

De: Jacques Pyrat [redacted]  
Objet: Re: asro\_pyrat création d'accès à notre hébergement pour afficher notre site web avec SoyezCréateurs  
Date: 2 septembre 2025 à 19:34  
À: admin\_ASRO admin@asro1918.org



Voilà, j'ai fini la preuve de concept du passage du site de la version actuelle à SPIP+SoyezCréateurs.  
<https://ww2.asro1918.org/>

Tes accès habituels fonctionnent : tu peux donc aller aussi dans écrire/ avec le login mot de passe habituels.

Bien à toi

Jacques Pyrat — [www.pyrat.net](http://www.pyrat.net) — *Création de sites Internet bien référencés – Expert SPIP*

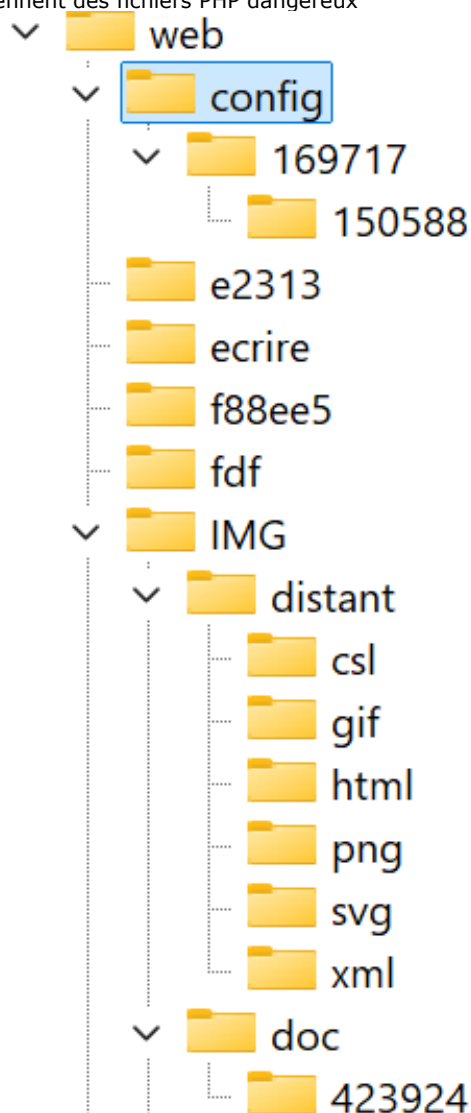


06 82 58 27 36

Le mar. 2 sept. 2025 à 19:00, Jacques Pyrat [redacted] écrit :  
Bonjour Claude,

L'accès FTP fonctionne. Je me suis créé un compte : krh\_jpyrat  
via <https://manager.infomaniak.com/v3/hosting/133102/hosting/7911/ftp-ssh>  
J'ai créé le sous domaine : [ww2.asro1918.org](https://ww2.asro1918.org) que tu peux visiter  
J'ai pu récupérer la base de données.

Quant au site actuel, il est hacké comme j'avais pas encore vu :  
Exemple : dans cette copie d'écran, tous les dossiers contenant des chiffres ont été rajouté par les hackers, et contiennent des fichiers PHP dangereux



Et le fichier index.php à la racine du site n'est plus celui de SPIP. Ce qui explique la redirection constaté depuis une recherche Google.

Dans IMG/, voici tous les fichiers PHP en trop

```
~/web/IMG$ find . -name "*.php" -type f
./pdf/.pdf.php
./png/.png.php
./zip/.zip.php
./jpg/.jpg.php
./jpg/index.php
./jpg/784109/index.php
./docx/.docx.php
./mp4/.mp4.php
./distant/svg/index.php
./distant/.distant.php
./logo_erreurs/.logo_erreurs.php
./logo/.logo.php
./mp3/.mp3.php
./m4v/.m4v.php
./webm/.webm.php
./xlsx/.xlsx.php
./mov/.mov.php
./m4a/.m4a.php
./doc/.doc.php
./doc/index.php
./doc/423924/index.php
./IMG.php
```

Bref, hacké en profondeur.  
Chance, la base de données n'a pas l'air d'être touchée.

À suivre

Jacques Pyrat — [www.pyrat.net](http://www.pyrat.net) — *Création de sites Internet bien référencés – Expert SPIP*



06 82 58 27 36

Le mar. 2 sept. 2025 à 17:23, admin\_ASRO <[admin@asro1918.org](mailto:admin@asro1918.org)> a écrit :

Cher Jacques,  
voici les détails de tes droits admin sur Hébergement + Domaine

### Administration des produits

Choisissez quels produits cet utilisateur peut administrer

Rechercher un produit  × [Attribuer les droits maximum sur les tous les produits](#)

Hébergement Web <span>1</span>	Domaine <span>1</span>
Service Mail	Swiss Backup