Candidats.fr / Pacte du Logiciel Libre législatives 2017 - Anomalie #3146

Tentative d'attaque sur la page https://campagnes.candidats.fr/legislatives2017/

10/05/2018 09:36 - Christian P. Momon

Statut:	Fermé	**Début:**	10/05/2018
Priorité:	Normale	**Echéance:**	
Assigné à:	Christian P. Momon	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:			

Description

Depuis 2 ou 3 semaines, des lots de centaines d'erreurs sont notifiées par courriel :

Error : The used SELECT statements have a different number of columns
Post : array (
)
[…]
Get : array (
'action' => 'liste_candidats',
'departement' => '-9064\' UNION ALL SELECT
5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,58
22,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,
5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,58
22,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,5822,
5822,5822,5822,5822,5822,5822,5822,5822,5822,5822#',
)
[…]
'QUERY_STRING' =>
'action=liste_candidats&departement=-9064%27%20UNION%20ALL%20SELECT%205822%2C5822%2C5822%2C5822%2C5
822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C
5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2
C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%
2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822
%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C582
2%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C58
22%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5822%2C5
822%2C5822%2C5822%2C5822%2C5822%23',

Ça sent la tentative d'attaque par injection SQL.

Historique

#1 - 10/05/2018 10:09 - Christian P. Momon

- Statut changé de Nouveau à Résolu

J'ai neutralisé le point d'attaque avec le code suivant :

```
if (!ctype_digit($args['departement'])) {
croak ('Bad departement parameter.');
}
```

#2 - 24/05/2020 12:39 - Christian P. Momon

- Statut changé de Résolu à Fermé

- Assigné à mis à Christian P. Momon