Université de Caen Normandie
UFR des Sciences
Département Informatique

Master 1 : Informatique

Rapport de projet: Récolte de témoignages anonymisés par des moyens cryptographiques

---

Thomas Berthelin (21909397)
Mahamat Ahmat Ahmat (21912949)

2023 - 2024

Table des matières

1 Présentation du projet

1.1 Problématique

L'université de Caen est un établissement très vivant où de nombreux événements sont organisés. Cependant, lors de ces événements, certaines personnes adoptent un comportement inapproprié, tel que le harcèlement ou la violence physique.

Malheureusement, les victimes de ces comportements ne témoignent souvent pas. Les raisons de ce silence peuvent être liées à la crainte de représailles, notamment dans le cadre de relations hiérarchiques, à la possibilité d'une mauvaise interprétation des faits observés, à l'isolement potentiel généré par une procédure de témoignage, ou encore au fait que trop peu de plaintes aboutissent, conduisant les victimes à considérer que témoigner « ne sert à rien ». Selon une étude réalisée par l'Organisation Internationale du Travail, de 2017 à 2019, 52% des femmes et 27% des hommes ont été victimes de harcèlement sexuel au travail, mais seulement 4% des femmes et 1% des hommes ont porté plainte.

L'objectif de notre projet est donc de mettre en place une plateforme sur laquelle les victimes ou témoins de ces violences lors des événements organisés par l'université pourront témoigner de manière anonyme, afin de ne plus craindre de représailles. Les victimes ayant témoigné contre la même personne pourront être mises en relation, ce qui pourrait potentiellement les rendre plus confiantes. Ainsi, si elles le souhaitent, elles pourront engager des poursuites.

1.2 Un projet d'actualité

Ce projet est très pertinent, en effet, le climat social en France se dégrade, avec une augmentation constante des violences et agressions. Cette tendance à la hausse n'épargne pas le monde professionnel, comme le souligne l'INSEE, indiquant que 22% des travailleurs français ont été victimes ou témoins de violence au travail au cours de l'année 2023, représentant une augmentation de 38% depuis le début de la dernière décennie. Les employés de l'université de Caen sont également touchés par cette problématique, soulignant ainsi l'importance de ce projet.

1.3 Qui sommes-nous ?

Nous sommes des étudiants en master 1 d'informatique en parcours à la carte et nous avons tous deux pris le parcours Cybersécurité. Dans le cadre de cette première année nous avons un projet à réaliser pendant les deux semestres. Nous avons choisi le sujet décrit plus tôt car il correspond au mieux au parcours que nous avons choisi pour le master. En effet, l'anonymisation que nous allons mettre en place dans le projet relève de la cryptographie, partie importante de la cybersécurité.

1.4 Encadrement du projet

Les encadrants du projet sont les enseignants-chercheurs, Adeline Roux-Langlois et Matthieu Dien, qui ont dirigé notre travail tout au long de la réalisation de ce projet. Le projet est à réaliser tout au long de l'année scolaire 2023 - 2024, avec un premier rendu au mois de janvier, afin de rendre compte de son avancement.

1.5 Plan du rapport

Dans un premier temps nous analyserons les besoins du projet, les technologies que nous utiliserons, ensuite nous vous expliquerons le développement du projet, et enfin nous conclurons.

2 Analyse du Besoin

Dans un premier temps nous allons analyser les publics ciblés par notre projet, puis les besoins des utilisateurs.Ensuite nous passerons en revue les fonctionnalités clés du projet qu'il va falloir implémenter.

2.1 Public cible

Victimes de Harcèlement ou de Violence : Groupe comprenant les individus qui ont subi du harcèlement ou de la violence lors des évènements organisés par l'université et qui hésitent à témoigner.

Témoins : Groupe comprenant les individus qui ont assisté à du harcèlement ou de la violence et qui hésitent à témoigner pour protéger la volonté de la victime ou par peur.

Organisateurs d'Événements et Institutions : Entités pouvant utiliser la plateforme pour mieux comprendre les incidents survenus lors de leurs évènements.

Chercheurs et Activistes : Groupe comprenant les individus s'intéressant à l'étude et à la lutte contre le harcèlement et la violence, et qui trouveront dans les données anonymes une source précieuse d'information.

Au vu de ce public cible et du contexte dans lequel notre projet s'inscrit, nous pouvons déjà voir que notre plateforme ne recevra pas énormément de témoignages et ne sera pas visitée par beaucoup de personnes.

2.2 Besoins des Utilisateurs

Nous devons clairement définir le besoin des utilisateurs afin d'en déduire les fonctionnalités que nous devrons implémenter et comment les implémenter.

Témoigner : L'utilisateur a besoin de pouvoir témoigner de l'incident qu'il a subi en quelques lignes.

Anonymat et Sécurité : L'utilisateur a besoin d'un anonymat total pour lui et pour la personne accusée dans ses témoignages, c'est le principal enjeu de notre projet.

Mise en relation : L'utilisateur a besoin d'être mis en relation avec les personnes qui ont témoigné contre la même personne que lui.

Ressources supplémentaires : L'utilisateur a besoin d'avoir accès rapidement à des ressources tel que des numéros d'appel d'urgence et des liens vers de site webs officiels qui proposent une aide plus directe.

2.3 Fonctionnalités clés

Définir les fonctionnalités clés est très important car cela permet de choisir les bonnes technologies mais aussi de trouver une ligne directrice au projet.

Création de comptes : Afin de témoigner, les utilisateurs doivent se créer un compte, cela leur permettra de témoigner et d'être mis en contact plus tard par mail.

Chiffrement des informations : Pour garder l'utilisateur et son agresseur anonymes nous devons stocker les informations de leurs identités chiffrées sur le serveur de façon à ce que même une personne ayant accès aux données ne puisse pas les trouver. Comme indiqué dans le sujet, nous utiliserons des moyens cryptographiques pour chiffrer ces informations, c'est à dire une méthode qui permet de rendre illisible par l'homme les données.

Comparaison d'identités chiffrées : Afin de mettre en relation les individus ayant témoignés contre la même personne, nous devons comparer les identités des agresseurs. Mais, comme nous l'avons vu plus tôt ces identités sont chiffrées, nous devons donc trouver une méthode de chiffrement qui nous permettra de comparer les identités une fois chiffrées.

Modération : Notre plateforme doit être gérée par un administrateur qui pourra empêcher d'utiliser à mauvais escient la plateforme. Une interface devra être mise en place pour faciliter cette tâche, mais aussi pour afficher à l'administrateur à qui il doit envoyer un mail de mise en relation.

3 Le choix des technologies

Nous avons analysé les besoins de ce projet, nous pouvons maintenant passer au choix des technologies. Ce choix est très important, les technologies les plus adaptées nous permettrons une optimisation de notre plateforme. Nous verrons dans un premier temps les contraintes imposées par le sujet, ensuite nous verrons quel langage de programmation nous avons choisi pour le site web puis quelle base de données nous utiliserons.

3.1 Contraintes

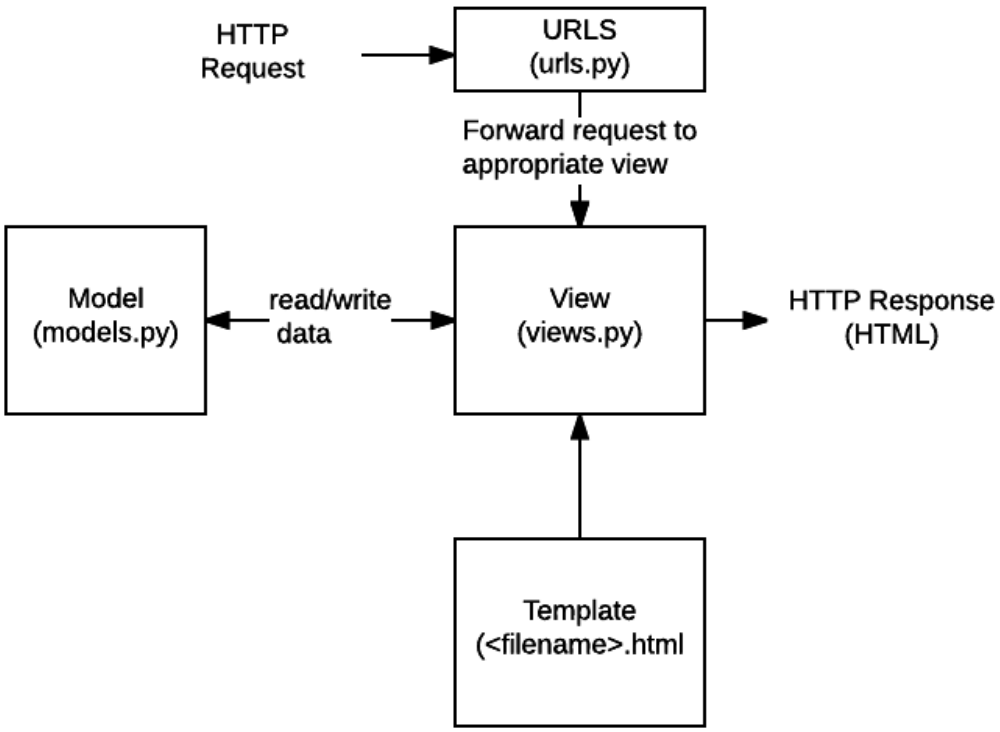
La seule contrainte imposée pour ce projet était d'utiliser les langages de programmation PHP ou Python. Les deux langages sont en effet adaptés pour le développement de ce projet, les deux langages permettent de bonnes performances, une facilité d'hébergement et une communauté active.
Nous avons choisi d'utiliser Python principalement parce qu'il existe énormément de librairies dédiées à la cryptographie développées avec, que nous pourrons réutiliser. Cela signifie que nous avons un accès facile à une multitude d'outils et d'algorithmes de chiffrement, de hachage et d'autres techniques de sécurité pour protéger les données sensibles de notre application web. Ces librairies sont très bien documentées et régulièrement mises à jour. Aussi, nous avons envie d'apprendre le framework Django. Django est un framework de Python, c'est-à-dire qu'il offre une structure organisée pour le développement d'applications web. Ce framework est utilisé par de grandes entreprises tel que Meta avec leur application Instagram, nous avons donc pensé que c'était une bonne idée de savoir s'en servir pour nos futurs emplois.

3.2 Django

Comme nous avons vu précédemment, notre site web sera fait avec le framework Django. Contrairement à la plupart des frameworks, Django utilise le modèle de conception MVT et non MVC.

MVC(Modèle- Vue- Contrôleur) Le modèle représente les données et la logique métier, la vue affiche l'interface utilisateur et le contrôleur traite les entrées de l'utilisateur et orchestre les actions.

MVT(Modèle-Vue-Template) Une variation du MVC. Dans le MVT, le modèle reste similaire au MVC, représentant les données et la logique métier. La vue dans Django est plus proche du contrôleur dans le MVC, gérant l'interaction avec le modèle et préparant les données pour l'affichage. Le template correspond à la vue dans le MVC et gère la présentation des données à l'utilisateur.

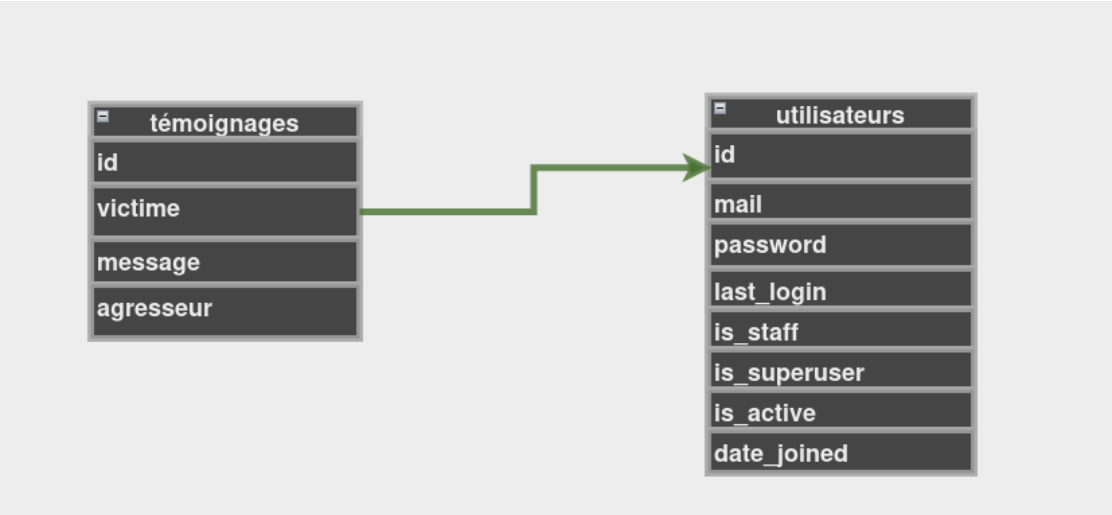


En résumé, la principale différence réside dans la manière dont la logique est organisée : dans le MVC, le contrôleur gère les interactions utilisateur et décide de la vue à afficher, tandis que dans le MVT de Django, cette logique est partagée entre la vue et le template, offrant une approche plus modulaire et simplifiée.

En plus de tout ça, une gestion des utilisateurs et une page d'administration sont présentes nativement dans le framework.

3.3 SQLite

Comme nous avons pu le voir dans la partie « Analyse du besoin », il n'y aura pas énormément d'échanges avec la base de données. Nous avons donc choisi SQLite, pratique pendant le développement, ne nécessitant pas de configuration, rapide, efficace et amplement suffisante pour le peu de données que notre projet accumulera au cours de son utilisation. C'est là que nous stockerons les informations des utilisateurs et les témoignages.



4 Développement

Une fois que nous avons choisi les technologies il ne nous reste plus qu'à implémenter la plateforme. Nous allons expliquer le déroulement du projet, puis nous parlerons du développement de la plateforme, et ensuite nous verrons les différents moyens cryptographiques mis en place.

4.1 Déroulement

Le projet s'est déroulé sur toute l'année scolaire 2023-2024, avec un rendu par semestre. Nous avons d'abord réalisé la plateforme permettant de témoigner et d'ensuite ajouter les moyens cryptographiques. En effet, séparer les deux parties est une idée judicieuse car nous avons pu rendre le site fonctionnel pour le premier rendu et ensuite nous concentrer sur la partie de la cryptographie, partie la plus compliquée, pour le rendu final. Nous avons eu des rendez-vous avec nos professeurs encadrants tout le long du projet, afin de nous introduire plus précisément au sujet, puis de nous guider tout le long.

4.2 Le site web

Nous avons donc réalisé le site web avec Django, il est entièrement responsive, c'est-à-dire que la page adapte la disposition de ses éléments afin qu'elle reste parfaitement lisible et fonctionnelle. Nous allons d'abord voir comment naviguer dedans, puis nous verrons quelles fonctionnalités nous avons implémentées.

4.2.1 Naviguer sur le site web

Nous avons mis en place une barre de navigation en haut de la page afin de naviguer entre les différentes pages du site. Lorsque le site est ouvert sur mobile, ou que les dimensions de l'écran ne permettent pas son affichage propre, la barre de navigation est remplacée par un bouton hamburger qui permet l'affichage d'un menu déroulant permettant de naviguer entre les pages. Les pages accessibles par la barre de navigation changent une fois connecté, pour accéder à des pages telles que celles pour témoigner ou celles pour voir nos témoignages.

4.2.2 Les fonctionnalités implémentées

Nous allons maintenant passer en revue les fonctionnalités implémentées sur le site web, et auxquelles l'utilisateur et l'administrateur ont accès.

Créer un compte et se connecter : Après avoir été accueilli par un paragraphe sur la page d'accueil, encourageant au témoignage et expliquant le principe de la plateforme, les utilisateurs sont invités à se connecter sur une page dédiée. Les utilisateurs ont donc la possibilité de se créer un compte et de s'y connecter, ils auront juste besoin de renseigner une adresse mail et un mot de passe. Ces informations seront stockées dans la base de données.

Témoigner : Nous avons évidement ajouté la page permettant de témoigner, accessible uniquement aux utilisateurs connectés et aux administrateurs. C'est un formulaire à remplir avec deux champs, un pour le nom de l'agresseur, et un dans lequel il faudra rédiger en quelques lignes le témoignage, en faisant bien attention à ne pas citer qui que ce soit dedans car cette partie ne sera pas chiffrée et donc il serait facile de remonter aux personnes impliquées. Un formulaire aussi simple permet de faciliter l'accès aux témoignages. Obliger une personne à mettre une date, un lieu ou encore d'autres informations prendrait plus de temps et ferait ressentir à la victime un côté plus officiel.

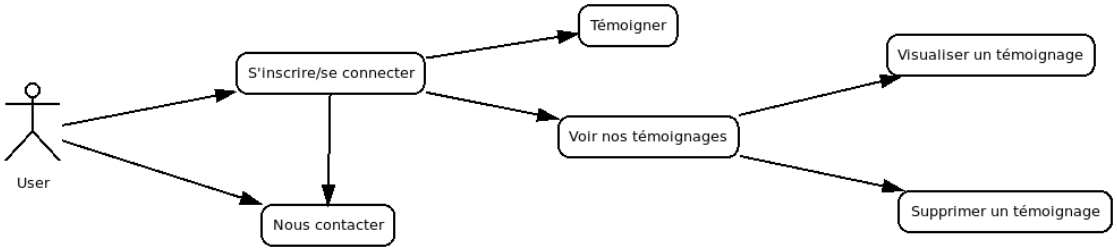
Visualiser nos témoignages : Nous avons ajouté une page permettant de visualiser la liste de nos témoignages, encore une fois accessibles seulement par les personnes connectées. Sur cette page s'affiche donc la liste des témoignages de l'utilisateurs avec, à droite de chacun, un bouton corbeille permettant de supprimer chaque témoignages individuellement. Lorsque l'utilisateur clique sur un témoignage une fenêtre pop-up s'affiche, contenant le témoignage.

Contacter l'administrateur : Une page permettant de contacter l'administrateur est aussi disponible, elle ne requière pas d'être connecté, c'est un formulaire qu'il faut remplir avec le corps du message et des champs tels que l'adresse mail ou le nom. Il est possible de ne pas renseigner une adresse mail valide mais c'est quand même mieux si on veut recevoir une réponse.

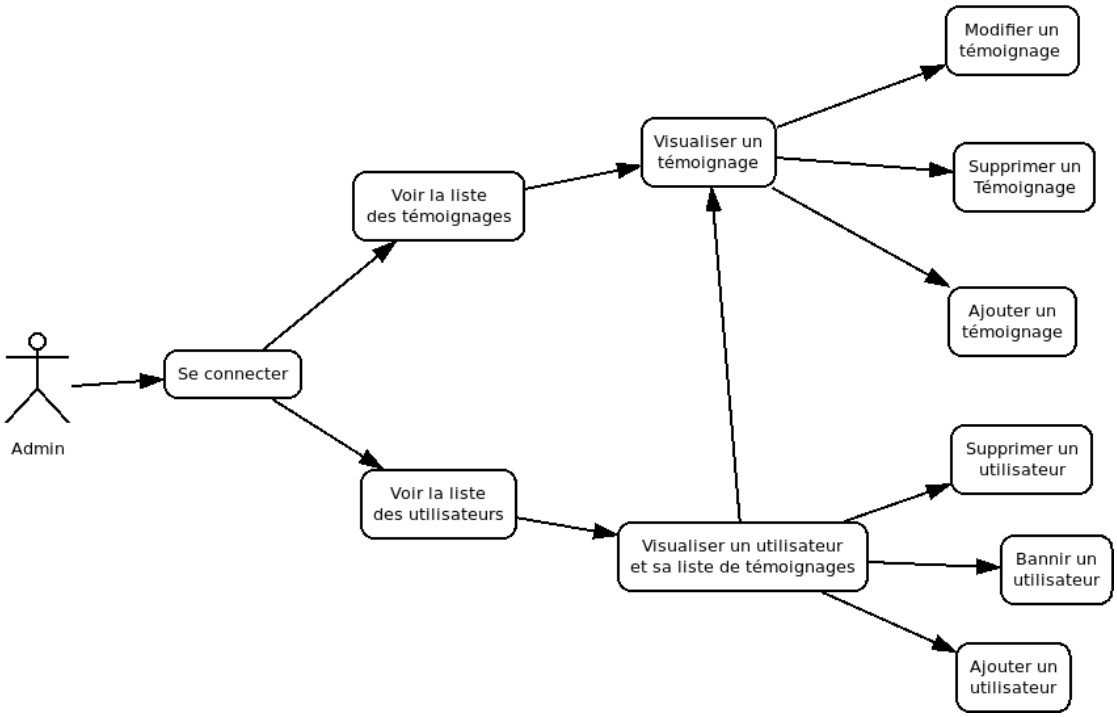
Administrer la plateforme : Comme dit précédement, une interface d'administration est disponible nativement dans le framework Django. Pour y accéder, depuis le navigateur, ajoutez « /admin » à la fin de l'url du site web. Vous arriverez ainsi sur une page vous demandant de vous connecter avec un compte administrateur. Une fois fait une page s'affiche, depuis laquelle vous pouvez accéder à la liste des utilisateurs, à leurs témoignages, et vous pouvez tout modifier à votre guise. Ainsi , si quelqu'un abuse du service il sera possible de supprimer son compte et de le bannir.

Mise en relation : Pour le moment, l'envoi de mails entre les utilisateurs se fait manuellement par l'administrateur. Étant donné que l'on ne s'attend pas à avoir beaucoup de témoignages cela ne pose pas de problème.

Voici, ci-dessous, des diagrammes, appelés Use Case. Le premier illustre ce que peut faire un utilisateur sur le site web :



Le deuxième représente ce que l'administrateur peut faire dans la partie administration du site web :



5 Les moyens cryptographiques

Comme nous avons pu le voir précédement, chiffrer certaines informations est crucial. Nous allons donc voir quels moyens cryptographiques nous avons mis en place pour chacune de ces informations.

5.1 Le mot de passe des comptes

Nous avons choisi d'utiliser l'algorithme de hachage SHA256 pour stocker les mots de passe des utilisateurs. SHA256 est une fonction de hachage cryptographique, c'est à dire une fonction mathématique qui prend des données en entrée et produit une sortie de longueur fixe (256bits), qui représente de manière unique ces données. Les fonctions de hachage sont souvent utilisées pour stocker des mots de passe de manière sécurisée, car elles rendent extrêmement difficile de retrouver le mot de passe d'origine à partir du haché, même si le haché est connu.

5.2 L'identité de l'agresseur

L'enjeu principal de ce projet est le chiffrement de l'identité de l'agresseur. Comme nous l'avons dit précédement il va falloir effectuer des comparaisons entre les noms des agresseurs, tout en les gardant illisibles pour que personne ne puisse retrouver leur identité. Nous allons voir les pistes explorées et la solution que nous avons finalement gardé.

SHA256 : Au départ nous voulions utiliser SHA256 pour rendre illisible l'identité de l'agresseur. Nous partions du principe que nous pourrions comparer le haché de ces identités grâce au déterminisme de cette méthode. L'atout majeur de cette méthode est aussi la raison qui nous empêche de nous en servir. En effet, si chaque nom donné à SHA256 donne le même résultat, alors il suffira à une personne possédant la liste des gens présents à l'évènement cité dans le témoignages de hacher à son tour chacun de ces noms et de comparer à celui du témoignage.

Ce genre d'attaque est très courant, le principe de tester toutes les valeurs possibles s'appelle « L'attaque par brut force ». Il va donc nous falloir une autre méthode, non déterministe afin de les éviter.

6 Conclusion, perspectives et pistes d'amélioration

Pour conclure, nous avons un site fonctionnel, il ne manque que le moyen cryptographique pour le nom de l'agresseur et quelques optimisations pour que le site soit complet. Nous avons appris à utiliser Django et avons pu mettre en place ce que nous avons appris durant notre formation à l'université (Base de données, CSS, HTML, JS, Python, gestion de projet, et bien d'autres encore).

Amélioration des mails Pour le moment, les mails de mise en relation sont envoyés à la main par l'administrateur, une amélioration serait la rédaction et l'envoi automatique des mails.

Ajout de fonctionnalités Par la suite, nous prévoyons d'ajouter plus de fonctionnalités pour une bonne expérience utilisateur, comme par exemple une section pour des questions réponses, ou bien laisser des publics pour encourager les autres victimes à témoigner et à briser le silence.

Perspective Le site est facile à administrer, nous pouvons donc le confier à plusieurs universités qui voudraient se fournir le même service.