Compte rendu de l'Analyse du site Perform Vision

Ce document représente la première version de l'audit du groupe "E-phenix" sur le projet du groupe de S3 "WebMicaa" pour la plateforme "Perform Vision", il est susceptible d'être enrichie au cours du travail suite à la découverte de nouveaux problèmes cachés ou de choix éditoriale de notre part vis à vis de contraintes.

1) Analyse générale du travail par rapport au sujet (Sofiane)

Les demandes exprimées pour les fonctionnalités du site peuvent être retrouvées dans le sujet des Saphir. Nous allons ici lister les fonctionnalitées attendues par rôle et mettre en couleur les points:

- Vert : Réalisé
- Orange : Partiellement ou doute sur la fonctionnalité
- Rouge : Non réalisé

NB : BDL = Bon de Livraison et BDD = Base de données

Pour le rôle prestataire :

- Se connecter (et changer ses mots de passes)
- Renseigner pour chacun de ses clients le bon de livraisons par le biais du formulaire adéquate :
    - Au fur et à mesure au cours du mois,
    - Ou en une seule fois lorsque le mois est échu
- De déclarer en avance des absences (optionnel)
- De générer un pdf de sa déclaration et le signer avec une signature électronique
- De générer un csv de sa/ses déclarations (optionnels)

Le Prestataire, remarque : Il semble qu'on puisse ajouter un bon de livraison avec comme champ à remplir, la composante, la date et le nom de la mission qui est censée être un type de BDL au vu de la bdd, donc heure, journée et demi journée (voir sujet pour mieux comprendre). Une fois le bon de livraison fait, on peut le regarder quand on est sur l'onglet "bon de livraison", on voit à l'intérieur la date, le jour et le commentaire que nous pouvons mettre. Il y a plusieurs dates donc on suppose que c'est les différents bon de livraisons qui ont été fait pour cette "mission".

Conclusions pour prestataire : Il faudra revoir la gestion et la création des BDL et même de la bdd car ce qu'ils ont fait n'est pas très clair.

Pour le rôle interlocuteur :

- Se connecter (et changer ses mots de passes)
- Consulter la liste des prestataires (et leur coordonnées) qui sont affectées à sa composante
- Consulter les BDL de chaque prestataire et :
    - Générer un pdf du BDL et le signer avec une signature électronique
    - Cocher les journées qui lui posent problème en cas de désaccord
    - Ajout de commentaires
- Consulter les déclarations d'absences (optionnels)

L'interlocuteur, remarque : La plupart des demandes ont été effectuées mais il manque des petits détails sur la consultation et la gestion des BDL.

Conclusion pour interlocuteur : Selon le temps disponible on pourra ajouter les options supplémentaires mais l'essentiel est là.

Pour le commercial :

- Afficher la liste de SES clients/composantes/interlocuteurs/prestataires
- Ajouter un interlocuteur client (ou modifier certains champs)
- Consulter les BDL des prestataires affectés à ses interlocuteurs clients

Le commercial, remarque : Pour ce qui est de consulter les BDL des prestataires affectés à ses interlocuteurs clients, on n'est pas sûr que cela soit bon parce que quand on clique sur la composante Y, on voit que le prestataire est Dupont Jean alors que le bon de livraison est au nom de Martin Marie.

Conclusion pour commercial : Régler les problèmes liés aux BDL

Pour le gestionnaire :

- Ajouter des prestataires (ou modifier certains champs)
- Gérer les affectations des prestataires dans les composantes
- Ajouter/modifier un client et lui ajouter au moins une composante, et affecter Cette dernière à au moins un commercial
- Consulter les BDLs des prestataires (et les déclarations d'absences)

Le gestionnaire, remarque : Pour l'ajout de prestataire cela marche mais il faudra revoir cela parce qu'on a l'impression que ce n'est pas nous qui choisissons si le prestataire est indépendant ou interne, lors de la création d'un prestataire, ça nous l'a mis en indépendant tout seul. Pour l'affectation des prestataire, cela ne marche pas, en tout cas il faudra revoir cela parce que on doit remplir nous même les champs au lieu que ça nous propose directement les prestataire existant que nous pouvons ajouter à la composante. Pour "ajouter/modifier un client et lui ajouter au moins une composante, et affecter cette dernière à au moins un commercial" il y a aucun endroit où c'est écrit qu'on peut ajouter un client, et pour affecter la composante à un

commercial ça ne marche pas non plus. Pour “consulter les BDLs des prestataires” on ne peut pas les consulter quand on va dans la rubrique “prestataire” et que l’on clique sur un prestataire, le seul moyens serait d’aller sur une composante pour voir la bdl d’un prestataire mais c’est une solution farfelu et on ne peut même pas le voir pour pour les prestataires.

Conclusion pour gestionnaire : Il va falloir régler les problèmes liés aux ajouts/modifications.

Pour l’Administrateur :

- Ajouter des gestionnaire
- Avoir les mêmes droits que les gestionnaire et commerciaux

L’administrateur remarque : Il a une interface similaire au gestionnaire.

Conclusion pour l’administrateur : On va ajouter une gestion des utilisateurs.

2) Audit Front-end (Michael et Nelson)

Le front-end a quelques problèmes d’affichages comme les champs input qui bougent et le responsive qui n’est pas présent (la page devient blanche si on réduit la fenêtre)

Le site à besoin d’un lifting pour un meilleur esthétique et une interface plus simple d’utilisation.

Voici les modifications envisagées :

Page login:

- Le background est une image floutée qu’on modifiera par un couleur de fond en dégradé
- Modifier la barre de navigation pour que ce soit cohérent avec le site
- Bloc de connexion à rétrécir
- Formulaire à rétrécir
- Modifier la couleur des bordures des formulaires
- Changer la couleur du bouton de connexion
- Pop-up pour choisir le rôle plus petit
- Supprimer l’image du pop-up
- Modifier la taille du pop-up

Page mission:

- Le background est une image floutée qu’on modifiera par un couleur de fond en dégradé
- Enlever les bars de navigation du tableau
- Changer la couleur du bouton pour créer une mission
- Modifier le formulaire de la page ajout mission qui sont trop longues
- Centrer les dernières infos du formulaire et les rétrécir

Page Société, page composantes, page prestataires, page commerciaux:

- Centrer le formulaire et le titre
- Rétrécir la longueur du formulaire

Page info société:

- Rétrécir la longueur du formulaire
- Rapprocher les blocs pour que ce soit moins espacé
- Modifier la couleur de bordure des blocs

Page info composante:

- Rétrécir la longueur du formulaire

Header:

- Modifier le bouton de déconnexion (optionnel)
- Nom du compte à mettre sur toute la ligne

Footer:

- Mettre un logo au lieu d'avoir le nom "Perform Vision"

Responsive:

- Mettre un menu hamburger pour les versions téléphones avec les différentes rubriques à la ligne.

3) Audit Back-end (Sofiane et Thibaud)

Au niveau du Back-end, le site suit le modèle MVC mais de sorte que chacun des contrôleurs correspond à un rôle, il y a donc des répétitions de fonctions dans les différents contrôleurs pour les pages communes. Au niveau du modèle beaucoup de fonctions sont très précises (par exemple pour modifier un champ dans une table on a une fonction par champ).

Code couleur :

- Rouge : priorité
- Orange : secondaire

Voici une liste des principaux problèmes rencontrés à ce jour :

- Il faut modifier les vues qui incluent des formulaires car ils ont mal fait le lien de l'action dans le form (retour page de connexion lors de l'ajout)
- Rendre fonctionnel les boutons mdp oublié
- Rendre fonctionnel les formulaires, ils ne fonctionnent pas vraiment pour l'instant (message d'erreur et message de réussite en utilisant de l'AJAX)
- Menu déroulant pour les formulaires afin de pouvoir sélectionner facilement les personnes.
- Lisibilité de la bdd lors de l'ajout d'une personne.

- **Aucun système de déconnexion/ système d'authentification !!!!**
- En modifiant le lien, on peut faire en sorte de donner n'importe quelle rôle à n'importe qui (ex: interlocuteur que nous pouvons rendre gestionnaire)
- Revoir la gestion des sessions (sessions qui sont détruite, donc impossible d'avoir plusieurs utilisateurs)
- Mot de passe visible dans la bdd
- Mauvaise utilisation de la fonction htmlspecialchars
- Améliorer le système de génération du mdp
- Le prestataire ne peut pas changer son mot de passe.

Vu la configuration de leur MVC, il faudrait tout refaire car la gestion est mauvaise et le code dur à lire. On n'aura pas le temps pour tout refaire donc on va garder leur structure actuelle et y greffer des modifications pour les ajouts de fonctions ainsi que résoudre les problèmes listés avant surtout au niveau de la sécurité et de la gestion des sessions.

4) Audit sécurité (Soheib)

Comme vu juste avant de nombreux problèmes de sécurité sont présents, une analyse de problèmes plus cachés à été réalisée pour trouver d'autres failles moins évidentes.

DÉCOUVERT AVEC LA SUITE D'OWASP

Problème 1 : priority:Mid

- Absence de Jetons Anti-CSRF (3)

  liens : http://127.0.0.1/SAES4/?controller=login&action=check_pswd

Description :

Aucun jeton Anti-CSRF n'a été trouvé dans un formulaire HTML.
La contrefaçon de requête intersites (Cross Site Request Forgery - CSRF) est une attaque qui consiste à forcer une victime à envoyer une requête HTTP vers une destination cible, sans qu'elle n'en aie ni connaissance ni intention, afin d'effectuer une action en se faisant passer pour la victime. La cause originelle est que les fonctionnalités de l'application sont appelées à l'aide d'URL ou d'actions de formulaires prévisibles et reproductibles. La nature de l'attaque est que le CSRF exploite la confiance qu'un site internet accorde à un utilisateur. En revanche, le cross-site scripting (XSS) exploite la confiance que l'utilisateur porte à un site internet. Comme XSS, les attaques CSRF ne sont pas nécessairement multi-sites, mais elles peuvent l'être. La contrefaçon de requête intersite est également connue sous les noms CSRF, XSRF, attaque en un clic (one-click attack), session riding, confused deputy et sea surf.

Les attaques CSRF sont efficaces dans de nombreuses situations, notamment:

* quand la victime a une session active sur le site cible.
    * quand la victime est authentifiée via HTTP auth sur le site cible.
    * quand la victime est sur le même réseau local que le site cible.

CSRF a d'abord été utilisée pour effectuer une action contre un site cible en utilisant les privilèges de la victime, mais des techniques récentes permettent d'avoir accès à des renseignements en accédant à la réponse. Le risque de divulgation d'informations est considérablement augmenté lorsque le site cible est vulnérable aux XSS, parce que XSS peut être utilisé comme une plateforme pour CSRF, permettant à l'attaque d'opérer dans les limites de la politique de même origine.

Solution possible: Ajouter un système de token CSRF dans les formulaires

Problème 2 : priority:Mid

- header CSP absent

Description :

La politique de sécurité du contenu (CSP) est une couche de sécurité supplémentaire qui permet de détecter et d'atténuer certains types d'attaques, notamment les attaques de type Cross Site Scripting (XSS) et les attaques par injection de données. Ces attaques sont utilisées pour tout, du vol de données à la défiguration de sites ou à la distribution de logiciels malveillants. Le CSP fournit un ensemble d'en-têtes HTTP standard qui permettent aux propriétaires de sites web de déclarer les sources approuvées de contenu que les navigateurs devraient être autorisés à charger sur cette page - les types couverts sont JavaScript, CSS, les cadres HTML, les polices, les images et les objets intégrables tels que les applets Java, ActiveX, les fichiers audio et vidéo.

Solution : (en phase de test)

Problème 3 : priority:Mid-high

- Decouverte de fichier caché : http://127.0.0.1/SAES4/.git/config

Description:

Contient les informations sur le Git, peut être considéré comme problématique à notre échelle surtout si inclus dans le script de production.
contenu du fichier:

```
[core]
  repositoryformatversion = 0
```

```
  filemode = true
  bare = false
  logallrefupdates = true

[remote "origin"]
  url = https://gitlab.sorbonne-paris-nord.fr/12200893/sae-s4-groupe-e-phenix.git
  fetch = +refs/heads/*:refs/remotes/origin/*

[branch "main"]
  remote = origin
  merge = refs/heads/main
```

Solution possible: essayer de rendre accessible le dossier git et/ou le changer de directory en changeant les permissions d'accès . Exemple, créer un utilisateur Git et lui donner le droit d'interagir avec ces fichiers et retirer le droit au serveur de les lire.

DÉCOUVERT EN ANALYSANT AVEC BURPSUITE

Problème 1 : priority:?

Description:

J'arrive à voir le contenu du post envoyé par le formulaire de connexion dans un header http en mettant en place un proxy espion. En entrant un email et un mot de passe, je peux

Solution possible : intégrer un chiffrement des données avant envoi dans le post (RSA?). Peut être passer par https en générant des certificats de sécurité dans la configuration apache?

Problème 2 : priority:?

Description:

j'arrive a trouver un token admin de marya qui traîne entre la page login et la page d'accueil qui est injectable par n'importe quelle autre utilisateur. En gros je peux passer admin si j'ai le token.

Solution:
recherche en cours

5) Conclusion de l'Audit

Beaucoup de problèmes venant de la conception initiale font que les modifications à apporter pour rendre le site fonctionnel et ergonomique nécessitent une refonte vu le temps accorder à la compréhension du fonctionnement.

Par manque de temps pour ce projet nous allons modifier un maximum de points essentiels surtout pour rendre le site fonctionnel et un peux plus sécurisé, nous n'aurons pas le temps d'effectuer toutes les modifications nécessaire mais allons essayé de traiter les points clefs de la manière dont ils ont été exprimés dans les points de cet audit.

6) Tableau des modifications (Rendu n°2)

Type	Problème	Modification	Auteurs	Date
Back-end	Les liens d'actions des formulaires ne sont pas fonctionnels	Modification des liens pour qu'ils target l'action et contrôleurs voulu	**Thibaud / Sofiane**	**17/05/2024**
Back-end / sécurité	Absence de Jetons Anti-CSRF dans les formulaires de connexion	Ajouter un système de token CSRF dans les formulaires	**Soheib**	**17/05/2024**
Front-end	Page login non responsive/ background mauvais/ le header et le footer ont des problèmes quand on passe au-dessus de plusieurs options et les block bouge	Le background est une couleur/ la page est responsive / correction du CSS pour empêcher les blocs de bouger / correction des problèmes pour le header et le footer	**Nelson / Michael**	**17/05/2024**
Back-end / sécurité	On peut accéder à n'importe quel page avec l'URL sans aucune vérifications de droits d'accès	Vérifications dans l'index du rôle et de l'état de la connexion avant de charger la page demandé, si pas de droits page d'erreur ou de connexion	**Thibaud / Sofiane**	**19/05/2024**
Back-end	Gestion des sessions avec constant redémarrage et destructions	Globalisation du session_start() et nettoyage des fonctions inutiles	**Thibaud / Sofiane**	**19/05/2024**
Back-end / sécurité	fichier caché visible: http://127.0.0.1/SAES4/.git/config	Séparation du dossier de pull du dossier de déploiement	**Soheib**	**22/05/2024**
Front-end	Textes peu visibles à cause de la couleur, les ombres ne sont pas utile, bouton ajouter mal placé, car il ne fait plus penser à un bouton de recherche et manque du bouton de recherche, problèmes de placement des bouton pour les dates	Modification des couleurs des textes, suppression des ombres, ajout d'un bouton de recherche et modification du placement du bouton ajouter sur plusieurs pages et recentrage des case pour les dates	**Nelson / Michael**	**22/05/2024**

Front-end	Le header n’a pas de mode menu hamburger/ Mettre un logo au lieu d’avoir le nom “Perform Vision” dans le footer / ajout du responsive sur toutes les pages/	Ajout du menu hamburger / création et ajout du Logo/ toutes les pages sont responsive/	**Nelson / Michael**	**24/05/2024**
Back-end / sécurité	Possibilité d’usurpation d'identité numérique en récupérant le token de connexion d’un administrateur sniffé sur le proxy	Chiffrement du token de bout en bout pour valider la transaction sans modifier le fonctionnement du site	**Soheib**	**24/05/2024**
Back-end	Le prestataire ne peut pas changer son mot de passe.	Ajout d’une fonction déjà existante mais manquante dans le controller prestataire.	**Sofiane**	**24/05/2024**
Back-end	Coordonnées manquante lors de la consultation de la liste des prestataires qui sont affectées à la composante de l’interlocuteur.	Ajout de la coordonnée manquante qui était l’adresse mail.	**Sofiane**	**24/05/2024**
Front-end	Blocs inutiles prennent de la place et moche,	Supprimer les blocs pour avoir des tableaux, amélioration du responsive et de plusieurs parties de CSS	**Nelson / Michael**	**28/05/2024**
Back-end	Manque de fonctionnalitée Admin	Ajout d’une page d'administration avec la liste des utilisateurs et en lui permettant de changer le rôles des utilisateurs et les supprimer.	**Soheib**	**31/05/2024**
Back-end	Champ de modification des personnes dans le “placeholder” ce qui ne permet pas une modification optimal.	Correction du problème en mettant les informations dans “value”.	**Sofiane**	**31/05/2024**
Back-end	Page blanche lors de l’ajout de l’interlocuteur et champs d’ajout non pratiques car il faut tout écrire à la main.	Correction du problème en mettant une alert javascript lorsque l’ajout à bien été effectué avec une redirection, et liste déroulantes qui récupère les informations de la base de données pour les composantes assigné au client précisément.	**Sofiane**	**31/05/2024**

Back-end	Pour ajouter un commercial il fallait que ce soit une personne déjà existante mais on pouvait rentrer n'importe qui et si la personne n'existait pas elle n'était pas ajoutée mais on avait aucun retour	Correction en mettant un menu déroulant avec les noms et emails des commerciaux pour choisir dans la liste	**Thibaud**	**31/05/2024**
Back-end	Champ de modification des composantes, du profil de la personne et des clients dans le "placeholder" ce qui ne permet pas une modification optimale.	Correction du problème en mettant les informations dans "value". Ajout en plus de message pour valider la modification et aussi un message d'erreur, et utilisation de la fonction "htmlspecialchars" pour les éléments de la base de données que nous utilisons sur la page. Ajout en plus de placeholder manquant.	**Sofiane**	**31/05/2024**
Back-end	Aucune gestion d'erreurs lorsqu'on ajoute un interlocuteur déjà existant. Nous avons un warning php à la place qui est problématique	Correction des erreurs lors de l'ajout d'interlocuteurs déjà existant dans une composante en restructurant la fonction "action_ajout_interlocuteur_dans_composante" et en modifiant "getIdComposante" afin de pouvoir utiliser des id ou des noms.	**Thibaud / Sofiane**	**05/06/2024**
Back-end	Lors de l'ajout de la composante, l'ajout ne se fait pas à cause de l'adresse et cela n'ajoutait pas de commercial.	Correction de l'ajout en modifiant la fonction d'ajout de composante	**Thibaud / Sofiane**	**05/06/2024**
Back-end	Lors de l'ajout d'une composante, il n'y a pas de liste déroulante avec les informations importantes à renseigner ce qui n'est pas du tout pratique.	Ajout de liste déroulante récupérant les informations importante dans la base de données afin de rendre l'ajout plus simple et limiter les erreurs	**Thibaud / Sofiane**	**05/06/2024**
Front-end	Amélioration requise	Amélioration des nouveaux tableaux qui on remplace les block, de tous les textes, des boutons et du header	**Nelson**	**05/06/2024**
Back-end	Les zone "mot de passe oublié" et "adresse mail	Fonctionnement des zones lorsqu'on clique dessus,	**Sofiane**	**08/06/2024**

	oublié” ne fonctionne pas	ce qui nous redirige vers une page ou il y a un mail à contacter pour pouvoir changer ses informations. Cela à été fait grâce à la création de l’action “oublie_mdp” et “oublie_mail”.		
Back-end	Barre de recherche non fonctionnel	Barre de recherche fonctionnel en ajoutant une fonction javascript qui cherche si ce qu’on écrit dans la barre de recherche existe sur une partie d’un élément, ex : si on met dans la barre de recherche “composante”, cela va nous afficher tous les éléments qui possède le mot composante dans leurs nom.	**Sofiane**	**08/06/2024**
Backend	Déploiement du git non automatisé	Utilisation d’un script bash pour automatiser le déploiement sur le serveur		
Back-end	Ajout d’un prestataire sans indication, on ne sait pas si on doit ajouter des prestataire déjà existant ou si cela crée un prestataire tout seul, et on ne sait pas si on doit ajouter ces prestataire à la mission qu’on veut ou juste celle reliée à la composante. Il n’y avait pas non plus de message de validation lors de l’ajout.	Correction en ajoutant des listes déroulantes avec les différents prestataires existants et n’appartenant pas encore à la composante en question. Ajout de la mission de la composante en “value” et ajout de “readonly” pour pas que la personne puisse le modifier. Pour finir, ajout d’un message de validation lors de l’ajout d’un prestataire.	**Sofiane**	**08/06/2024**
Front-end	Responsive pas adapter pour mobile/menu hamburger pub	Tous les problèmes sont résolus	**Nelson / Michael**	**09/06/2024**
Back-end	Erreur lors de la consultation des informations d’une mission car aucune vérification si il y a des informations ou non.	Mise en place de conditions vérifiant si il y a bien des informations pour les ajouter dans le controller prestataire action_afficher_bdl.	**Sofiane**	**10/06/2024**
Back-end	Manque de listes déroulante lors de l’ajout d’un bon de livraison ce qui rend l’ajout du bdl plus compliqué.	Ajout d’une liste déroulante pour savoir les composantes existantes et les missions appartenant au prestataire afin de rendre plus logique et simple l’ajout de bons de livraison..	**Sofiane / Thibaud**	**10/06/2024**

7) Auteurs

Rédaction et analyse 1) par Sofiane

Rédaction et analyse 2) par Nelson et Michael

Rédaction et analyse 3) par Sofiane et Thibaud

Rédaction et analyse 4) par Soheib

Remplissage du tableau 6) par chaque membre du groupe lors d'une réalisation

Mise en commun et mise en forme du document par Thibaud

Mise en place du git et readme par Soheib