La faille

Koné, Gorlt, Heyd, Contal

Description

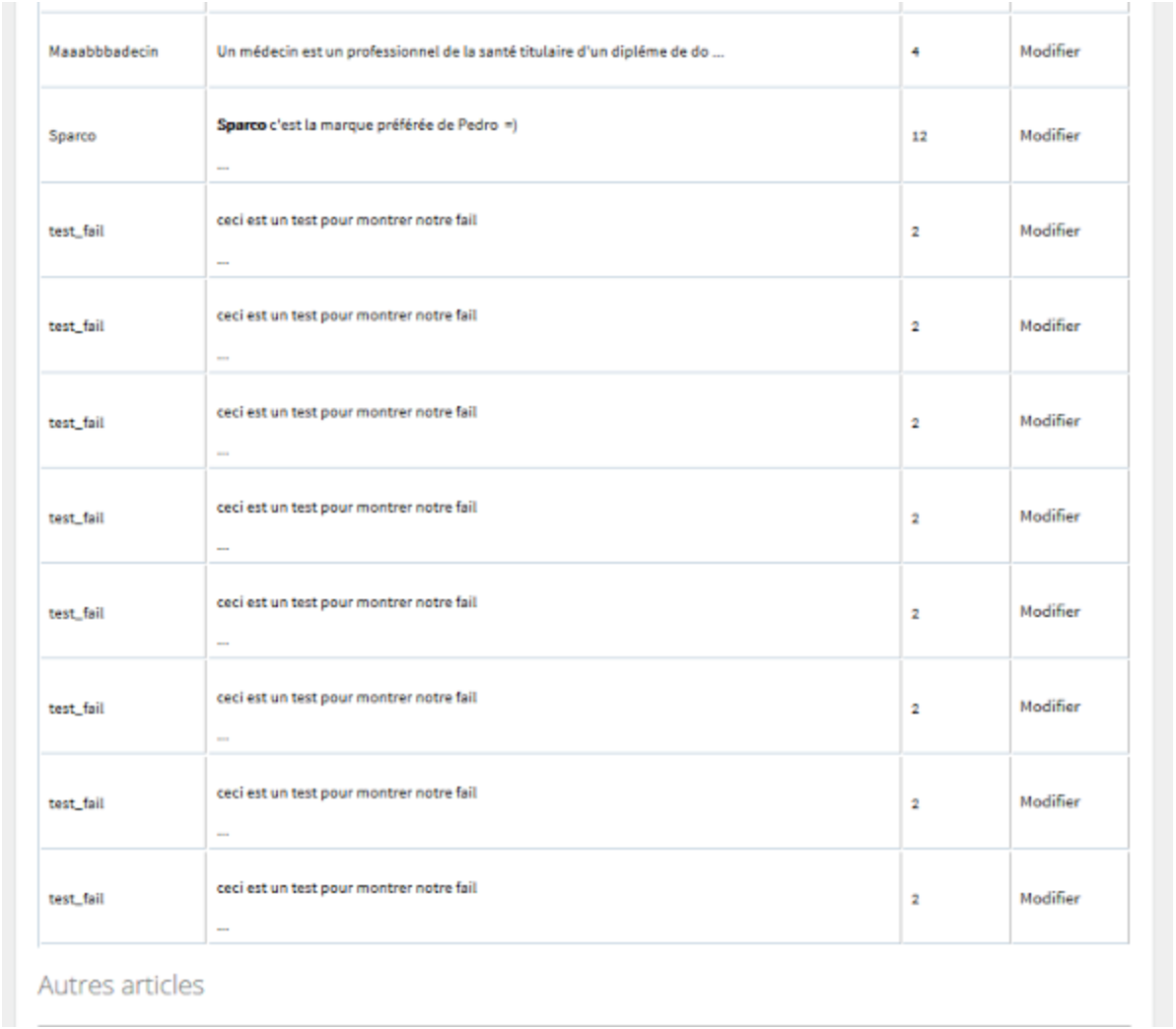
Nous pouvons affirmer, sans capilotraction[1], que la faille se situe dans une des pages les plus fréquentées par les utilisateurs : celle de **sauvegarde de modifications d'un article** (ou de création).

Elle consiste à peupler (jusqu'à l'infini) la table **Article** en effectuant des **rafraîchissements** en boucle lors de l'affichage du message de validation de la sauvegarde.

Afin d'accéder à cette page, il suffit à l'utilisateur de cliquer sur le bouton "**Sauvegarder**". S'affiche alors un message de confirmation ainsi qu'un "loader" signifiant à l'utilisateur qu'il va être redirigé. Il lui suffit d'appuyer sur F5 afin de découvrir la faille : la page se rafraîchit et apparaît de nouveau le message de confirmation : une nouvelle occurrence est alors créée !

[1] action de tirer par les cheveux

L’utilisateur peut alors voir que la faille est bien présente en retournant sur le **dashboard** : on peut alors voir que la liste est alors remplie de doublons d’articles :



Maaabbbadecin	Un médecin est un professionnel de la santé titulaire d'un dipléme de do ...	4	Modifier
Sparco	**Sparco** c'est la marque préférée de Pedro =) ...	12	Modifier
test_fail	ceci est un test pour montrer notre fail ...	2	Modifier
test_fail	ceci est un test pour montrer notre fail ...	2	Modifier
test_fail	ceci est un test pour montrer notre fail ...	2	Modifier
test_fail	ceci est un test pour montrer notre fail ...	2	Modifier
test_fail	ceci est un test pour montrer notre fail ...	2	Modifier
test_fail	ceci est un test pour montrer notre fail ...	2	Modifier
test_fail	ceci est un test pour montrer notre fail ...	2	Modifier
test_fail	ceci est un test pour montrer notre fail ...	2	Modifier

Autres articles

On voit d’ailleurs que les numéros de version ne sont pas incrémentés.

Origine et correction

Sur les sites web, on remarque que les failles les plus basiques viennent d'IDs erronés ou lors d'insertion de données. Ici, nous avons choisi de mettre en avant le processus d'écriture en base de données en laissant libre la démultiplication de données lors de la sauvegarde.

Cette faille est dû à la complexité du code de la page d'édition d'articles : en effet, il est possible depuis cette page de **créer** ou de **modifier** un article, ce qui impose des paramètres différents. Pour un développeur, il est tout à fait possible de mettre en place cette faille, de manière volontaire ou non, et bien souvent, par incurie[2].

Dans notre cas, afin de s'embosser[3] de cette faille, nous pouvons modifier le code de façon à ce qu'une vérification supplémentaire des paramètres passés dans la variable POST se fasse.

[2] manque de soin
[3] se protéger