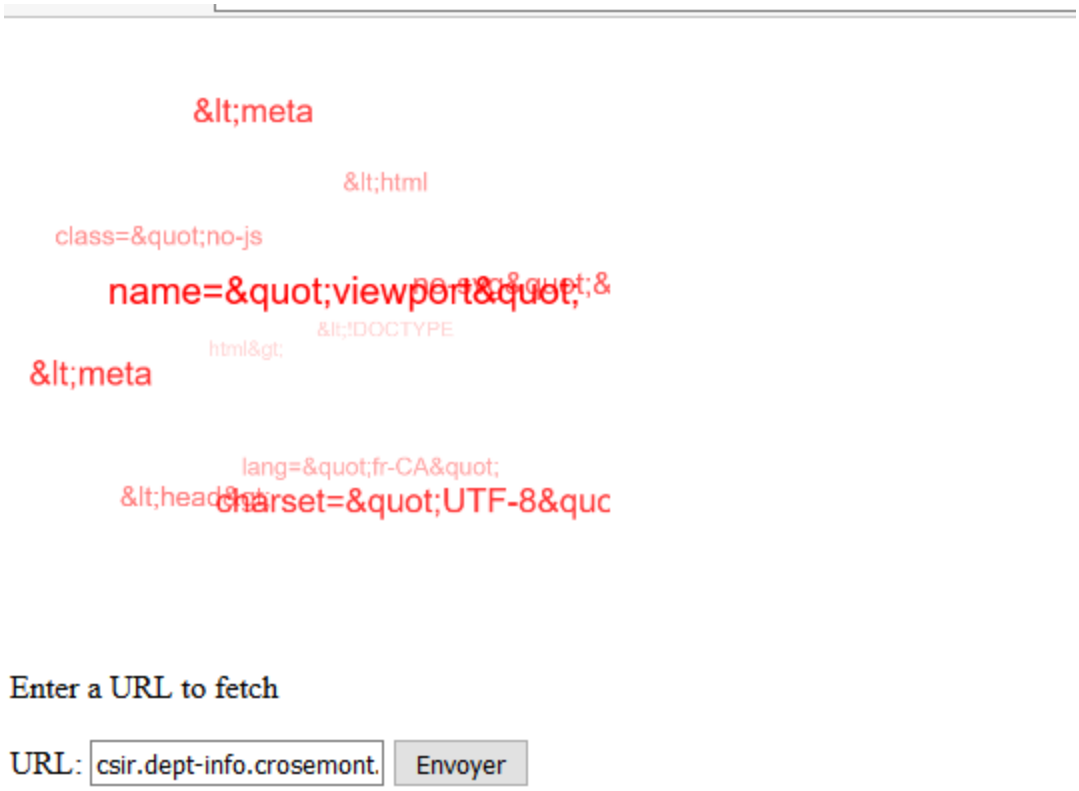
Curling in the cloud

Ici nous avons un service web qui va aller chercher une page donnée en paramètre.

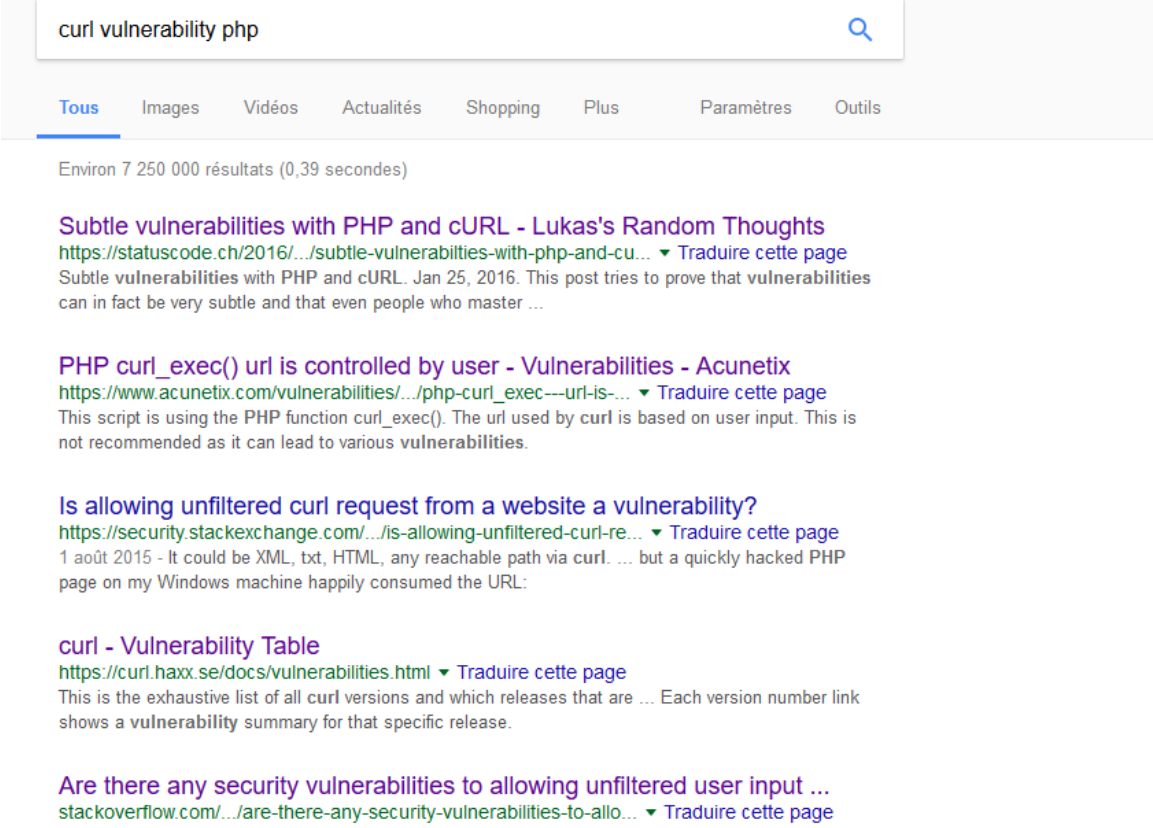


Il va ensuite afficher à l'utilisateur quelques mots du code source. Pourquoi ? Pourquoi pas…

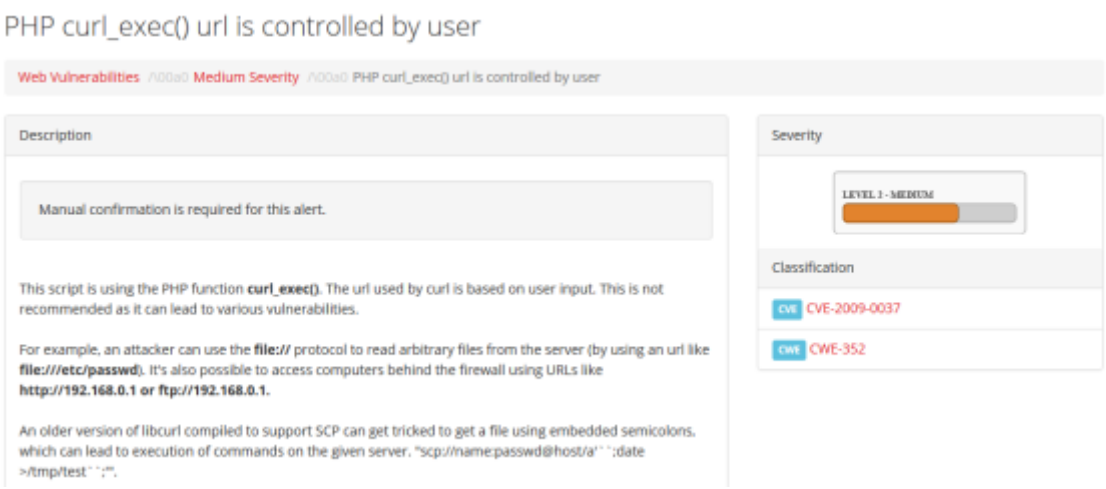
Suite à une recherche avec les mots clés « curl php » sur Google nous pouvons voir que Curl est une bibliothèque « qui vous permet de vous connecter et de communiquer avec différents types de serveurs, et ce, avec différents types de protocoles. »

http://php.net/manual/fr/intro.curl.php

La suite logique serait de faire une deuxième recherche sur curl. Cependant, nous allons rechercher s'il y existe des vulnérabilités ou de mauvaises implémentations connues.

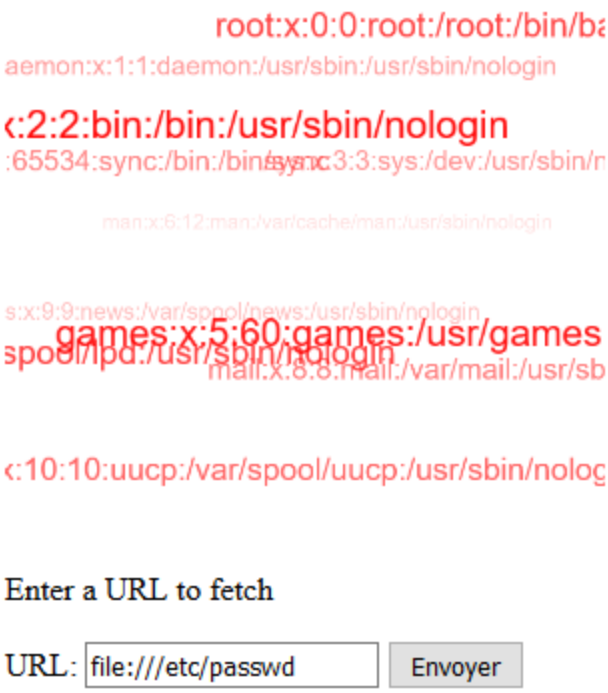


!!



Voilà quelque chose d'intéressant.

Si l'entrée d'un utilisateur n'est pas bien filtrée. Celui-ci sera en mesure de changer le fonctionnement prévu ! Essayons file://



Et voilà le fichier passwd du serveur. Il nous reste qu'à chercher notre flag !

http://www.acunetix.com/blog/articles/server-side-request-forgery-vulnerability/

https://www.acunetix.com/vulnerabilities/web/php-curl_exec---url-is-controlled-by-user