

# Write-up du challenge d'OSINT "Web et amie"

## Énoncé

J'ai envoyé mon livre (un petit recueil de poèmes de mes pensées) à une bonne amie mais elle ne l'a jamais reçu. J'ai entendu des rumeurs d'un flag caché aux tréfonds du Web. Je veux bien ce flag.

Signé le créateur du challenge, Richard Dufour

## Solution

Étant donné qu'on n'a pas de fichier, il va falloir jouer aux devinettes avec ce qu'on a. On a trois informations principales pour débiter les recherches : le nom "Richard Dufour", le fait que son livre soit un recueil de poèmes et le fait qu'il a une amie qui interviendra probablement au cours de nos recherches.

On commence par un dorking classique sur Google avec par exemple "Richard Dufour" mais c'est un nom courant, on ajoute alors des mots comme "poèmes" ou "recueil de poèmes" et on tombe sur le livre de Richard qui est "Pensées instantanées".

Notre site internet utilise des cookies pour mémoriser vos préférences de navigation et réaliser des statistiques de visites. En poursuivant votre navigation, vous en acceptez l'utilisation. [Pour en savoir plus et paramétrer cliquez-ici.](#) [J'accepte](#)

Aide 05 57 411 411 Envoi sous 48h Paiement sécurisé Suivi de commande

**le-livre.fr**  
la boutique du village du livre

Toutes collections Rechercher un livre, un auteur ... Se connecter S'inscrire

Home » Livres » Généralités » Livres rares » Dédicace, envoi » Dédicace, envoi

Achetez cet article issu de nos Livres  
**Pensées instantanées + envoi de l'auteur**

Auteur	: Richard dufour - pauline renoire (illustrations)	Référence	: RO20255848
Editeur	: CHEZ L'AUTEUR	ISBN 10	: 2958361616
Impression	: 2023	ISBN 13	: 978-8-2958-3616-1
Etat	: Bon état	EAN 13	: 9782958361617
Disponibilité	: 1 en stock	Classement Dewey	: 97.2
		Fiche créée le	: 07/12/2023

Prix : 29,80 €

Description  
CHEZ L'AUTEUR. 2023. In-8. Broché. Bon état, Couv.... [Plus d'informations.](#)

Acheter cet article  
**29,80 €**  
[Ajouter au panier](#)

Satisfait ou remboursé 14 jours pour changer d'avis Envoi sous 48h Expédition du Lundi au Vendredi, toute l'année. Paiement à l'expédition Le montant de votre achat est prélevé à l'expédition Support chat ou téléphone Discuter avec des experts ou vous appeler immédiatement

En stock du même auteur

Chat

On remarque que Richard était en collaboration avec une illustratrice "Pauline RENOIRE", peut-être est-ce son amie qui devait recevoir le livre. Une recherche approfondie sur elle ne mène à rien.

On continue alors à parcourir les sites où le livre est mis à la vente, on tombe sur l'annonce présente sur "delcampe.net" qui comporte une question de "tarentuledu91" qui dit : "Je suis l'amie qui devait avoir ce livre, ce n'est pas grave l'auteur m'as redonné un exemplaire, mais c'est très marrant. Elsa Roussau".




← → ↻ 🔒 🔍 <https://www.google.com/search?channel=fs&client=ubuntu-sn&q=tarentuledu91> ☆ 📄 📧 📧 📧 📧


Google "tarentuledu91" ✕ 🔍

Produits Images Vidéos Actualités Livres Finance Tous les filtres Outils SafeSearch

Environ 2 résultats (0,17 secondes)

Essayez avec cette orthographe : "tarentule du 91"

 Metacritic  
<https://www.metacritic.com/user/tarentuledu91/>  
Aucune information n'est disponible pour cette page.  
Découvrir pourquoi

 Metacritic  
<https://www.metacritic.com/movie/porco-rosso>  
**Porco Rosso**  
tarentuledu91. Feb 25, 2024. Très bon film de Hayao Miyazaki, j'aime beaucoup. Il fait réfléchir sur la société, le regard des autres, l'amour et la vie en ...  
★★★★★ Note : 83 % - 11 votes


Recherches associées :

- laputa: castle in the sky review
- nausicaä
- kiki's delivery service review
- princess mononoke
- ponyo clips
- only yesterday
- the wind rises
- the secret world of arrietty

Afin d'afficher les résultats les plus pertinents, nous avons omis quelques entrées qui sont très similaires aux 2 entrées actuelles.  
Si vous le souhaitez, vous pouvez relancer la recherche pour inclure les résultats omis.

En regardant les films et surtout la série TV qu'elle a critiquée, elle révèle son vrai prénom "Elsabeth" et qu'elle "aime bien aller sur Pinterest".


← → ↻ 🔒 🔍 <https://www.metacritic.com/user/tarentuledu91/?filter=shows> 🏠 📄 📧 📧 📧 📧

 Games Movies TV Shows Music News Search Register

**tarentuledu91**

Movies 4 TV Shows 1


**User Overview in TV Shows**

  
AVG. USER SCORE

**USER SCORE DISTRIBUTION**  
Positive 1 (100%)  
Mixed 0 (0%)  
Negative 0 (0%)  
**HIGHEST USER SCORE** 8 **Elsbeth: Season 1**  
**LOWEST USER SCORE** 8 **Elsbeth: Season 1**

**TV Shows Scores** Recently Added

**Elsbeth: Season 1**

  
USER SCORE  
tarentuledu91

FEB 26, 2024

C'est marrant c'est presque comme mon prénom Elsabeth, hâte de voir cette série! J'aime bien aller sur Pinterest sinon

REPORT

On continue les recherches sur Pinterest avec un dorking sur son prénom, on ne trouve pas directement son compte mais en visitant un compte au hasard, on peut observer la composition de l'URL pour essayer de retrouver son compte avec son nom ou son pseudo.

← → ↻ [https://www.google.com/search?client=ubuntu-sn&hs=q0G&sca\\_esv=F7010a6fa6b14553&channel=fs&q=elsabeth\\*site:pinterest.fr&nfpr=1&sa=X&ved=2ahUKEw...](https://www.google.com/search?client=ubuntu-sn&hs=q0G&sca_esv=F7010a6fa6b14553&channel=fs&q=elsabeth*site:pinterest.fr&nfpr=1&sa=X&ved=2ahUKEw...)

Google

"elsabeth" site:pinterest.fr


Images Vidéos Produits Actualités Livres Finance

Tous les filtres Outils

SafeSearch




Environ 90 résultats (0,22 secondes)

Essayez avec cette orthographe : **"elsabeth"** site:pinterest.fr

 [pinterest.fr](https://www.pinterest.fr)  
<https://www.pinterest.fr> > elsa... > Traduire cette page

**Elsabeth Christine (elsabethchristine) - Profile**  
 E: Elsabeth Christine. elsabethchristine. 127 abonnés. · 24 abonnements. S'abonner.

Images :


1795 Elisabeth Alexeievna by C... Pinterest

Elisabeth Shue | Elisabeth shu... Pinterest


Pin of Linda Rodriguez på Act... Pinterest

Commentaires

6 autres images


 [pinterest.fr](https://www.pinterest.fr)  
<https://www.pinterest.fr> > elsab... > Traduire cette page

**Elsabeth Moreau (elsabethmoreau) - Profile**  
 Elsabeth Moreau. elsabethmoreau. 0 abonné. · 0 abonnement. S'abonner. elsabethmoreau n'a enregistré aucune Épingles pour le moment.

 [pinterest.fr](https://www.pinterest.fr)  
<https://www.pinterest.fr> > elsab... > Traduire cette page


Avec son nom complet "Elsabeth Roussau", on peut saisir "/elsabethroussau" dans l'URL et on parvient ainsi à trouver son compte sous le pseudo "elsabethroussau". Sur Pinterest, la page d'Elsa contient une publication et un lien dans sa bio. La publication mentionne un slogan ou une marque "La Tarentule Créative" et rien de plus, l'image ne contient à priori aucune information particulière quand on la passe à [Apérisolve](#).

← → ↻ [https://www.pinterest.fr/elsabethroussau/\\_created](https://www.pinterest.fr/elsabethroussau/_created)


 Explorer

Recherchez des idées pour des diners faciles, sur la mode, etc.


Se connecter S'inscrire




**Elsabeth Roussau**  
 @elsabethroussau  
 pin.it/OrNuHg2jI · j'ai un nouveau Pinterest avec mon nouveau nom de famille que j'ai modifié  
 0 abonné · 0 abonnement

 [S'abonner](#)

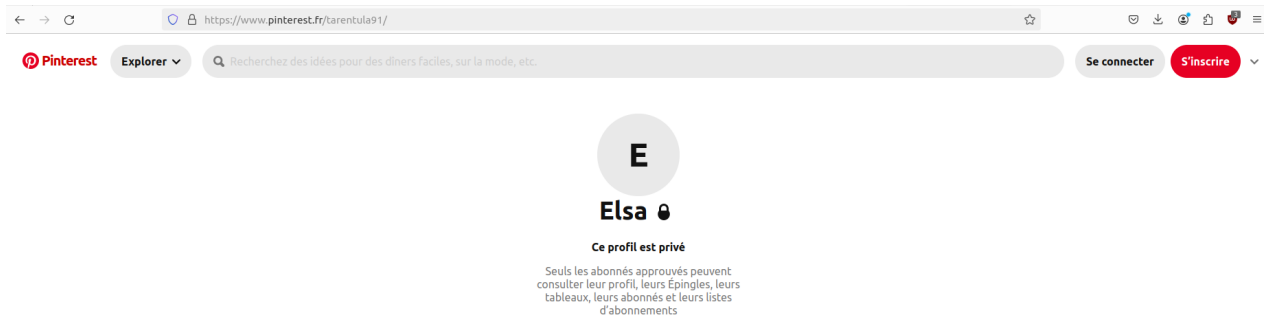
Créées Enregistrées



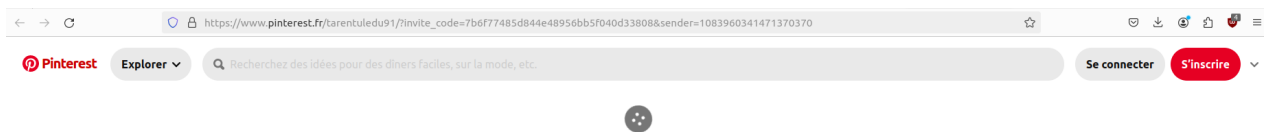
**Elsabeth Roussau**  
 Elsabeth Roussau = La Tarentule  
 Creative #elsabethroussau

 Elsabeth Roussau




Le lien dans sa bio contient un code d'invitation menant à un autre compte qui est privé et qui semble être consultable uniquement en passant par un code d'invitation.



Ici, la page charge à l'infini, je ne sais pas si c'est parce que le code d'invitation n'est plus valide ou autre chose. La piste Pinterest s'est donc arrêtée là pour moi mais j'ai pu continuer les recherches avec sa marque.



En effectuant cette fois-ci un dorking Google sur sa marque "La Tarentule Créative", on tombe sur son profil Reddit (attention aux résultats Google pour les arachnophobes) et notamment sur sa publication où elle mentionne encore "La Tarentule Créative".

← → ↻ [https://www.reddit.com/user/tarentula91/comments/1b2bzcp/la\\_tarentule\\_creative/](https://www.reddit.com/user/tarentula91/comments/1b2bzcp/la_tarentule_creative/)   Rechercher dans utarentula91   ...

Populaires

THÉMATIQUES

Gaming

Sports

Business

Crypto

Télévision

Célébrités

En voir plus

RESSOURCES

À propos de Reddit

Publicités

Aide

Blog


Carrières

Presse


Communautés

Le meilleur de Reddit

Thématiques

 utarentula91 • 8 y a 2 j  
tarentula91

**La Tarentule Creative !**




↑ 1 ↓

0




Partager

+ Ajouter un commentaire

 **Soyez la première personne à commenter**  
Personne n'a encore répondu à cette publication.  
Partagez vos pensées et lancez la conversation.

<https://preview.redd.it/la-tarentule-creative-v0-bvxsncw3dlc1.png?width=500&format=png&auto=webp&s=39ca7336fdb43eaaa91e5a3f50398f5baef7994>

En consultant son profil, on remarque un lien vers son compte Twitter (X).

← → ↻ <https://www.reddit.com/user/tarentula91/>   Rechercher dans utarentula91   ...

Populaires

THÉMATIQUES

Gaming

Sports

Business

Crypto

Télévision

Célébrités

En voir plus

RESSOURCES

À propos de Reddit

Publicités

Aide

Blog


Carrières

Presse

Communautés

Le meilleur de Reddit

Thématiques


 **latarentulea91**  
utarentula91

Vue d'ensemble

Publications

Commentaires

Nouvelles

 utarentula91 • 8 y a 2 j

**La Tarentule Creative !**

<https://preview.redd.it/la-tarentule-creative-v0-bvxsncw3dlc1.png?width=500&format=png&auto=webp&s=39ca7336fdb43eaaa91e5a3f50398f5baef7994>

↑ 1 ↓

0

Partager

**latarentulea91** ...

S'abonner

Discuter

1

0

28 févr. 2024

Karma de pu...

Karma de com...

Jour du gâteau

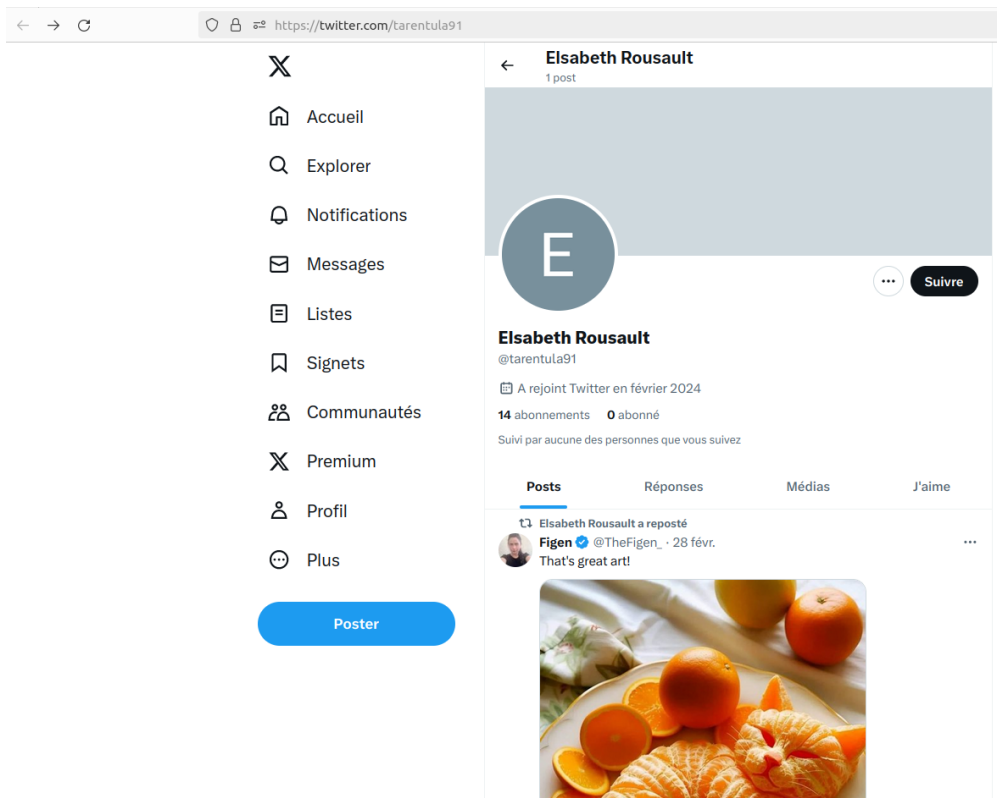
LIENS

Twitter

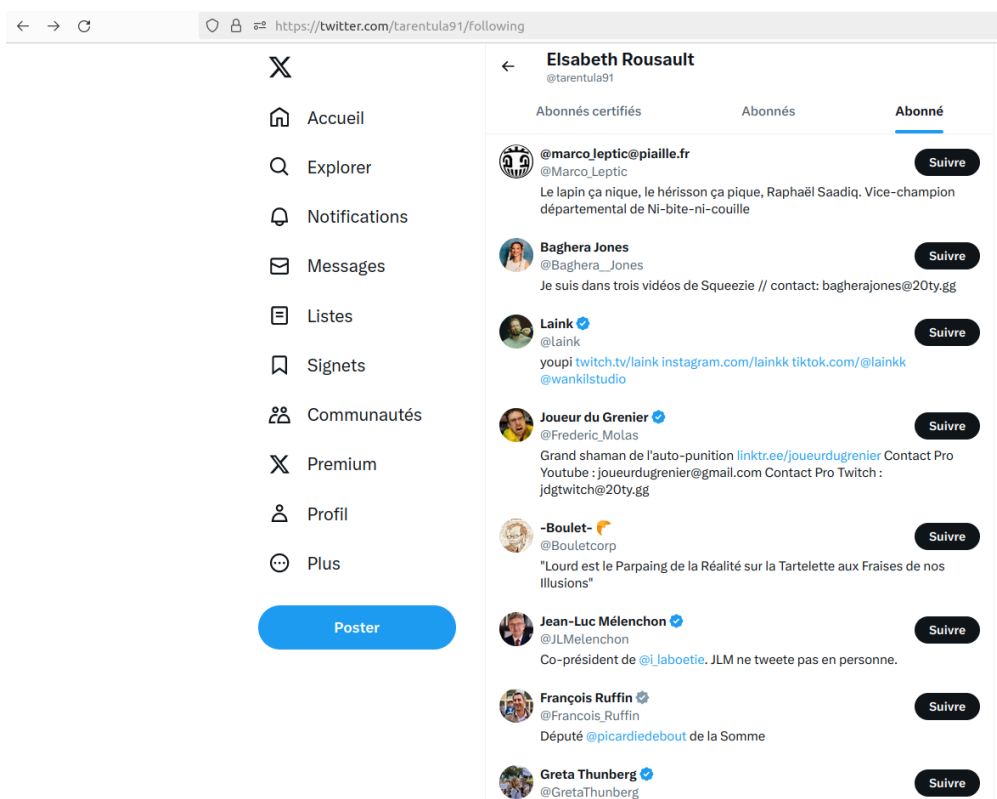
VITRINE DE TROPHÉES

New User

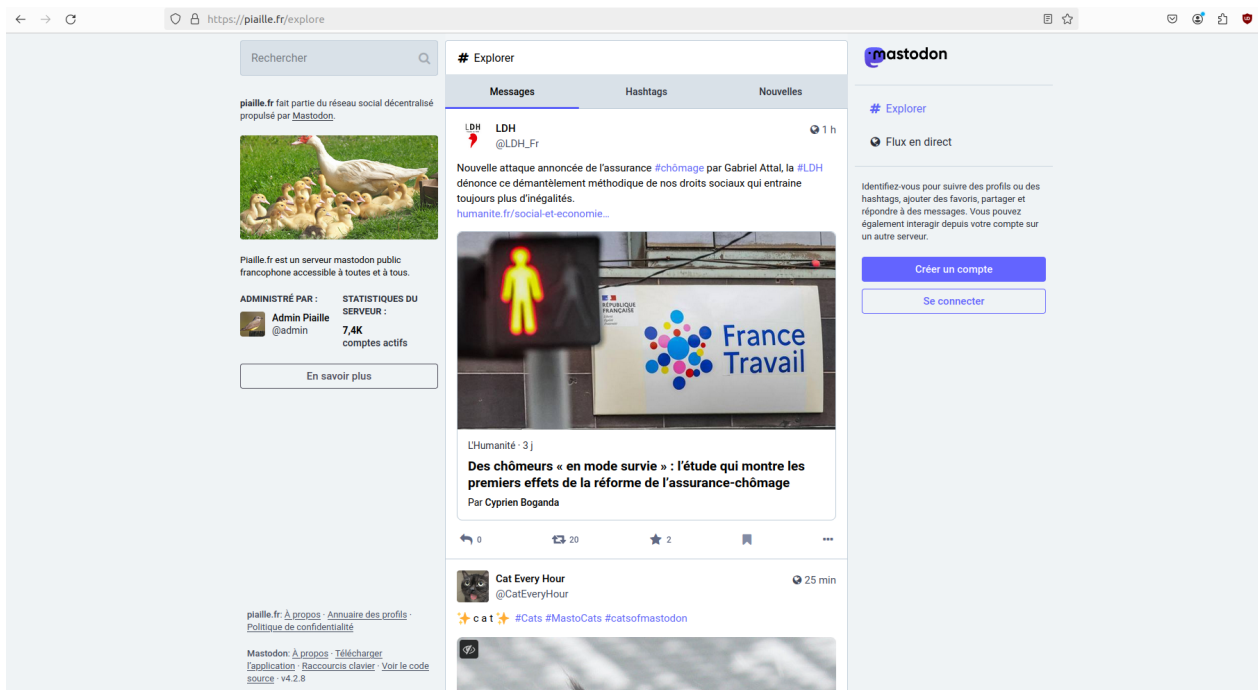
Une fois sur son compte Twitter, on observe ses posts, ses réponses, ses médias et ses mentions "J'aime" mais cela ne donne rien d'intéressant.



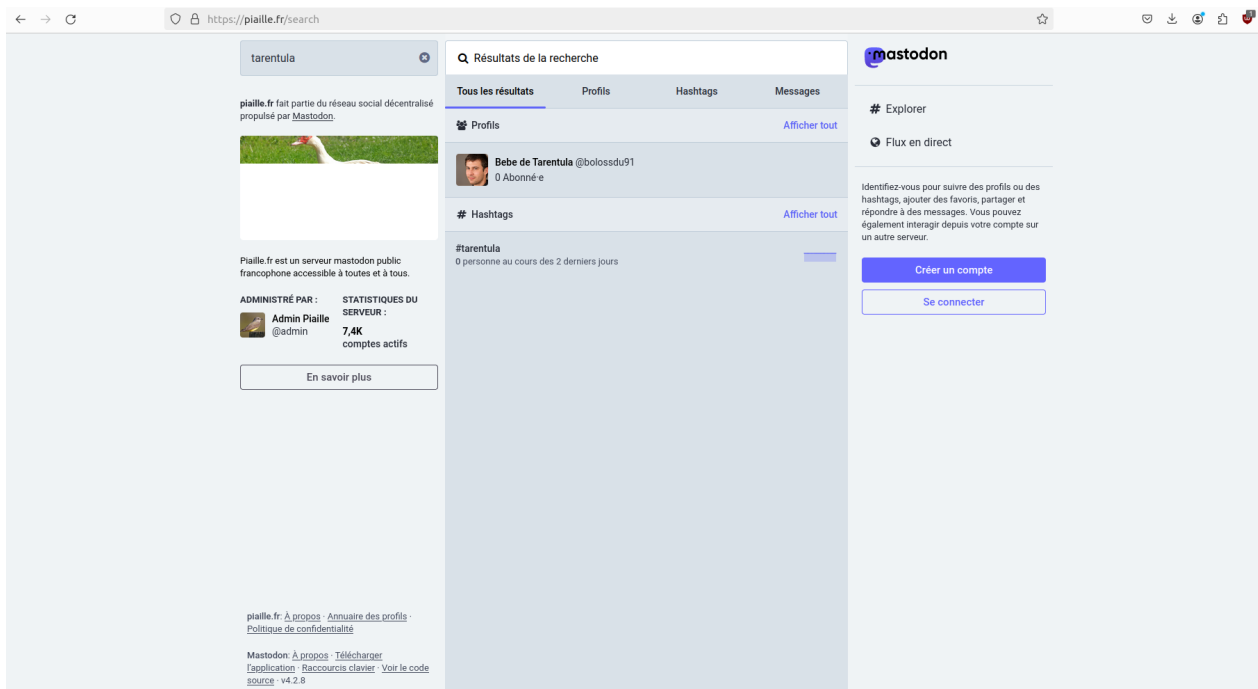
La dernière piste ici est alors de regarder ses abonnements qui contiennent les comptes d'influenceurs et de marques qui sont généralement proposés à la création d'un compte. En plus de ces comptes connus, on retrouve deux comptes avec "@piaille.fr" dans leur pseudo.



En copiant-collant sur Google, on tombe sur le serveur Mastodon "piaille.fr", d'ailleurs Elisabeth est abonnée au compte officiel de Mastodon sur Twitter.

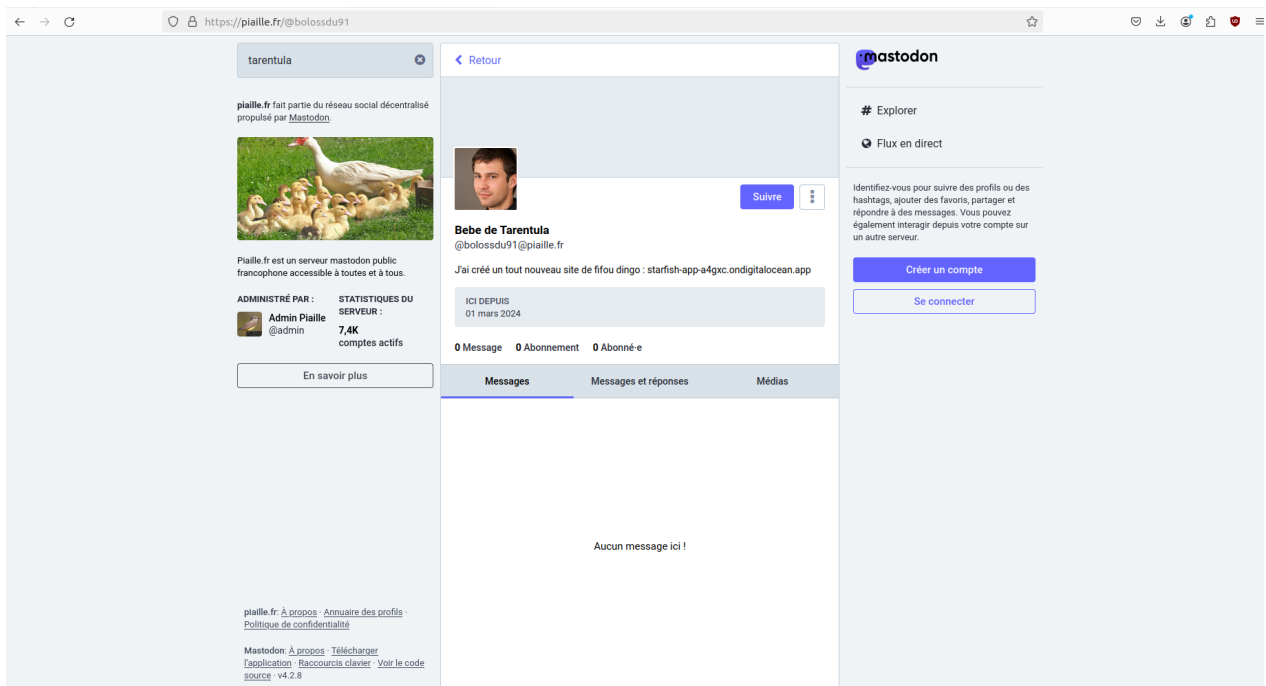


Une fois sur le serveur, une remontée sur le flux en direct paraît longue à effectuer, on peut lancer une recherche avec des mots déjà rencontrés comme "tarentule", "elsa", "elsabeth". Ces recherches mènent parfois à des posts plus ou moins récents sur le serveur mais rien de pertinent. En recherchant "tarentula" qui est le pseudo d'Elsabeth (tarentula91) sur Reddit et Twitter, on tombe sur un profil "@bolosdu91" dont le nom est "Bebe de Tarentula" et dont l'image semble avoir été générée par IA.



En consultant son profil, il dit dans sa bio qu'il a créé un nouveau site, on va donc le visiter.





En visitant le site, on a une illustration avec un message nous disant d'ajouter un paramètre "?message" dans l'URL avec une valeur arbitraire.



Par exemple avec "?message=oui", cela fonctionne et le site renvoie le flag.

```

/ ouile flag a trouvé était : \
\ l4_t4r3ntul3_35t_cr3471v3 /
  \  ^ ^ \
  \ (oo) \
  \ ( ) \
  \ ||----w ||
  \ ||

```