanction.

Au cours de notre année de formation, une présentation des bonnes pratiques liées au respect du Règlement Général sur la Protection des Données nous a été dispensée par des élèves en formation Data Protection Officer. A la suite de cet aperçu, nous avons reçu une liste des vérifications à effectuer sur les sites que nous pouvons être amenés à administrer.

La liste se présente sous forme de tableau, gracieusement mis à disposition par Antoine Maherault :

Audit RGPD - Site Web				
Critère	**Mesures**			**Application**
Transparence	Politique de confidentialité	Lien clairement visible sur chaque page du site.		
		Politique de confidentialité distincte des CGU / CGV.		
		Comprend les mentions suivantes :	Identité et coordonnées de l'organisme responsable du traitement informatique des données personnelles : le délégué à la protection des données (DPO) par exemple.	
			Finalité poursuivie par le traitement : à quoi vont servir les données personnelles collectées.	
			Base légale justifiant le traitement : il peut s'agir du consentement de l'internaute, du respect d'une obligation prévue par un texte juridique, de l'exécution d'un contrat, etc.	
			Caractère obligatoire ou facultatif du recueil de données personnelles : les conséquences pour l'internaute en cas de non-fourniture des données.	
			Destinataires des données personnelles : qui va recevoir et accéder aux données.	
			Durée de conservation des données personnelles.	
			Droits de l'internaute : le droit de refuser la collecte, le droit d'accéder, de rectifier et d'effacer ses données.	
			Droit de l'internaute d'introduire une réclamation auprès de la Cnil.	
			Au besoin, existence d'un transfert des données personnelles vers un pays n'appartenant pas à l'Union européenne.	
Recueil du consentement	Newsletter	Utilisation d'une case à cocher (acte positif clair), ne pouvant être pré-cochée par défaut, spécifique au traitement concerné.		
		Présence d'un lien en fin de newsletter permettant à l'utilisateur de se désinscrire et de retirer son consentement.		
		Existence d'un registre des consentements pour ce traitement.		
	Cookies	Proposer une interface de recueil du consentement.		
		L'interface comprend :	Liste des finalités poursuivies.	
			Lien vers la liste des tiers qui déposent des traceurs.	
			Une explication des conséquences qui s'attachent à une acceptation ou un refus.	
			Un bouton pour accepter et refuser (refuser les traceurs devant être aussi aisé que de les accepter).	
			Un second niveau d'interface doit permettre à l'utilisateur de faire un choix sur la finalité de traceurs.	
		Existence d'un registre des consentements pour ce traitement.		
		Faciliter la ré-évaluation du consentement en présentant une icone relative aux cookies sur chaque page du site internet.		
Exercice des droits	Existence d'un formulaire facilitant l'exercice des droits			
Analyse du trafic	Respect de l'interdiction d'utilisation de Google Analytics (sauf utilisation de serveur mandataire)			

Pentesting

Un test de pénétration, aussi appelé pentest, est la simulation d'attaque informatique contre un ordinateur ou une application web. L'utilité est de vérifier s'il y a des vulnérabilités exploitables par les utilisateurs malveillants. Dans le contexte de la sécurité d'appli web, "pentester" est souvent utilisé pour augmenter l'efficacité du firewall applicatif.

D'après le site de cyber-sécurité Imperva, il peut y avoir cinq différentes méthodes de pentesting :

1. Testing externe

Vise les ressources d'une entreprise visible sur internet, par exemple son application web, ses email ou son DNS (serveurs de nom de domaine). Le but est d'accéder et d'extraire les données importantes.

2. Testing interne

Celui qui teste l'application web a accès directement derrière le pare-feu et simule une attaque par un infiltré aux mauvaises intentions. Ce n'est pas forcément la simulation d'un employé malhonnête, ça peut être le scénario d'un employé dont les identifiants sont volés par une attaque de phishing.

3. Testing à l'aveugle

La personne qui teste a seulement le nom de l'entreprise ciblée. Ce scénario donne un aperçu en temps réel de la façon dont une vraie attaque de l'application se déroulerait.

4. Variante de testing à l'aveugle

Les personnes chargées de la sécurité n'ont aucune information en amont de la simulation d'attaque. Cette simulation se rapproche d'autant plus d'une situation réelle car les personnes chargées de la cybersécurité n'ont pas toujours le temps de lever des défenses contre une tentative de pénétration du système.

5. Testing ciblé

Dans ce scénario, les pentesteurs et le personnel de sécurité travaillent ensemble et communiquent leurs opérations. C'est un entraînement efficace qui donne au département de sécurité un aperçu en temps réel du point de vue du hacker.

J'ai abordé le sujet du pentesing car je le trouve pertinent quant au sujet de la veille contre les vulnérabilités d'une application web. Cependant, mise à part tester les formulaires et faire quelques tests de requêtes en GET (dans la barre d'adresse), je ne suis pas assez compétent dans ce domaine.

Troubleshooting

Description d’une situation de travail ayant nécessité une recherche, effectuée par le candidat durant le projet, à partir de site anglophone

Lors de l’installation de Prestashop en local (sur mon ordinateur), la création de base de donnée a eu un soucis:

> “1: Erreur SQL sur la requête *Index column size too large. The maximum column size is 767 bytes.”*

J’ai donc lancé une recherche du message d’erreur sur internet en anglais. La première solution qui m’a été proposée se trouvait dans un forum de la communauté de Prestashop. Ci après le dialogue entre les différents interlocuteurs, suivi de ma traduction.

Extrait du site anglophone, utilisé dans le cadre de la recherche décrite précédemment, accompagné de la traduction en français effectuée par le candidat sans traducteur automatique (environ 750 signes).

- **MiguelPeixoto** : I'm doing a PS 1.7.7.0 fresh install and I'm getting this error: "SQL Index column size too large. The maximum column size is 767 bytes". Collation: Tried with utf8_bin and utf8mb4_bin
  Does anyone know what the problem can be ?

- **Nette :** I have got the same problem. It is my first Installation of a Webshop with a New hoster. I am just beginning my Business.

- **MiguelPeixoto :** I managed to solve the problem temporarily, by altering the sql instructions, creating the database. But the PS Team should incorporate these changes urgently.

  For new installations:

  Find the following file "install/data/db_structure.sql"

  Replace all

  “ENGINE = ENGINE_TYPE DEFAULT CHARSET = utf8mb4 COLLATION;”

  WITH

  “ENGINE = ENGINE_TYPE DEFAULT CHARSET = utf8mb4 ROW_FORMAT = DYNAMIC COLLATION;”

Traduction en français :

- **MPeixoto:** Je fais une première installation de PS [NDLR: Prestashop] et j'obtiens cette erreur: l'index SQL de colonne est trop grand. La taille maximale est de 767 bits. Collation [2]: j'ai essayé avec utf8_bin et utf8mb4_bin. Est-ce que quelqu'un sait ce que peut être le problème?

- **Nette :** J'ai le même problème. C'est ma première installation d'une boutique en ligne avec un nouvel hébergement en ligne. Je viens à peine de lancer ma société.

- **MPeixoto:** J'ai réussi à résoudre le problème temporairement, en changeant les instructions SQL lors de la création de la base de données. Mais l'équipe Prestashop devrait intégrer ces changements urgemment.

Pour de nouvelles installations:

Trouver le fichier : "install/data/db_structure.sql"

Remplacer la totalité de cette ligne:

"ENGINE = ENGINE_TYPE DEFAULT CHARSET = utf8mb4 COLLATION;"

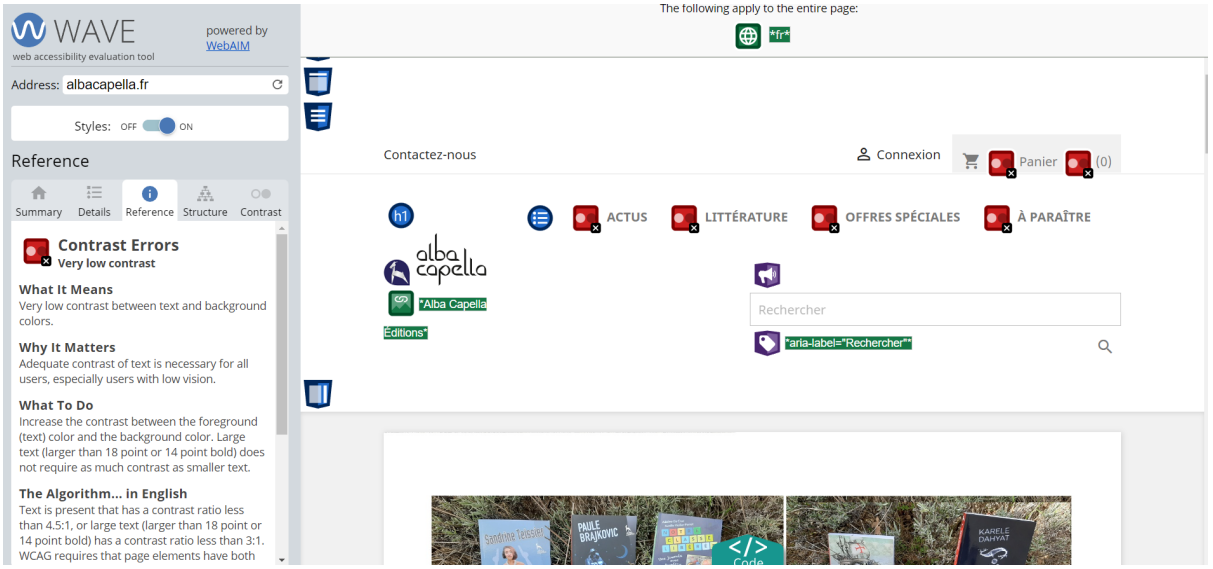
Avec :

"ENGINE = ENGINE_TYPE DEFAULT CHARSET = utf8mb4 ROW_FORMAT = DYNAMIC COLLATION;"

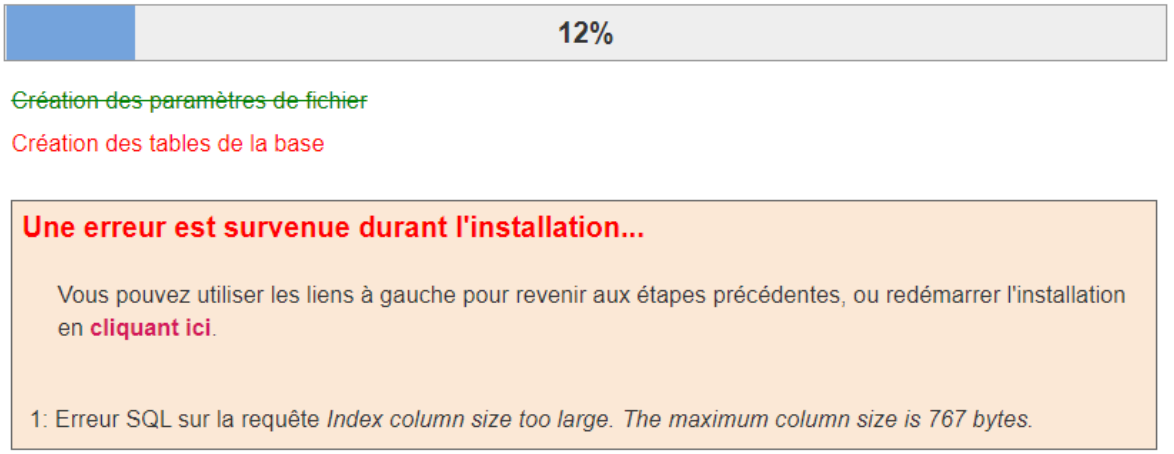
[2] COLLATION : lors du classement d'une colonne de base de donnée, on peut définir une clause de tri, ou sorting. L'assemblage détermine comment les données sont classées et comparées. C'est souvent important en ce qui concerne l'internationalisation.

Annexes

Ci-dessous une capture d'écran du rapport WAVE, après avoir scanné le site pour trouver les défauts d'accessibilité



Voici le message d'erreur que j'ai dû débugger lors de l'installation de Prestashop en local



Sources

https://www.w3.org/WAI/fundamentals/accessibility-principles/fr#standards
https://www.w3.org/WAI/people-use-web/user-stories/fr#shopper
https://www.immuniweb.com/websec/albacapella.fr/RRIzIayw/
https://www.houseoftest.net/en/2016/02/basic-security-testing-website-input-fields-look-lack-input-limitations/
https://cheatsheetseries.owasp.org/cheatsheets/XSS_Filter_Evasion_Cheat_Sheet.html
https://bb.enter-solutions.net/topic/1075/des-modules-et-des-hacks-liste-non-exhaustive-des-modules-pr%C3%A9sentant-un-risque
https://www.imperva.com/learn/application-security/penetration-testing/