Liste des figures

Figure 1 : logo de AMIIS 12
Figure 2: Logo UML 15
Figure **3:**Logo Entreprise Architect 15
Figure 4:diagramme de cas d'utilisation de l'internaute 16
Figure 5:diagramme de cas d'utilisation de l'adhérent 19
Figure 6: bout de code de l'évenement (suspendre adhérent) 21
Figure 7:diagramme de cas d'utilisation de membre de bureau 22
Figure 8:diagramme de cas d'utilisation de l'admin 23
Figure 9:diagramme de séquences 25
Figure 10:diagramme de d'activité LOGIN 26
Figure 11:diagramme de récupération mot de passe 27
Figure 12:diagramme de l'ajout d'un nouveau projet/news 27
Figure 13:diagramme de garder la session active 28
Figure 14:diagramme de classes 29
Figure 15: logo HTML5 31
Figure 16: logo CSS3 31
Figure 17: logo PHP 31
Figure 18:logo javaScript 31
Figure 19:logo XAMPP 32
Figure 20:logo MySQL 32
Figure 21:logo phpMyAdmin 32
Figure 22: logo swiftMailer 33
Figure 23:HOME 34
Figure 24:AMIIS Members 35
Figure 25:AMIIS Membership 35
Figure 26: AMIIS Projects 36
Figure 27: NEWS 36
Figure 28: contact us 37
Figure 29: JOIN US 37
Figure 30:profil adhérent actif 38
Figure 31:alerte adhérent pendu 38
Figure 32: alerte adhérent suspendu 38
Figure 33: dachboard ADMIN 38
Figure 34: add user 39
Figure 35:add news 39
Figure 36: add project 40
Figure 37: Liste users 40
Figure 38: liste projects 41
Figure 39:liste news 41
Figure 40:liste messages 41
Figure 41: répondre du message 42
Figure 42: page du login 43
Figure 43: page reset password ..... .42

Figure 44: erreur email inexistant 43
Figure 45: envoie d'email 42

Figure 46:email reçu 44
Figure 47:email expiré 44
Figure 48: email du mot de passe changé avec succés 44
Figure 49:injection SQL exemple 46
Figure 50: le bout de code de vérification des champs 47
Figure 51: appélation de la fonction 48
Figure 52: exemple d'exploitation des failles 49
Figure 53: vérification de la session 49
Figure 54: le bout de code de la fonction de vérification de téléchargement 49

Table des matières

Liste des figures....6
Table des matières....7
Introduction générale....8
Chapitre I : contexte général du projet....9
1. Organisme d'accueil: l'association AMIIS....10
2. Description du projet....10
2.1 L'étude de l'existant :....10
2.2 Problématique et solutions....11
2.2.1 Problématique....11
2.2.2 Solutions :....11
Chapitre II : Modélisation et conception du projet....12
1. Outils de conception....13
2. Définition des acteurs....13
3. Modèle fonctionnel du système....14
3.1Cas d'utilisation de l'internaute....14
3.2 Cas d'utilisation de l'adhérent....17
3.3 Cas d'utilisation du membre de bureau....20
3.4 Cas d'utilisation de l'admin....21
4. Quelques diagrammes UML....22
4.1 Le diagramme de séquence de la demande d'adhésion....23
4.2 Le diagramme d'activité du LOGIN....24
4.3 Le diagramme d'activité de la récupération du mot de passe....24
4.4 Le diagramme d'activité de l'ajout d'un nouveau projet ou news....25
4.5 Le diagramme d'activité de garder la session active....26
4.6 Le diagramme de classes....27
Chapitre III : Modélisation et conception du projet....12
1. Outils de développement....30
1.1 Les technologies de développement....30
1.2 Outils/Logiciels utilisé....31
2. Présentation de l'application....32
2.1HOME....33
2.2 AMIIS Members....34
2.3 AMIIS Membership....34
2.4 Projects....35
2.5 News....35
2.6 Contact Us....36
2.7 JOIN US....36
2.8 Profil d'un adhérent activé....37
2.9 Alerte pour adhérent pendu....37
2.10 Alerte pour adhérent suspendu....37
2.11 Dashboard admin....37
2.12 Add user....38
2.14 Add project....39
2.15 Liste users....39
2.16 Liste projects....40
2.17 Liste news....40
2.18 Liste messages....40
2.19 Réponse du message....41
Sécurité du site....45

1. les failles XSS....46
1.1 Définition....46
1.2 L'exploitation des failles par les pirates informatiques....46
2. Injection SQL....46
2.1Définition....46
2.2 Types des injections SQl....47
2.3 Exemple d'exploitation des injections SQL par les pirates....47
2.4 Filtration, vérification et nettoyage des inputs....48
Conclusion....50
Webographie....51

Introduction générale

Les technologies médicales progressent chaque année de 10%, représentantes aujourd'hui un marché de 200 milliards d'euros. En croissance constante depuis 50 ans, et remarquable ces dernières années. L'ingénierie et l'innovation des leaders et des start-ups dans le domaine de la santé contribuent donc, de façon significative aux progrès médicaux.

C'est à la croisé des domaines de la santé et la technologie que *l'**A**ssociation **M**arocaine d'**I**ngénierie et d'**I**nnovation en **S**anté* a été née.

Nous étions menés à créer un site web qui permet de présenter l'association et de réserver un espace aux membres de cette association pour le partage des idées et des innovations en relation au thème de santé. C'est un site regroupant toute innovation et solution des produits réalisés par des ingénieurs, des professeurs, des médecins, et des chercheurs qui sacrifient leur développement à la médecine tout en utilisant les nouvelles technologies.

Ce rapport est réparti en trois chapitres principaux.

Le premier chapitre porte sur la description du lieu de stage avec une description du projet, ainsi que l'étude de l'existant.

Le deuxième chapitre présente une analyse des besoins fonctionnels et techniques ainsi l'étude et la conception adoptée dans ce travail illustrées par des diagrammes UML.

Le troisième chapitre présente les interfaces réalisées du site web, les outils techniques et les différents langages de programmation et de modélisation utilisés.

Chapitre I

Contexte générale du projet

1. Organisme d'accueil: l'association AMIIS

Figure 1 : logo de AMIIS

L'Association Marocaine d'Ingénierie et d'Innovation en Santé AMIIS est une association apolitique et autonome créée par des enseignants chercheurs issus des deux domaines de l'ingénierie et de la santé, notamment, de la Faculté des Sciences et Techniques de Fès et de la Faculté de Médecine et de Pharmacie de Fès. Dans le souci d'avoir une forte implication de la part des chercheurs en médecine ayant beaucoup de contraintes de temps liées à la nature de leur travail, l'AMIIS est assiégée à la Faculté de Médecine et de Pharmacie de Fès, en partenariat avec le Centre Hospitalier Universitaire HASSAN II.

Elle vise à développer une recherche appliquée en santé dans le contexte marocain, par:

- Le développement de nouvelles solutions et produits innovants.
- Le développement de nouvelles approches et de nouveaux outils d'enseignement de la santé basés sur les TIC.
- La création d'un environnement durable pour les jeunes startups.

2. Description du projet

2.1 L'étude de l'existant :

L'Association AMIIS a un site web vitrine constitué de trois pages web statiques dans leq quelles se présentent certaines caractéristiques de l'association comme les services offerts par celle-ci, les objectives qu'elle veut atteindre et ses promesses aux startups dans le domaine d'innovation et d'ingénierie en santé. Une page est utilisée pour présenter les membres de cette association et une pour afficher les informations de contact.

Ce site ne répondait pas aux besoins des membres qui veulent partager leurs idées et leurs innovations avec les autres membres de cette association et avec le grand public. Le site est considéré donc inactif et ne permet pas l'interaction entre membres.

De plus, un réel besoin de gestion des adhésions des nouveaux membres se sent. En effet, l'Association Marocaine d'Ingénierie et d'Innovation en Santé exige une demande d'adhésion

rédigée par le chercheur ou industriel désirant adhérer à l'association et qui doit être déposée manuellement au bureau administratif. Une réponse sera formulée par les membres du bureau qui décident d'accepter ou non les nouvelles demandes d'adhésion.

D'autre part, les projets innovants, en cours ou achevés, dans le domaine de l'innovation et de l'ingénierie en santé représentent des informations enrichissantes à partager entre les membres de l'AMIIS. L'un des objectifs du site web de l'AMIIS est d'offrir une plateforme de soumission de soumission, de validation et de publication de ces projets.

2.2 Problématique et solutions :

2.2.1 Problématique :

D'après l'étude de l'existant, nous avons tenu que l'association a besoin d'un espace de partage entre les membres, et les principaux problèmes peuvent être résumés dans les points suivants :

- Gestion d'adhésion manuelle exhaustive et fatigante.
- Manque d'une base de données commune pour le stockage des données.
- Pas d'espace de partage des projets et des nouveautés entre les membres.

3.4.1 Solutions :

Après une réunion avec la vice-présidente et la secrétaire générale, membres fondatrices de l'association, et après note analyse profonde des besoins des membres de cette association, nous avons pu cibler les problèmes et de concevoir des solutions afin de répondre à ces besoins et d'accomplir les objectifs de notre projet, qui sont :

- ☑ Créer un site web regroupant en premier lieu les informations sur AMIIS.
- ☑ Mettre en valeur les workshops réalisés par AMIIS.
- ☑ Donner la possibilité de demander l'adhésion à travers le site.
- ☑ Gérer les adhérents et leurs statuts.
- ☑ Créer un espace commun entre les membres de l'association pour partager leurs projets et leurs idées ainsi que leurs innovations servant le domaine médical.
- ☑ Gérer les projets et leurs statuts.
- ☑ Notifier les membres et le public par les dernières nouveautés en leur permettant de s'inscrire à la newsletter.
- ☑ Sécuriser les données publiées dans le site web de l'association.

Chapitre II

Modélisation et conception

Du projet

Dans ce chapitre nous abordons la partie conception du projet, dans laquelle, nous détaillons les différents éléments de la conception, en utilisant le langage de modélisation graphique UML.

1. Outils de conception

les outils de modélisation suivants sont ceux qui nous ont servis dans l'étape de la conception :

- **UML**

Figure 2: Logo UML

figure3 : Logo UML

UML, c'est l'acronyme anglais pour « Unified Modeling Language ». On le traduit par « Langage de modélisation unifié ». La notation UML est un langage visuel constitué d'un ensemble de schémas, appelés des diagrammes, qui donnent chacun une vision différente du projet à traiter. UML nous fournit donc des diagrammes pour représenter le logiciel à développer :

son fonctionnement, sa mise en route, et les actions susceptibles d'être effectuées par le logiciel.

- **Entreprise Architecte**

Figure 3:Logo Entreprise Architect

Enterprise Architect est un logiciel de modélisation et de conception UML, édité par la société australienne Sparx Systems. Couvrant, par ses fonctionnalités, l'ensemble des étapes du cycle de conception d'application, il est l'un des logiciels de conception et de modélisation les plus reconnus.

2. Définition des acteurs :

Premièrement, il fallait se poser la question « Qui interagira avec notre site ? » et bien que la réponse éclaircisse les acteurs à qui notre site sera réalisé, nous sommes menés à les identifier :

- ✓ **Internaute** : tout visiteur du site, qui peut demander l'adhésion à l'association AMIIS.
- ✓ **Adhérent** : membre de AMIIS.
- ✓ **Membre de bureau** : qui est un membre du bureau administratif de l'AMIIS.
- ✓ **Administrateur** : Admin du site .

3. Modèle fonctionnel du système

3.1Cas d'utilisation de l'internaute :

Un internaute est tout visiteur du site, il a la possibilité de consulter le site c'est à dire en premier lieu, consulter la page d'accueil avec les dernières nouveautés. Il peut aussi consulter les projets dont il a le droit de voir, donc seulement ceux déjà approuvés par l'administrateur. Il peut aussi effectuer une recherche au niveau des projets et au niveau du site en entier.

L'internaute peut aussi s'inscrire à la newsletter pour recevoir les dernières actualités dans sa boite de l'adresse email qu'il a saisit dans le formulaire d'inscription. De plus, il peut contacter l'administrateur à travers un formulaire de contact, qui représente une fonctionnalité offerte par la majorité des sites web.

S'il désire devenir membre de l'AMIIS, il peut demander l'adhésion à travers un formulaire d'adhésion. A partir de ce moment, il devient un adhérent avec statut « pendu ».

Diagramme de cas d'utilisation de l'internaute :

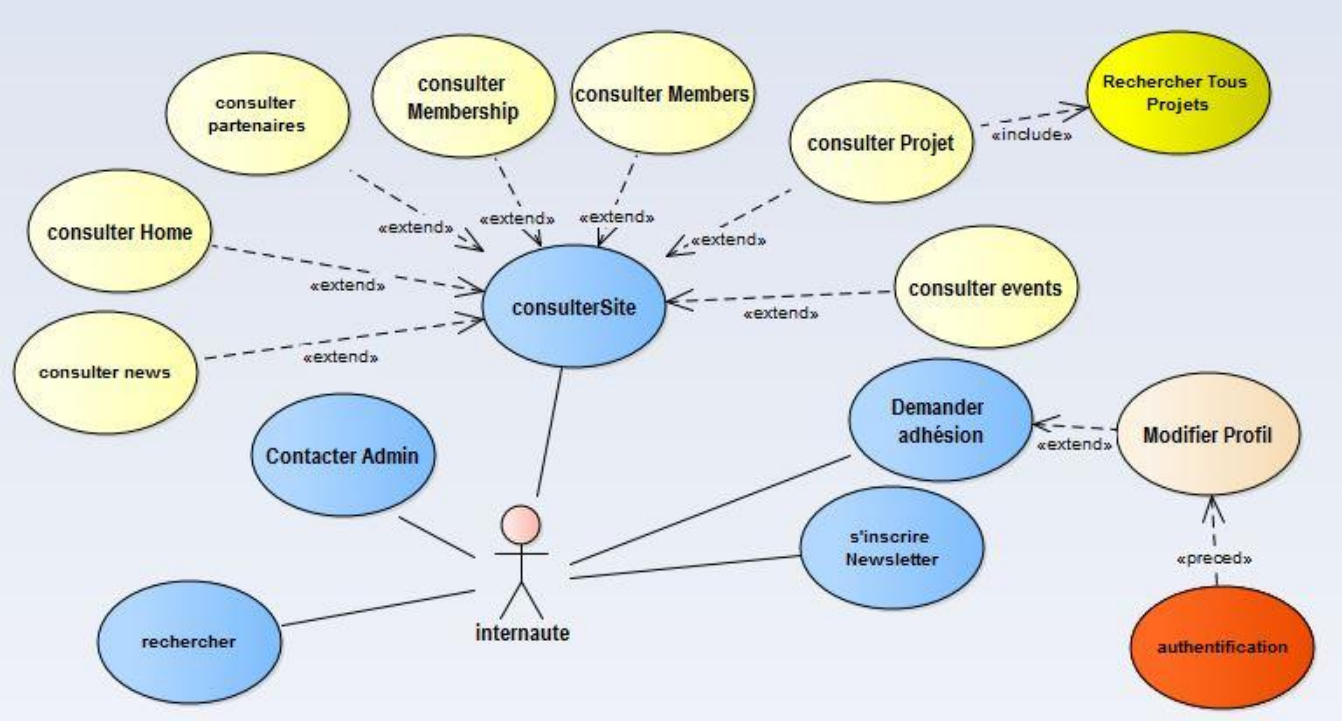

Figure 4:diagramme de cas d'utilisation de l'internaute

En résumé, les fonctionnalités accessibles à un internaute sont :

- ✓ Consulter le site.
- ✓ S'inscrire à la newsletter.
- ✓ Effectuer une recherche dans le site.
- ✓ Contacter l'admin.
- ✓ Demander l'adhésion.
- ✓ Modifier son profil: dès qu'il demande l'adhésion, l'internaute devient identifié par un login (email) et un mot de passe qu'il saisit dans le formulaire de la demande. La fonction « Modifier profile » lui permet de modifier l'une de ces deux informations.

Description

- **Demande d'adhésion :**

  Ce cas d'utilisation permet à l'internaute de demander l'adhésion afin de devenir membre de l'AMIIS.

  Scénario :

  1. L'internaute clique sur le bouton (join us)
  2. Le système renvoie le formulaire d'adhésion
  3. L'internaute remplit les champs du formulaire et valide
  4. Le système vérifie les champs
     4.1 L'email saisit ne doit pas figurer dans les emails de la base de données
     4.2 Le système filtre les champs (enlever les espaces doublés du début et de la fin du champ …)
  5. Le système stocke les données dans la base de données
  6. Le système lui affiche un message de remerciement d'adhésion

  La demande apparait dans la dashboard de l'administrateur et les membres de bureau

  Scénario alternatif :

  Si l'un des champs contient une information erronée

  - Le système lui renvoie un message d'erreur devant le champ de l'information erronée.
  - Les informations sont à ressaisir

  Une fois cette demande est soumise, l'adresse email est stocké dans la base de données l'internaute n'est plus considéré un visiteur, il est actuellement un adhérent avec statut « *en attente » ou « pending »*, c'est-à-dire un adhérent qui attend que sa demande soit validée par l'administrateur du site.

- **Contacter AMIIS**

  Scénario :

  1. clique sur le menu « CONTACT US ».
  2. le système renvoie un formulaire
  3. la personne remplit les champs du formulaire.
  4. le système vérifie la saisie et la filtre (Si l'email est sous la forme « ---@--.--»)
  5. le système enregistre les informations saisies dans la base de données.
  6. le système renvoie une fenêtre de remerciement.

- **Inscription à la newsletter**

  Ce cas d'utilisation est valable pour tous les internautes qui sont intéressés par les nouveautés de AMIIS.

Scénario :

1. S’inscrire à la newsletter
2. Le système renvoie un formulaire qui contient un seul champ pour entrer l’email
3. La personne entre l’email
4. Le système vérifie si l’email respecte bien la forme d’un email (----@---.---)
5. L’email est stocké dans la base de données s’il s’agit d’un nouvel email, sinon il est ignoré.

- **Consulter projets**

  La consultation des projets est d’afficher le titre du projet et sa description sans voir tous les détails, la consultation des détails nécessite une authentification

  1.cliquer sur « PROJECTS »

  2.le système lui renvoie la liste des projets

  3.si l’internaute désire consulter tous les détails d’un projet il doit s’authentifier

  4.en cliquant sur le titre du projet le système lui dirige vers la page d’authentification

- **Recherche**

  Ce cas d’utilisation est une fonction dans le site que tous les membres et les internautes peuvent utiliser. Il s’agit de la recherche dans les projets et les actualités (nouveautés).

3.2 Cas d'utilisation de l'adhérent

Après authentification, le système donne à l'adhérent l'opportunité de consulter tous les détails des projets qu'un simple internaute ne peut voir.

En plus, il lui donne la possibilité de soumettre un nouveau projet, le modifier et le supprimer bien avant que l'administrateur le valide.

Le même traitement s'applique pour les news. L'internaute soumet une news, il paut la modifier et la supprimer avant sa validation par l'admin et sa publication en ligne.

Nous différencions ici entre trois statuts d'adhérent :

Actif : membre de AMIIS qui respecte le règlement intérieur.

En attente ou Pending : son adhésion n'est pas encore approuvée par l'administrateur.

Suspendu : membre d'AMIIS bloqué temporairement. Généralement, la suspension se déclenche à la fin de chaque année en attendant que l'adhérent s'acquitte de ses frais d'adhésion.

Diagramme de cas d'utilisation de l'adhérent:

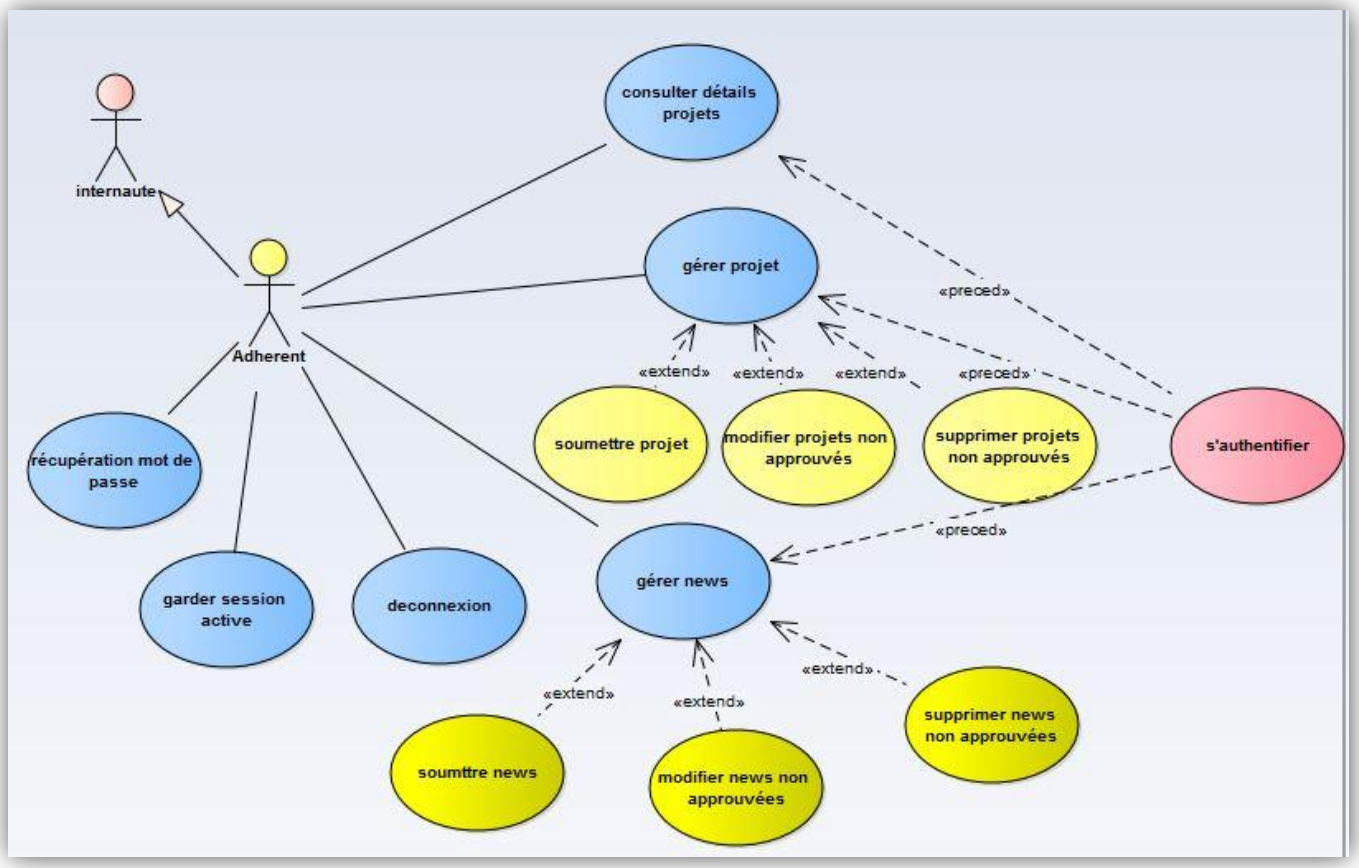

Figure 5:diagramme de cas d'utilisation de l'adhérent

Description :

En plus des fonctionnalités d'un internaute, et après une authentification, un adhérent peut :

- ✓ Modifier son profil : ses informations et sa photo.

- ✓ Garder session active : en cliquant sur « remember me ».
- ✓ Récupérer son mot de passe
- ✓ Se déconnecter

Les fonctionnalités suivantes ne sont accessibles que pour les adhérents avec statut « actif » :

- ✓ Consulter le détail des projets : voir tous les détails des projets approuvés par l'admin.
- ✓ Gérer les projets : ajouter un nouveau projet, supprimer ou modifier les projets non encore approuvés par l'admin.
- ✓ Gérer les news : ajouter une nouvelle « news », supprimer et modifier ses news si elles ne sont pas encore approuvées par l'admin.

- **Gestion des projets / news**

Ce cas d'utilisation est le même pour la gestion des projets et les news. Il s'agit d'ajouter, supprimer et modifier un projet/une news.

Pour publier une news :

1. Il faut aller à « ajouter news »
2. Le système renvoie un formulaire
3. La personne remplit les champs de ce formulaire
4. La personne valide la news
5. Le système vérifie les champs obligatoires et si leur syntaxe est correcte
6. Les informations sont enregistrées dans la base de données et apparaissent dans le panel admin.
7. Tant que la news n'est pas encore approuvée par l'admin, deux icônes apparaissent dans la page de la gestion « my news » donnant le droit de modifier ou supprimer la news.
8. Si l'admin accepte la news, elle est publiée dans le site. L'adhérent qui l'a soumise n'aura plus le droit de la modifier ou la supprimer.
9. Sinon l'admin et la personne ont la décision de supprimer cette news ou de la modifier.

- **Récupération du mot de passe :**

Ce cas d'utilisation est une fonction que tous les adhérents ont le droit de faire s'ils ont oublié leur mot de passe.

Pour le récupérer, une procédure doit être suivie :

1. Cliquer sur « forgot my password »
2. Le système renvoie un formulaire avec un seul champ à remplir (email)
3. L'adhérent doit fournir son email
4. Le système vérifie si l'email existe dans la base de données ou pas
   - Si l'email n'existe pas on lui affiche une erreur
   - Sinon
     1. Le système génère un token qui est une chaine de caractères aléatoire de 90 lettres (s'expire dans deux heures)
     2. Le système envoie un email contenant le lien de récupération
     3. L'adhérent clique sur le lien dans l'email

- Si le délai d'expiration est dépassé, le système renvoie un message d'erreur et demande la re-saisie de l'email afin de lui générer un nouveau token
- Sinon le système lui revoie un formulaire pour saisir le password et le confirmer. Le token n'existe plus dans la base de données après le changement du mot de passe.

➢ **Garder ma session active :**

1. Cliquer sur « remember me »
2. Le système crée deux cookies dont la première (PID) contient l'ID de l'utilisateur, la deuxième cookie (SS save session) qui se compose d'une chaine de caractères aléatoire hachée par les deux fonctions MD5 et SHA1 et les stocke dans la base de données avec une durée de vie de 30 jours.
3. Après que la personne ferme le navigateur et l'ouvre de nouveau, le système consulte et compare la cookie dans la base de données avec celle dans le navigateur.
   - Si elles sont identiques le navigateur ne demande pas à l'adhérent l'authentification
   - Sinon, ou au cas où les données du navigateur sont supprimées, ou si la durée de vie de la cookie dépasse 30 jours, le système lui demande une nouvelle authentification.

➢ **Rechercher**

Dans le panel de chaque personne apparait une barre de recherche avec deux boutons à cotés, le premier est un combobox dont on distingue entre les thèmes de recherche, après que l'on choisit un thème, cette recherche s'effectue selon ce dernier, alors elle ne se fait que dans la colonne du thème précisé.

NB : chaque début d'année, un événement est lancé automatiquement pour suspendre tous les adhérents comme montre la figure suivante :

```
MySQL [db_amiis]> show create event suspendAdherant\G;
*************************** 1. row ***************************
               Event: suspendAdherant
           time_zone: SYSTEM
        Create Event: CREATE DEFINER=`root`@`localhost` EVENT `suspendAdherant`
                      ON SCHEDULE EVERY 1 YEAR STARTS '2018-01-01 00:00:00'
                      ON COMPLETION NOT PRESERVE ENABLE DO update db_amiis.users
                      set users.statut="suspended"
                      where users.role="adherant"
character_set_client: utf8mb4
collation_connection: utf8mb4_unicode_ci
  Database Collation: latin1_swedish_ci
1 row in set (0.00 sec)
```

Figure 6: bout de code de l'évenement (suspendre adhérent)

3.3 Cas d'utilisation du membre de bureau

Le membre du bureau est un modérateur du site. Il hérite toutes les fonctions d'un adhérent. De plus, il a certains privilèges par rapport à un adhérent, que nous résumons dans les points suivants :

- Un adhérent ne peut voir que les projets qu'il a soumis lui-même ou les projets déjà validés par l'admin alors qu'un membre de bureau peut consulter la liste des projets non encore validés par l'admin et consulter leur statut sans pouvoir le changer.
- Un membre du bureau a la possibilité de lister toutes les news et effectuer une recherche dans ces news.
- Il a aussi la possibilité de consulter la liste des nouveaux adhérents et leur statut sans le pouvoir de le changer. Il peut consulter aussi l'historique d'adhésion de tous les membres pendant les années passées.
- Un membre du bureau peut aussi répondre aux messages que les internautes envoient également à l'admin.

Diagramme de cas d'utilisation du membre de bureau :

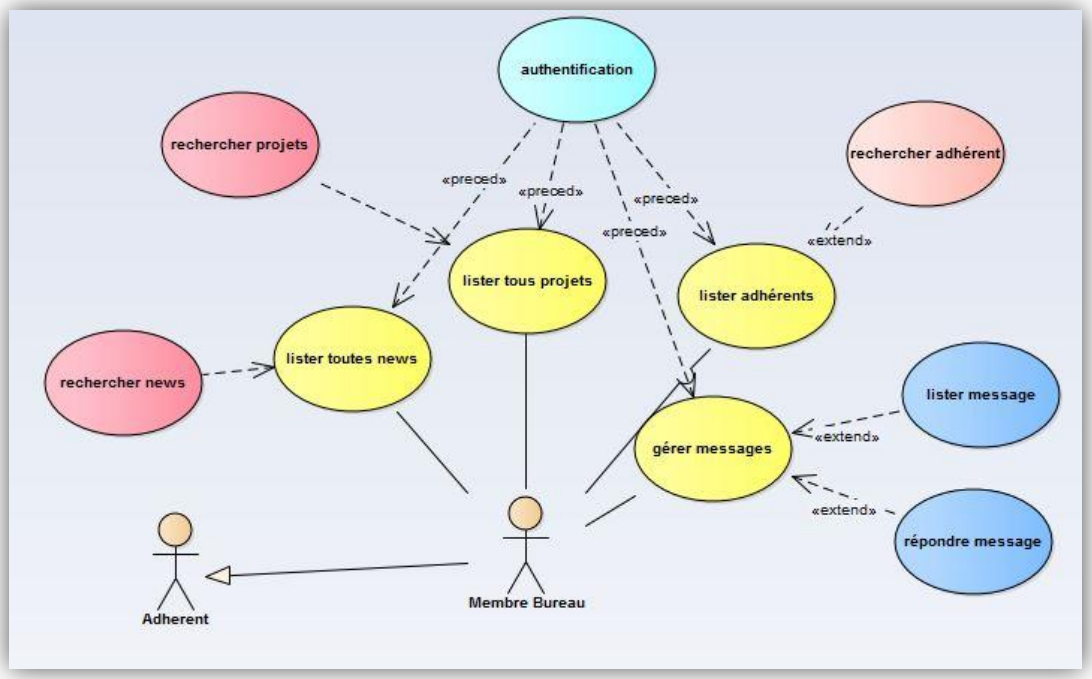

Figure 7:diagramme de cas d'utilisation de membre de bureau

Description :

Après une authentification, un membre du bureau peut:

- ✓ Lister et rechercher dans toutes les news : y compris les news non encore publiées.
- ✓ Lister et rechercher dans tous les projets : y compris les projets non encore approuvés par l'admin.
- ✓ Lister et rechercher dans les adhérents : voir tous les membres même ceux avec statut « pending », c'est-à-dire qui viennent d'envoyer une demande d'adhésion mais non encore approuvée par l'admin.

- ✓ Gérer les messages : dans la liste des messages, le site offre au membre de bureau la possibilité d'envoyer des réponses.

- **Gérer message**

Ce cas d'utilisation est commun entre l'admin et le membre de bureau et il s'agit de lister les messages reçus dans le « CONTACT US »

Dans la liste des messages, il y a deux boutons (deux options) pour chaque message, un pour voir le détail du message et l'autre pour y répondre.

Dès qu'il y a un nouveau message, il apparait dans la liste des messages, le membre du bureau et l'admin sont les seuls qui peuvent répondre à ce message. Une seule réponse par chaque message est possible et cette dernière s'envoie directement du site à l'adresse email fournie par l'internaute dans le formulaire « CONTACT US ».

3.4 Cas d'utilisation de l'admin

L'administrateur hérite toutes les fonctions d'un membre du bureau. De nouvelles fonctionnalités lui sont ajoutées comme le montre la figure suivante :

Diagramme de cas d'utilisation du membre de l'admin:

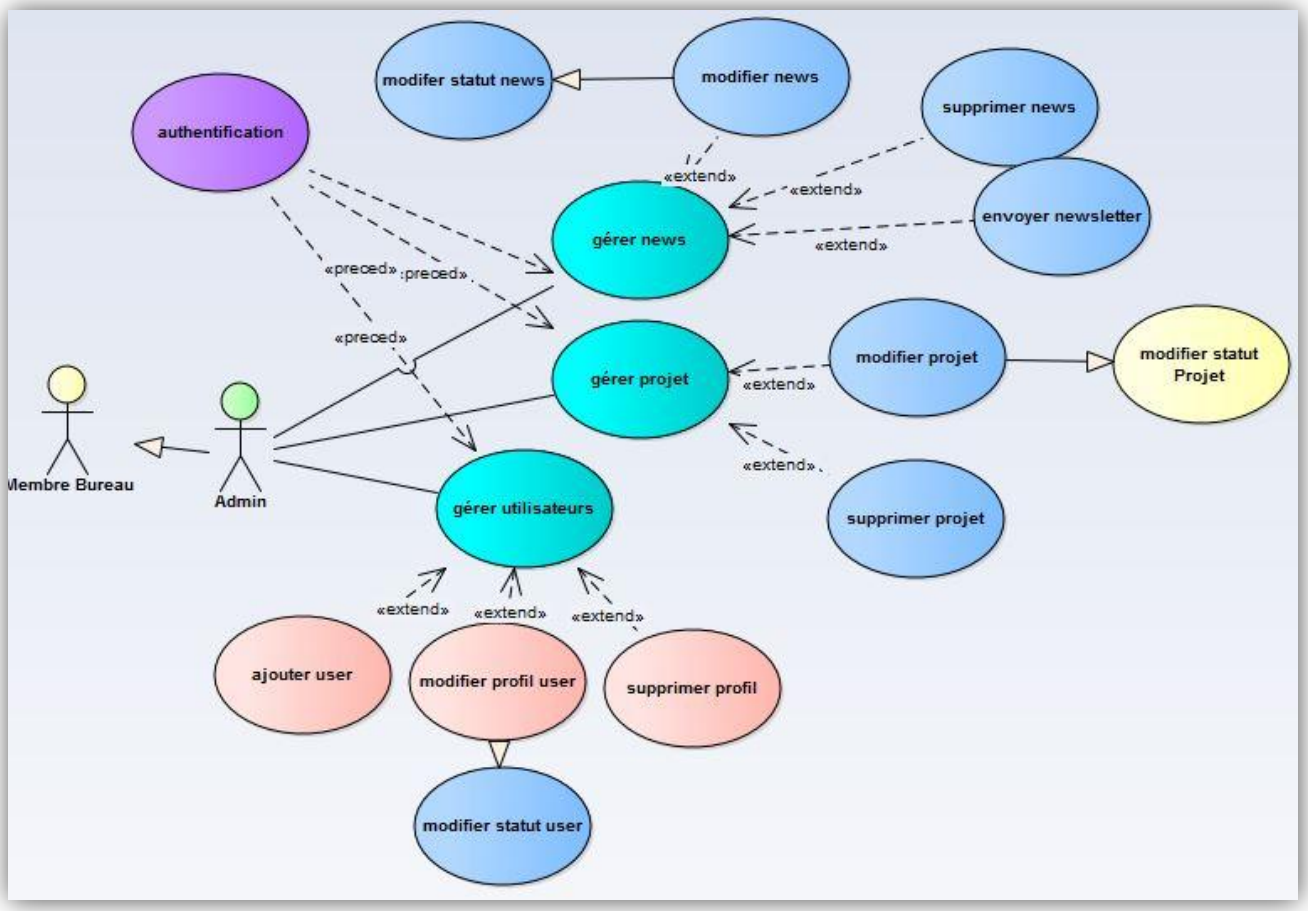

Figure 8:diagramme de cas d'utilisation de l'admin

Description :

- ✓ Gérer les utilisateurs : ajouter et supprimer et modifier les profils de ces utilisateurs et leur statut.
- ✓ Gérer les projets : approuver, supprimer, modifier les projets des utilisateurs ainsi que ses propres projets.
- ✓ Gérer les news : ajouter, modifier, supprimer news et envoyer la newsletter du mois.
- ✓ Gérer les demandes d'adhésion : approuver la demande de la personne qui désire être membre de l'AMIIS ou la refuser.
- ✓ Gérer les messages : il l'hérite déjà du membre de bureau

4. Quelques diagrammes UML

Dans la suite, nous présentons quelques diagrammes UML explicitant avec plus de détail les fonctionnalités du système. Pour ne pas alourdir ce rapport, nous avons choisi de présenter :

- Le diagramme de séquence de la demande d'adhésion
- Le diagramme d'activité du LOGIN
- Le diagramme d'activité de la récupération du mot de passe
- Le diagramme d'activité de garder la session active
- Le diagramme d'activité de l'ajout d'un nouveau projet ou news
- Le diagramme de classes

4.1 Diagramme de séquence pour la demande d'adhésion :

Le diagramme de séquence suivant montre exactement le déroulement de la demande d'adhésion qui se fait par l'internaute qui désire devenir membre de l'AMIIS.

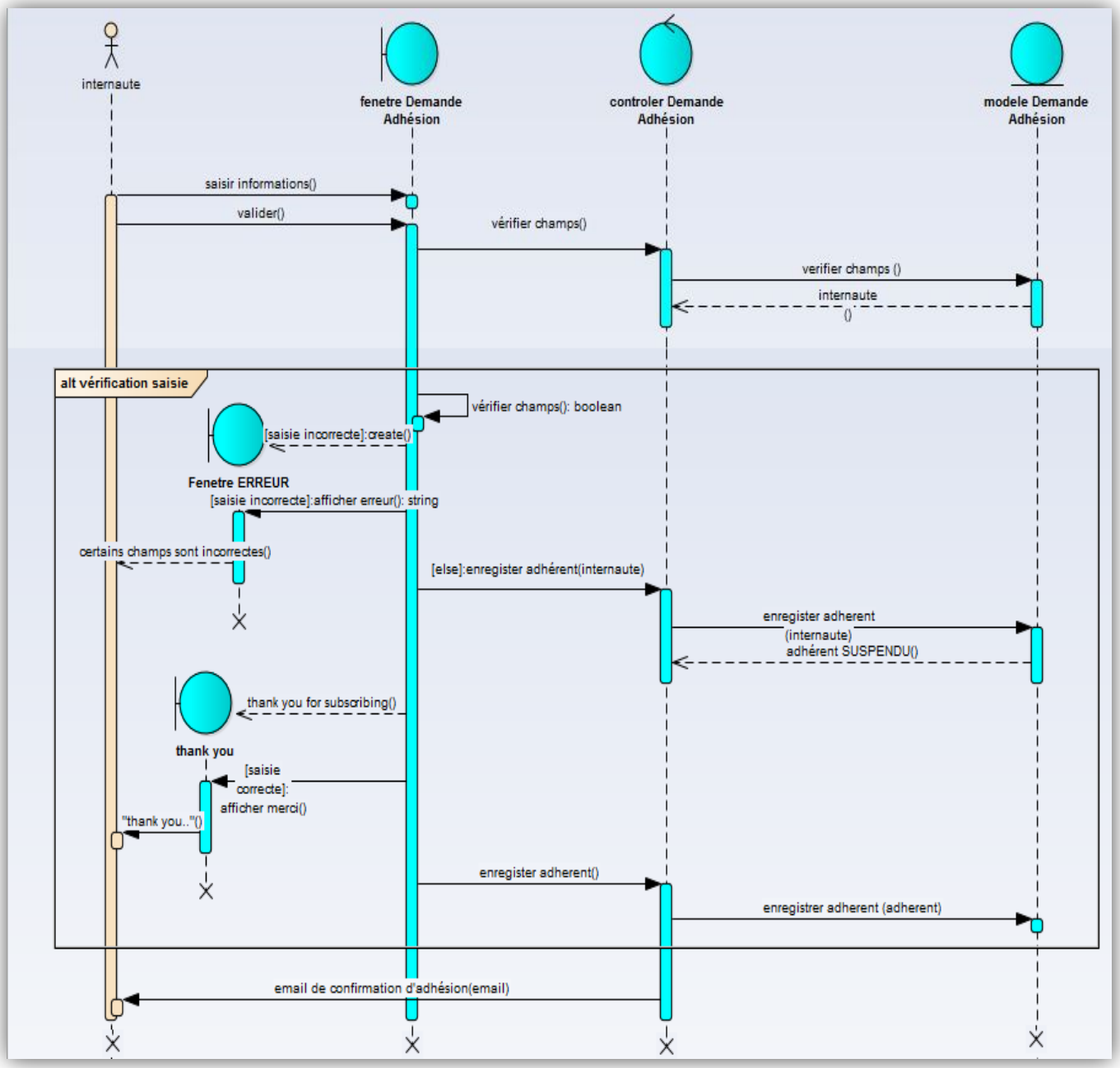

Figure 9:diagramme de séquences

4.2 Diagramme d'activité LOGIN :

C'est une étape nécessaire pour que les adhérents, les membres de bureau et l'admin du système puissent accéder à leur espace réservé dans le site.

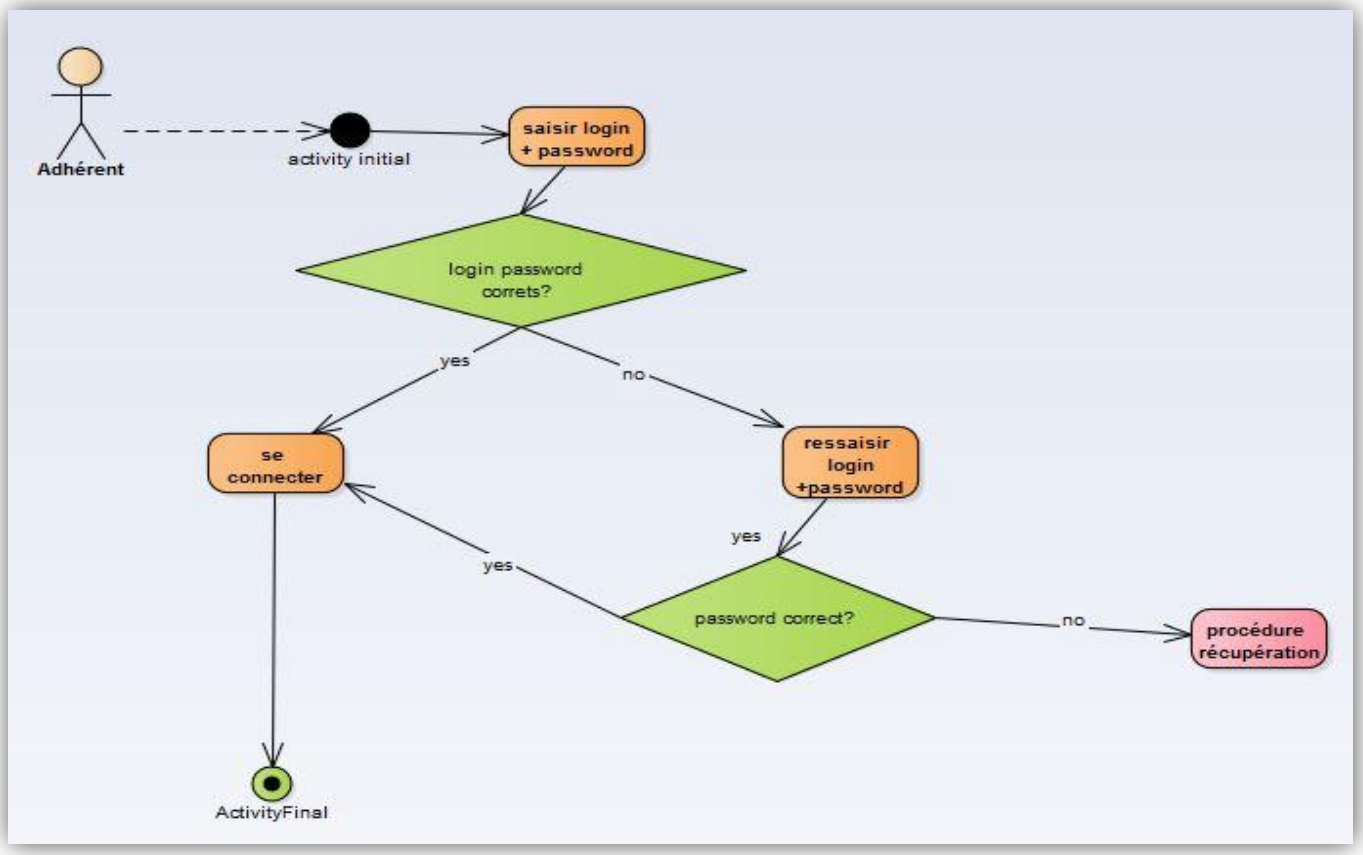

Figure 10:diagramme de d'activité LOGIN

après l'authentification chaque acteur du système à le droit de faire plusieurs fonctions relatives exactement à son role.

4.3 Diagramme d'activité de la récupération du mot de passe :

La possibilité de récupérer le mot de passe est offerte à tous les adhérents quelque soit leur statut et quelque soit la période d'adhésion, pour cela il faut suivre cette procédure de récupération :

Premièrement il faut cliquer sur « forget my password », le système lui mènera à une autre page où il doit saisir à nouveau son email, le système vérifie si l'email existe dans la base de données et génère une chaine de caractère aléatoire de 90 lettres et lui envoie un email contenant un lien avec cette chaine (le nouveau mot de passe) que sa duré de vie ne dépasse pas 2heures , après cette duré limite d'expiration l'email n'est pas utile et il faut commencer la procédure de la récupération à nouveau, après qu'il clique sur le lien il se dirigera vers un formulaire où il doit saisir son nouveau mot de passe et le confirmer.

Ce diagramme montre le déroulement de la récupération du mot de passe.

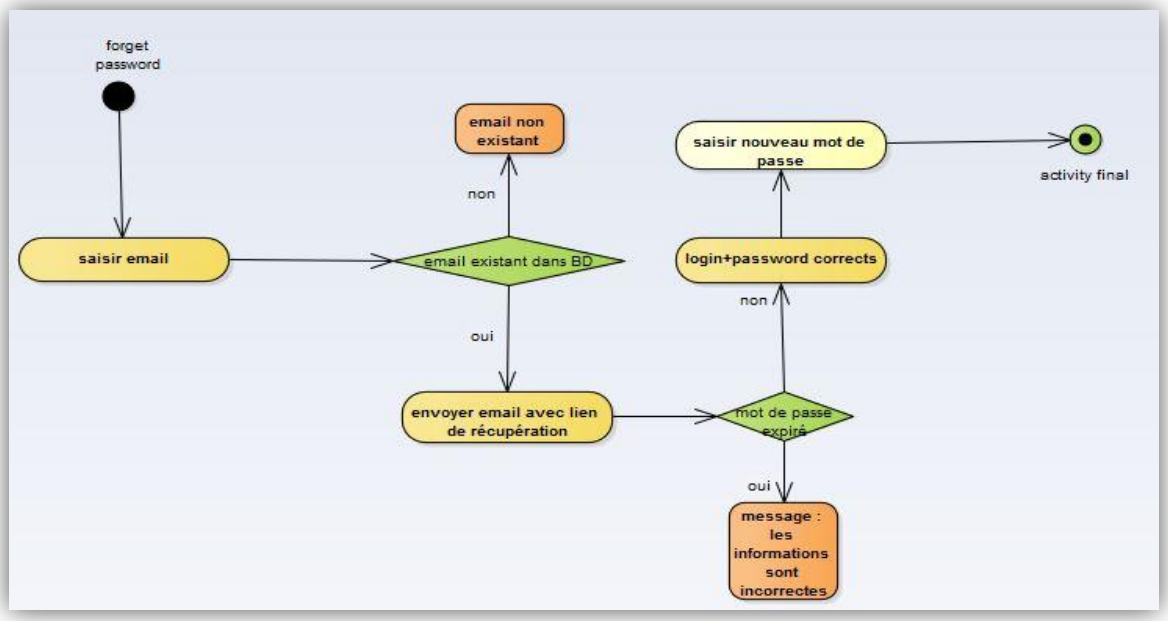

Figure 11:diagramme de récupération mot de passe

4.4 Diagramme d'activité de la création d'un nouveau projet/news :

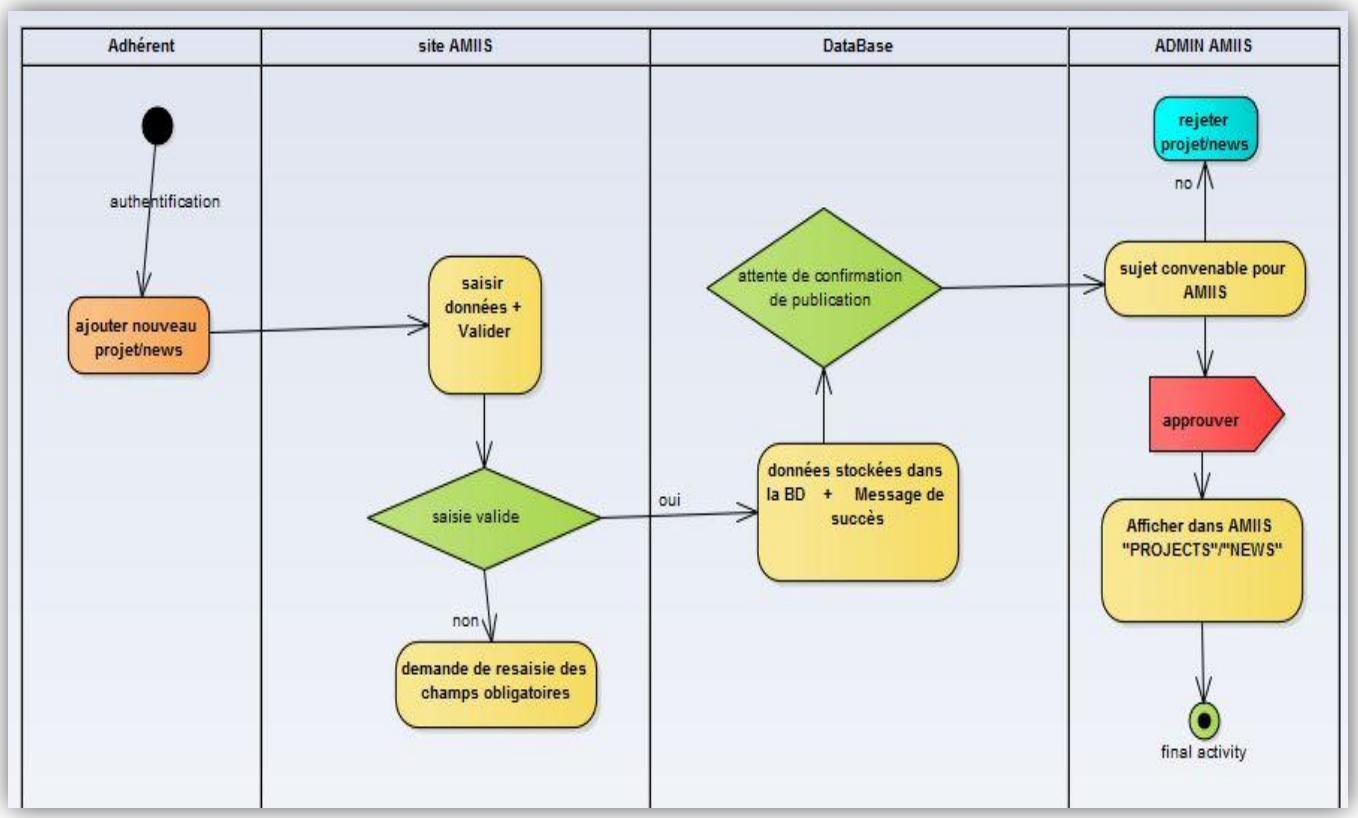

Figure 12:diagramme de l'ajout d'un nouveau projet/news

4.5 Diagramme d'activité de garder session active :

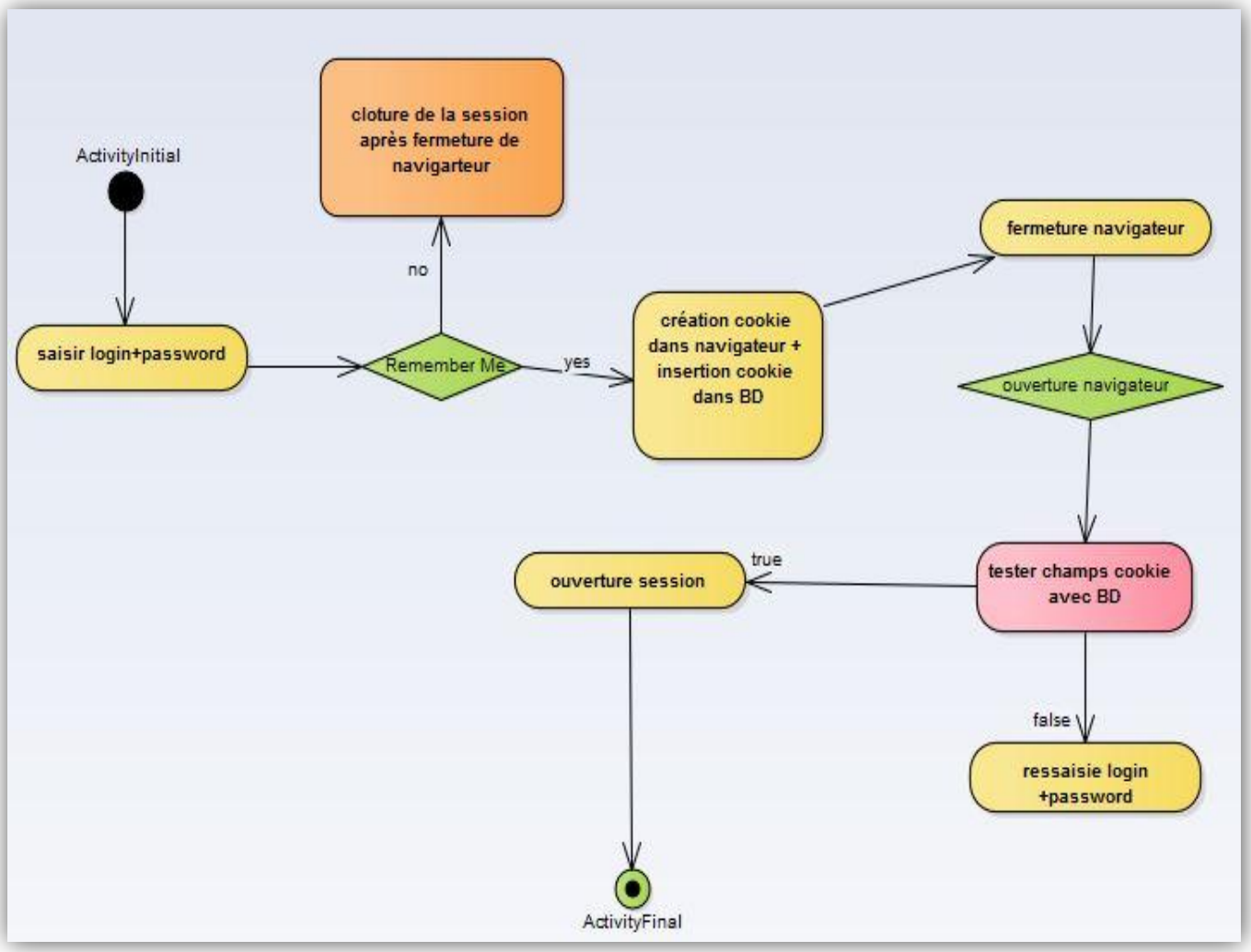

Figure 13:diagramme de garder la session active

4.6 Diagramme de classes:

Un diagramme de classes représente la structure statique du système sous forme de classes et de relations entre classes.

L'intérêt du diagramme de classes est de modéliser les entités du système d'information. Ces informations sont regroupées dans des classes qu'on peut utiliser dans la programmation orienté objet.

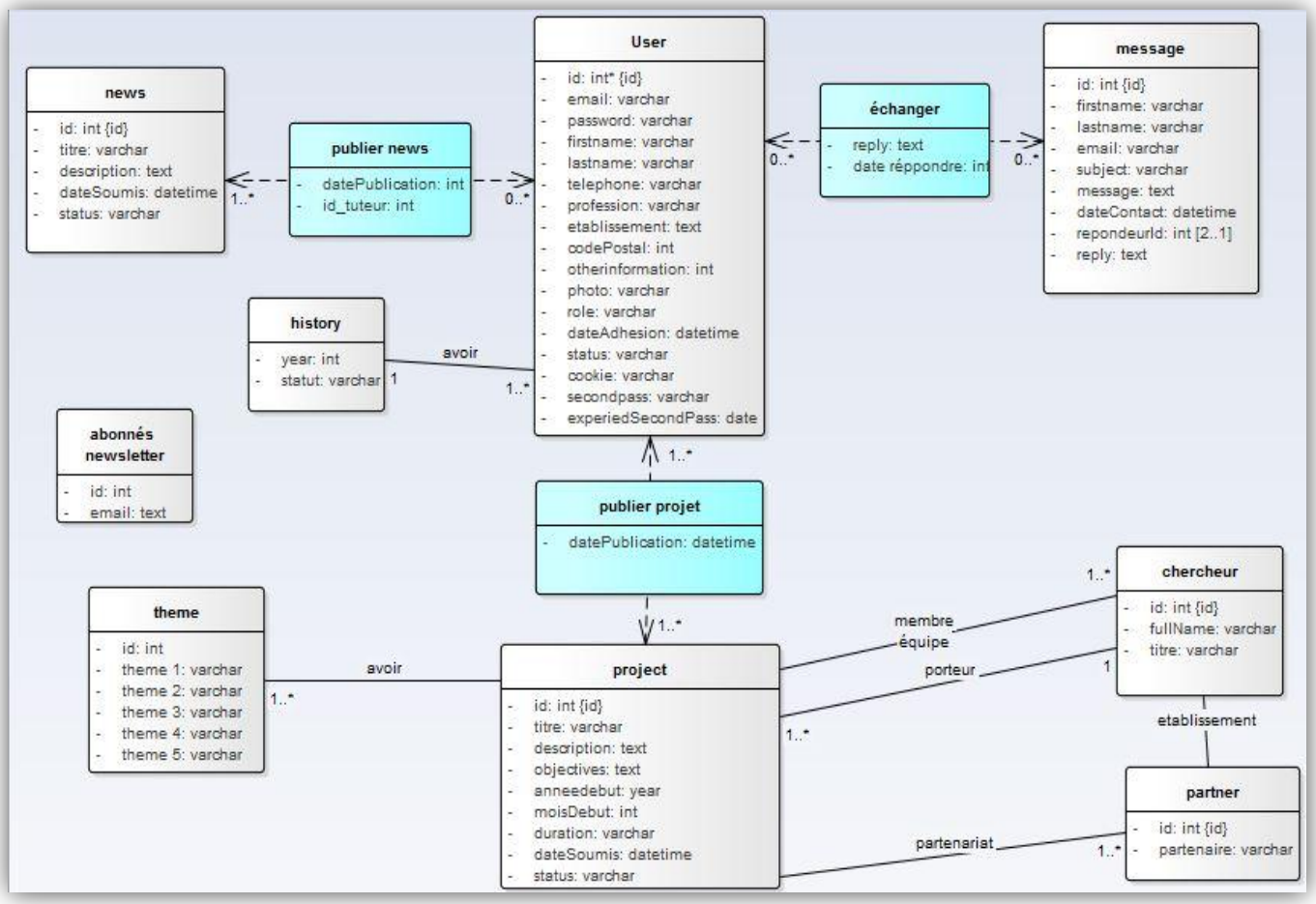

Figure 14:diagramme de classes

Chapitre 3:

Réalisation de l'application

1.Outils de développement

1.1 Les technologies de développement

- Html5

Figure 15: logo HTML5

HTML est un langage informatique de description conçu pour permettre la création des sites Web. Il est constamment révisé et évolué pour satisfaire les exigences de l'audience Internet croissante sous la direction du W3C, l'organisation chargée de concevoir et de maintenir la langue. Il est souvent utilisé conjointement avec le langage de programmation JavaScript et des feuilles de style en cascade (CSS).

La définition de HTML est HyperText Markup Language. HyperText est la méthode par laquelle vous vous déplacez sur le Web - en cliquant sur un texte spécial appelé hyperliens qui vous amène à la page suivante. Markup (balisage) est ce que les balises HTML font pour le texte à leur intérieur. Ils le marquent comme un certain type de texte (texte en italique, par exemple).

- CSS3

Figure 16: logo CSS3

Les feuilles de styles (en anglais "Cascading Style Sheets", abrégé CSS) sont un langage qui permet de gérer la présentation d'une page Web. Le langage CSS est une recommandation du World Wide Web Consortium (W3C), au même titre que HTML ou XML.

Les styles permettent de définir des règles appliquées à un ou plusieurs documents HTML. Ces règles portent sur le positionnement des éléments, l'alignement, les polices de caractères, les couleurs, les marges et espacements, les bordures, les images de fond, etc. Le but de CSS est séparer la structure d'un document HTML et sa présentation.

- PHP

Figure 17: logo PHP

PHP est un langage de programmation informatique essentiellement utilisé pour produire à la volée des pages web dynamiques. Dans sa version 5 lancée en juillet 2004, PHP s'est imposé comme le langage de référence sur le web en raison de sa simplicité, de sa gratuité et de son origine de logiciel libre.

- **JavaScript**

Figure 18:logo javaScript

JavaScript (souvent raccourci à JS) est un langage léger, interprété, orienté objet, fonctionne sur le côté client du Web, qui peut être utilisé

pour concevoir / programmer la manière dont les pages Web se comportent lors de l'événement, mais il est également utilisé dans de nombreux environnements sans navigateurs. Il s'agit d'un langage de script multiparadigme basé sur un prototype qui est dynamique et qui supporte des styles de programmation orientés objet, impératifs et fonctionnels.

1.2 Outils/Logiciels utilisé

- **Xampp**

Figure 19:logo XAMPP

XAMPP est un ensemble de logiciels permettant de mettre en place facilement un serveur Web local, un serveur FTP et un serveur de messagerie électronique. Il s'agit d'une distribution de logiciels libres offrant une bonne souplesse d'utilisation, réputée pour son installation simple et rapide. Ainsi, il est à la portée d'un grand nombre de personnes puisqu'il ne requiert pas de connaissances particulières et fonctionne, de plus, sur les systèmes d'exploitation les plus répandus.

- **MySQL**

Figure 20:logo MySQL

MySQL est un système de gestion de base de données relationnelle open source. Il est basé sur le langage de requête de structure (SQL), qui est utilisé pour ajouter, supprimer et modifier des informations dans la base de données. Les commandes SQL standard telles qu'ADD, DROP, INSERT et UPDATE peuvent être utilisées avec MySQL.il peut être utilisé pour une variété d'applications, mais est le plus souvent trouvé sur les serveurs Web. Un site Web qui utilise MySQL peut inclure des pages Web qui accèdent aux informations d'une base de données. Ces pages sont souvent appelées «dynamiques», ce qui signifie que le contenu de chaque page est généré à partir d'une base de données lorsque la page est chargée. Les sites Web qui utilisent des pages Web dynamiques sont souvent appelés sites Web basés sur la base de données.

- **phpMyAdmin**

Figure 21:logo phpMyAdmin

phpMyAdmin (PMA) est une application Web de gestion pour les systèmes de gestion de base de donnéesMySQL réalisée principalement en PHP et

distribuée sous licence GNU GPL.Il s'agit de l'une des plus célèbres interfaces pour gérer une base de données MySQL sur un serveur PHP. De nombreux hébergeurs, gratuits comme payants, le proposent ce qui évite à l'utilisateur d'avoir à l'installer.Cette interface pratique permet d'exécuter, très facilement et sans grandes connaissances en bases de données, des requêtes comme les créations de table de données, insertions, mises à jour, suppressions et modifications de structure de la base de données, ainsi que l'attribution et la révocation de droits et l'import/export. Ce système permet de sauvegarder commodément une base de données sous forme de fichier .sql et d'y transférer ses données, même sans connaître SQL.Les requêtes SQL restent possibles, ce qui permet de les tester interactivement lors de la création d'un site pour les utiliser ensuite en batch (c'est-à-dire en différé) une fois au point.

swiftMailer

Figure 22: logo swiftMailer

Swift Mailer s'intègre dans n'importe quelle application web écrite en PHP 5, offrant une approche orientée objet flexible et élégante pour envoyer des emails avec une multitude de fonctionnalités.

- Envoyer des emails en utilisant SMTP, sendmail, postfix ou une implémentation de transport personnalisée de votre choix
- Serveurs de support nécessitant un nom d'utilisateur et un mot de passe et / ou un cryptage
- Protège des attaques par injection d'en-tête sans supprimer le contenu des données de requête
- Envoyez des emails HTML / multipart compatibles MIME
- Utiliser des plugins pilotés par événements pour personnaliser la bibliothèque
- Gérez les grandes pièces jointes et les images en ligne / incorporées avec peu d'espace mémoire

2.Présentation de l'application

2.1 HOME

Figure 23:HOME

2.2 AMIIS Members

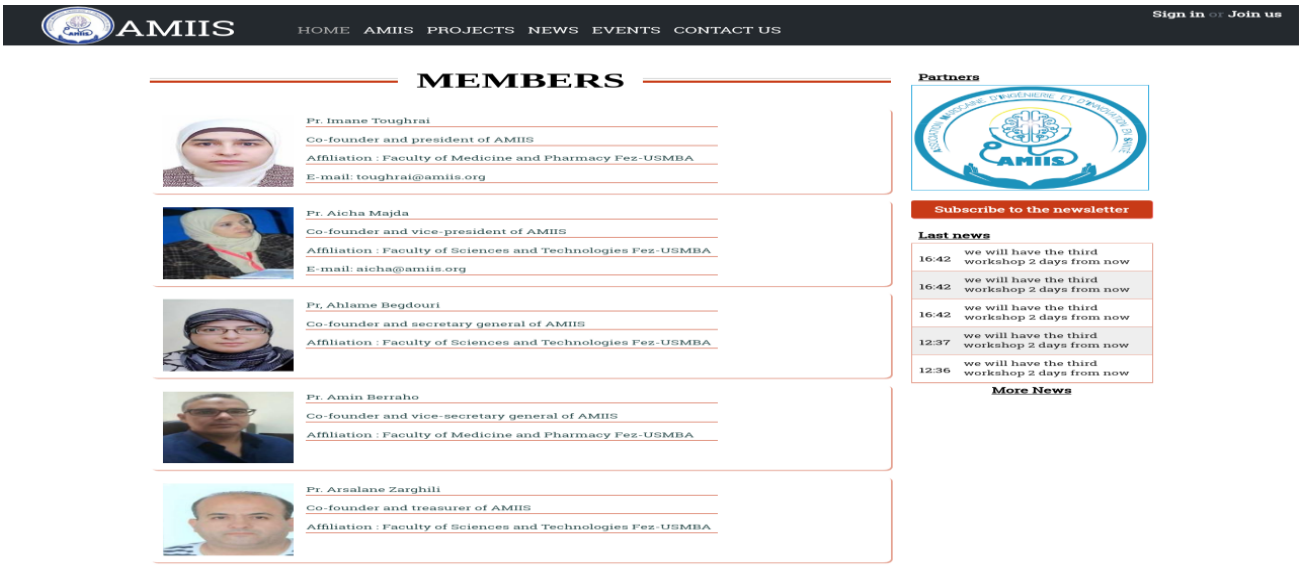

Figure 24:AMIIS Members

2.3 AMIIS Membership

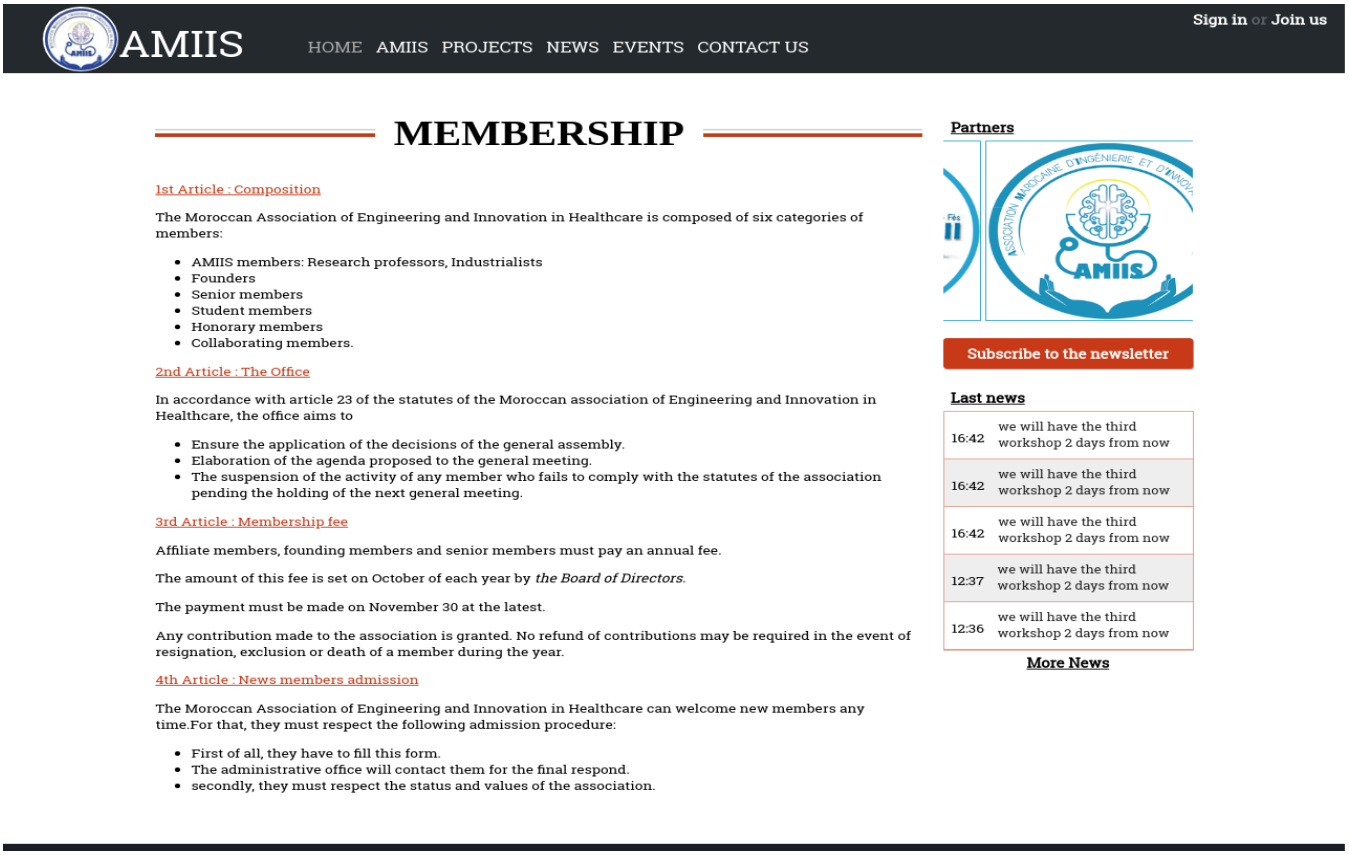

Figure 25:AMIIS Membership

2.4 Projects

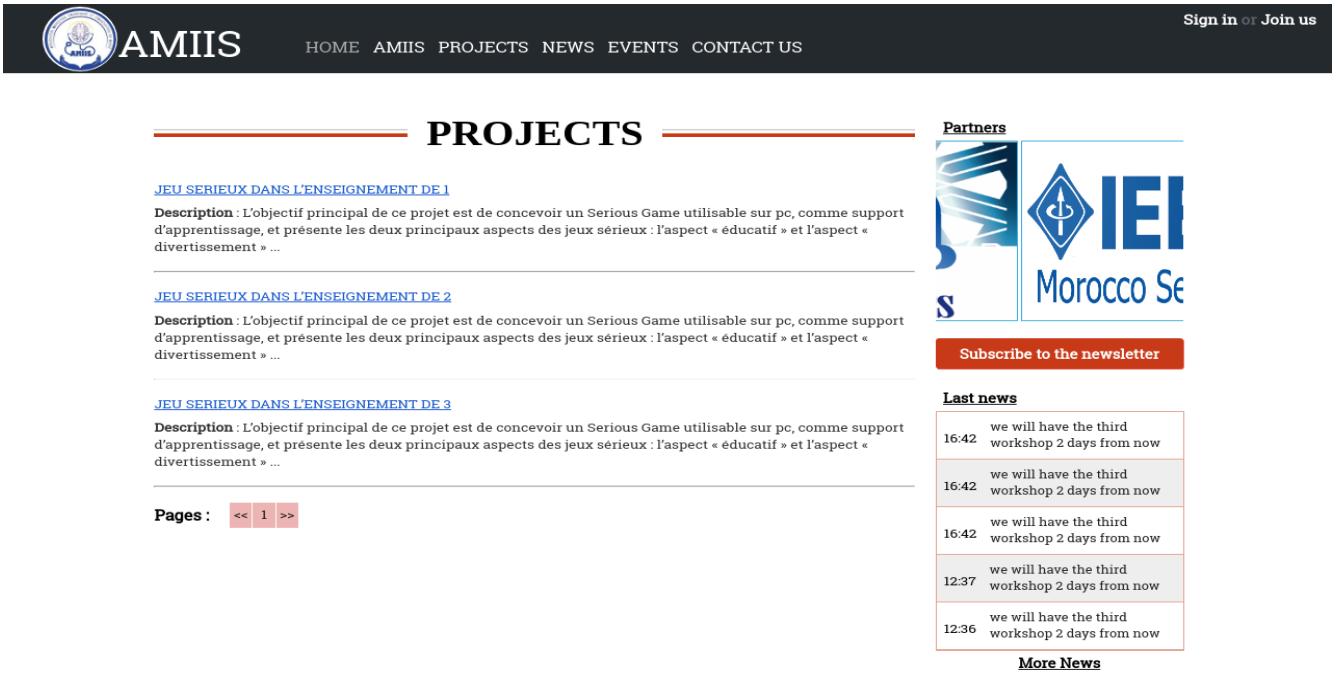

Figure 26: AMIIS Projects

2.5 News

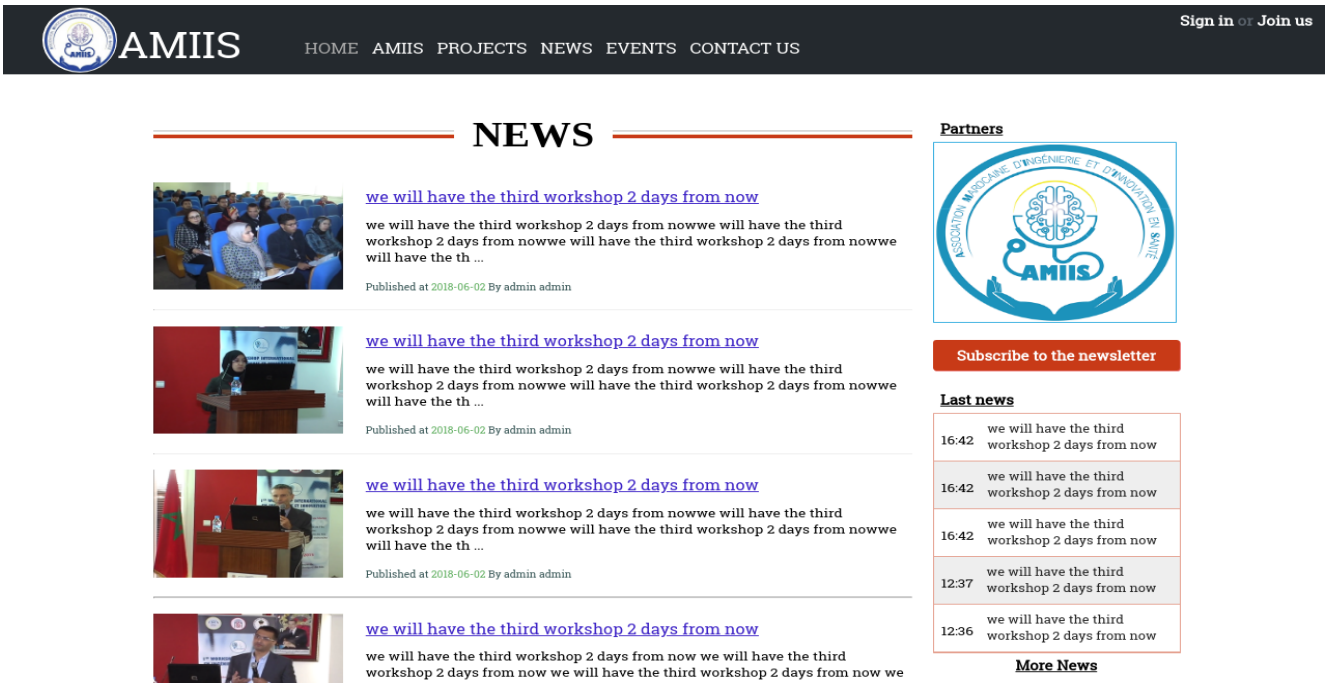

Figure 27: NEWS

2.6 Contact Us

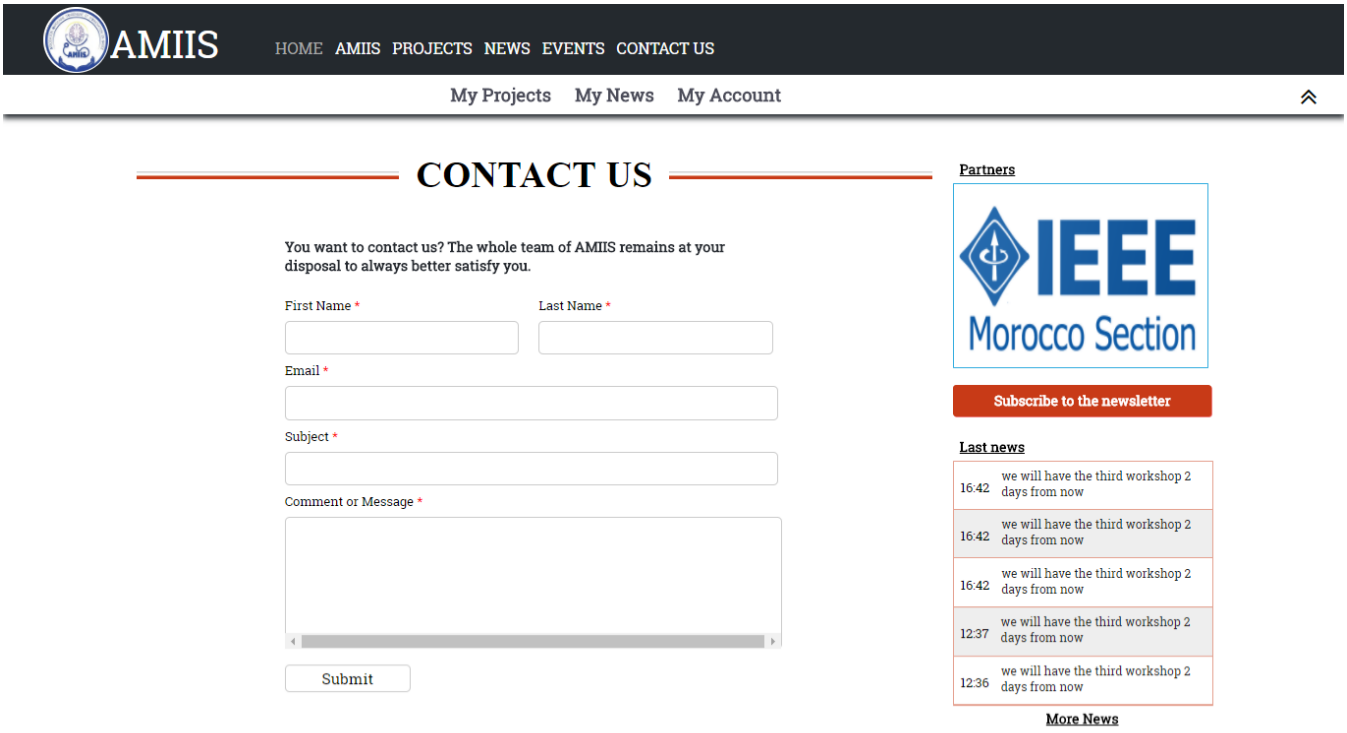

Figure 28: contact us

2.7 JOIN US

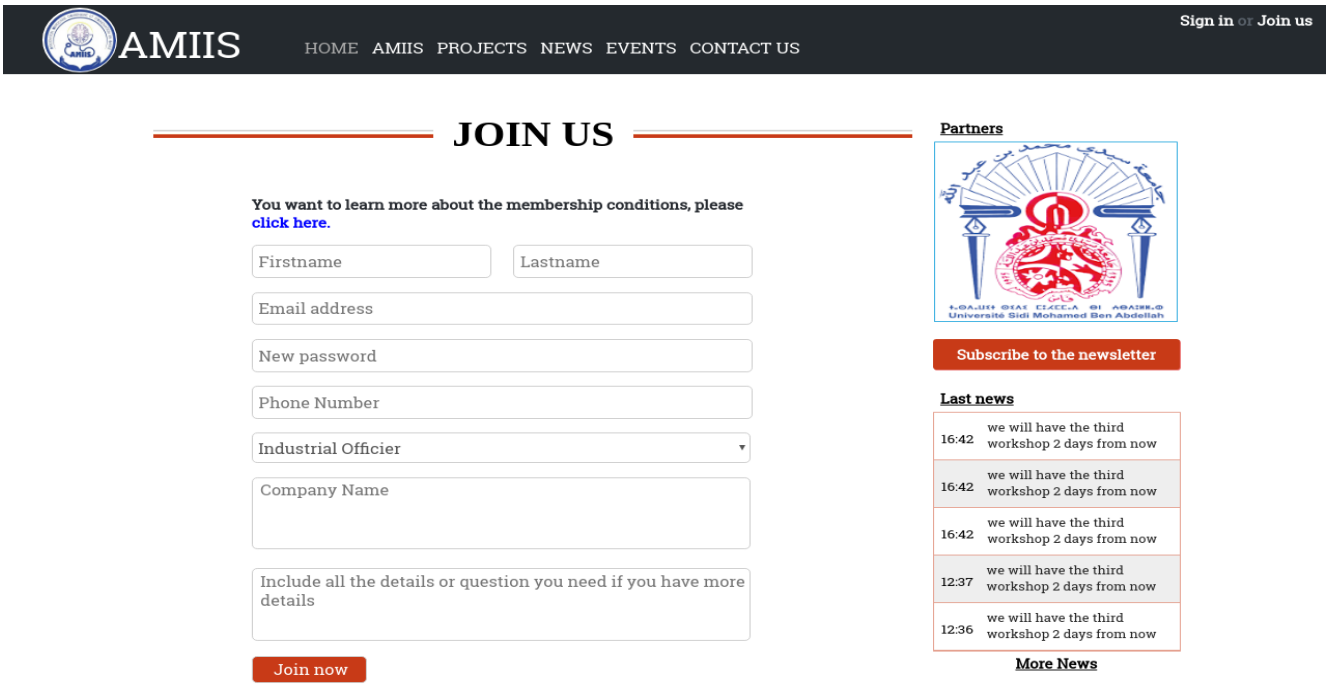

Figure 29: JOIN US

2.8 Profil d'un adhérent activé

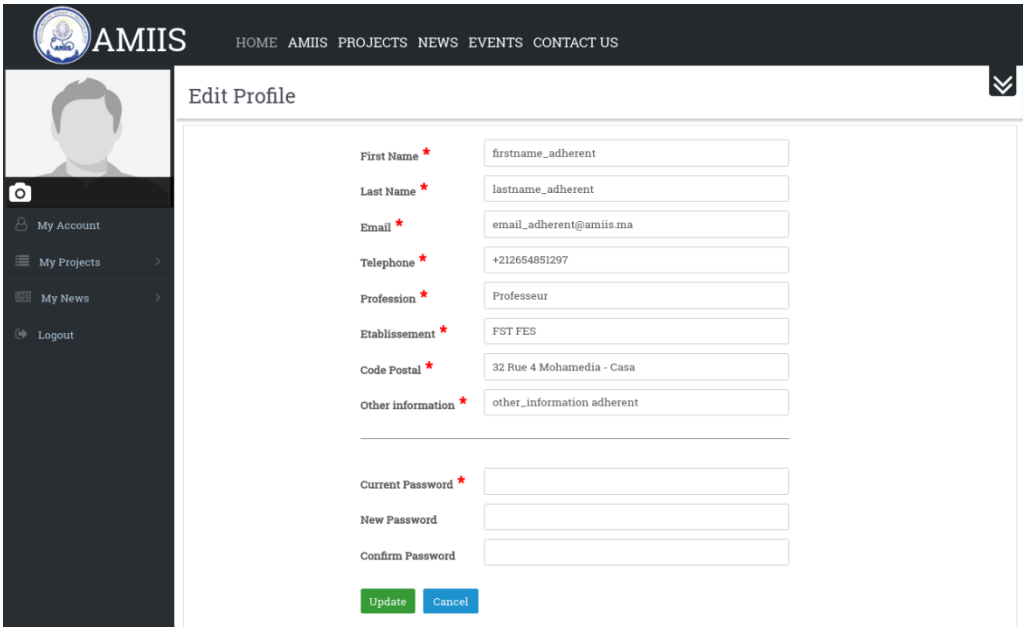

Figure 30:profil adhérent actif

2.9 Alerte pour adhérent pendu

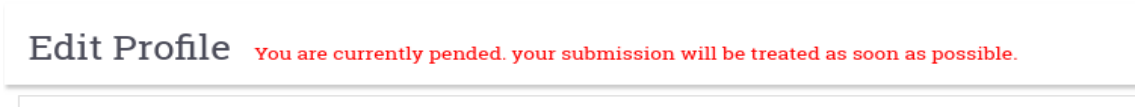

Figure 31:alerte adhérent pendu

2.10 Alerte pour adhérent suspendu

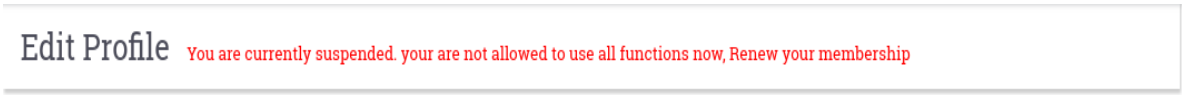

Figure 32: alerte adhérent suspendu

2.11 Dashboard admin

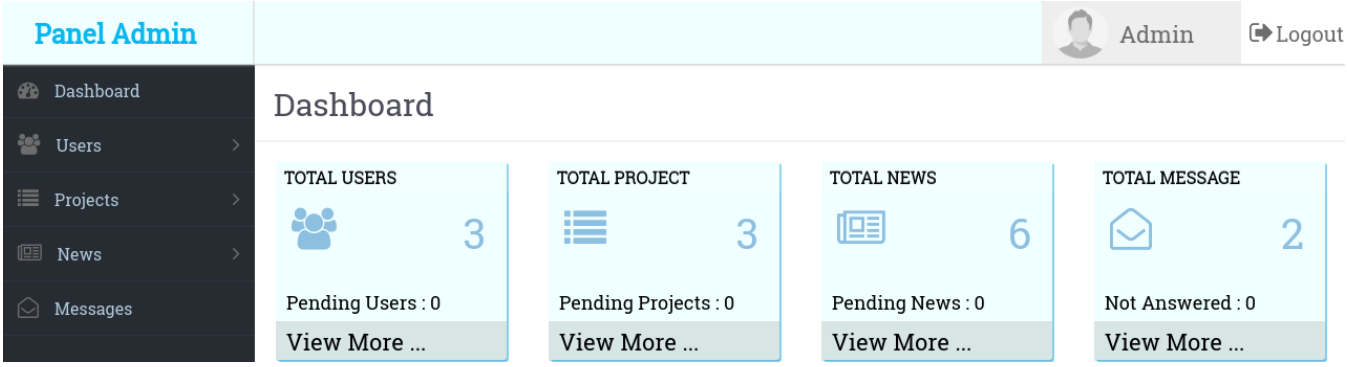

Figure 33: dachboard ADMIN

2.12 Add user

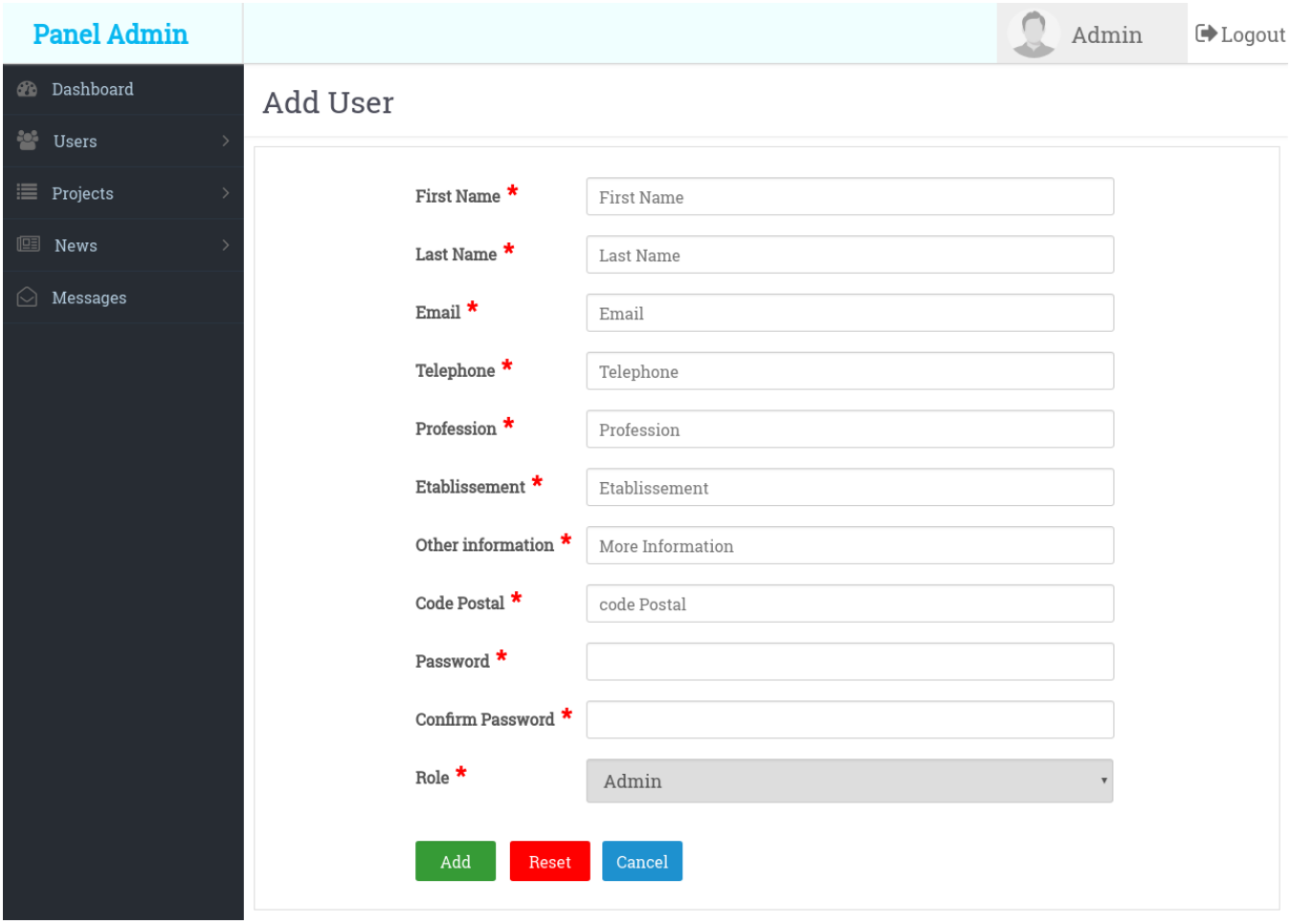

Figure 34: add user

2.13 Add news

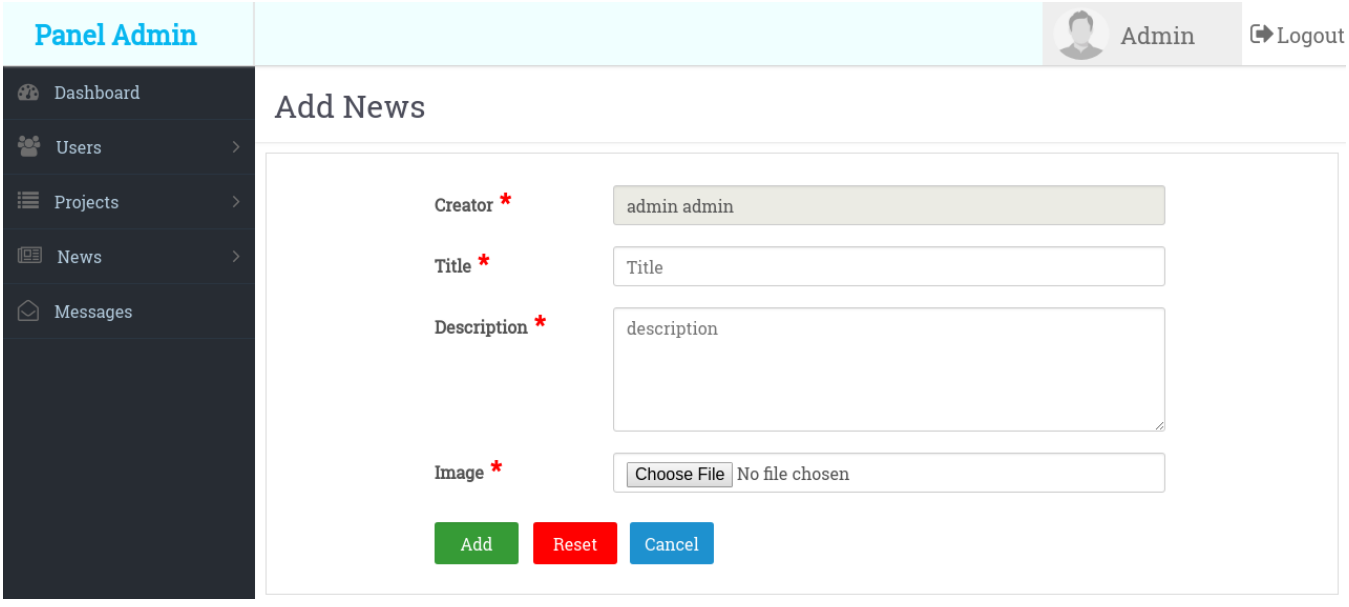

Figure 35:add news

2.14 Add project

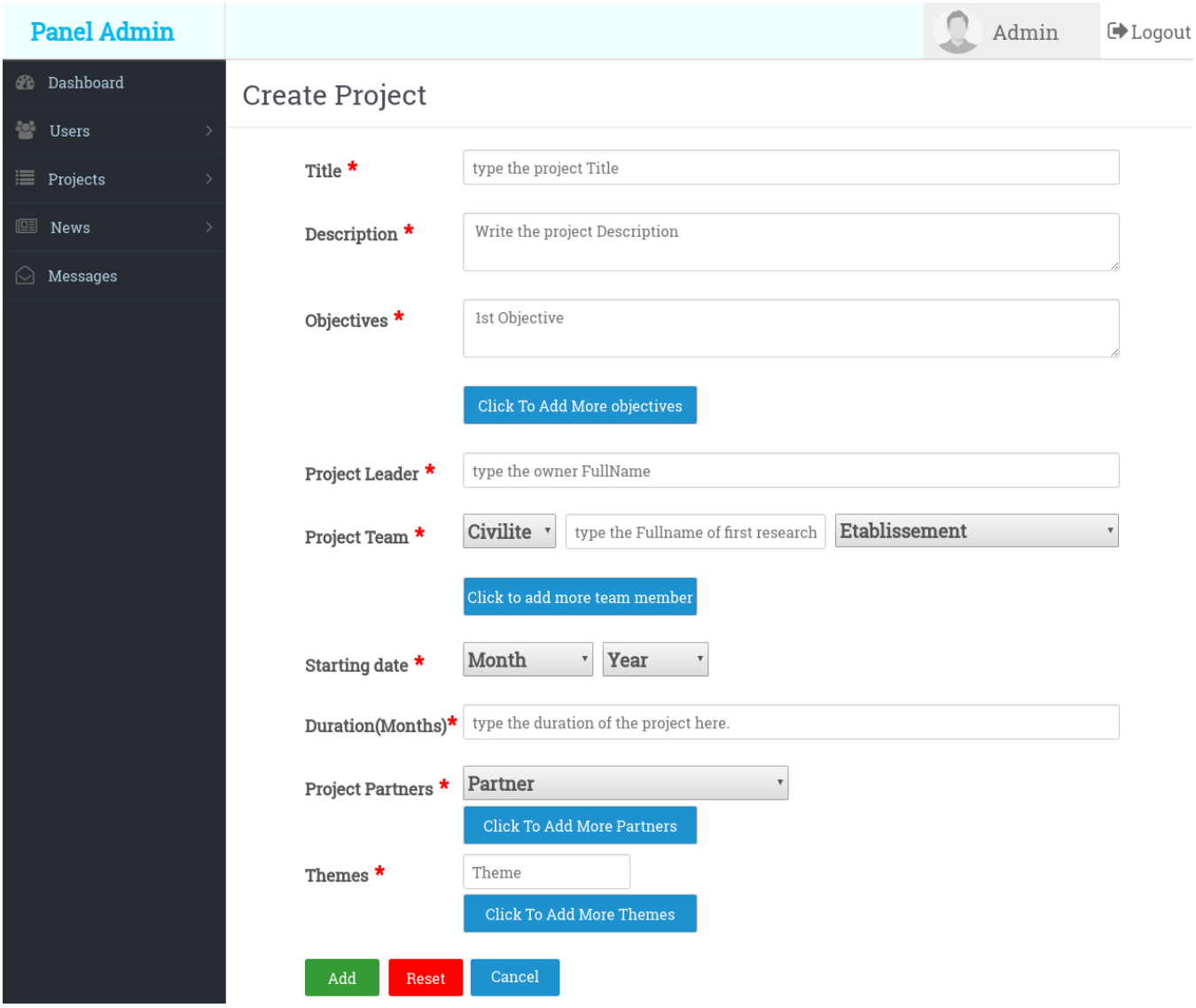

Figure 36: add project

2.15 Liste users

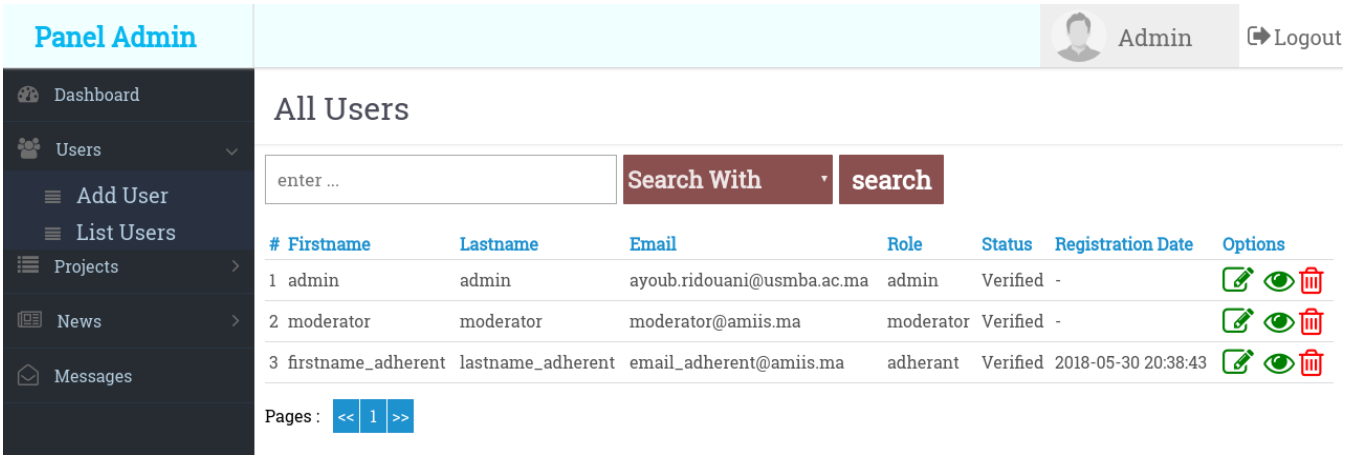

Figure 37: Liste users

2.16 Liste projects

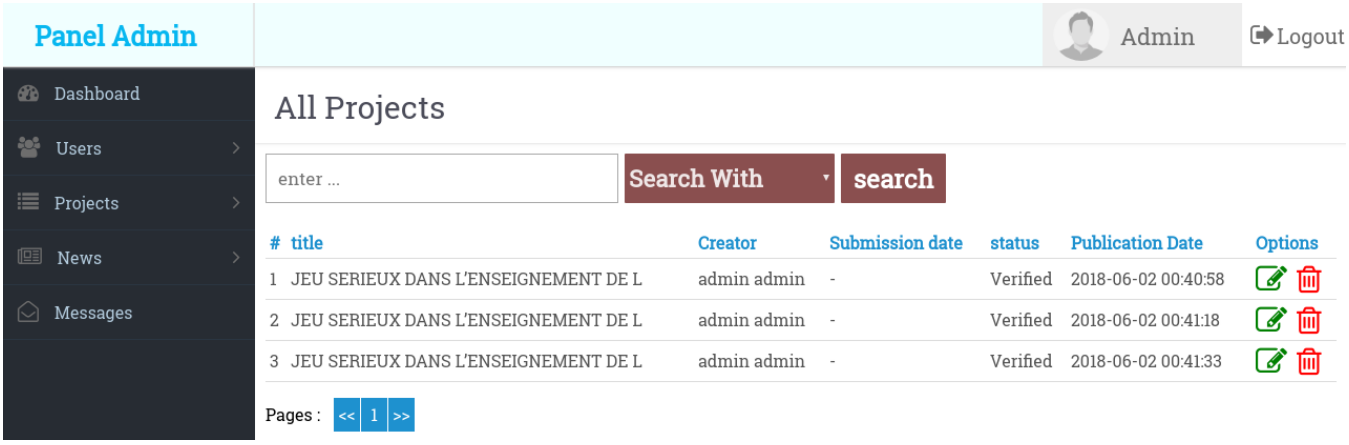

Figure 38: liste projects

2.17 Liste news

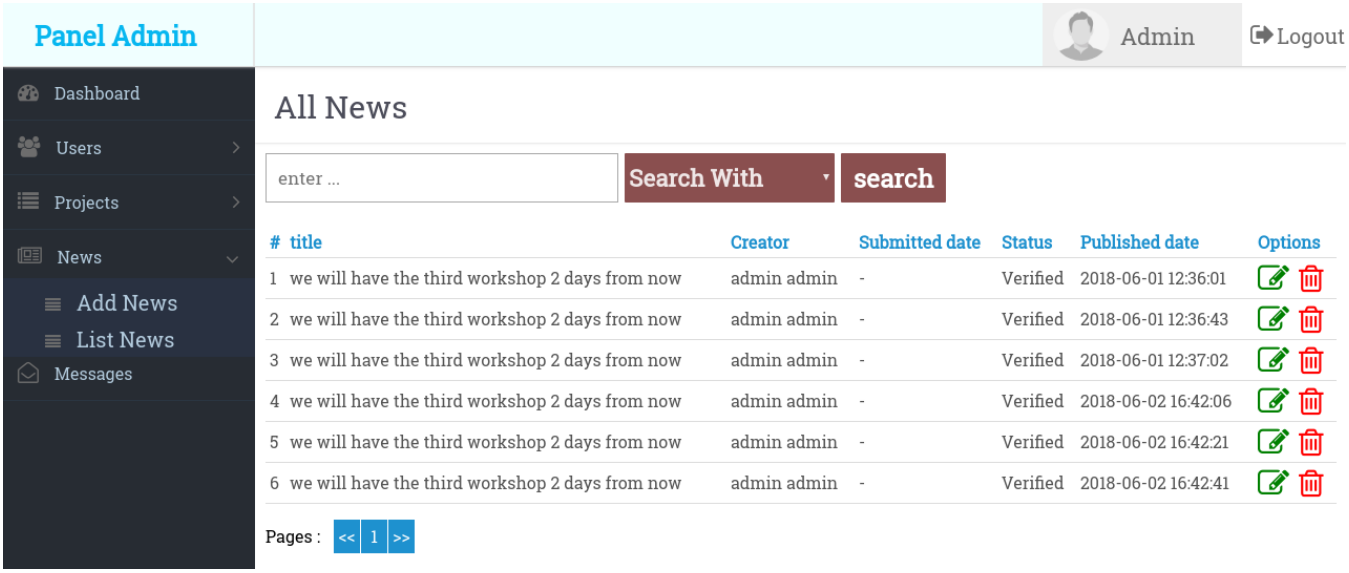

Figure 39:liste news

2.18 Liste messages :

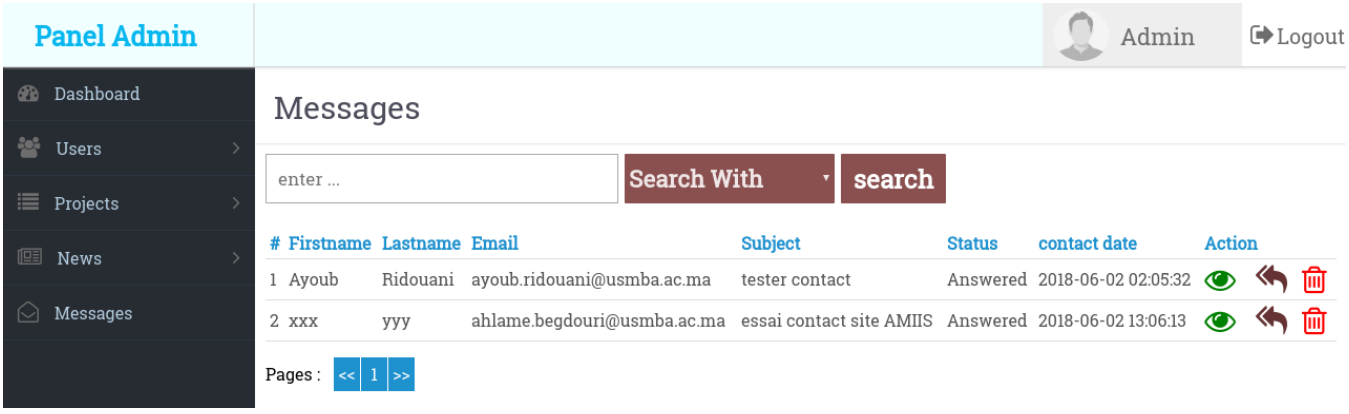

Figure 40:liste messages

2.19 Réponse du message

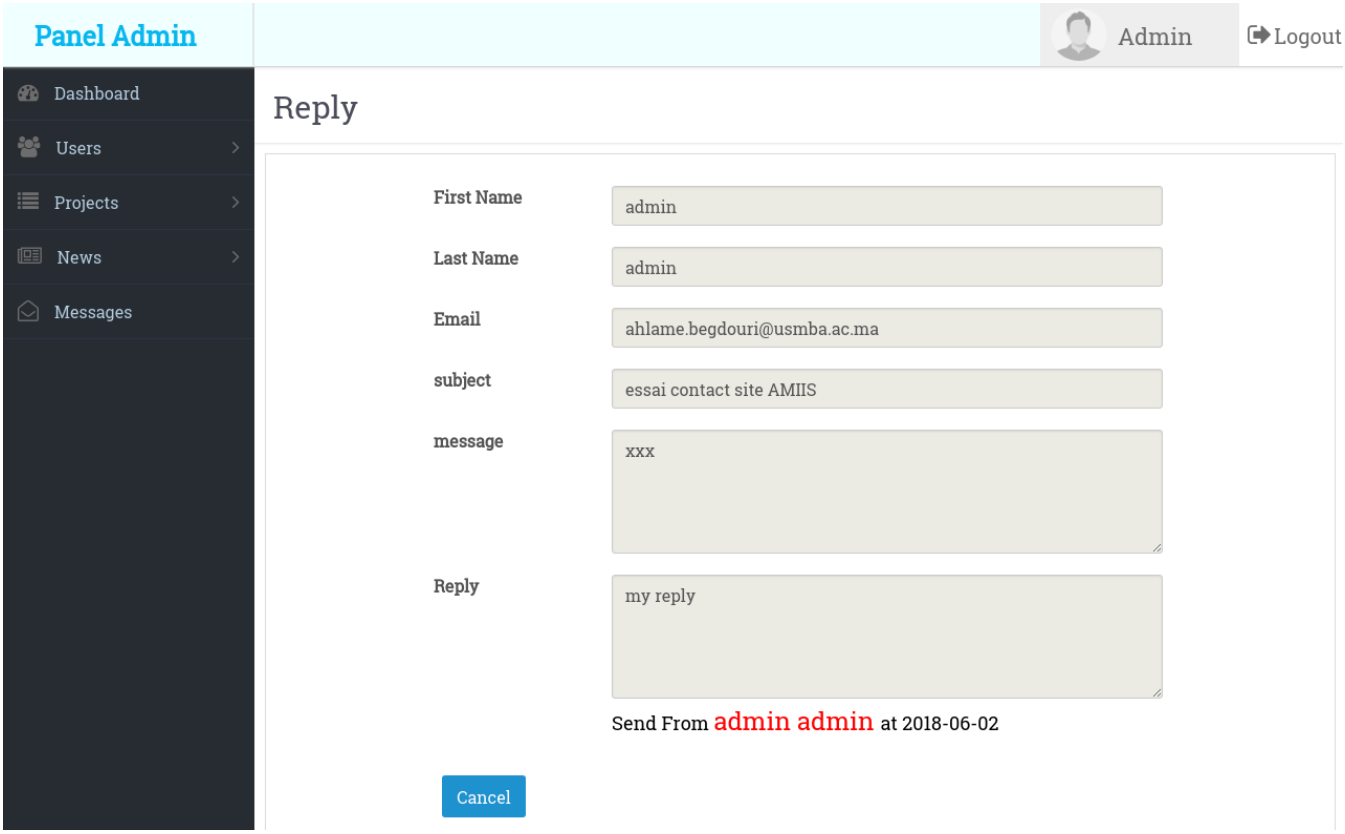

Figure 41: répondre du message

La page du login :

Figure 42: page du login

Reset password :

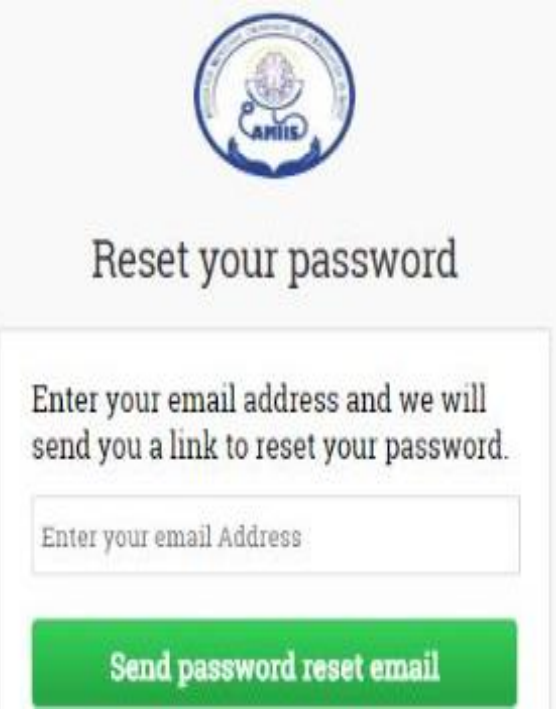

Figure 43: page reset password

Erreur de l'email inexistant

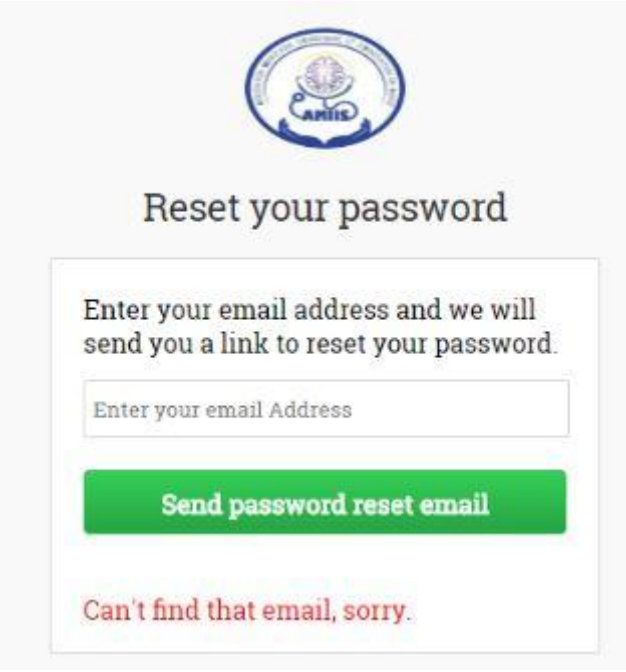

Figure 44: erreur email inexistant

l'envoie d'email

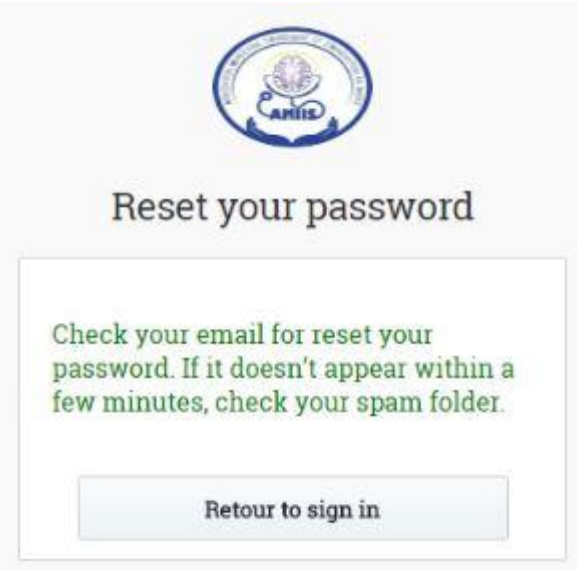

Figure 45: envoie d'email

l’email reçu :

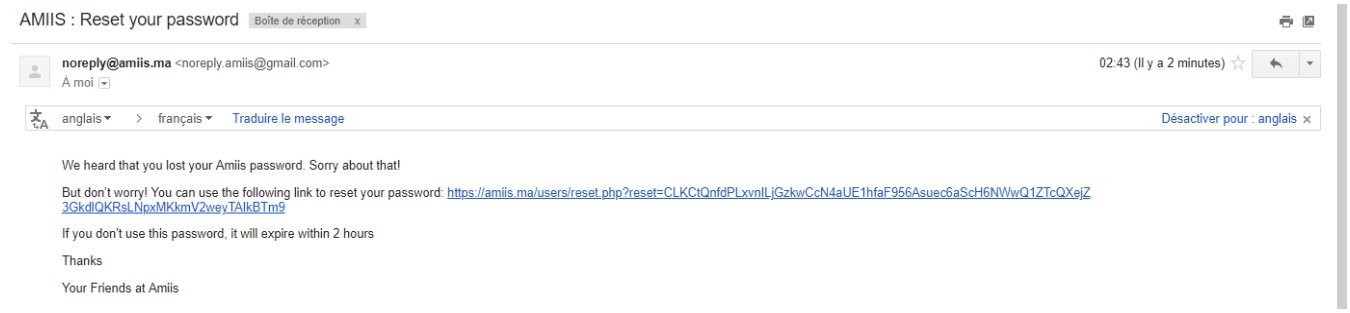

Figure 46:email reçu

email expiré:

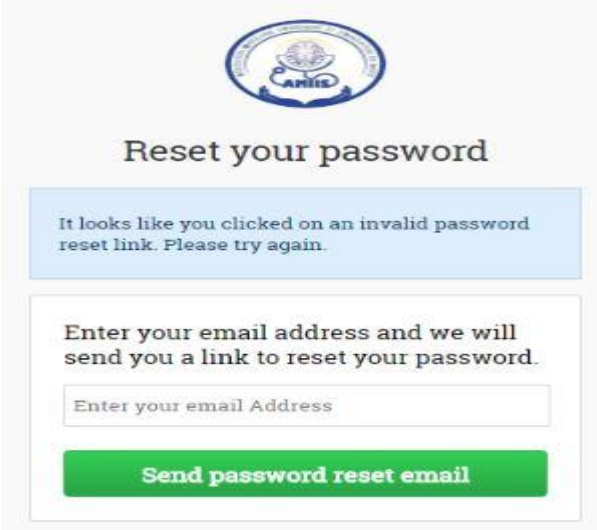

Figure 47:email expiré

Email mot de passe changé avec succès :

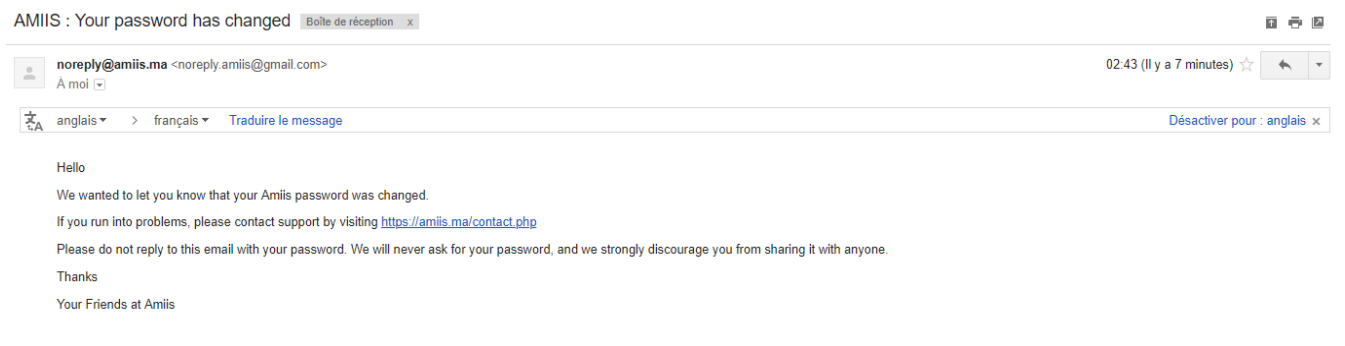

Figure 48: email du mot de passe changé avec succès

Sécurité du site

1. les failles XSS

1.1 Définition

Cross Site Scripting ou les abréviations XSS sont des vulnérabilités de sécurité répandues dans les programmes Web. Grâce à ces failles, un attaquant injecte un code de programme malveillant, généralement dans le langage JavaScript, où le navigateur exécute les commandes de code lorsque la page est chargée sur la deuxième personne (victime).

Le code est injecté par l'attaquant de plusieurs façons: la victime doit cliquer sur le lien XSS, ou attendre que la victime navigue sur une page du site contenant une vulnérabilité de ce type (magasin XSS).

1.2 L'exploitation des failles par les pirates informatiques

En exploitant les failles XSS, les pirates peuvent voler des soi-disant cookies, afin qu'ils puissent attraper votre identité dans un programme qui a une échappatoire.

Les pirates peuvent également transformer votre navigateur en une page contenant des logiciels malveillants, tels que les virus et autres.

Ils peuvent également convertir votre navigateur en une page très similaire à la page du programme que vous visitez (par exemple, le logiciel de la banque) et voler vos mots de passe.

Ces vulnérabilités sont également exploitées pour contourner la protection dans votre navigateur ou votre navigateur.

Ce ne sont que quelques-unes des attaques et pas toutes. Il n'y a pas de limite à l'exploitation de XSS, cela dépend de l'imagination et du professionnalisme de l'attaquant dans ce domaine.

2.Injection SQL

2.1 Définition

La faille SQLi, abréviation de SQL Injection, soit injection SQL en français, est un groupe de méthodes d'exploitation de faille de sécurité d'une application interagissant avec une base de données. Elle permet d'injecter dans la requête SQL en cours un morceau de requête non prévu par le système et pouvant en compromettre la sécurité.

2.2 Types des injections SQl

- la méthode *blind based* (associée à sa cousine la *time based*), qui permet de détourner la requête SQL en cours sur le système et d'injecter des morceaux qui vont retourner caractère par caractère ce que l'attaquant cherche à extraire de la base de données. La méthode *blind based*, ainsi que la *time based*, se basent sur la réponse du serveur : si la requête d'origine renvoie bien le même résultat qu'à l'origine (et indique donc que le caractère est valide) ou ne renvoie pas le même résultat (et indique donc que le caractère testé n'est pas le bon). La time based a pour seule différence qu'elle se base sur le temps de réponse du serveur plutôt que sur la réponse en elle-même.
- la méthode *error based*, qui permet de détourner la requête SQL en cours sur le système et d'injecter des morceaux qui vont retourner champ par champ ce que l'on cherche à extraire de la base de données. Cette méthode profite d'une faiblesse des systèmes de base de données permettant de détourner un message d'erreur généré par le système de base de données et préalablement volontairement provoquée par l'injection SQL pour lui faire retourner une valeur précise récupérée en base de données .

2.3 Exemple d'exploitation des injection SQL par les pirates

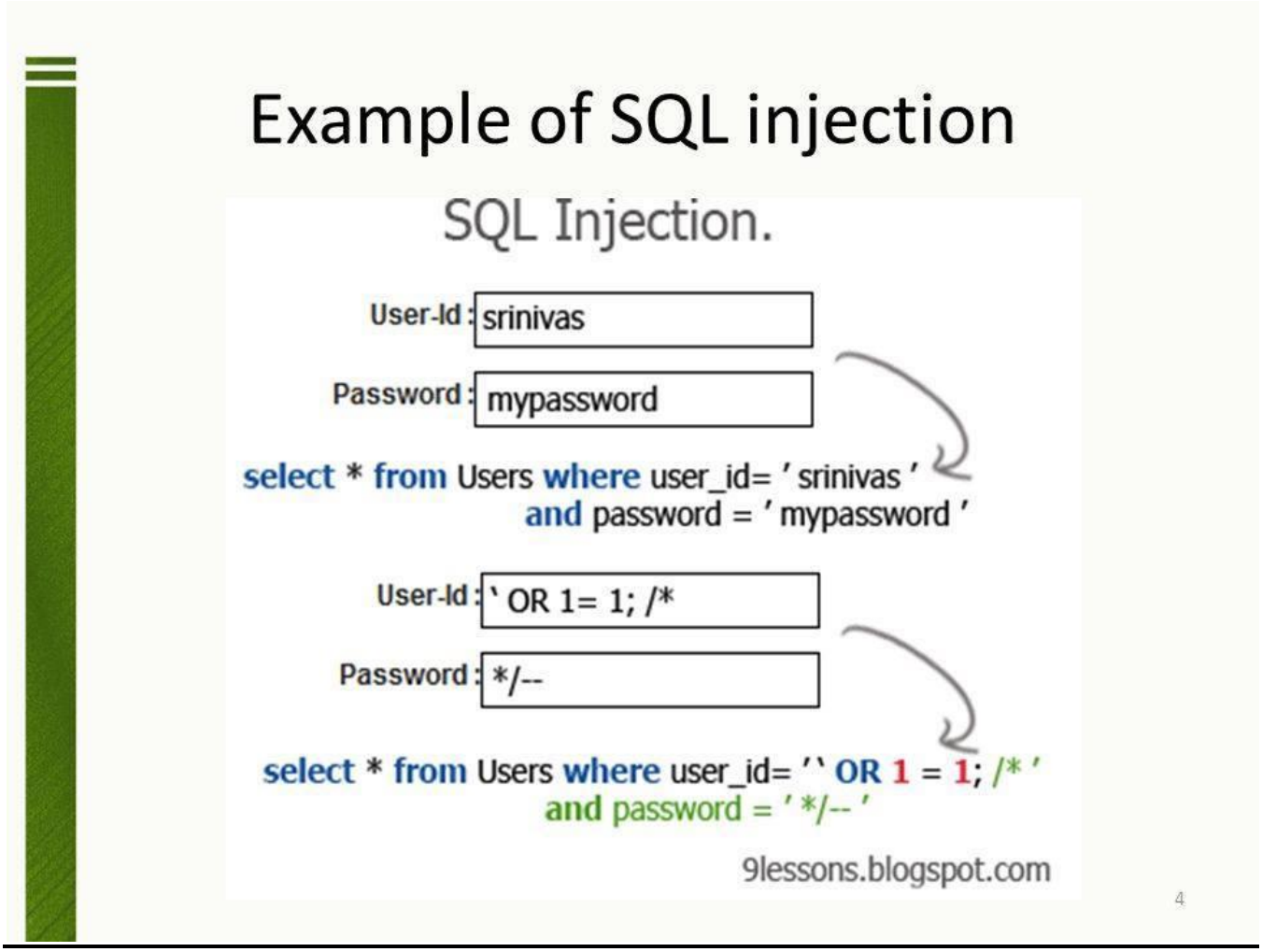

Figure 49:injection SQL exemple

2.4 Filtration, vérification et nettoyage des inputs

Il s'agit d'une fonction globale à deux paramètres, la donnée et son type, qui sert à filtration, vérification et nettoyage des champs insérer par l'utilisateur.

C'est une fonction globale, paramétrable et développable pour sécuriser notre site afin d'éviter les failles ou vulnérabilités que cause les failles XSS et l'injection SQL

La figure suivante présente le bout de code de cette fonction qui traite trois types de données email, les string et les entiers:

```php
<?php
function check_data($data,$type){
    $error=0;
    if($type=="email"){
        if(!is_string($data)) ++$error;
        $data = trim($data);
        $data = strip_tags($data);
        $data = htmlspecialchars($data,ENT_QUOTES);
        $data = filter_var($data, FILTER_SANITIZE_EMAIL);
        if($data != filter_var($data, FILTER_VALIDATE_REGEXP,array("options"=>array("regexp"=>"/^[a-z0-9._%+-]+@[a-z0-9.-]+\.[a-z]{2,4}$/")))) ++$error;
        if(!filter_var($data, FILTER_VALIDATE_EMAIL)) ++$error;
    }
    elseif($type=="string"){
        if(!is_string($data)) ++$error;
        $data = trim($data);
        $data = strip_tags($data);
        $data = htmlspecialchars($data,ENT_QUOTES);
        //if($data != filter_var($data, FILTER_VALIDATE_REGEXP,array("options"=>array("regexp"=>"/[a-zA-Z0-9_-\.,\(\)]+/")))) ++$error;
        $data = filter_var($data, FILTER_SANITIZE_STRING);
    }
    elseif($type=="int"){
        if(!is_numeric($data)) ++$error;
        $data = trim($data);
        $data = strip_tags($data);
        $data = htmlspecialchars($data,ENT_QUOTES);
        $data = filter_var($data, FILTER_SANITIZE_NUMBER_INT);
        if($data != filter_var($data, FILTER_VALIDATE_REGEXP,array("options"=>array("regexp"=>"/^[0-9]+$/")))) ++$error;
        if(!filter_var($data, FILTER_VALIDATE_INT)) ++$error;
    }
    else{
        // OK :)
    }
    return $error;
}
?>
```

Figure 50: le bout de code de vérification des champs

Le premier test de '*if*' concerne le champ « email », en premier lieu, lorsque l'email est insérer, la fonction vérifie si l'email est un string, s'il n'est pas le cas une alerte sera afficher pour déclarer cette erreur et effectue les tests suivant sur cette chaine de caractères :

- Trim() : pour enlever les espaces du début et de la fin du string entré.
- strip_tags () : tente de retourner la chaîne str après avoir supprimé tous les octets nuls, toutes les balises PHP et HTML du code, et elle utilise le même moteur de recherche que fgetss(), en cas d'erreur elle incrémente la variable $error.
- Htmlspecialchars() : Convertit les caractères spéciaux en entités HTML. Certains caractères ont des significations spéciales en HTML, et doivent être remplacés par des entités HTML pour conserver leurs significations. Cette fonction retourne une chaîne de caractères avec ces modifications.
- 1er filter_var() : nettoyage des caractère pour email.
- 2ème filter_var() : vérifie si la donnée correspond exactement à la forme de l'expression régulière citée.
- 3ème filter_var : vérifie finalement si la données est un email.

La figure suivante présente l'appellation de la fonction :

```
if(check_data($_POST['firstname'],"string")==0
        && check_data($_POST['lastname'],"string")==0
        && check_data($_POST['email'],"email")==0
        && check_data($_POST['telephone'],"string")==0
        && check_data($_POST['profession'],"string")==0
        && check_data($_POST['etablissement'],"string")==0
        && check_data($_POST['codePostal'],"string")==0
        && check_data($_POST['password'],"string")==0
        && check_data($_POST['autreInformation'],"string")==0
        && check_data($_POST['nv_password'],"string")==0){
```

Figure 51: appélation de la fonction

Pas uniquement les $_POST qui sont prise et vérifiés par cette fonction mais aussi les $_GET, les valeurs récupérés par ces deux méthodes ne sont pas stockés dans la base de données que si tous les champs sont insérés correctement, et si l'un de ces champs est erroné aucune interaction avec la base de données ne sera faite, et le système renvoie des alertes qui décrivent les erreurs commises.

- ***Vérification des fichiers téléchargés (file upload):***

Les fichiers téléchargés représentent un risque important pour les applications. La première étape de nombreuses attaques consiste à obtenir du code pour attaquer le système. Ensuite, l'attaque doit seulement trouver un moyen d'exécuter le code. L'utilisation d'un téléchargement de fichier aide l'attaquant à accomplir la première étape.

Les conséquences du téléchargement illimité de fichiers peuvent varier, notamment une prise en charge complète du système, un système de fichiers ou une base de données surchargée, la transmission d'attaques à des systèmes dorsaux, des attaques côté client ou un simple remplacement. Cela dépend de ce que fait l'application avec le fichier téléchargé et surtout où il est stocké.

- ***exemple d'exploitation de la vulnérabilités : file upload (LFI ou RFI)***

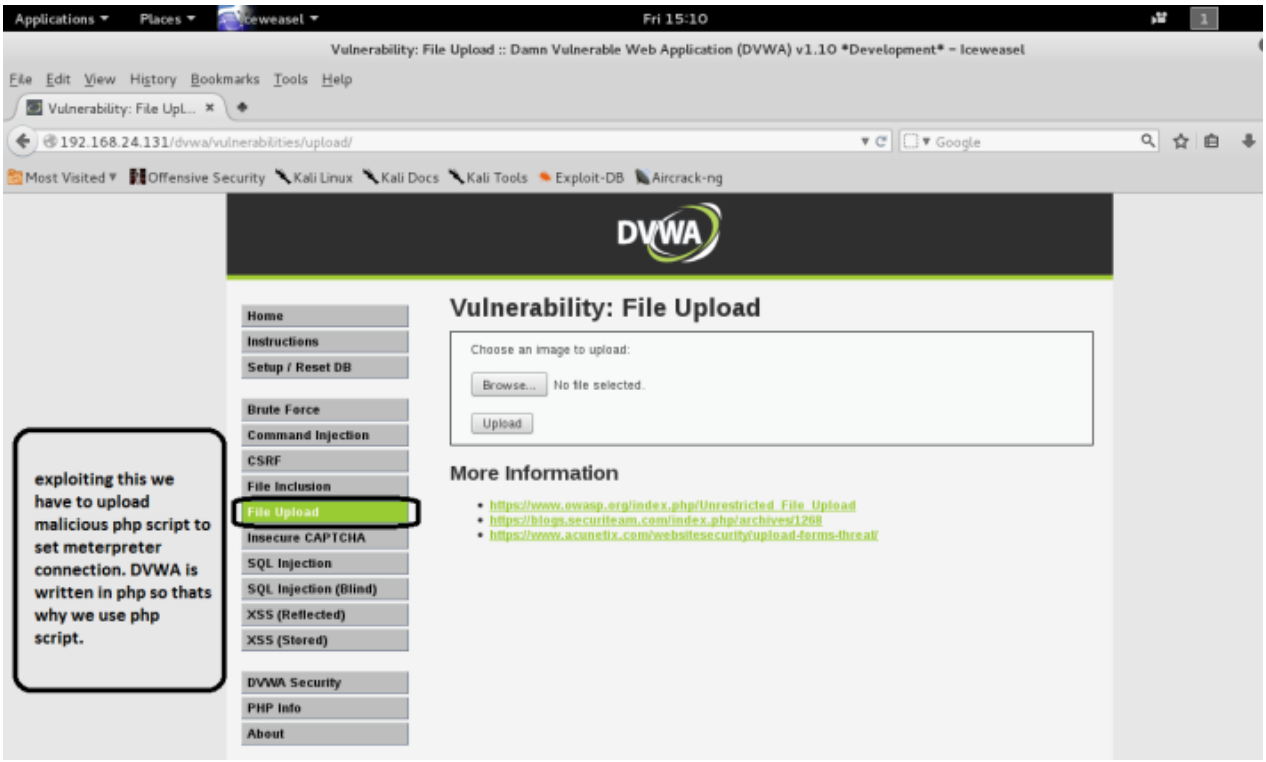

Figure 52: exemple d'exploitation des failles

La figure suivante présente le bout de code pour vérifier la session ou l'authentification entre le client et le serveur pour éviter les problèmes de ***broken*** authentification ou l'authentification ***bypass***.

```php
<?php
ob_start();
session_start();
if(!isset($_SESSION["userEmail"])
    || !isset($_SESSION["userId"])
    || !isset($_SESSION["userRole"])
    || ($_SESSION["userRole"] != "admin" && $_SESSION["userRole"] != "moderator")){
     header("Location: ../users/login.php");
     exit();
}
?>
```

Figure 53: vérification de la session

La figure suivante présente le bout de code de la fonction qui vérifie si le fichier téléchargé est réellement une photo.

```php
if($_SERVER['REQUEST_METHOD']=="POST" && isset($_FILES["photo"])){
        $file = basename($_FILES["photo"]["name"]);
        $error = 1;
        if ($_FILES["photo"]["size"] > 3000000){
            echo "<script>alert('Sorry, your photo is too large.');</script>";
            $error = 0;
        }

        $imageFileType = strtolower(pathinfo($file,PATHINFO_EXTENSION));
        if($imageFileType != "jpg" && $imageFileType != "png" && $imageFileType != "jpeg"){
            echo "<script>alert('Sorry, only JPG, JPEG, PNG photo are allowed.');</script>";
            $error = 0;
        }

        $foo = "images/" . rand(100,241574654) . "." . $imageFileType;
        if($error == 1){
            if(move_uploaded_file($_FILES["photo"]["tmp_name"],$foo)){
                $stmt5=$con->prepare("update users set photo=:photo where id=:id");
                $stmt5->bindParam(':id',$_SESSION["userId"],PDO::PARAM_INT);
                $stmt5->bindParam(':photo',$foo,PDO::PARAM_STR);
                $stmt5->execute();
                header("location:" . $_SERVER['HTTP_REFERER']);
            }else{
                echo "<script>alert('Sorry, there was an error uploading your file.');</script>";
            }
        }else{
            echo "<script>alert('Sorry, there was an error uploading your file.');</script>";
        }
    }
```

Figure 54: le bout de code de la fonction de vérification de téléchargement

Conclusion

Notre mission durant ce stage consistait à étudier et à développer un site web de l'Association Marocaine d'Ingénierie et d'Innovation en Santé, dans le but de répondre aux besoins du ses membres et afin de trouver une solution de la problématique et de leur offrir un espace commun de partage entre membre, et une interface pour les internautes qui désire d'être membre de cette association.

Notre projet est présenté sous trois axes principaux. Dans un premier temps, nous avons présenté le lieu du stage AMIIS siégée dans la faculté de médecine de Fes. Nous avons donné une vision sur la problématique de ce projet, et proposé une solution informatisée, afin de déterminer un cahier de charge bien structuré. Dans la deuxième partie, nous avons présenté les différentes étapes de la conception de notre siteweb ainsi que les choix de réalisations et les outils utilisés. Finalement, nous avons soumis les interfaces graphiques réalisées.

Ce stage nous a permis, sur le plan technique de raffiner notre formation, puisque nous avons pu connaître d'autres outils informatiques. Et d'autre part sur le plan humain, de développer l'esprit du travail d'équipe.

webographie

- http://php.net/manual/en/
- https://www.owasp.org/index.php/Unrestricted_File_Upload
- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.owasp.org/index.php/SQL_Injection
-
- https://openclassrooms.com/courses/dynamisez-vos-sites-wavecjavascript (Cours du java Script).
- https://fr.wikipedia.org/wiki/Injection_SQL
- https://openclassrooms.com/courses/administrez-vos-bases-de-donnees-avec-mysql/triggers
- http://amiis.ma/
- https://www.w3schools.com/icons/fontawesome_icons_intro.asp
- https://swiftmailer.symfony.com/docs/introduction.html
- https://stackoverflow.com/questions/11516291/css-get-height-of-screen-resolution
- http://ww2.fmp-usmba.ac.ma/blog/amiis/