



DOSSIER DE SYNTHESE

Stage pour le diplôme de développeur
d'application à ELAN FORMATION

Arnaud FLORENCE

Période du 03/09/20018 au 26/10/2018



APPLICATION DE GESTION D'AUDIT GCA

CREATION/GESTION D'AUDIT

MODIFICATIONS CRM

L'OUTIL DE GESTION DE RELATION CLIENT

DOSSIER DE SYNTHESE

Arnaud FLORENCE

Table des matières

A PROPOS DE MOI	3
PRENEZ VOTRE ELAN !	3
PRESENTATION DE L'ENTREPRISE	3
Richard Bertrand, directeur fondateur	4
RG... QUOI ?	5
PROJET « GCA »	6
PARTIE 1 : TECHNOLOGIES UTILISEES	6
INSTALLATION	7
PARTIE 2 : PRESENTATION DU PROJET	8
VOUS AVEZ DIT MCD/MLD ? :	9
PARTIE 3 : DESIGN PATTERN	11
MVT (MODEL VIEWS TEMPLATES)	11
PARTIE 4 : MAIS ÇA DONNE QUOI ?	15
AXES D'AMÉLIORATION :	23
MODIFICATION CRM (quelques exemples) :	23
QU'EST-CE QU'UN CRM	23
QUELQUES EXEMPLES :	24
AJOUT D'UN LIEN ONEDRIVE :	24
FILTRE PERSONNALISE DJANGO :	25
ENVOI DE MAIL AUTOMATIQUE :	25
CONCLUSION :	26

A PROPOS DE MOI

Je m'appelle Arnaud, j'ai 32 ans et j'ai suivi une formation de Développeur web à Elan formation.

Mon parcours est plutôt éclectique. Je suis passé de la Boulangerie/Pâtisserie à commercial et par divers emplois. J'ai étudié le graphisme et mon intérêt pour l'informatique ainsi que les encouragements de mon entourage m'ont orienté vers la programmation. Une première expérience en alternance en BTS SIO option programmation en 2013 n'a pu se concrétiser suite à des difficultés à trouver une entreprise étant à ce moment âgé de plus de 26 ans. Grâce à une motivation accrue ainsi qu'à diverses expériences professionnelles, c'est finalement plus de 5 ans après que l'opportunité d'effectuer la formation de « Développeur Logiciel PHP » s'est présentée.

PRENEZ VOTRE ELAN !

ELAN Formation, c'est plus de 25 ans d'expérience dans les domaines de la Bureautique, la PAO, le Multimédia, d'Internet, des Techniques de secrétariat. C'est des formations sur mesure et totalement individualisées. Possibilité de monter un dossier en partenariat avec des OPCA (Organismes Paritaires Collecteurs Agréés) et optimiser ainsi les recherches de financement.



ELAN est un organisme de formation local. A ce titre, il dispose de locaux sur STRASBOURG, SELESTAT, HAGUENAU, SAVERNE, COLMAR, MULHOUSE, METZ et **NANCY**

PRESENTATION DE L'ENTREPRISE

Crée en 2007, dans la lignée du décret d'application de la loi informatique et libertés, Actecil, expert conformité en gestion des données personnelles, accompagne les organismes privés ou publics dans leur démarche de conformité liée aux législations encadrant l'usage des données à caractère personnel (loi informatique et libertés en France, loi 09-08 au Maroc, ...).

Actecil protège les organismes des contentieux, lourds et coûteux en accompagnant tous les projets de mise en conformité, au travers de missions de :

- **Conseil : état des lieux/diagnostic et audit,**
- **Accompagnement à la mise en conformité**
- **Cil externe/cil externe mutualise**
- **Formations**
- **Outils logiciels.**



Première société de conseil privée à avoir obtenu le **label Cnil gouvernance informatique et libertés** en décembre 2015, **Actecil détient également 9 labels Cnil** et accompagne dans leur démarche de mise en conformité, de nombreux organismes privés et publiques de tous secteurs : santé, bailleurs sociaux, mairies et collectivités, centres de gestion, transports, vidéo protection, centres d'appels, ntic, rh, banques, assurances,

Primée depuis 3 ans comme entreprise innovante, l'expertise, le dynamisme et la valeur ajoutée d'Actecil auprès de ses clients sont récompensés notamment par le label i-novia.



[Richard Bertrand, directeur fondateur](#)

Richard Bertrand est directeur fondateur d'Actecil groupe, et exerce notamment le métier de correspondant à la protection des données à caractère personnel (CIL) désigné auprès de la cnil pour des organismes publics et privés français et étrangers.

Référent de la protection des données personnelles, il est membre de l'AFCDP et est intervenu sur demande de la commission nationale de l'informatique et des libertés lors de la journée des cils organisée au Sénat au mois d'avril 2011.

(Dsi) pour de grands groupes et ayant exercé près de quinze ans en Allemagne, il a eu l'opportunité de s'intéresser et d'être confronté très tôt aux législations de la protection des données en vigueur au sein de l'Union Européenne. **Outre le respect à la tranquillité et à la vie privée auxquels tout un chacun doit pouvoir bénéficier, elle permet à chaque entreprise de :**

- Disposer des fondamentaux pour valoriser et pérenniser son patrimoine informationnel.
- Mettre en œuvre les moyens techniques et organisationnels pour sécuriser les informations,
- Ne travailler qu'avec des données à jour,
- Savoir qui dispose de quelle information et pour quelle finalité,

- Imposer aux sous-traitants des règles strictes pour éviter tout dérapage ne sont que quelques obligations issues des textes, qui bien que primordiales, sont souvent mises de cote par manque de temps ou d'intérêt.

Actecil est présent en Ile-de-France, Grand Ouest, Sud-Est, Sud-Ouest, Midi-Roussillon, Franche-Comté, Alsace, Hauts de France, Océan Indien, Caraïbes, Nouvelle-Calédonie, Maghreb.

RG... QUOI ?



Le règlement européen (RGPD ou GDPR) définit le régime de protection des données en Europe dans tous les secteurs d'activités, organismes privés ou publics :

- Les droits des personnes propriétaires des données,
- Obligation de designer un dpo, interne ou externe,
- Obligation de tenue du registre des traitements,
- Apporter la preuve du respect des exigences,
- Responsabilisation des sous-traitants,
- Amendes jusqu'à 20 millions d'euros ou 4% du CA mondial,
- Analyses d'impact obligatoires,
- Notification des failles de sécurité



Actecil accompagne ses clients vers la conformité à travers diverses solutions allant de la sensibilisation jusqu'à la mise en conformité en passant par des formations et des outils.

PROJET « GCA »

PARTIE 1 : TECHNOLOGIES UTILISEES

Langages utilisés :

- **Python** 2.7 et 3.7.1. C'est un langage de programmation orienté objet. L'entreprise utilise ce langage plus que le PHP car le python permet autant la défense que l'attaque ce qui est nécessaire pour une entreprise basée sur la sécurité de données informatique.
- **HTML** (HyperText Markup Language) : c'est le langage de balisage conçu pour représenter les pages web.
- **CSS** (Cascading Style Sheets) : Ce sont des feuilles de style en cascade, formant un langage informatique qui décrit la présentation des documents HTML et XML.

Outils supplémentaires :

- Framework ¹ **Django** 1.9 et 2.1.2. est un cadre de développement web open source en Python.
- Système d'exploitation **Linux**
- **Mercurial** est un logiciel de gestion de versions décentralisé disponible sur la plupart des systèmes Unix et Windows. Utilisation de Tortoisehg pour l'interface graphique.
- **Git** est un logiciel de gestion de versions décentralisé. C'est un logiciel libre créé par Linus Torvald, auteur du noyau Linux.
- Utilisation de **Slack** pour communiquer au sein de l'entreprise
- Utilisation de **Redmine** pour l'attribution des tâches
- **MockFlow** pour faire les maquettes de l'application
- **Xmind** pour structurer l'application
- Base de données en **SQL**² géré avec **MySQL Workbench** et **SQLite browser**

¹ **Framework** se distingue d'une simple bibliothèque logicielle

² **SQL**: Structured Query Language, traduit langage de requêtes structure est un langage de définition, de manipulation et de contrôle de données pour les bases de données relationnelles.

INSTALLATION ! :

Pour commencer, il a fallu installer une partition avec le système d'exploitation linux pour travailler. Une fois achevée, l'installation de Python a été nécessaire pour pouvoir utiliser le langage et par la suite Django qui est le Framework.

L'environnement de travail étant prêt, c'est au tour de Slack, une plateforme de collaboration de gestion de projet pour pouvoir communiquer entre nous dans l'entreprise. Pour finir Redmine qui est une application web libre de gestion de projets et créer le dossier de stockage du projet en privé sur bitbucket (qui est un service web d'hébergement et de gestion de développement logiciel utilisant les logiciels de gestion de versions Git et Mercurial).

Voilà je suis prêt à travailler !



PARTIE 2 : PRESENTATION DU PROJET

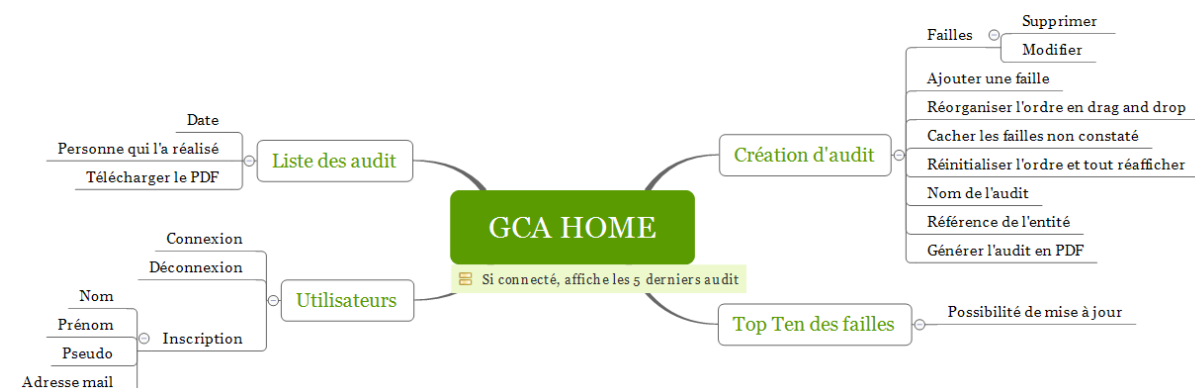
La demande consistait à créer une application web permettant de faire un rapport d'audit sur les failles détectées. L'équipe informatique teste les failles possibles sur le site du client puis lui édite un rapport sur les points faibles à corriger pour être en conformité avec la loi RGPD.

Dans ce rapport, la référence client doit apparaître ainsi que l'auditeur et un résumé des tests effectués et les failles trouvées.

On doit donc avoir :

- Des données client (références)
- La personne qui audite (nom, prénom, email)
- La date de l'audit ainsi que les failles détectées à cette date
- Informations sur les plus grandes failles (top 10 basé sur OWSAP)
- Statistiques
- Une liste de failles permettant de créer l'audit et de le personnaliser

L'OWASP (Open Web Application Security Project) est un nouveau type d'organisation. L'absence de pressions commerciales leur permet de fournir des informations impartiales, pratiques et rentables sur la sécurité des applications. L'OWASP n'est affiliée à aucune entreprise de technologie, bien qu'ils soutiennent l'utilisation éclairée de la technologie de sécurité commerciale. Semblable à de nombreux projets de logiciels libres, l'OWASP produit de nombreux types de documents d'une manière collaborative et ouverte. La Fondation OWASP est un organisme à but non lucratif qui assure le succès à long terme du projet.

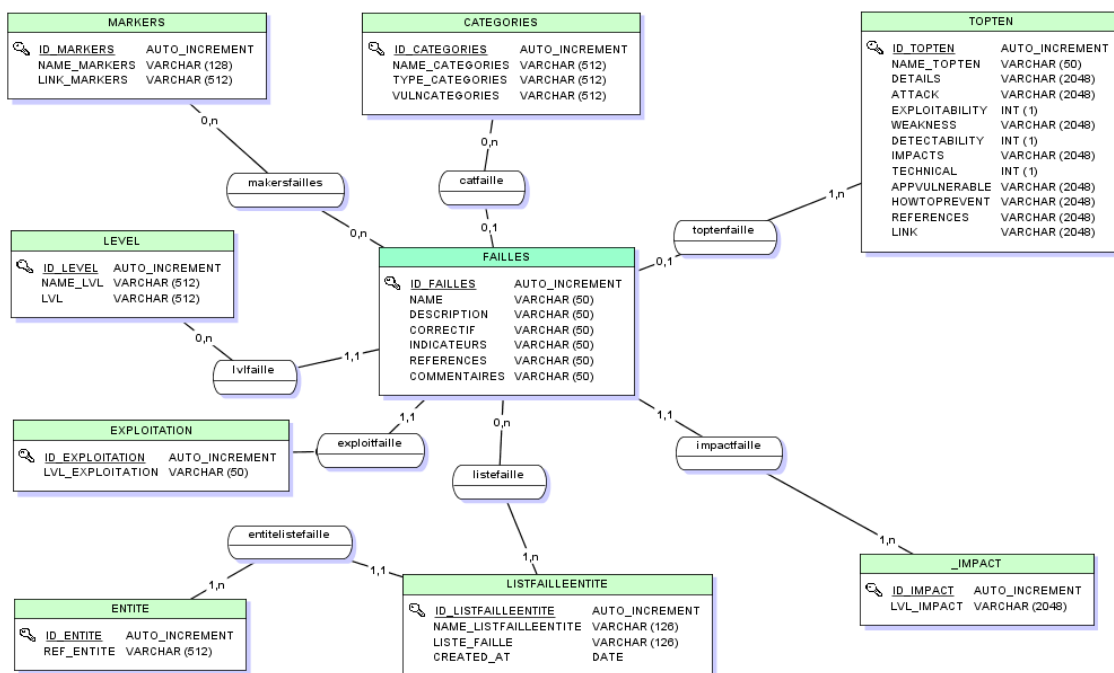


VOUS AVEZ DIT MCD/MLD ? :

MCD : le modèle conceptuel des données a pour but d'écrire de façon formelle les données qui seront utilisées par le système d'information. Il s'agit donc d'une représentation des données, facilement compréhensible, permettant de décrire le système d'information à l'aide d'entités.

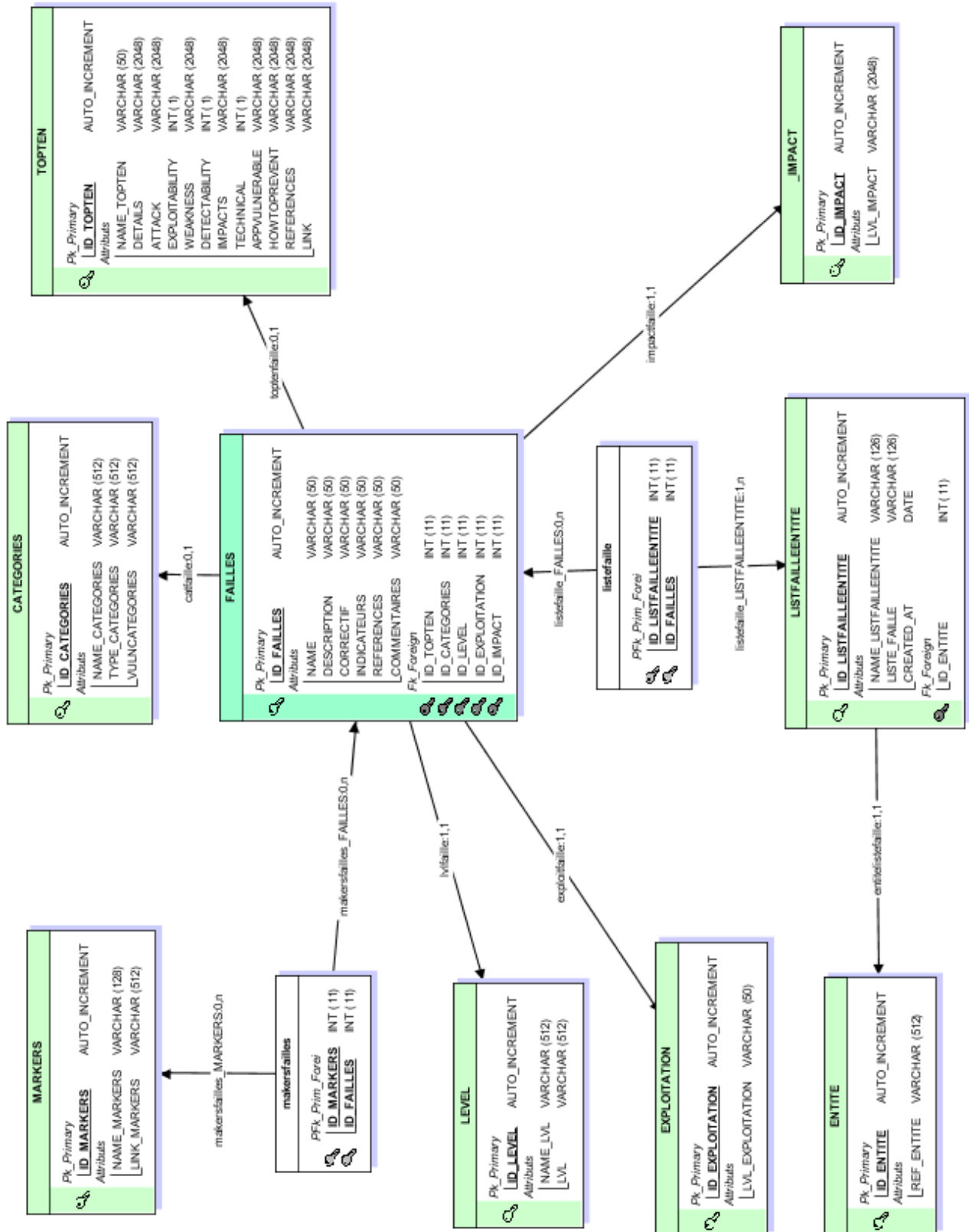
MLD : le modèle logique de données est la modélisation logique des données qui tient compte du niveau organisationnel des données. Il s'agit d'une vue logique en terme d'organisation de données nécessaire à un traitement.

Jmerise est un outil de modélisation qui m'a permis de faire le MCD et le MLD. Afin d'avoir une bonne vue globale de mon application et donc des models que je devrais créer dans l'application. Sur Django, quand on crée un projet et qu'on crée un model par défaut, la base de données est en SQLite³. J'ai conservé ce mode de fonctionnement pour mon projet.



1MCD

³ **SQLite** : est une bibliothèque écrite en langage C qui propose un moteur de base de données relationnelle accessible par le langage SQL.

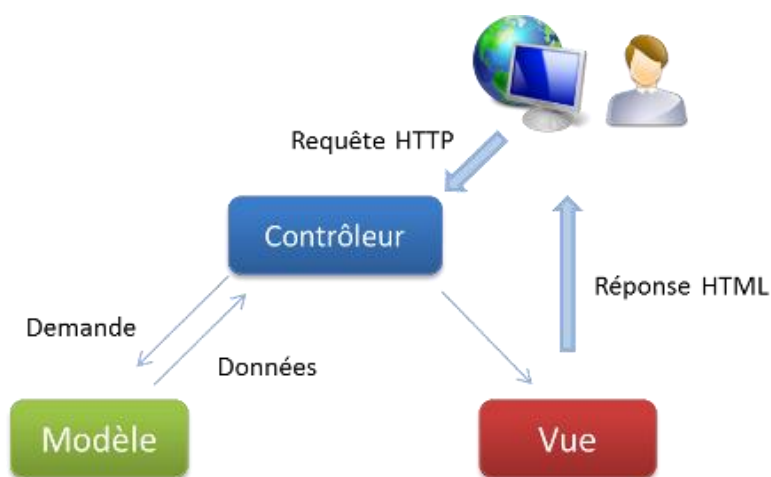


PARTIE 3 : DESIGN PATTERN

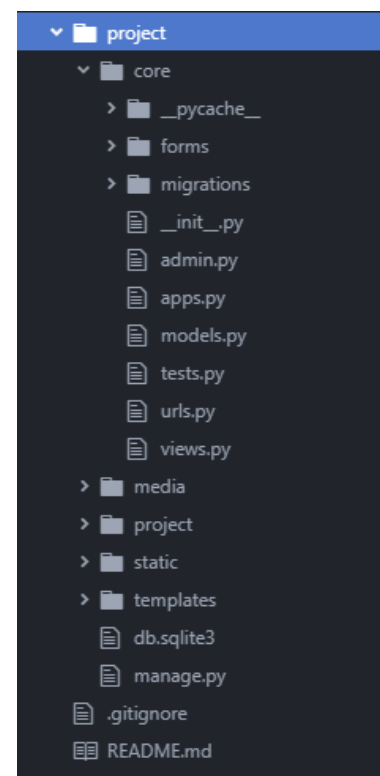
En informatique, et plus particulièrement en développement logiciel, un patron de conception (souvent appelé *design pattern*) est un arrangement caractéristique de modules, reconnu comme bonne pratique en réponse à un problème de conception d'un logiciel. Il décrit une solution standard, utilisable dans la conception de différents logiciels.

Les patrons de conception décrivent des procédés de conception généraux et permettent en conséquence de capitaliser l'expérience appliquée à la conception de logiciel. Ils ont une influence sur l'architecture logicielle d'un système informatique.

MVT (MODEL | VIEWS | TEMPLATES)



En Python c'est l'architecture MVT orientée autour de trois pôles : le **modèle**, la **vue** et le **Template**. Elle s'inspire de l'architecture MVC en PHP, très répandue dans les Framework web. Son objectif est de séparer les responsabilités de chaque pôle afin que chacun se concentre sur ses tâches.



Modèle

Le modèle interagit avec la base de données. Sa mission est de chercher dans une base de données les items correspondant à une requête et de renvoyer une réponse facilement exploitable par le programme.

Les modèles s'appuient sur un ORM⁴ (*Object Relational Mapping*, ou Mapping objet-relationnel en français).

Un ORM traduit les résultats d'une requête SQL en objets Python avec lesquels vous pouvez interagir. De même, il permet d'écrire une requête SQL en Python

Dans un projet Django, chaque application contient un document `models.py` qui réunit les différents modèles utilisés.

```
82 class Weaknesses(TimespantedModel):
83     name = models.CharField(max_length=256)
84     description = models.CharField(max_length=2048)
85     # correctif
86     patch = models.CharField(max_length=2048)
87     # indicateurs
88     benchmark = models.CharField(max_length=1024)
89     comm = models.CharField(max_length=2048, null=True, blank=True,)
90     # Références
91     markers = models.ManyToManyField(Markers, blank=True,)
92     #Link with topten and categorie
93     topten = models.ForeignKey('TopTen', on_delete=models.SET_NULL, null=True, blank=True,)
94     categorie = models.ForeignKey('Categories', on_delete=models.SET_NULL, null=True, blank=True,)
95     impact = models.ForeignKey('Impact', on_delete=models.SET_NULL, null=True, blank=True,)
96     exploit = models.ForeignKey('Exploitation', on_delete=models.SET_NULL, null=True, blank=True,)
97     lvl_weakness = models.ForeignKey('Level', on_delete=models.SET_NULL, null=True, blank=True,)
98
99     def __str__(this):
100         return this.name
```

⁴ **ORM** traduit les résultats d'une requête SQL en objets Python avec lesquels vous pouvez interagir. De même, il permet d'écrire une requête SQL en Python

Template

Un template est un fichier HTML qui peut recevoir des objets Python et qui est lié à une vue. Il est placé dans le dossier templates. Un template peut interpréter des variables et les afficher.

```
home.html
1  {% extends 'base.html' %}
2  {% load i18n %}
3
4  {% block body %}
5
6  {% if user.username %}
7  <h1>{% trans 'Bonjour' %} {{user.username}}</h1>
8  <h2>Récapitulatif de mes derniers audits diagnostiqué :</h2>
9
10 <table class="highlight">
11   <thead>
12     <tr>
13       <th>Nom de l'audit</th>
14       <th>Ref de l'entreprise</th>
15       <th>Date de création</th>
16       <th>Pdf</th>
17     </tr>
18   </thead>
19
20   {% for listaudit in listaudits%}
21   <tbody>
22     <tr>
23       <td>{{listaudit.name_audit}}</td>
24       <td>{{listaudit.entite}}</td>
25       <td>{{listaudit.created_at|date:'d-m-Y'}}</td>
26       <td><a href="{% url 'core:audit' listaudit.id %}"><i class="material-icons">send</i></a></td>
27     </tr>
28   </tbody>
29   {% endfor %}
30
31 </table>
32 {% else %}
33 <h1>Bienvenue</h1>
34
35 <p>Vous devez être connecté ou enregistré. </p>
36
37 <a href="{% url 'core:register' %}">S'enregistrer</a> /
38 <a href="{% url 'core:login' %}">Connexion</a>
39
40 {% endif %}
41
42 {% endblock %}
```

Vue

La vue joue un rôle central dans un projet structuré en MVT : sa responsabilité est de recevoir une requête HTTP et d'y répondre de manière intelligible par le navigateur.

La vue réalise également toutes les actions nécessaires pour répondre à la requête :

- si une interaction avec la base de données est requise, la vue appelle un modèle et récupère les objets renvoyés par ce dernier.
- si un gabarit est nécessaire, la vue l'appelle.

Dans un projet Django, les vues de chaque application sont regroupées dans le document `views.py`.

Chaque vue est associée à une url et les urls d'un projet sont regroupées dans le fichier `urls.py`.

Une vue est une méthode qui génère le contenu à renvoyer à une requête. Il s'agit d'une méthode qui renvoie une réponse à une requête HTTP.

```
43 # -----Home Page with List-----
44 def home(request):
45     user=request.user
46     if user is not None:
47         if user.is_active:
48             listaudits = ListFaillesEntite.objects.filter(user=user)[:5]
49             context = {
50                 'listaudits' : listaudits,
51             }
52             return render(request,'home.html', context)
53     return render(request,'home.html')
```

PARTIE 4 : MAIS ÇA DONNE QUOI ?

1) La page principale :

Dans la page principale, le but est d'informer si on est connecté ou non.

Si on est connecté, des informations récapitulatives s'affichent. Comme on peut remarquer sur la maquette, une liste des 5 derniers audits réalisés par la personne connectée. Il est possible, par le menu, d'accéder au top 10 des failles de sécurité, à la page de création d'audit ou encore à la liste de tous les audits effectués.

GCA

liste audit

créer un audit






top ten

Bonjour pseudo

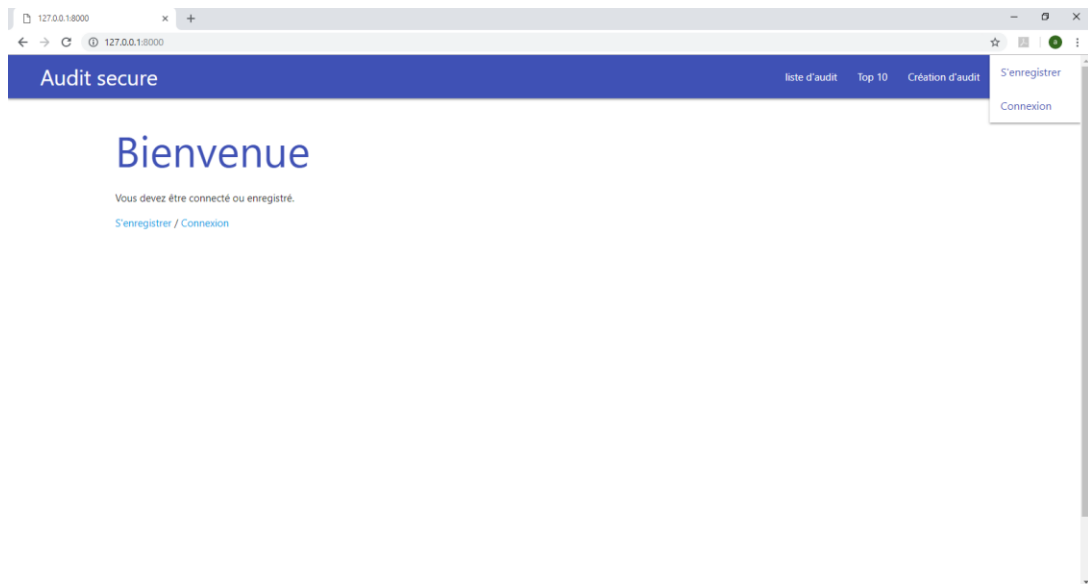
Deconnexion

Bonjour PSEUDO

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc maximus, nulla ut commodo sagittis, sapien dui mattis dui, non pulvinar lorem felis nec erat

Audit	Date	PDF
Liste 1	date 1	
Liste 2	date 2	
Liste 3	date 3	
Liste 4	date 4	
Liste 5	date5	

Ici c'est la capture d'écran du site quand on est Déconnecté.



2) Page d'enregistrement :

Sur cette maquette du formulaire d'inscription, on peut constater le menu au format mobil ainsi que les infos pour l'inscription.

Sur les captures d'écran, on peut observer le formulaire d'inscription, la touche en haut à gauche le menu. Quand on appuie dessus c'est un menu latéral qui apparaît (5 et 4). Le menu varie si on n'est pas connecté, on n'a pas accès à la liste des audits et on ne peut pas créer d'audit, uniquement voir la liste des failles.

4 Page connexion mobil

The image shows a mobile registration page for 'GCA'. At the top is a blue header with a hamburger menu icon on the left and the text 'GCA' on the right. Below the header, the word 'Inscription' is displayed in a large, blue, sans-serif font. Underneath, there are four input fields: 'Prenom' and 'Nom' (split into two columns), 'Pseudo', and 'Password'. Below these fields is an 'Email' input field. At the bottom left, there is a blue button with the text 'S'ENREGISTRER' in white capital letters.

3 Menu non connecté

The image shows a vertical menu for a non-connected user. It has a blue header with the text 'Bonjour' in white. Below the header, there are three items: 'S'enregistrer', 'Connexion', and 'Top 10'. Below these, there is a section titled 'Liste failles'. The menu is partially obscured by a grey vertical bar on the right side.

The image shows a vertical menu for a connected user named 'alore'. It has a blue header with the text 'Bonjour alore' in white. Below the header, there are three items: 'Top 10', 'Liste d'audit', and 'Création d'audit'. The menu is partially obscured by a grey vertical bar on the right side.

2 Menu connecté

3) Page du top 10 :

GCA
liste audit
créer un audit
top ten
Bonjour pseudo

TOP TEN

TOP TEN 1 <p> Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc maximus, nulla ut commodo sagittis, sapien dui mattis dui, non pulvinar lorem felis nec erat Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc maximus, nulla ut commodo sagittis, sapien dui mattis dui, non pulvinar lorem felis nec erat. Aliquam egestas, velit at condimentum placerat, sem sapien laoreet mauris, dictum porttitor lacus est nec enim. Vivamus feugiat elit lorem, eu porttitor ante ultrices id. Phasellus suscipit tellus ante, nec dignissim elit imperdiet nec. Nullam fringilla feugiat nisl. Ut pretium, metus venenatis dictum viverra, dui metus finibus enim, ac rhoncus sem lorem vitae mauris. Suspendisse ut venenatis libero. Suspendisse lorem felis, pretium in maximus id, tempor non ipsum </p> <div>MODIFIER</div>
TOP TEN 2
TOP TEN 3
TOP TEN 4
TOP TEN 5
TOP TEN 6
TOP TEN 7
TOP TEN 8
TOP TEN 9
TOP TEN 10

Ci-dessus la maquette de la page qui représente le top 10 des failles répertoriées sur OWSAP. Le but de cette page est d'avoir un récapitulatif des failles les plus courantes afin de rester à jour et d'être cohérent par rapport à l'audit et pour insister sur certains points critiques lors du rapport avec celle-ci à l'appui.






Dans la capture d'écran ci-dessous, on peut voir toute la liste où l'on peut dérouler chaque faille pour avoir le détail comme pour la première. On a aussi l'année, cela permet de rester à jour et de constater quand elle a été classifiée. Certaines failles sont simplement reconduites l'année suivante car elles n'ont pas bougé et donc nécessité de mise à jour. Pour les mettre à jour, seuls ceux connectés pourront, en appuyant sur le bouton « modifier » à la fin du descriptif de la faille. Pour les autres, le bouton ne sera pas présent.

Top 10 des failles

<p>A1-2017-Injection</p> <p>details :</p> <p>Almost any source of data can be an injection vector, environment variables, parameters, external and internal web services, and all types of users. Injection flaws occur when an attacker can send hostile data to an interpreter.</p> <p>niveau d'exploitabilité : 3</p> <p>weaknes :</p> <p>Injection flaws are very prevalent, particularly in legacy code. Injection vulnerabilities are often found in SQL, LDAP, XPath, or NoSQL queries, OS commands, XML parsers, SMTP headers, expression languages, and ORM queries. Injection flaws are easy to discover when examining code. Scanners and fuzzers can help attackers find injection flaws.</p> <p>prevalence : 2</p> <p>detectability : 3</p> <p>impacts :</p> <p>Injection can result in data loss, corruption, or disclosure to unauthorized parties, loss of accountability, or denial of access. Injection can sometimes lead to complete host takeover. The business impact depends on the needs of the application and data.</p> <p>technical : 3</p> <p>application :</p> <p>An application is vulnerable to attack when: User-supplied data is not validated, filtered, or sanitized by the application. Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter. Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records. Hostile data is directly used or concatenated, such that the SQL or command contains both structure and hostile data in dynamic queries, commands, or stored procedures. Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection. The concept is identical among all interpreters. Source code review is the best method of detecting if applications are vulnerable to injections, closely followed by thorough automated testing of all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs. Organizations can include static source (SAST) and dynamic application test (DAST) tools into the CI/CD pipeline to identify newly introduced injection flaws prior to production deployment.</p> <p>how to :</p> <p>Preventing injection requires keeping data separate from commands and queries. The preferred option is to use a safe API, which avoids the use of the interpreter entirely or provides a parameterized interface, or migrate to use Object Relational Mapping Tools (ORMs). Note: Even when parameterized, stored procedures can still introduce SQL injection if PL/SQL or T-SQL concatenates queries and data, or executes hostile data with EXECUTE IMMEDIATE or exec(). Use positive or "whitelist" server-side input validation. This is not a complete defense as many applications require special characters, such as text areas or APIs for mobile applications. For any residual dynamic queries, escape special characters using the specific escape syntax for that interpreter. Note: SQL structure such as table names, column names, and so on cannot be escaped, and thus user-supplied structure names are dangerous. This is a common issue in report-writing software. Use LIMIT and other SQL controls within queries to prevent mass disclosure of records in case of SQL injection.</p> <p>references :</p> <p>https://www.owasp.org/index.php/OWASP_Proactive_Controls#2:_Parameterize_Queries</p> <p>link :</p> <p>https://www.owasp.org/index.php/Top_10-2017_A1-Injection</p> <p>MODIFIER</p>
A2-2017-Broken Authentication
A3-2017-Sensitive Data Exposure
A4-2017-XML External Entities (XXE)
A5-2017-Broken Access Control
A6-2017-Security Misconfiguration
A7-2017-Cross-site Scripting(XSS)
A8-2017-Insecure Deserialization
A9-2017-Using Components with Known Vulnerabilities
A10-2017-Insufficient Logging & Monitoring






4) Page récapitulative des audits crée :

GCA				
		liste audit	créer un audit	top ten
				Bonjour pseudo
				Deconnexion

Liste d'audit				
Personne	Nom Audit	Référence client	Date	PDF
Arnaud	Liste 1	#ACT01012018	date 1	
Pierre	Liste 2	#ELN01012018	date 2	
Sophie	Liste 3	#ACT01012018	date 3	
Pierre	Liste 4	#ELN1012018	date 4	
Pierre	Liste 5	#ACT01012018	date5	

Sur la maquette de la liste récapitulative de tous les audits faits, on a accès à la date de création, le nom de l'auditeur, la référence du client, le nom de l'audit et on peut télécharger et consulter l'audit déjà fait. C'est un historique.

GCA				
		Top 10	Liste d'audit	Création d'audit
				Bonjour afluence

Liste des Audits				
PAR DATE		PAR AUDITEUR		PAR CLIENT
Nom de l'auditeur	Nom de l'audit	Ref de l'entreprise	Date de création	Pdf
arnaud florence	troisième audit	#ACT01012019	08-11-2018	
admin	test	#ELAN01012019	05-11-2018	
admin	dfsdfsdfsdfsdf	#ACT01012019	05-11-2018	
arnaud florence	ififdfdd	#ACT01012019	29-10-2018	
arnaud florence	first	#ELAN01012019	29-10-2018	

Sur la capture d'écran du site on peut constater que j'ai rajouté des filtres. On peut donc voir les listes créées par date, par auditeur ou encore par référence client.

5) Le cœur de l'application :

Voici la maquette du cœur de cette application, l'endroit où l'on fait notre audit. Ici la demande était d'avoir une liste de failles personnalisées que l'on pouvait organiser dans l'ordre que l'on souhaitait, modifier ou supprimer et aussi cacher les listes qui n'ont pas été constatées. Par la suite, on devrait pouvoir générer un rapport d'audit.

The screenshot displays the GCA application interface. At the top, a blue header bar contains the logo 'GCA' and navigation links: 'liste audit', 'créer un audit', 'top ten', and 'Bonjour pseudo'. Below the header, there are three buttons: 'RESET', 'CREER FAILLES', and 'CREER AUDIT'. A form section includes a 'REF CLIENT' dropdown menu with two options: '#ELA01012018' and '#ACT01012018'. Below this is an 'Input Text nom audit' field. A modal window titled 'FAILLE PERSO 3' is open, showing a description and a patch for a vulnerability. The modal has a 'Modifier' button and a 'Supprimer' button. Below the modal, there are two more entries for 'FAILLE PERSO 1' and 'FAILLE PERSO 2', each with a small icon and a red 'X' button. At the bottom, a 'SUCCESS' message is displayed with the text 'Direction liste'.

Sur la capture d'écran du site ci-dessous, on choisit la référence du client dans un premier temps dans une liste déroulante. Si le client n'existe pas, on peut le créer en cliquant sur le bouton en haut « créer une réf client » (voir la 2eme capture d'écran). Ensuite, on donne un nom à l'audit que l'on fait (exemple : premier audit ou dans le cas la « test »). Une fois ces champs renseignés, on obtient la liste des failles personnalisées. Comme pour le top 10, en cliquant sur le titre une partie se dévoile avec les informations. Il est possible changer l'ordre des failles avec un glisser déposer en maintenant le clic sur la petite icône en haut à gauche

de la faille que l'on veut bouger. C'est possible de supprimer une faille de la liste si celle-ci n'a pas été détectée. On peut également modifier le contenu de chaque liste ou la supprimer définitivement. Le bouton « reset » en haut permet de réinitialiser l'ordre des failles et aussi les faire réapparaître. En cliquant sur créer une faille, on peut en créer une nouvelle et sur créer un PDF, on génère l'audit. Un petit pop-up « succès » apparaît et soit on attend quelques secondes que la page se rafraichisse, soit on clique sur le lien du pop-up pour aller dans la liste des audits où il a été enregistré.

GCA
Top 10
Liste d'audit
Création d'audit
Bonjour admin

Success !
LISTE AUDIT

Liste des failles

RESET
RENDU PDF
AJOUTER UNE FAILLE
NOUVEAU CLIENT

#ACT01012019

Nom de l'audit
test

EV1 / Persistent HTML Injection / XSS

level 1 critique

description :
L'injection HTML est la possibilité pour un utilisateur de contrôler un point d'entrée en insérant du code HTML arbitraire dans une page Web vulnérable. Cette vulnérabilité peut avoir de nombreuses conséquences, comme la divulgation des cookies de session d'un utilisateur qui pourraient être utilisés pour usurper l'identité de la victime, ou, plus généralement, elle peut permettre à l'attaquant de modifier le contenu de la page vu par les victimes. <script>alert('Il y a une faille XSS')</script> L'insertion de code n'a de limite que la taille maximum du champ ou le filtrage des caractères. Un attaquant peut parvenir à insérer du javascript malveillant distant afin d'infecter les navigateurs des clients.

correctif :
Rechercher si Magento dispose d'un plugin permettant de filtrer les noms et prénoms qui d'ailleurs ne sont pas censé recevoir des balises HTML PHP propose des fonctions permettant d'encoder sous forme d'entités HTML une chaîne de caractères : strip_tags() Permet de supprimer tous les tags HTML non souhaités (tous tags sauf ceux passés en paramètre de la fonction) htmlspecialchars() Permet de convertir les caractères &','<> sous forme d'entités HTML htmlentities() Permet de convertir tous les caractères sous forme d'entités HTML y compris les caractères à, é, è, etc... Dans des framework évolués (tel que Symfony) est proposé un mécanisme permettant d'échapper automatiquement (escaping) les données qui transitent d'un contrôleur à la vue (objet "Decorator") ou entre le contrôleur et le modèle de données (méthode bind()) des formulaires). Ce qui revient à protéger les données venant de n'importe quel vecteur d'attaque (BDD, paramètres HTTP, etc.).

indicateurs :
Exploitation de la vulnérabilité : **facile**
Impact : **important**

Références :
[https://www.owasp.org/index.php/XSS_\(Cross_S...](https://www.owasp.org/index.php/XSS_(Cross_S...)

Top 10 :
https://www.owasp.org/index.php/Top_10-2017_...

Categorie :
html

MODIFIER
SUPPRIMER

faible password

level 2 perfectible

cable

level 3 modéré

AXES D'AMÉLIORATION :

Il y a plusieurs points que je n'ai pas eu le temps d'intégrer en voici quelques exemples :

- Ajouter des statistiques sur les failles les plus utilisées
- Plus de gestion d'erreur dans les champs
- La possibilité d'ajouter des images dans les audits
- Des champs de texte customisables en plus dans l'audit
- Certains formulaires de modification intégrés dans des modales pour éviter de recharger des pages
- La traduction en anglais et en français
- La possibilité d'avoir l'audit en document Word
- Une pagination pour la liste des audits

MODIFICATION CRM (quelques exemples) :

En parallèle de mon projet de stage, j'ai aussi participé à l'ajout de quelques fonctionnalités dans le CRM de l'entreprise. J'ai donc dû commencer par me familiariser avec le code de l'application. Comme l'application a été réalisée en python 2.7 avec Django 1.9, il y avait quelques différences entre ce que j'ai appris/connu.

QU'EST CE QU'UN CRM :

C'est une application de gestion de la relation client (GRC), ou en anglais **Customer Relationship Management** (CRM). C'est l'ensemble des outils et techniques destinés à capter, traiter, analyser les informations relatives aux clients et aux prospects, dans le but de les fidéliser en leur offrant ou proposant des services.

En ce qui concerne les applications informatiques, il s'agit notamment des progiciels qui permettent de traiter directement avec le client, que ce soit sur le plan de la vente, du marketing ou du service, et que l'on regroupe souvent sous le terme de « FrontOffice », ceci par opposition aux outils de « back-office » que sont les [progiciels de gestion intégrés](#) (pgi / erp).

QUELQUES EXEMPLES :

AJOUT D'UN LIEN ONEDRIVE :

Une de mes missions a été d'intégrer un lien OneDrive dans les projets. J'ai procédé à l'ajout d'un champ pour le lien mais également d'un petit tutoriel quand on clique sur le point d'interrogation à côté du champ. Lorsqu'on clique dessus, une modale s'ouvre avec le tutoriel et les explications pour savoir comment récupérer un lien one drive. Lorsqu'on clique également sur le titre du champ, un nouvel onglet s'ouvre et nous emmène directement sur OneDrive ou sur la page de connexion.

Account:

Link OneDrive
 ?

Start date mission/abonnement:
2018-09-13 Today

End date planned mission/abonnement:
 Today

Expected amount:

☐ Reimbursement of travel

Lors du retour sur la page d'un projet, on peut donc distinguer en vert le lien OneDrive ou si on a été autorisé par le chef de projet, on peut consulter les documents, à défaut on nous indique qu'on ne dispose pas des droits. Si aucun lien OneDrive n'a été enregistré, il est indiqué dans le champ en rouge comme ci-dessous.

Account:	[Non] Geispolsheim	OneDrive:	Aucun lien onedrive
Date start:	Aug. 24, 2018	Reimbursement of travel:	No
Deadline:	Sept. 2, 2018	Date modified:	Aug. 24, 2018, 4:41 p.m. By KIEHL Alexandre
		Cloud	
OneDrive:	✓ Lien onedrive		
Reimbursement of travel:	No		
Date modified:	Sept. 10, 2018, 5:13 p.m. By KIEHL Alexandre		

FILTRE PERSONNALISE DJANGO :

Pour le lien OneDrive, j'ai aussi eu l'occasion de pouvoir créer un filtre personnalisé dans Django. Les filtres sont utilisés par la suite dans les Templates HTML.

Par exemple le filtre |date :

```
<p>{{listaudit.created_at|date:'d-m-Y'}}</p>
```

Ce filtre permet de filtrer la date prise dans la base de données dans le format jour/mois/année.

Dans l'exemple ci-dessous le filtre regarde le début de la chaîne de caractère retourné. S'il n'y a pas http :// ou https :// il va le rajouter sinon il fait rien.

Pourquoi ce filtre ?

Lors de l'enregistrement du lien internet, l'adresse pouvait ne pas commencer par « http » ou « https » et donc l'application renvoyait une erreur. Elle ne comprenait pas qu'il s'agissait d'un lien internet.

```
1  from django import template
2  register = template.Library()
3
4  @register.filter
5  def link(l):
6      result = l.startswith('https://');
7      result1 = l.startswith('http://');
8      if not result or result1:
9          if result1:
10             l.replace(l, 'http://' + l)
11             return (l)
12             return l.replace(l, 'http://' + l)
13     else:
14         return (l)
15
```

ENVOI DE MAIL AUTOMATIQUE :

J'ai pu également ajouter quelques lignes de code pour pouvoir programmer l'envoi d'un mail automatique lorsqu'un ticket d'incident est créé dans une boîte mail personnalisée. L'envoi est effectué par une boîte mail créée pour l'application qui s'appelle (ne-pas-répondre).

CONCLUSION :

L'approche d'un autre langage et la conception d'une petite application simple ainsi que l'apport de modifications à une application existante s'est avéré être une excellente et enrichissante expérience. J'ai dû faire appel à toutes les notions inculquées durant ma formation de titre de « Développeur logiciel ». J'ai eu quelques difficultés au début à m'adapter à une ancienne version de Python et de Django tout en ayant à comprendre le fonctionnement du CRM. Mais cette expérience m'a permis de voir certains fonctionnements tels que l'envoi de mails automatique ou encore la traduction dans plusieurs langues d'une application.

Par la suite, l'autre difficulté a été de devoir gérer le débogage/ajout du CRM avec mon projet de stage. J'ai essayé de faire 3 jours CRM et 2 jours Projet suivant l'importance et la priorité des problèmes du CRM.

L'application n'est aujourd'hui qu'en Alpha et je suis amené à continuer le développement de cette application.

