Epoll - Vote en ligne

FPW - 2009

Olivier Thauvin

12 juin 2009

Plan

Généralités

http ://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Généralités

http ://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Est-ce bien ?

- Impossibilité de contrôle par l'électeur (voir la commission électorale)

Généralités

http ://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Est-ce bien ?

- Impossibilité de contrôle par l'électeur (voir la commission électorale)
  - techniquement compliqué

Généralités

http ://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Est-ce bien ?

- Impossibilité de contrôle par l'électeur (voir la commission électorale)
  - techniquement compliqué
  - logiciel souvent opaque

Généralités

http ://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Est-ce bien ?

- Impossibilité de contrôle par l'électeur (voir la commission électorale)
  - techniquement compliqué
  - logiciel souvent opaque
  - contrôle visuel impossible

Généralités

http ://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Est-ce bien ?

- Impossibilité de contrôle par l'électeur (voir la commission électorale)
  - techniquement compliqué
  - logiciel souvent opaque
  - contrôle visuel impossible
- le syndrome "L'ordinateur ne se trompe jamais"

Généralités

http ://fr.wikipedia.org/wiki/Vote_électronique

Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques.

Est-ce bien ?

- Impossibilité de contrôle par l'électeur (voir la commission électorale)
  - techniquement compliqué
  - logiciel souvent opaque
  - contrôle visuel impossible
- le syndrome "L'ordinateur ne se trompe jamais"

Références

- http://www.ordinateurs-de-vote.org/
- http://www.cnil.fr/

Plan

Contexte

LATMOS

- Laboratoire CNRS

Contexte

LATMOS

- Laboratoire CNRS
- Laboratoire Atmosphères, Milieux, Observation Spatiales

Contexte

LATMOS

- Laboratoire CNRS
- Laboratoire Atmosphères, Milieux, Observation Spatiales
- Environ 300 personnes

Contexte

LATMOS

- Laboratoire CNRS
- Laboratoire Atmosphères, Milieux, Observation Spatiales
- Environ 300 personnes
- 4 sites (Verrières le Buisson, Vélizy, Paris et St Maur)

Contexte

LATMOS

- Laboratoire CNRS
- Laboratoire Atmosphères, Milieux, Observation Spatiales
- Environ 300 personnes
- 4 sites (Verrières le Buisson, Vélizy, Paris et St Maur)

CL

- Conseil de laboratoire
- 3 membres de droits
- 10 membres élus parmis les personnels
- des personnels invités

Pourquoi ?

Le LATMOS

Demande de vote électronique de la direction

Pourquoi ?

Le LATMOS

Demande de vote électronique de la direction

Logiciel libre

Rien de bien satisfaisant

Pourquoi ?

Le LATMOS

Demande de vote électronique de la direction

Logiciel libre

Rien de bien satisfaisant

solutions payantes

Entre 1500 et 5000 euros

Pourquoi ?

Le LATMOS

Demande de vote électronique de la direction

Logiciel libre

Rien de bien satisfaisant

solutions payantes

Entre 1500 et 5000 euros

Sujet intéressant

Surtout quand il me donne des arguments contre

Résumé

Application web

Résumé

Application web

- accessible avec un simple navigateur

Résumé

Application web

- accessible avec un simple navigateur
- envoi des identifiants par mail

Résumé

Application web

- accessible avec un simple navigateur
- envoi des identifiants par mail
- pas d'intervention de l'administrateur

Résumé

Application web

- accessible avec un simple navigateur
- envoi des identifiants par mail
- pas d'intervention de l'administrateur

Les fondations

- Perl (http://www.perl.org/)
- Catalyst (http://www.catalystframework.org/)

Résumé

Application web

- accessible avec un simple navigateur
- envoi des identifiants par mail
- pas d'intervention de l'administrateur

Les fondations

- Perl (http://www.perl.org/)
- Catalyst (http://www.catalystframework.org/)
- PostgreSQL (http://www.postgresql.org)

Plan

Création du vote

La commission électorale

1. demande de création

Création du vote

La commission électorale

1. demande de création
2. confirmation de la demande (par mail)

Création du vote

La commission électorale

1. demande de création
2. confirmation de la demande (par mail)
3. configuration du vote (dont date début/fin)

Création du vote

La commission électorale

1. demande de création
2. confirmation de la demande (par mail)
3. configuration du vote (dont date début/fin)
4. inscription des électeurs

Création du vote

La commission électorale

1. demande de création
2. confirmation de la demande (par mail)
3. configuration du vote (dont date début/fin)
4. inscription des électeurs
5. envois des identifiants au électeurs

Le vote

Les électeurs

1. réception du mail avec url, login et mot de passe

Le vote

Les électeurs

1. réception du mail avec url, login et mot de passe
2. authentification sur le site

Le vote

Les électeurs

1. réception du mail avec url, login et mot de passe
2. authentification sur le site
3. choix

Le vote

Les électeurs

1. réception du mail avec url, login et mot de passe
2. authentification sur le site
3. choix
4. confirmation des choix

Le vote

Les électeurs

1. réception du mail avec url, login et mot de passe
2. authentification sur le site
3. choix
4. confirmation des choix
5. affichage du numéro du bulletin

Le vote

Les électeurs

1. réception du mail avec url, login et mot de passe
2. authentification sur le site
3. choix
4. confirmation des choix
5. affichage du numéro du bulletin
6. réception d'un accusé de réception par mail

Le dépouillement

La commission électorale

1. consolidation des choix libres si besoin

Le dépouillement

La commission électorale

1. consolidation des choix libres si besoin
2. marquage des bulletins invalides

Le dépouillement

La commission électorale

1. consolidation des choix libres si besoin
2. marquage des bulletins invalides

Dès la fin du vote

- Les résultats (provisoires) sont disponibles
- La liste de bulletins est disponible

Anonymat

stockage

Pas de relation entre l'électeur et le bulletin

Anonymat

stockage

Pas de relation entre l'électeur et le bulletin

Émargement

Mail	IP	heure de vote
thauvin@latmos.ipsl.fr	134.157.16.151	2009-03-19 15:31:56

Anonymat

stockage

Pas de relation entre l'électeur et le bulletin

Émargement

Mail	IP	heure de vote
thauvin@latmos.ipsl.fr	134.157.16.151	2009-03-19 15:31:56

Le bulletin

Id	Contenu
f4f667c78a2178095c3bae4d	oui

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible
- *crypt* UNIX MD5

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible
- *crypt* UNIX MD5
- mot de passe aléatoire (électeurs)

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible
- *crypt* UNIX MD5
- mot de passe aléatoire (électeurs)
- *salt* aléatoire

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible
- *crypt* UNIX MD5
- mot de passe aléatoire (électeurs)
- *salt* aléatoire

Stockage des mots de passe

En clair :

`password`

Version chiffrée :

`$1$aqsedfrt$sxdgVrlCwHx6VdBpRAx6m1`

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible
- ne peut être retrouvé

Stockage des mots de passe

En clair :

`password`

Version chiffrée :

`$1$aqsedfrt$sxdgVrlCwHx6VdBpRAx6m1`

Les mots de passe

Méthode utilisée

- chiffré de manière irréversible
- ne peut être retrouvé
- méthode fiable

Stockage des mots de passe

En clair :

`password`

Version chiffrée :

`$1$aqsedfrt$sxdgVrlCwHx6VdBpRAx6m1`

Éviter les tricheries

Côté base de données

Éviter les tricheries

Côté base de données

- le vote est transactionnel (tout ou rien)

Éviter les tricheries

Côté base de données

- le vote est transactionnel (tout ou rien)
- contraintes référentielles

Éviter les tricheries

Côté base de données

- le vote est transactionnel (tout ou rien)
- contraintes référentielles

Contrôle par l'utilisateur

- nombre de votants et nombre de bulletins disponibles

Éviter les tricheries

Côté base de données

- le vote est transactionnel (tout ou rien)
- contraintes référentielles

Contrôle par l'utilisateur

- nombre de votants et nombre de bulletins disponibles
- liste d'émargement disponible

Éviter les tricheries

Côté base de données

- le vote est transactionnel (tout ou rien)
- contraintes référentielles

Contrôle par l'utilisateur

- nombre de votants et nombre de bulletins disponibles
- liste d'émargement disponible
- liste des bulletins disponible dès la fin du vote

Les problèmes

Les problèmes

Le Mail

- n'est pas chiffré

Les problèmes

Le Mail

- n'est pas chiffré
- est interceptable

Les problèmes

Le Mail

- n'est pas chiffré
- est interceptable

La base de données

Les problèmes

Le Mail

- n'est pas chiffré
- est interceptable

La base de données

- lecture : accès aux résultats avant la fin du vote

Les problèmes

Le Mail

- n'est pas chiffré
- est interceptable

La base de données

- lecture : accès aux résultats avant la fin du vote
- écriture : modification des résultats (mais cela devrait se voir)

Les problèmes

Le Mail

- n'est pas chiffré
- est interceptable

La base de données

- lecture : accès aux résultats avant la fin du vote
- écriture : modification des résultats (mais cela devrait se voir)

L'application elle même

S'assurer de l'intégrité du code

Bilan

Est-ce parfait ?

Bilan

Est-ce parfait ?

Bien sûr

Bilan

Est-ce parfait ?

Bien sûr

des bogues ?

Bilan

Est-ce parfait ?

Bien sûr

des bogues ?

Aucun !

Bilan

Est-ce parfait ?

Plein de choses sont à revoir :

- la partie validation du vote

des bogues ?

Bilan

Est-ce parfait ?

Plein de choses sont à revoir :

- la partie validation du vote
- certaines parties du code devraient être plus robustes

des bogues ?

Bilan

Est-ce parfait ?

Plein de choses sont à revoir :

- la partie validation du vote
- certaines parties du code devraient être plus robustes
- des validations des données à ajouter
- ...

des bogues ?

Bilan

Est-ce parfait ?

Plein de choses sont à revoir :

- la partie validation du vote
- certaines parties du code devraient être plus robustes
- des validations des données à ajouter
- ...

des bogues ?

Pas de connu à ce jour pour cette version.

Bilan

Est-ce parfait ?

Plein de choses sont à revoir :

- la partie validation du vote
- certaines parties du code devraient être plus robustes
- des validations des données à ajouter
- ...

des bogues ?

Pas de connu à ce jour pour cette version.

Promesse :

Avoir quelque chose à proposer pour le vote du CL (en 15 jours)

Plan

Référence : la CNIL

Essayer d'appliquer :

Délibération n. 03-036 du 1er juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.

CNIL : Verrouillage de l'urne

L'ouverture devrait necessiter plusieurs personnes

- l'application peut demander plusieurs mot de passe
- pas de solution fiable au niveau des données

CNIL : Chiffrement

Données en clair dans la base

- Le gestionnaire SQL y a accès
- Elles sont des les backup

CNIL : Chiffrement

Données en clair dans la base

- Le gestionnaire SQL y a accès
- Elles sont des les backup

Chiffrer les bulletins

- chiffrer...
  Opérationnel pour la prochaine version
  - Clef asymétrique pour le vote
  - Bulletins chiffré avec clef symétrique aléatoire
  - Clef des bulletins chiffré avec clef du vote

CNIL : Chiffrement

Données en clair dans la base

- Le gestionnaire SQL y a accès
- Elles sont des les backup

Chiffrer les bulletins

- chiffrer...
  Opérationnel pour la prochaine version
  - Clef asymétrique pour le vote
  - Bulletins chiffré avec clef symétrique aléatoire
  - Clef des bulletins chiffré avec clef du vote
- ...sur le poste du votant
  Pb : comment supporter les différents OS ?
  - javascript ? applet java ?
  - application sur le poste + XML/RPC ?

Somme de contrôle de l'application

La CNIL dit :

"L'application doit effectuer une somme de contrôle de son code"

Somme de contrôle de l'application

La CNIL dit :

"L'application doit effectuer une somme de contrôle de son code"

Ma réponse :

- l'appli se contrôle elle même ? !

Somme de contrôle de l'application

La CNIL dit :

"L'application doit effectuer une somme de contrôle de son code"

Ma réponse :

- l'appli se contrôle elle même ? !

```
sub check { print "Cheksum OK: " .
    "17ca809b185d59563d8776bac260c4b6\n" }
```

Somme de contrôle de l'application

La CNIL dit :

"L'application doit effectuer une somme de contrôle de son code"

Ma réponse :

- l'appli se contrôle elle même ? !

```
sub check { print "Cheksum OK: " .
    "17ca809b185d59563d8776bac260c4b6\n" }
```

- les gestionnaires de paquets le font (`rpm`, `dpkg`, ...)

Somme de contrôle de l'application

La CNIL dit :

"L'application doit effectuer une somme de contrôle de son code"

Ma réponse :

- l'appli se contrôle elle même ? !

```
sub check { print "Cheksum OK: " .
    "17ca809b185d59563d8776bac260c4b6\n" }
```

- les gestionnaires de paquets le font (`rpm`, `dpkg`, ...)
- il faudrait aussi controler :
  - `perl` + les modules utilisés
  - le SGDB
  - le système (kernel, programmes, ...)

Idées

Idées

- pouvoir changer son vote
  - est-ce raisonnable ?
  - il faut retrouver l'ancien bulletin

Idées

- pouvoir changer son vote
  - est-ce raisonnable ?
  - il faut retrouver l'ancien bulletin
- support de plusieurs langues (i18n)

Idées

- pouvoir changer son vote
  - est-ce raisonnable ?
  - il faut retrouver l'ancien bulletin
- support de plusieurs langues (i18n)
- rendre un vote privé

Idées

- pouvoir changer son vote
  - est-ce raisonnable ?
  - il faut retrouver l'ancien bulletin
- support de plusieurs langues (i18n)
- rendre un vote privé
- votes non anonymes

Idées

- pouvoir changer son vote
  - est-ce raisonnable ?
  - il faut retrouver l'ancien bulletin
- support de plusieurs langues (i18n)
- rendre un vote privé
- votes non anonymes
- pouvoir redemander un mot de passe (électeurs)

Idées

- pouvoir changer son vote
  - est-ce raisonnable ?
  - il faut retrouver l'ancien bulletin
- support de plusieurs langues (i18n)
- rendre un vote privé
- votes non anonymes
- pouvoir redemander un mot de passe (électeurs)
- sortie imprimable des résultats
  Fait : sortie en `pdf` avec LaTeX.

Idées

- pouvoir changer son vote
  - est-ce raisonnable ?
  - il faut retrouver l'ancien bulletin
- support de plusieurs langues (i18n)
- rendre un vote privé
- votes non anonymes
- pouvoir redemander un mot de passe (électeurs)
- sortie imprimable des résultats
  Fait : sortie en `pdf` avec LaTeX.
- redondance des données (CNIL)

Idées

- pouvoir changer son vote
  - est-ce raisonnable ?
  - il faut retrouver l'ancien bulletin
- support de plusieurs langues (i18n)
- rendre un vote privé
- votes non anonymes
- pouvoir redemander un mot de passe (électeurs)
- sortie imprimable des résultats
  Fait : sortie en `pdf` avec LaTeX.
- redondance des données (CNIL)
- ...

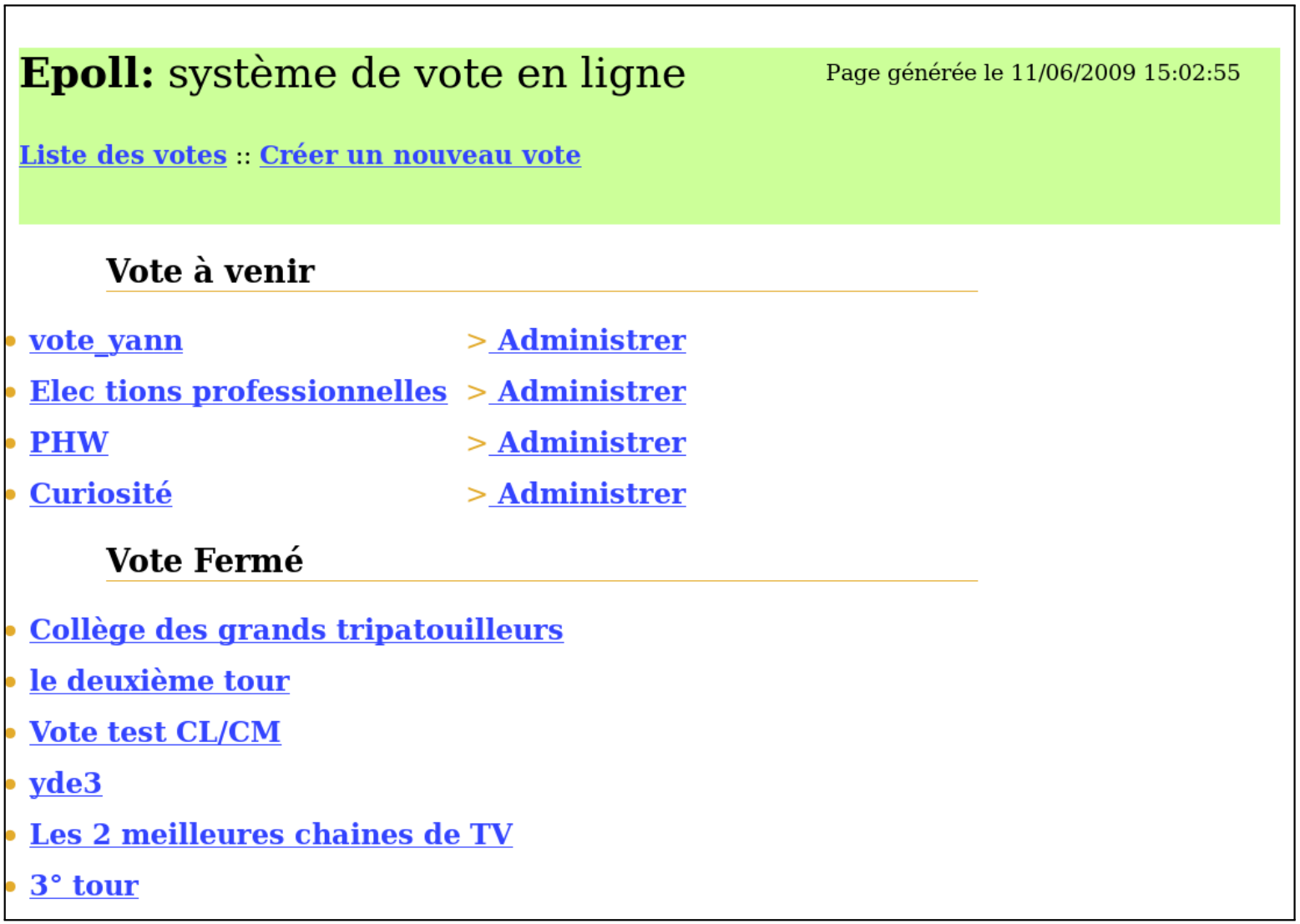
Plan

Tester en live :

La démo

http://forge.ipsl.jussieu.fr/epoll/demo

Page principale



Epoll: système de vote en ligne

Page générée le 11/06/2009 15:02:55

Liste des votes :: Créer un nouveau vote

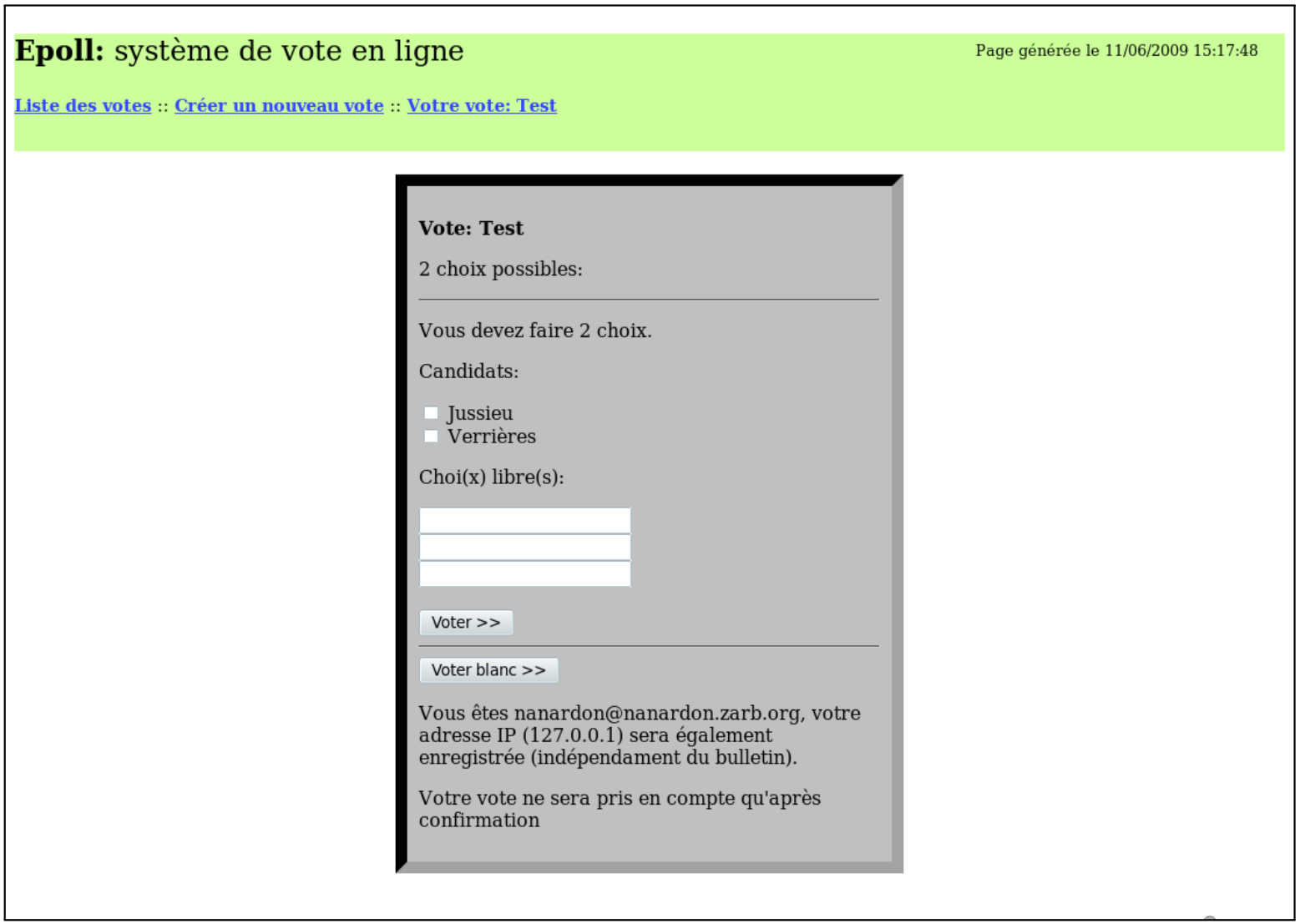
Vote à venir

- vote_yann > Administrer
- Elec tions professionnelles > Administrer
- PHW > Administrer
- Curiosité > Administrer

Vote Fermé

- Collège des grands tripatouilleurs
- le deuxième tour
- Vote test CL/CM
- yde3
- Les 2 meilleures chaines de TV
- 3° tour

Le vote


Epoll: système de vote en ligne
Page générée le 11/06/2009 15:17:48
Liste des votes :: Créer un nouveau vote :: Votre vote: Test
Vote: Test
2 choix possibles:
Vous devez faire 2 choix.
Candidats:
Jussieu
Verrières
Choi(x) libre(s):
Voter >>
Voter blanc >>
Vous êtes nanardon@nanardon.zarb.org, votre adresse IP (127.0.0.1) sera également enregistrée (indépendamment du bulletin).
Votre vote ne sera pris en compte qu'après confirmation

Présentation des résultats

Epoll: système de vote en ligne

Page générée le 11/06/2009 15:08:15

Liste des votes :: Créer un nouveau vote :: Votre vote: Les 2 meilleures chaines de TV

Administrer

Les 2 meilleures chaines de TV

Scrutin ouvert du **26/03/2009 11:30:00** au **26/03/2009 11:40:00**

Ont voté: 5 / 6
Bulletins: 5

Bulletin:

1. Arte
2. France 5
3. Game One
4. M6

Resultats:

Nombre de choix à retenir: 2

Participations: 5 / 6 (83.33)

Nombre de vote(s) exprimé(s): 3 (60.00%)

Score:

Légende:	Majorité Absolue	Elus	Non élu

Score	Ligne N°	choix	Nb voix	%	
1	1	Arte	3	100.00	
2	2	eurosport	1	33.33	
2	3	tf1	1	33.33	

Lites des bulletins

Liste des bulletins:

numéro	Id	contenu (=> corrigé en) (*: hors liste)	remarque
1	1504e9e7db4763025da4d2ad50268782	• tf1 * • banane *	Invalidé
2	4b840a247d6bda3b9978a992f5ed1d34	• Arte • %tf* * (=> tf1)	
3	6794de3c1c6930702e71740eefa91d66	• Arte • eurosport *	
4	6dd767e2b99c1e4647dc317fe721f8cd	• Arte	
5	9b16048eb3c34a84bff824b4d5007ee4	• France 5 • candidat 1 *	Invalidé

Liste des votants:

Numéro	Electeur	Emargement
1	christian dot malique at aerov dot jussieu dot fr	A voté
2	christian dot malique at latmos dot ipsl dot fr	
3	francis dot dalaudier at aerov dot jussieu dot fr	A voté
4	francis dot vivat at latmos dot ipsl dot fr	A voté
5	philippe dot weill at aero dot jussieu dot fr	A voté
6	yann dot delcambre at aerov dot jussieu dot fr	A voté

Epoll 1.01 POWERED BY catalyst

Plan

Les modules PERL utilisés

Base de données

- `DBI`
- `DBD::Pg`

Les modules PERL utilisés

Base de données

- `DBI`
- `DBD::Pg`

Cryptographie

- `Crypt::RSA`
- `Crypt::DES`
- `XML::Simple` (format d'archivage)

Les modules PERL utilisés

Base de données

- `DBI`
- `DBD::Pg`

Cryptographie

- `Crypt::RSA`
- `Crypt::DES`
- `XML::Simple` (format d'archivage)

WEB / Mail

- `Catalyst` (`Template Toolkit`, `C::P::Session`)
- `LaTeX::Driver`
- `Mail::Mailer`

Les modules PERL utilisés

Base de données

- `DBI`
- `DBD::Pg`

Cryptographie

- `Crypt::RSA`
- `Crypt::DES`
- `XML::Simple` (format d'archivage)

WEB / Mail

- `Catalyst` (`Template Toolkit`, `C::P::Session`)
- `LaTeX::Driver`
- `Mail::Mailer`

Questions et remarques

Le projet

http://forge.ipsl.jussieu.fr/epoll:

- le code
- la documentation
- lien vers la liste de diffusion
- le lien vers la démo

Questions et remarques

Le projet

http://forge.ipsl.jussieu.fr/epoll:

- le code
- la documentation
- lien vers la liste de diffusion
- le lien vers la démo

Avez-vous :

- des questions ?
- des remarques ?
- des critiques ?