

Authentification

Titre de la mission : authentification

Description :

lors de mon stage de 2 ieme année chez Inovyn, j'ai eu pour mission la création d'un site-web pour permettre aux employées de créer des tickets. Pour que chaque employé puisse accéder au site, ils doivent passer par une étape d'authentification à l'aide d'un fr (identifiant d'inovyn) et un mot de passe (modifiable par la suite).

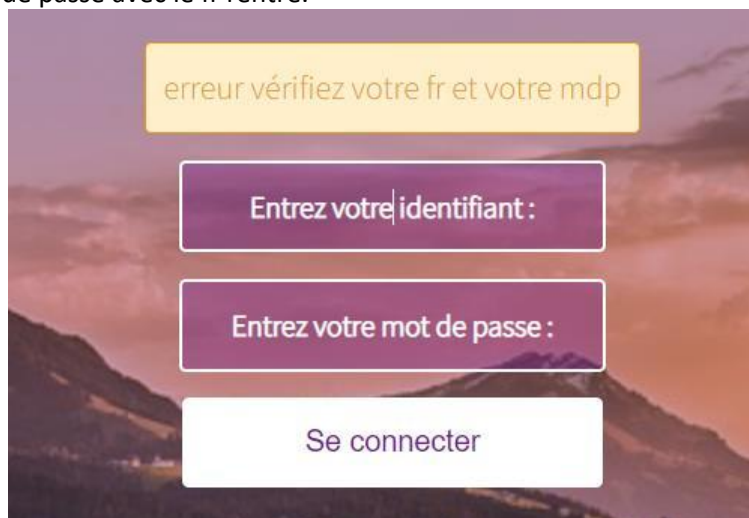


Voici le design de la page de connexion.

Pour la partie traitement, un formulaire est envoyé en méthode post et une méthode du controller ConnexionController récupère le fr et le mdp rentré.

Une requête est lancée pour trouver le mdp dans la base de données en fonction du fr. Ensuite je compare le mot de passe récupéré depuis la base de données avec le mot de passe rentré par l'utilisateur.

S'ils sont identiques l'utilisateur a accès à la suite du site sinon il obtient un message d'erreur et doit ressaisir son mot de passe et son fr, la même situation se produit si la requête ne trouve pas de mot de passe avec le fr rentré.



Bien sûr le message d'erreur ne dit pas si c'est le mdp ou le fr qui est faux, cela rajoute de la sécurité.

Pour éviter d'écrire les mots de passe en dur dans la base de données et rajouter de la sécurité il faut chiffrer les mots de passe.

Pour cela j'ai utilisé une fonction de php sha1() qui permet de hacher le mot de passe, lorsqu'elle reçoit une chaîne de caractères, elle la retourne sous la forme d'un nombre hexadécimal d'une taille de 40 caractères.

hello → aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d

Mais cette fonction peut facilement être contournée par des rainbow tables qui sont des bases de données de mots avec tous les hash pré-calculés, avec ça on peut retrouver le mot de passe.

Pour contourner ce problème il faut ajouter un grain de sel, c'est-à-dire une variable connue au début du mot de passe et à la fin et le hasher avec la fonction, comme cela même si le mot de passe est déchiffré grâce à une rainbow tables il n'est pas utilisable.

Grainhello → 303c4f5fc1991a09d76d711595aaf6a769a25e37

L'authentification permet l'autorisation, les simples utilisateurs sont renvoyés vers la version du site avec restriction, alors que l'administrateur est renvoyé vers la version avec tous les droits.

Date de réalisation : 09/02/2022

Durée prévue : 1 jour

Durée réelle : 1 jour et demi

Justification des écarts :

la recherche sur les bonnes pratiques à avoir avec le mot de passe dans la base de données et la manière de le chiffrer ont pris plus de temps que prévu.

Environnement technologique :

J'écris mon code avec visual studio code, j'utilise le framework Laravel, et une base de données sur sql server.

Je développe sur un serveur de développement IIS

Seul ou en équipe :

mission vécue seul

Compétences mobilisées :

1.1.1 Recenser et identifier les ressources numériques

Prendre connaissance des équipements de l'entreprise :

Ils travaillent sur windows 10, ils ont un serveur IIS de développement et un serveur IIS de production, le labware est un logiciel qui les aide dans leur travail d'analyse des échantillons (grande base de données).

J'écris mon code avec visual studio code, j'utilise le framework Laravel, et une base de données sur sql server.

1.1.2 Exploiter des référentiels, normes et standards adoptés par le prestataire informatique

Une norme de Laravel consiste à utiliser des layout pour pouvoir économiser de code et ne pas recréer la même page à chaque fois. Mise en place des layout pour économiser du code, nom de table et normes de la bdd économie de place sur la bdd en mettant des chiffres lorsque cela est possible.

1.1.3 Mettre en place et vérifier les niveaux d'habilitation associés à un service

Lors de l'authentification au site, l'administrateur (maitre de stage) est repéré par rapport aux simples utilisateur (employées). C'est alors que le procédé d'autorisation prend place et accorde plus de droits sur le site à l'administrateur.

L'administrateur a une version du site spéciale où il peut voir tous les tickets, modifier le mdp de n'importe qui etc... alors que l'utilisateur ne peut que voir ces propres tickets et modifier son propre mot de passe. Cette autorisation se fait grâce à la base de données. Un champ de la table user nommés statuts comporte soit user soit admin, et en fonction de ce champs l'autorisation est donnée ou pas.

1.1.6 Vérifier le respect des règles d'utilisation des ressources numériques

- Les mots de passe des utilisateurs sont hashés dans la base de données grâce aux grains de sel dans le code source. Même l'administrateur ne peut avoir accès aux mots de passe des utilisateurs en consultant la base de données.
- Les administrateurs ne peuvent pas consulter n'importe quelle donnée des utilisateurs depuis le site-web. Seules les informations des tickets des utilisateurs sont consultables depuis le site.
- Un utilisateur n'a accès qu'à ses propres données sur le site.

1.2.1 Collecter, suivre et orienter des demandes

Une demande du cahier des charges voulait que l'utilisateur puisse choisir de se connecter ou de s'inscrire, j'ai proposé de directement inscrire les utilisateurs dans la base de données avec un mot de passe provisoire, comme cela ils n'ont plus qu'à se connecter et changer leur mot de passe.

1.2.3 Traiter des demandes concernant les applications

Mon maitre de stage m'a demandé de créer un site pour gérer un service de ticket de A à Z en reprenant le design de l'ancien projet KPI.

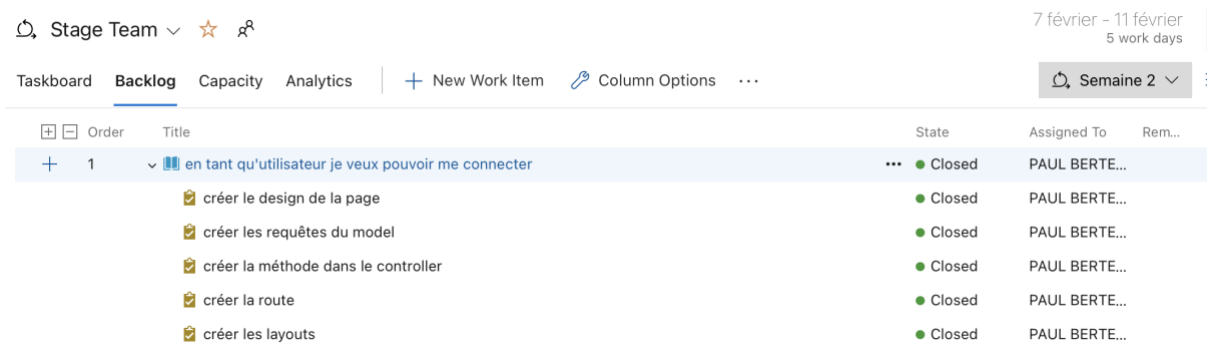
1.3.3 Participer à l'évolution d'un site Web exploitant les données de l'organisation

Réutilisation de certains codes du précédent site, notamment le projet KPI développé en laravel par un précédent étudiant.

Le site contient dans sa base de données de nombreuses informations de l'entreprise (fr, et données des utilisateurs, mail, secteur ...)

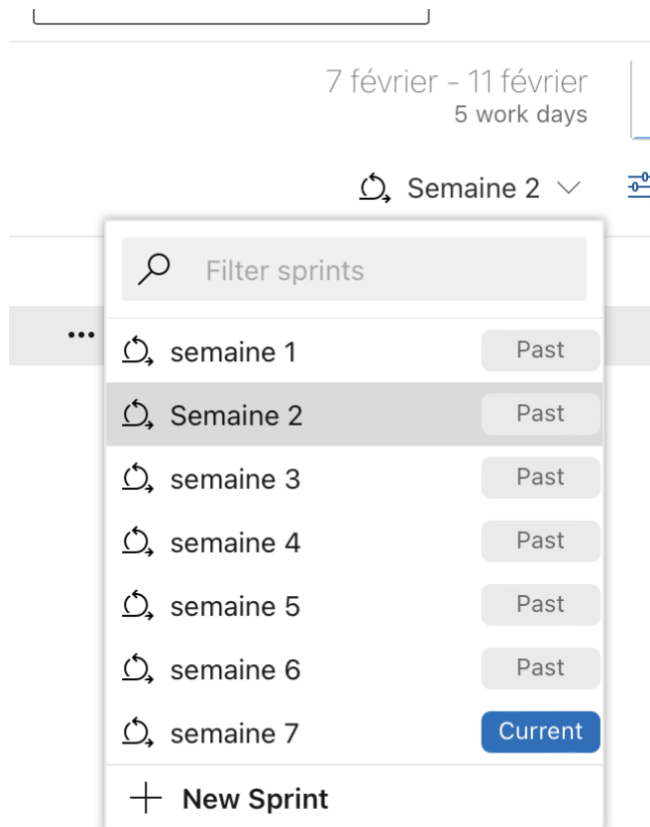
1.4.2 Planifier les activités

Pour planifier mes activités j'ai utilisé un outil de gestion de projet qui permet de créer des user stories avec des tâches. Il permet aussi de créer des sprints pour prévoir les activités dans la semaine.



The screenshot shows a Jira project interface for 'Stage Team'. The 'Backlog' tab is selected, displaying a list of work items. The first item is a user story: 'en tant qu'utilisateur je veux pouvoir me connecter'. It has a priority of 1 and is in a 'Closed' state. Below the user story, there are five sub-tasks, all of which are also in a 'Closed' state and assigned to 'PAUL BERTE...'. The interface includes navigation tabs like 'Taskboard', 'Capacity', and 'Analytics', as well as a date range selector for 'Semaine 2' (February 7 - 11, 5 work days).

Order	Title	State	Assigned To	Rem...
1	en tant qu'utilisateur je veux pouvoir me connecter	Closed	PAUL BERTE...	
	créer le design de la page	Closed	PAUL BERTE...	
	créer les requêtes du model	Closed	PAUL BERTE...	
	créer la méthode dans le controller	Closed	PAUL BERTE...	
	créer la route	Closed	PAUL BERTE...	
	créer les layouts	Closed	PAUL BERTE...	



Dans ces tasks je peux donner un temps, une description...

[TASK 169](#)

169 créer la méthode dans le controller

PAUL BERTELLI 0 comments [Add tag](#)

State	● Closed	Area	Stage
Reason	Completed	Iteration	Stage\Semaine 2

Description

créer la méthode qui permet d'authentifier les personnes grace au requêtes des méthodes du model, et renvoyer la bonne view.

Discussion

Add a comment. Use # to link a work item, ! to link a pull request, or @ to mention a person.

Planning

Effort (Hours)

Original Estimate
3

Remaining

Completed
4