
Master thesis : Design and development of a distributed, secure and resilient vault management system

Auteur : Mathonet, Grégoire

Promoteur(s) : Leduc, Guy

Faculté : Faculté des Sciences appliquées

Diplôme : Master en sciences informatiques, à finalité spécialisée en "computer systems and networks"

Année académique : 2016-2017

URI/URL : <http://hdl.handle.net/2268.2/2602>

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.

Utilisation de Whigi Helios

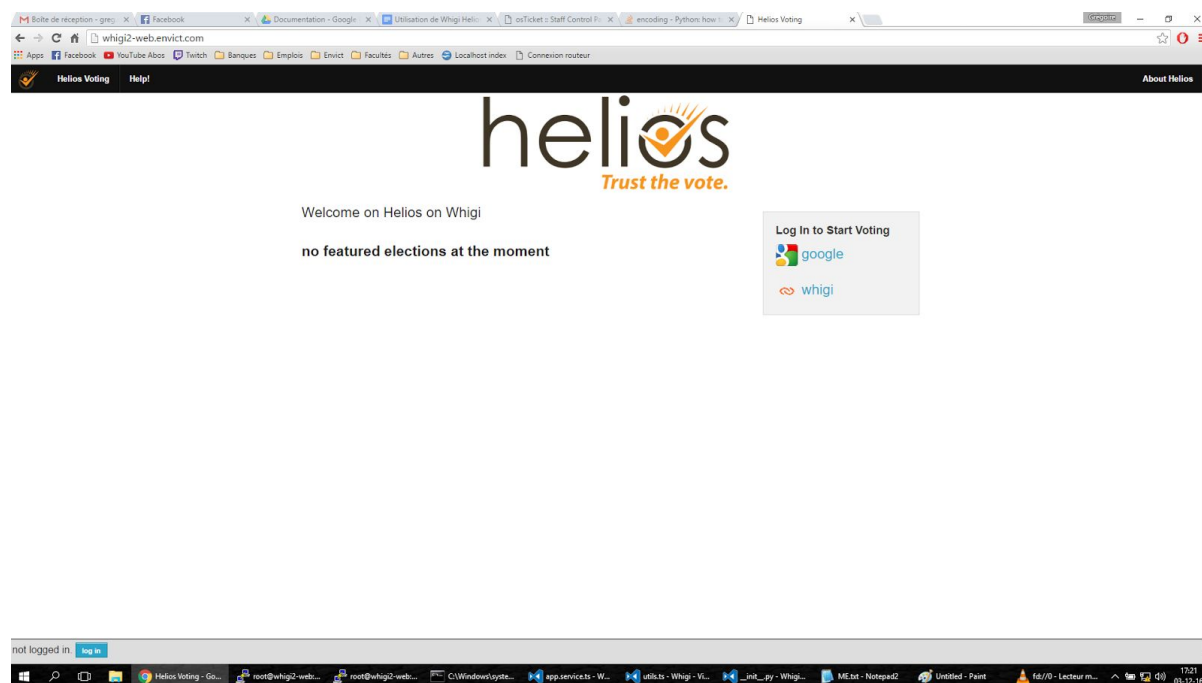
Whigi Helios permet d'utiliser des comptes Whigi pour se connecter, et de fournir une liste blanche de personnes autorisées à se connecter ainsi.

Une personne utilisant son compte Whigi pour se connecter est considéré comme utilisateur régulier par le système, et il se verra donné le droit de démarrer des votes seulement si c'est le cas de tous les utilisateurs réguliers.

Lors d'une élection, les gens qui votent ne sont pas des utilisateurs réguliers: ce sont des pseudo comptes identifiés uniquement par login / mot de passe, dont la validité n'est que celle de l'élection, et qui ne véhiculent aucune autre information (les votes sont anonymes!) Whigi donne alors ces informations par partage Whigi plutôt que par email. La plateforme envoie tout de même un mail, mais via Whigi. Il est alors aussi possible de définir un nombre de voix par utilisateurs, ce qui est plus pratique que d'utiliser une voix = un email.

Ce guide permet de visualiser tout le processus sur un exemple.

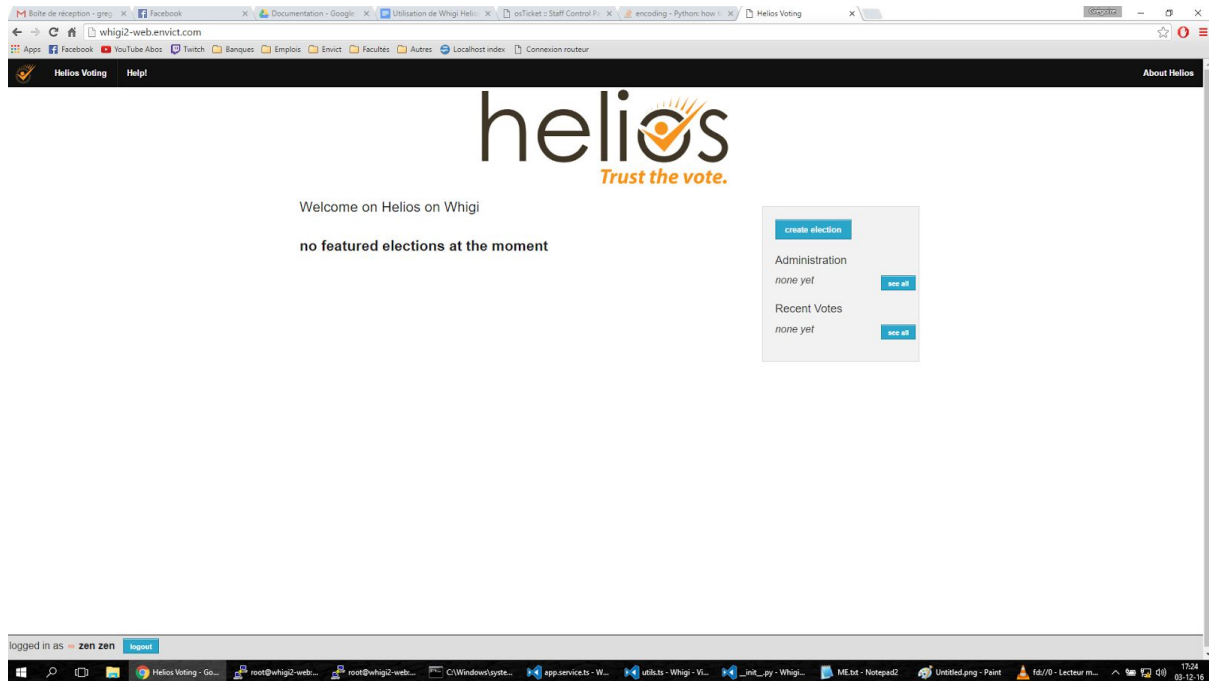
1. Connexion classique



Cliquez sur whigi pour une connexion directe par Whigi. Si vous n'avez pas l'option, c'est que le serveur est démarré sans cette option, auquel cas demandez à l'administrateur de l'activer.

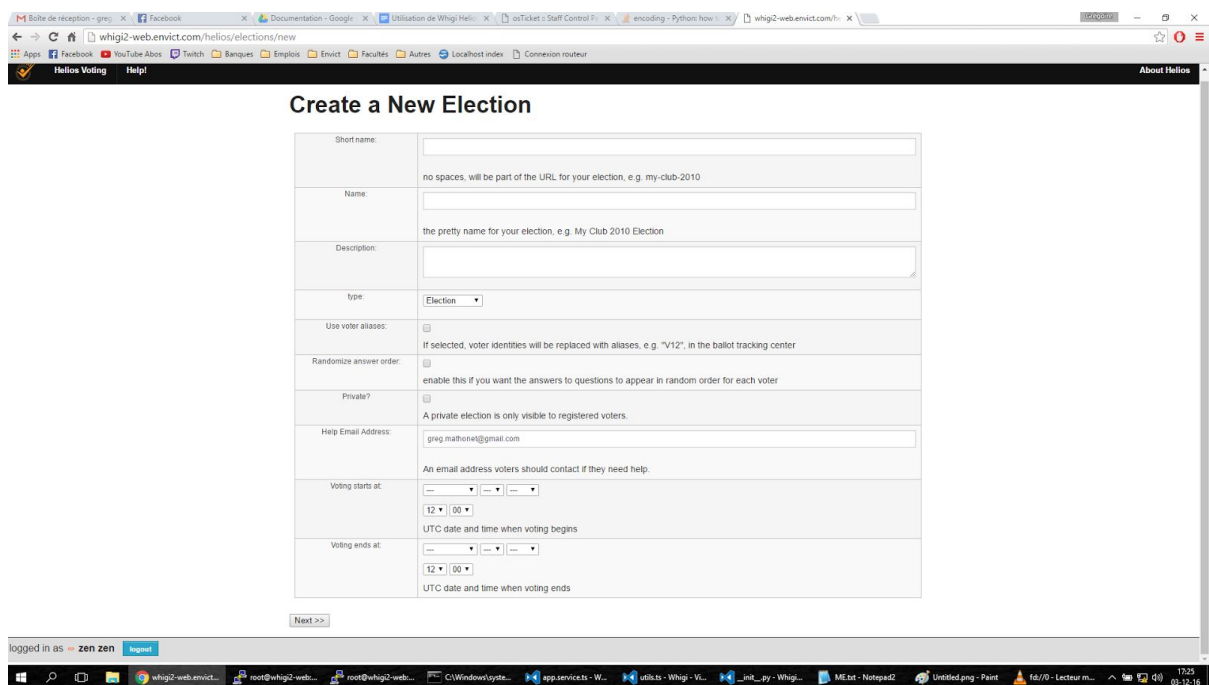
Il aura besoin d'un compte Whigi administrateur de référence, qui est le compte admin du site.

2. Création



Une fois connecté (vous devrez peut être entre temps vous connecter à Whigi et accepter un partage d'informations), vous arrivez sur l'écran de gestion, qui dans notre cas permet de créer une élection en cliquant sur "Create election". Si vous n'avez pas l'option, demandez à votre administrateur de vous la fournir.

3. Détails



Vous devez maintenant remplir quelques détails, tels que si l'élection est privée ou non (seulement des gens invités par vos soins peuvent voter avec des faux comptes comme expliqués ci dessus, ou tout compte, entier ou non, peut voter).
Rapportez vous à la documentation d'Helios pour plus d'information.

4. Questions & Trustees

Spécifiez les questions que vous voulez poser et les trustees pour la révélation (ne les modifiez pas à moins de bien savoir ce que vous faites). Ces interactions ne sont pas modifiées.

5. Votants

AG Decembre — Bulk Upload Voters [\[back to election\]](#)

If you would like to specify your list of voters by name and email address, or by Whigi accounts, you can bulk upload a list of such voters here. Please note that if you use Whigi accounts, you won't be able to email users afterwards. The benefit of using Whigi accounts is to be able to specify a weight for each user.

Please prepare a text file of comma-separated values with the fields:

```
<is_whigi:bool>,<unique_id>,<email>,<full name>
<is_whigi:true>,<whigi_username>,<num_voices>
```

For example:

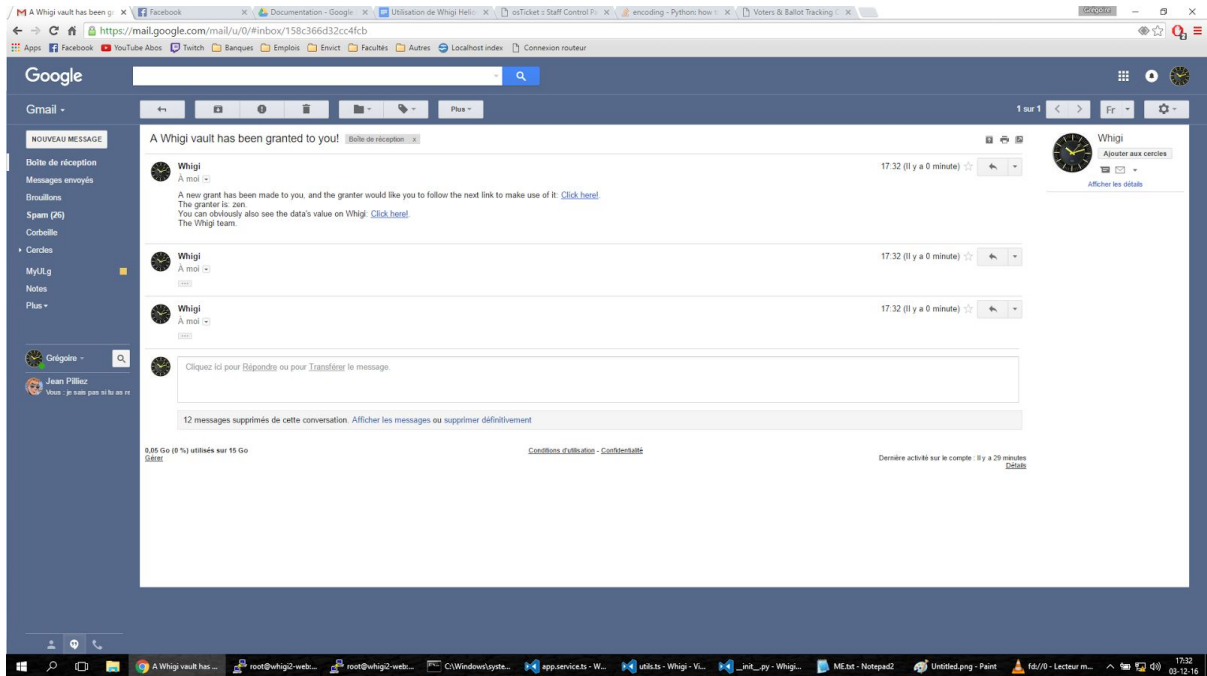
```
false,benadida,ben@adida.net,Ben Adida
true,bobsmith
...
```

The easiest way to prepare such a file is to use a spreadsheet program and to export as "CSV".

No file chosen

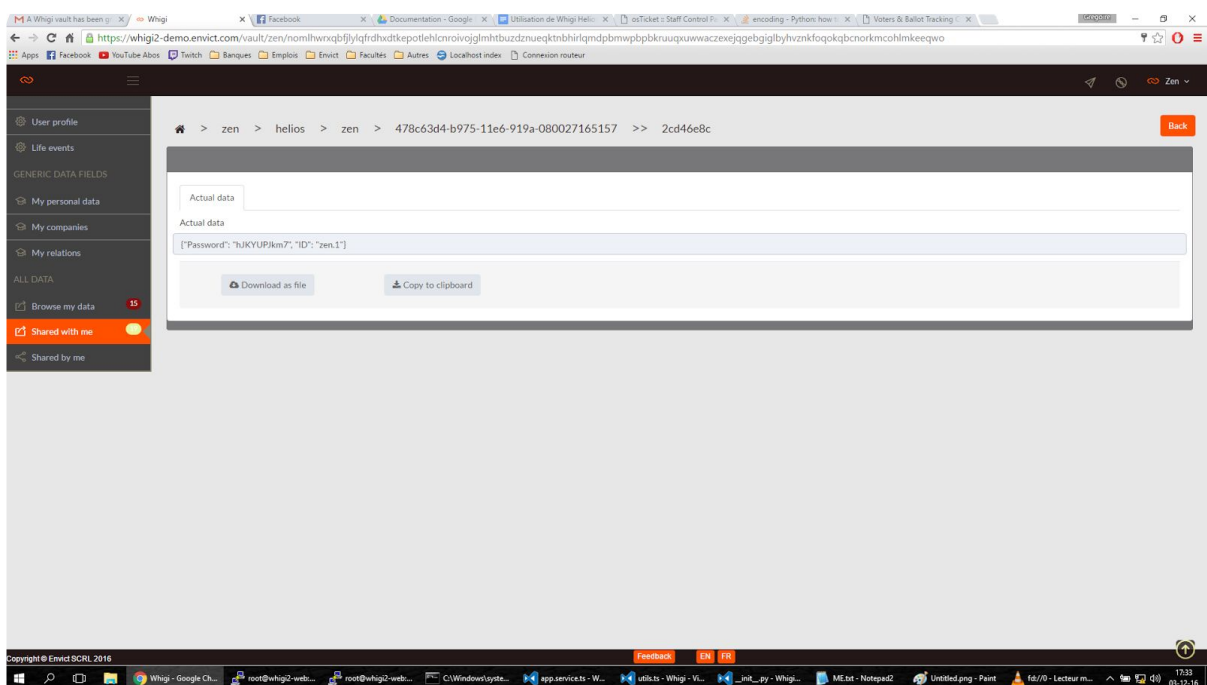
En cliquant sur "voters and ballots" puis sur "bulk upload voters", vous arriverez sur cet écran qui vous présente le choix entre les utilisateurs Whigi ou des utilisateurs classiques. Seuls les utilisateurs Whigi existants seront importés, vous ne pouvez créer de compte à la volée avec ses informations.
Choisissez votre fichier, vérifiez le résultat (si l'utilisateur a spécifié un nom public, vous le verrez alors), et validez. Maintenant, vous pouvez retourner sur votre tableau de bord, geler les questions, et démarrer le vote.

1'. Mail



Vos utilisateurs reçoivent alors un mail de ce type les invitant à se rendre sur votre élection avec les données qu'ils ont reçues dans Whigi. Ils peuvent donc recevoir plusieurs voix.

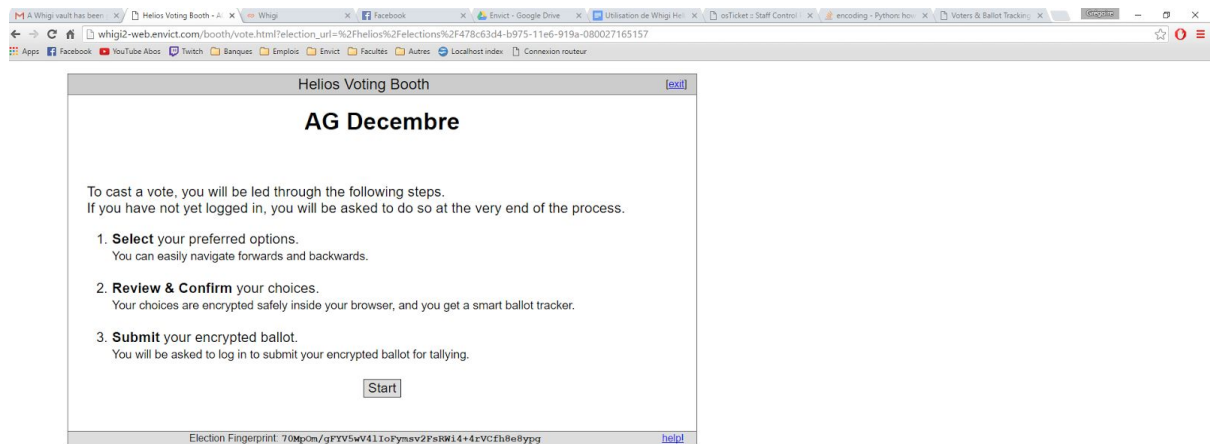
2'. Whigi



Le lien vers Whigi permet de voir son mot de passe et login pour ce vote. Le vote crée une sous classification dans l'arborescence des partages de sorte que l'utilisateur pourra toujours retrouver sa donnée.

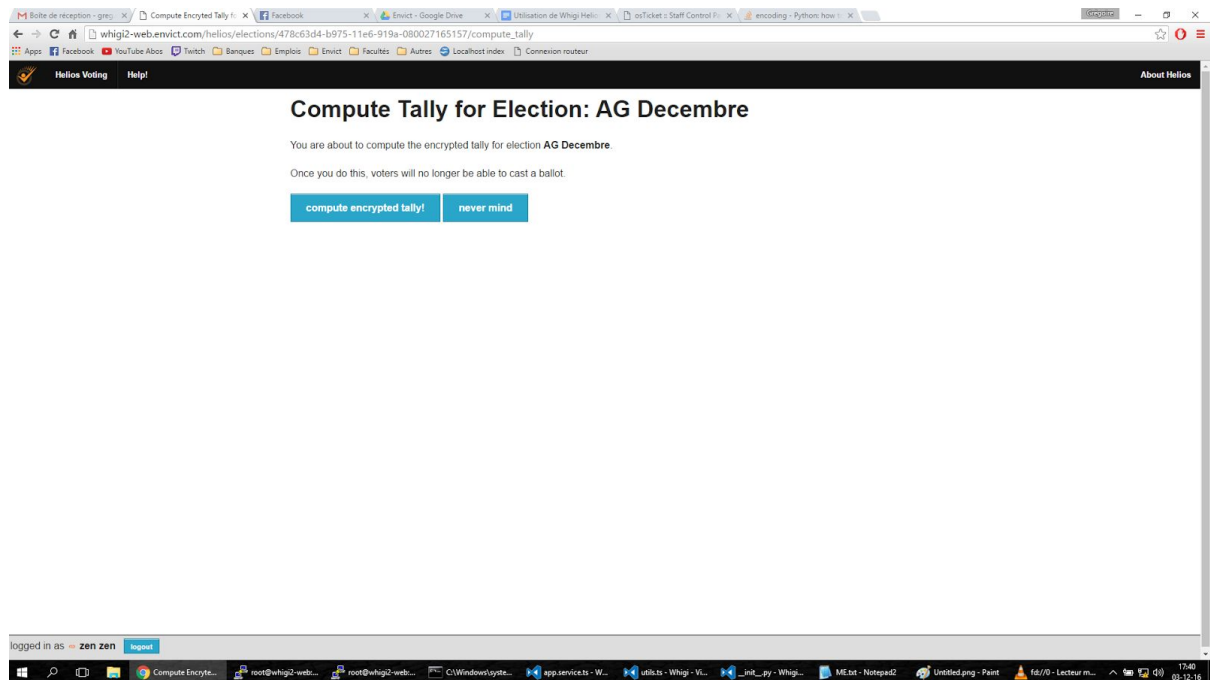
Ce partage est rendu invalide par le retrait de sa voix à un votant, ou l'archivage des résultats. Les partages sont alors révoqués.

3'. Vote

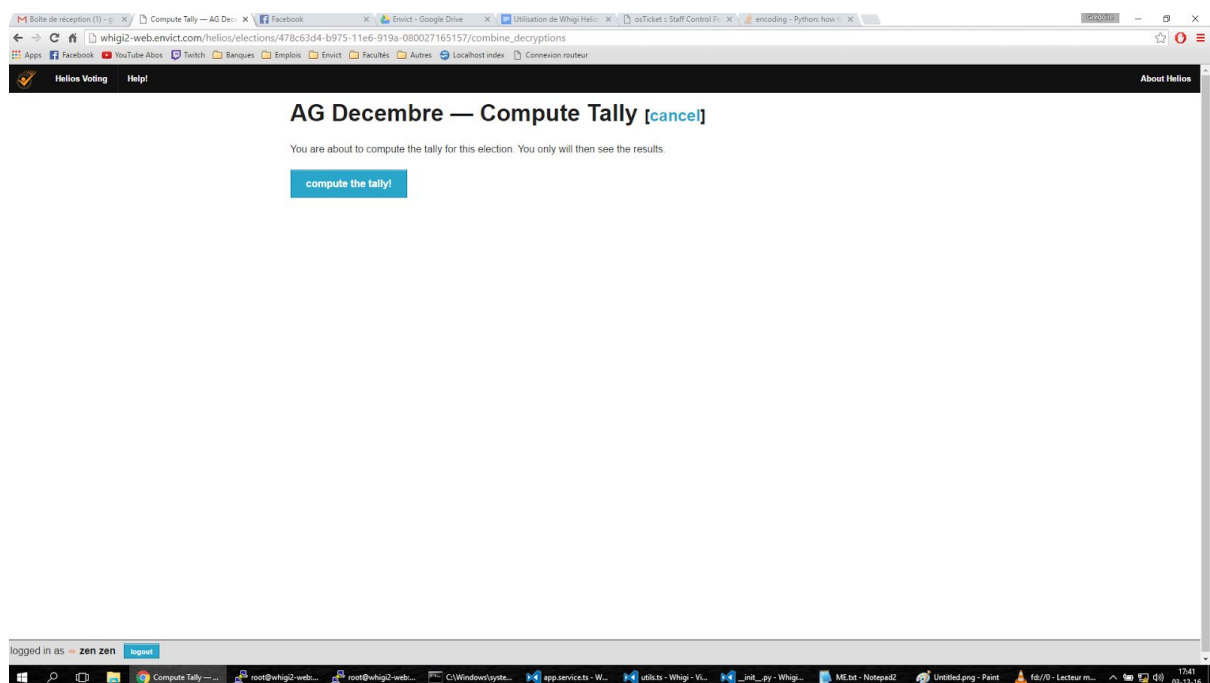


Après s'être connecté avec les infos reçues, vos utilisateurs sont alors confrontés une fois par voix à ce formulaire, totalement classique pour Helios. Vous n'avez plus qu'à attendre qu'ils l'aient tous validé.

6. Décryption et Résultats



Une fois que tout le monde a voté, que vous voulez arrêter le vote, ou que la date d'échéance est arrivée, vous pouvez combiner les votes ensemble. Cela est l'interface classique d'Helios pour l'admin du vote.



Dès que RSA a terminé son boulot, vous pouvez calculer les résultats et les afficher, puis éventuellement les partager.

Si vous les partagez, les login des comptes transitoires sont encore valides pour les voir, tant que vous n'archivez pas l'élection.

AG Decembre

private election created by [zen zen](#) [archive it](#)

[questions \(1\)](#) | [voters & ballots](#) | [trustees \(1\)](#)

Next Step: [release result](#)

The result displayed below is visible only to you.
Once you release the result, it will be visible to everyone.

Tally

Question #1

Accept ROI	
Yes	2
No	1

[Audit Info](#)