Le 21/11/2019,

Objet : Présentation du forfait ACCOMPAGNEMENT DE REFONTE DE SITE-ECOMMERCE

Pour la suite "DOMAINE" est à remplacer par votre nom de domaine, par exemple touchweb.fr. Ce forfait se déroule en 3 phases :

Phase 1 : Préparation de l'environnement de refonte (www-refonte/preprod-refonte)

- **Configuration de www-refonte.DOMAINE** sur votre serveur de production (ou silo de production si vous bénéficiez d'une infrastructure haute-disponibilité)

- (**OPTIONNEL) Installation initiale sur www-refonte.DOMAINE du CMS de votre choix** (Prestashop / Wordpress – pour le cas spécifique d'autres solutions telle que Magento / Pimcore / Akeneo / Dolibarr / Shopware / etc : nous vous invitons à vous rapprocher d'un pool développement spécialisé susceptible de vous facturer l'intervention)

- **Mise en conformité HTTPS** de www-refonte.DOMAINE et mise à disposition d'un lien MEDIA (media-refonte.DOMAINE **non déployé** sur CDN) sous réserve de la présence d'un certificat SSL WILDCARD sinon il faudra acheter un certificat MULTI DOMAIN avec 1 sous domaine supplémentaire spécifiquement pour ce site)

- Création de l'application sur l'hyperviseur (Manager TW) sous l'onglet « Production en création » interdit à l'indexation pour les moteurs de recherche et protégé par htpasswd (popup réclamant un login/password) sauf contre ordre de votre part

- **Configuration de preprod-refonte.DOMAINE** sur votre serveur de préproduction et régénération initiale sur la base de la sauvegarde de l'installation vierge précédemment effectuée (un délai peut s'ajouter lorsque des tiers sont attendus dans le cadre de cette installation initiale)

- Soumission des accès FTPES / SSH / PMA TEMPORAIRES à ces deux sites Internet – qui changeront au moment de la mise en ligne

- **Période de grâce sur les sauvegardes** dans la limite de 150Go surconsommé évitant un éventuel arbitrage défavorable à ce niveau **pendant 2 mois maximum**

NB : la préproduction est un clone conforme à la production, reconstruite à partir des sauvegardes du matin de la production. Pour la quasi-totalité de notre clientèle, cela n'ayant aucun sens de resauvegarder une sauvegarde, ***les préproductions ne sont jamais sauvegardées par défaut****. Cela permet à nos clients de réaliser des économies, autant côté hébergeur via des VPS plus petits que côté contrat de sauvegarde multi-site. Dans ce contexte,* ***il convient de NE PAS travailler sur une préproduction sur la durée qui N'EST PAS un environnement de développement.*** *Toutes les données pouvant être irrémédiablement perdues à tout moment.*

Phase 2 : Accompagnement à la mise en production finale

- **Prise de RDV pour la permutation - un délai de prévenance de 5 jours ouvrés doit être observé**, l'intervention doit nécessairement se dérouler sur les plages horaires du contrat d'Infogérance. Si vous souhaitez une intervention hors plage (non couverte par votre contrat d'infogérance), compter 300€ supplémentaire du lundi au samedi de 7h à 21H ou 600€ sur les autres plages.

- Si nécessaire : plan de migration à établir par le développeur en charge de la refonte si des actions sont attendues côté TOUCHWEB (clonage de base, clonage d'un fragment du SI, etc)

- Désactivation temporaire du CDN (bypass) pour éviter que le CDN ne vous cause du tort pendant la mise en ligne avec purge forcée du contenu (à deux reprises : à la désactivation puis avant la réactivation)

- **Aide au remplacement de tous les liens www-refonte.DOMAINE vers www.DOMAINE (et mécaniquement media-refonte.DOMAINE vers media.DOMAINE)**. Cela peut ponctuellement nécessiter le concours du développeur en charge du fait de persistance non souhaitée de l'ancien lien www-refonte.DOMAINE.

Il est à **parfaitement** comprendre que c'est rigoureusement la même mécanique que celle qui "transforme" les liens www-refonte en preprod-refonte exploitée sur la préproduction qui sera utilisée par TOUCHWEB pour transformer les liens www-refonte en www sur la production. Si problème il y a à ce niveau, il est nécessairement déjà présent sur preprod-refonte.DOMAINE, **il peut donc être constaté en amont par le développeur en charge AVANT que TOUCHWEB ne procède en production.**

- **Permutation à chaud**, **le trafic va être redirigé vers le nouveau site Internet SANS ARRÊT DE SERVICE** (sauf si c'est imposé par des tiers dans l'éventualité par exemple d'un processus de récupération de données contraignant à une fermeture administrative) – **En cas de défaut, il est possible de rebasculer immédiatement sur l'ancien site** (les deux sites étant totalement indépendants - sous réserve que les développeurs en charge de la refonte n'aient pas dégradés cette indépendance)

Hors demande de rollback, l'ancien site devient définitivement inaccessible en production - uniquement sa préproduction reste disponible (voir phase 3.)

Dans l'éventualité d'une demande expresse de rebascule sur l'ancien site Internet (rollback) du fait d'un défaut majeur du nouveau site, la première demande est incluse dans le forfait, les éventuelles autres sont facturées 200€ l'unité.

Phase 3 : Mise en conformité de la nouvelle préproduction et archivage pour 6 mois de l’ancien site Internet

- **Le lien de l’ancienne préproduction preprod.DOMAINE sera modifié pour preprod-old.DOMAINE.** Cette ancienne préproduction sera **conservée pendant une période de 6 mois** (sauf contre ordre de votre part). Tous les accès sur le serveur de production de l’ancien site seront définitivement coupés pour des raisons de sécurité liées à l’arrêt définitif du maintien à jour. **NB : les anciens accès à l'ancienne préproduction restent PLEINEMENT fonctionnels et identiques (seul le lien change).**

- Fin de la période de grâce sur les sauvegardes – ne pas hésiter à nous demander des purges pour limiter les frais de conservation de l’ancien site Internet (par exemple : supprimer tous les visuels – souvent très consommateur d’espace disque) - Ne pas hésiter également à nous réclamer la dernière sauvegarde pour archivage par vos soins.

- **La nouvelle préproduction sera renommée preprod.DOMAINE au lieu de preprod-refonte.DOMAINE**

- Mise en conformité des accès sur les nouveaux liens avec nouvelle soumission (les accès TEMPORAIRES devront être définitivement supprimés)

- Mise à jour de l’hyperviseur sur les nouveaux liens officiels

NB : Ces mises en conformité de liens d'accès engendrent obligatoirement une régénération (destruction irrémédiable / reconstruction sur la base des sauvegardes du matin) des préproductions.

A l'issu des 6 mois, l'ancienne préproduction sera irrémédiablement supprimée (incluant le reliquat de données en production) sauf contre ordre formel de votre part. Veillez à bien nous réclamer ce qui est nécessaire en temps et en heure à ce propos si vous souhaitez récupérer une dernière sauvegarde.

Ce forfait est exclusivement réservé aux clients en compte de TOUCHWEB SAS et est facturé 500€ + 50€ par éventuelle sous boutique. Dans l'éventualité d'un projet souffrant d'un entremêlement sévère inter CMS (comme par EXEMPLE, un Wordpress imbriqué dans l'arborescence d'un Prestashop / Magento), ce forfait souffrira d'une surfacturation de 200€.

Pour le cas spécifique de nos clients GRAND COMPTE (forfait à plus de 550€ HT / mois), le forfait est offert dans la limite de 4 fois (4 refontes pour 4 applications métier - souvent site E-Commerce) tous les 5 ans.

NB : Le forfait de base exclu toute assistance et conseil s'inscrivant dans le cadre d'une AMOA (assistance à maîtrise d'ouvrage) ou d'une MOA (maîtrise d'ouvrage). Toutes questions ou conseils relatifs à la refonte devront être pris en charge par l'équipe missionnée par le client qui doit obligatoirement être composée d'au moins un chef de projet digital de niveau confirmé à senior (MOA).

Si le forfait d'infogérance consommé par le CLIENT est adapté à son chiffre d'affaires dépendant à la disponibilité de son site E-Commerce, le CLIENT est éligible à une remise de 50% sur tous les frais suscités.

Si le client le juge nécessaire, il peut réclamer un pack d'heures "OPTION AMOA", par lot de 8 heures indivisible et non remboursable, facturé 120€ / heure (soit 960€), ces heures sont considérées consommées même si non utilisées, dans le semestre succédant la facturation du présent forfait. A noter que nos clients GRAND COMPTE bénéficie gratuitement d'un lot de 8 heures.

Cette option **non obligatoire** (OPTION AMOA) si elle est réclamée n'engage en aucune manière la responsabilité de TOUCHWEB SAS et ne bénéficie d'aucun engagement, ni de résultat ni de moyen, il s'agit uniquement d'assister via des conseils le CLIENT et/ou l'équipe missionnée par le CLIENT dans le cadre de la refonte.

Tous les horaires sont exprimés au format GMT+1 et tous les prix sont exprimés hors-taxe.

Annexe 1 : informations importantes qui doivent apparaitre dans le devis relatif à la refonte soumis par l'équipe missionnée par le client.

IMPORTANT : nous vous invitons à réclamer formellement à l'équipe technique que vous aurez choisi pour réaliser la refonte :

- de garantir l'intégrité de votre référencement naturel ou à défaut de garantir l'intégrité de vos liens internes qui doivent toujours "pointer" vers les bonnes pages. **Si vous souhaitez modifier la structure de vos permaliens (votre développeur saura de quoi il s'agit), il est obligatoire de mettre en place un plan de redirection.**

- de bénéficier d'une MEDIA URL fonctionnelle, c'est à dire d'un lien différent de celui du site; généralement media.DOMAINE; exploité pour distribuer vos contenus statiques: images et css, possible js, etc.

- de bénéficier d'un système de cache professionnel (PageCache Ultimate pour Prestashop, W3 Total Cache pour Wordpress, ou équivalent) permettant d'obtenir un TTFB optimal ou à défaut de s'engager à réaliser toutes les optimisations nécessaires et suffisantes pour avoir un TTFB hors cache optimal

- et sous réserve de faisabilité, que le système de cache professionnel retenu exploite Memcache ou Redis (des ajustements seront nécessaires à notre niveau - allocation spécifique à configurer - NB : Page Cache Ultimate pour Prestashop le gère)

Il est nécessaire que ces points importants soient exprimés formellement et cela doit se traduire obligatoirement par une tâche claire et précise dans le devis relatif à la refonte auprès du tiers en charge.

Nous vous invitons également à réclamer un point sur les technologies dépendantes et leurs cycles de vie associés **afin de vous éviter d'éventuels surcoûts à court terme**. Vous pouvez utiliser ce document comme support : https://www.touchweb.fr/cycle-de-vie en ayant bien en tête que cette refonte est "censée" vous accompagner **à minima** 4 ans.

Par exemple, réclamer une refonte sous Prestashop en version 1.6, officiellement en fin de vie depuis l'été 2019, donc qui ne sera plus jamais mis à jour vous exposera à des choses très désagréables courant 2023/2024 (incluant une impossibilité probable de trouver des modules professionnels de qualité ainsi qu'une suppression prévue des logiciels systèmes compatibles). **Toujours dans cet exemple**, si l'on part du principe que la durée de vie de cette refonte sera d'environ 5 ans, cela vous emmène courant 2025, on peut donc raisonnablement affirmer qu'il serait tout à fait irresponsable de choisir la branche 1.6 pour cette refonte et bien que la branche 1.7 soit très imparfaite, cela reste l'option la moins préjudiciable à moyen terme.

Annexe 2 : éléments importants à vérifier avant la mise en ligne de la refonte

Ces points à vérifier sont bloquants pour la mise en ligne, il vous sera réclamé AVANT la mise en ligne qu'ils ont été vérifiés avec soin et rigueur, point par point.

Certains points de contrôle nécessitent une compétence de niveau CONFIRMÉ en ingénierie logicielle (donc 10 000+ heures de développement - généralement 5 ans d'expérience) - si nécessaire on peut vous mettre en relation avec des profils ayant les compétences requises.

Liste des éléments à vérifier pour éviter un échec partiel ou total de projet :

1. S'assurer que tous les anciens liens de votre site E-Commerce fonctionnent toujours et pointent vers les mêmes pages

Il est fondamental de préserver le mapping de vos liens et des pages associées ou le cas échéant, de mettre en place un plan de redirection - généralement un fichier .htaccess qui liste tous les anciens liens et les redirige intelligemment vers les nouveaux.

Nous vous invitons à la vigilance à ce propos - **une petite erreur d'inattention peut engendrer des désastres**, dégradant notoirement et durablement le référencement naturel du site acquis depuis des années, comme par exemple un import produit de masse partiellement en erreur, décalant l'identifiant produit initial de un, et décalant la numérotation de *tous* les produits et donc **modifiant tous les liens de votre catalogue**.

Si le chiffre d'affaires annuel dépendant au trafic organique (celui généré par les SERP dont Google) est supérieur à 250 000€ HT - **il est vivement conseillé (pour ne pas dire obligatoire) de mettre un hyperviseur SEO** dans la boucle de la refonte (Semrush / A href / etc)

2. Si des imports de données depuis l'ancien SHOP vers le nouveau SHOP sont nécessaires (ce qui est fort probable), nous vous invitons à la vigilance.

Le processus d'importation récupère les anciennes données **EN L'ETAT - nous insistons : EN L'ETAT** DONC il est probable que des données issues des pages type CMS ou encore des descriptions de produits contiennent des liens qui "pointent" vers l'ancien SHOP (l'actuelle production : www ou équivalent).

ATTENTION 1 : si ces liens importés pointent vers un emplacement de l'ancien site (bien que toujours en production au moment des imports), et que cet emplacement n'a pas fait l'objet d'une récupération (par exemple un sous répertoire oublié du dossier img/cms/), vous ne pourrez pas constater sur votre www-refonte que ces liens sont morts étant donné qu'ils pointent sur l'ancien site et que cet ancien site possède cet emplacement et les fichiers relatifs.

Nous vous suggérons de surveiller la présence de liens www en base de données (via une recherche sur PHPMyAdmin) APRES vos imports afin de constater que les emplacements des éventuels fichiers vers lesquels ils pointent ont effectivement été récupérés sur le www-refonte.

ATTENTION 2 : Vos modules professionnels d'import ne sont pas intelligents et vont partir du principe que vous n'AVEZ PAS modifié certaines données sensibles (qu'on appelle tables maîtres), tel que des codes TVA, des codes PAYS, ou encore des états de commande. Il arrive, bien que ponctuellement, que certains modules (comme des transporteurs) imposent des modifications de ces données, comme un identifiant pays forcé sur une valeur donnée. Cela peut avoir pour conséquence après l'import, d'avoir reventilé des milliers de commande sur le mauvais pays, pouvant fausser vos données comptables, **PAR EXEMPLE** : le pays BELGIQUE sur l'ancien SHOP reventilé sur le pays CHINE sur le nouveau SHOP, engendrant des TVA erronées possiblement sur des milliers de commande.

ATTENTION 3 : Veillez à ne pas créer de bombes à retardement en récupérant des fragments de données de la base historique qui peuvent, plusieurs mois / années après la refonte, engendrer des dysfonctionnements sévères. Par **EXEMPLE** sur Prestashop, si vous récupérez en l'état la table des commandes (orders) donc que vous récupérez tacitement les associations commandes / paniers (colonne id_cart de la table orders), si vous ne récupérez pas également la table des paniers (carts) OU si vous n'initialisez pas l'AUTO INCREMENT de la table des paniers (cart) à la valeur maximale + 1 du champ id_cart de la table orders, du fait des protections anti corruptions de Prestashop, vous engendrerez à terme un incident majeur empêchant l'ajout de produit au panier du fait d'un collision d'identifiant contre les id_cart historiques.

3. Le site de refonte (www-refonte.DOMAINE) DOIT rester rigoureusement isolé du site principal (www.DOMAINE)

Il est **important** que l'équipe que vous avez missionnée pour cette refonte respecte l'autonomie et l'indépendance du www-refonte dans le cadre de votre refonte.

Si cette indépendance n'a pas été respectée, cela peut rendre impossible un éventuel rollback réclamé du fait d'un dysfonctionnement sévère détecté à la mise en ligne, contraignant TW à jouer un PRA sur la base de la dernière sauvegarde disponible (ce qui engendre toujours des pertes irrémédiables de données)

4. Récupération des clés/token historiques nécessaires au fonctionnement des mécaniques d'authentification des clients

Nous vous invitons à la vigilance sur la récupération de ces données sensibles, sous peine de contraindre tous vos clients à réclamer un nouveau mot de passe. Cela peut avoir des impacts notoires à dramatiques sur le CA suivant la cible :

MG 2 : app/etc/env.php
PS 1.6 : config/settings.inc.php
PS 1.7 : app/config/parameters.php
WP : wp-config.php

5. Le module de mise en cache de vos pages est pleinement fonctionnel

Il est essentiel qu'un module de mise en cache soit configuré et pleinement fonctionnel avant la mise en ligne.

Votre développeur doit vérifier avec rigueur le TTFB des pages en cache (il saura ce que c'est) qui DOIT être inférieur à 250ms à minima - 150ms si le site E-Commerce est hébergé sur serveur physique.

Sous réserve que vous ayez un accès SSH : les TTFB sont enregistrés dans les historiques du front end si Apache2 est exploité (disponible dans les chroots jails dans le dossier /var/log/apache2/).

Voici un EXEMPLE de commande pour isoler des TTFB anormalement élevés (pour l'EXEMPLE supérieur à 5 000 000us soit 5 secondes ET sur les 500 dernières entrées d'historique) - à ajuster avec le chemin complet de l'historique à analyser :

awk -F'TTFB:"|us"' '$2 > 5000000' /var/log/apache2/access.FILENAME.log

Vous pouvez croiser cet ouput avec les historiques des slow logs du pool FPM d'attribution (variable suivant la version PHP exploitée) - également disponible dans votre chroot jail dans /var/log/php/.

Vous pouvez également nous réclamer à tout moment une mise à disposition de Blackfire.io - géré par nos outils sous réserve que vous ayez un abonnement chez Blackfire.io.

6. Le module de sitemap est pleinement fonctionnel

Une attention particulière doit être portée sur le module de génération du sitemap de votre site Internet, soumis à Google Webmaster Tools.

Pour le cas spécifique de Prestashop, veillez à configurer avec soin les exclusions - à discuter avec votre spécialiste en référencement naturel.

ATTENTION : vous devrez détruire / reconstruire le(s) sitemap(s) après la normalisation des liens jouée à la phase 2 vu que tous les liens changeront. Veillez à le noter dans votre TODO post phase 2.

7. Isolation et contrôle des liens non dynamiques présents dans les codes sources

Nous vous invitons à tenir un inventaire rigoureux des liens non dynamiques (c'est à dire de toutes les séquences www-refonte.*, media-refonte.* etc) présents dans les fichiers.

Exemple de commande **SSH** pour rechercher "rapidement" la séquence "www-refonte" dans les fichiers sources :

find {path_to_cms} -type f ! -path "/img/*" ! -path "*/cache/*" -exec grep -Hn "www-refonte" {} \; -print | grep "www-refonte" | awk {'print $1'}*

Si vous n'avez pas de compétence sous SSH (profil non devops) OU que le CLIENT refuse de valider les CGU spécifiques relatives : ne pas hésiter à nous le réclamer en veillant à nous fournir les séquences à rechercher.

NB : si vous utilisez des symlinks par exemple parce que vous avez déphasé votre arborescence pour mieux gérer vos déploiements en (semi) automatique via des outils tel que Capistrano, veillez à bien remplacer "find" dans la commande précédente par "find -L" sinon les fichiers et répertoires disponibles via des symlinks hors arborescence soumise à la commande find seront ignorés de la recherche)

Ces séquences **NE SONT PAS** réécrites par nos mécaniques de normalisation de liens maîtres et doivent donc faire l'objet d'une prise en charge manuelle par vos soins planifiée de manière concomitante à la permutation à chaud de vhost succédant la normalisation de liens maîtres (phase 2 - point 3 et 4)

8. La couverture de la MEDIA URL est CONFORME (plus de 80% des assets distribués par ce biais)

Lorsque vous mettez en place la MEDIA URL, il est essentiel de contrôler qu'elle est effectivement prise en charge sur un maximum d'assets.

Selon le CMS retenu (dont Prestashop), il n'est pas rare de croiser des modules qui ne respectent pas les configurations du Prestashop à ce propos.

En cas de difficultés, vous trouverez une aide ici : https://www.touchweb.fr/aide/cdn

9. Veillez à toujours configurer des timeouts conformes lorsque vous incluez des services tiers

Lorsque vous configurez une API, et que vous êtes amenés à utiliser cURL, file_get_contents, etc, si l'application métier (souvent site E-Commerce) souffre d'une dépendance (plus ou moins forte sur le FRONT et/ou le BACK) au fonctionnement de cette API, il est obligatoire de configurer en bonne intelligence des timeouts reflétant cette dépendance.

Par exemple, s'il y a une dépendance FORTE à un FRONT en ce sens ou si l'API subit un incident sévère cela peut casser le FRONT, ALORS dans ce cadre précis et sous réserve de non-criticité de l'API (donc excluant par exemple des API sensibles comme des transporteurs / banques nécessaires au fonctionnement d'un tunnel d'achat) il est obligatoire de configurer un TIMEOUT inférieur à 2 secondes et si possible 1 seconde maximum.

Vous pouvez être plus souple si la dépendance est contre un BACK, 30 à 45 secondes autorisées et le cas échéant si c'est en tâche planifiée, les tolérances peuvent être nettement plus élevées.

En cas de carence à ce propos, vous exposez notre CLIENT commun à des incidents sévères par héritage d'incident sévère de service tiers.

Nous vous invitons à considérer ceci : penser qu'une API tierce ne subira jamais d'incident n'est que pure innocence, et si c'est vous qui la gérez, cela peut être assimilé à de l'arrogance.

L'innocence et l'arrogance sont les pires ennemis de la continuité optimale de service des applications métiers.

10. Les instructions d'arrêts secs de programme sont strictement interdites sans explication

Les WSOD engendrés par des arrêts secs de programmes (généralement script PHP) sans explication sont assimilés sur les infrastructures sous infogérance TW comme étant des actes malveillants et peuvent engendrer un arrêt immédiat de la relation commerciale du fait des préjudices financiers abusifs que les WSOD peuvent engendrer sur le marché des TPE à plus de 500 000€ / an

Nous vous invitons à vous interdire strictement de couper sans explication l'exécution de vos scripts.

Ceci est **PAR EXEMPLE** strictement interdit :

if(!$service_ok) die();

Veillez à fournir des explications permettant une origination dans un délai raisonnable, ce qui suit est autorisé :

if(!$service_ok) die('Le service est KO');

11. Inventaire des tâches planifiées à éditer / ajouter / supprimer

Le CLIENT ou le cas échéant son référent technique doit vous communiquer la liste **exhaustive** des tâches planifiées - type **WEBCRON** donc configurées sur des sites spécialisés tel que cron-job.org ou encore le Manager TW **ET** type **CRONTAB** donc configurées côté serveur (systématique ici sur les crons abusivement longues pour éviter des configurations dangereuses de timeout sur les frontends Apache2/Nginx/HaProxy)

Après avoir réalisé cet inventaire avec rigueur, nous vous invitons à nous fournir la liste précise des actions souhaitées sur les WEBCRON ET les CRONTAB (ajout/édition/suppression)

12. Contrôle de fonctionnement des emails transactionnels ET des modules envoyant des emails

Il est essentiel que vous contrôliez le bon fonctionnement des emails transactionnels (confirmation inscription CLIENT, rappel mot de passe, etc.) ainsi que la configuration des modules envoyant des emails - susceptible d'avoir été configuré par vos soins pour *NE PAS* envoyer d'email pendant le développement de la refonte (soit via des bypass dans les codes sources, soit via une désactivation via la gestion du module).

Veiller à bien tester les emails transactionnels ET à bien vous noter l'ensemble des éventuels bypass / configurations à éditer/supprimer sur les éventuels modules nécessaires.

13. Contrôle par sondage qu'il n'y a aucun défaut sur les images

Nous vous prions d'être vigilant sur les images incluant les éventuelles miniatures générées (dynamiquement : Magento / Drupal ou manuellement Prestashop / Wordpress) par votre application métier (souvent site E-Commerce).

Pour se faire, nous vous suggérons d'ouvrir la console de développeur sur Firefox ou Chromium (Chrome / Edge) puis à surveiller avec soin la présence d'éventuelles redirections type 301/302 sur des appels d'image - possiblement en anomalie ou d'erreurs 404.

Par **EXEMPLE** sur Prestashop, il peut arriver que le processus de génération des miniatures dans tous les formats que vous avez renseigné dans le backoffice de Prestashop soit partiellement en anomalie, cela peut générer une volumétrie anormalement élevée d'images en erreur quand vous consultez une page - susceptible de passer inaperçu si les images ne sont pas visibles "directement" dans la ligne de flottaison.

Toujours dans cet **EXEMPLE**, c'est à dire de visuels "cassés" sur Prestashop, possiblement hors ligne de flottaison, la seule manière de le détecter "simplement" est de consulter la console de développeur (F12 sur Firefox / Chrome). Dans l'éventualité d'images relatives à des fiches produits pour Prestashop, les éventuelles 301 générées par l'absence des miniatures attendues vont engendrer une volumétrie anormale d'appels côté serveur - augmentant - possiblement abusivement - les appels type PAGE (la redirection 301 de Prestashop redirigeant vers la homepage), **ce défaut est donc susceptible d'engendrer des bannissements.**

14. Contrôle de fonctionnement des trackers ET des flux (Google Shopping / Lengow / etc)

Si notre CLIENT commun travaille avec un spécialiste ADS (Google ADS / Facebook ADS / etc), pour piloter le ROI (retour sur investissement) des campagnes publicitaires, il est essentiel de contrôler avec soin et rigueur que les différents trackers "remontent" **effectivement** le chiffre d'affaires réalisé **sur TOUS les moyens de paiement disponibles** - à refaire valider en bonne intelligence avec le spécialiste ADS ou équivalent suivant les us et coutumes du CLIENT.

ATTENTION 1 : une carence à ce propos peut engendrer **des tensions fortes entre le CLIENT et son spécialiste ADS. "Pourquoi ai-je perdu 80% de mon CA (Chiffres d'affaires) à la mise en ligne ?"** Alors que tout va bien.

ATTENTION 2 : Si vous gérez des flux comme PAR EXEMPLE Google Shopping, veillez à vérifier avec soin que les données exportées sont parfaitement cohérentes avec les précédentes sous peine de gérer des doublons et de potentiellement vous faire "soft ban" par Google Shopping. Une attention particulière DOIT être portée sur l'identifiant unique des produits qui DOIT être préservé sous peine de contraindre l'éventuel spécialiste ADS dans la boucle de refaire toute sa campagne. Le CA dépendant à ces flux pour certains clients est supérieur à 10% de leur CA global, un dysfonctionnement à ce niveau peut donc leur être - très - préjudiciable.

15. Contrôle de la cyber-sécurité

Nous vous invitons à vérifier avec soin que les modules / plugins que vous utilisez sont libres de vulnérabilités connues (CVE) et d'entreprendre une relecture rapide pour constater qu'il n'y a aucun défaut manifeste sur des CWE triviales (path traversal / broken access control / injection SQL / injection PHP) détectable en moins de 5 minutes.

Personne chez TW ne vous tiendra rigueur de ne pas mener un audit sécurité complet - aucun CLIENT sur le marché des TPE n'ayant le budget pour cela, nous ne vous tiendrons également pas rigueur de ne pas avoir vu de vulnérabilités profondes nécessitant une analyse avancée par un devsecops confirmé à senior.

Néanmoins, il est rappelé qu'à compter de Septembre 2023, **toute vulnérabilité critique de sécurité (classifiées CVSS 3.1 9+/10) ET toute fuite de données personnelles (broken access control / path traversal) triviales, détectables en moins de 5 minutes, seront considérés comme étant de la malveillance par négligence volontaire.**

Nous vous invitons donc à rester vigilants sur ce sujet sensible, des réseaux criminels de plus en plus qualifiés agressent les écosystèmes E-Commerce, il est donc essentiel de devenir sérieux - si vous ne l'êtes pas déjà - en matière de cybersécurité.

*Depuis plus de 10 ans, la remédiation des piratages de nos clients a toujours été **OFFERTE.** Ce n'est donc pas une source de profit pour notre société et dans ce contexte, il est impératif d'anticiper au mieux ce type d'incident.*

16. Contrôle du préfix des tables en base de données

Par suite de la vague d'attaque contre l'écosystème ECommerce de Q2/Q3 2022, il est devenu au 22/07/2022 strictement interdit d'utiliser le préfix de tables en base de données par défaut de la solution que vous avez retenu.

Merci d'obligatoirement mettre un préfix respectant la complexité **minimale** suivante : [a-z0-9]{6}_ avec au moins une lettre ET un chiffre.

Une négligence de votre part à ce propos **expose gravement notre CLIENT commun à des attaques de type INJECTION SQL** du fait de noms prédictibles de table en base de données.

Pour rappel : un module bancaire largement exploité a été concerné pendant la vague d'attaque de 2022 ainsi qu'un module officiel d'une solution métier, cela signifie que même des modules sensibles (pour ne pas dire critique) peuvent être vulnérables à des attaques triviales par injection SQL.

Dernière mise à jour : 10/12/2024