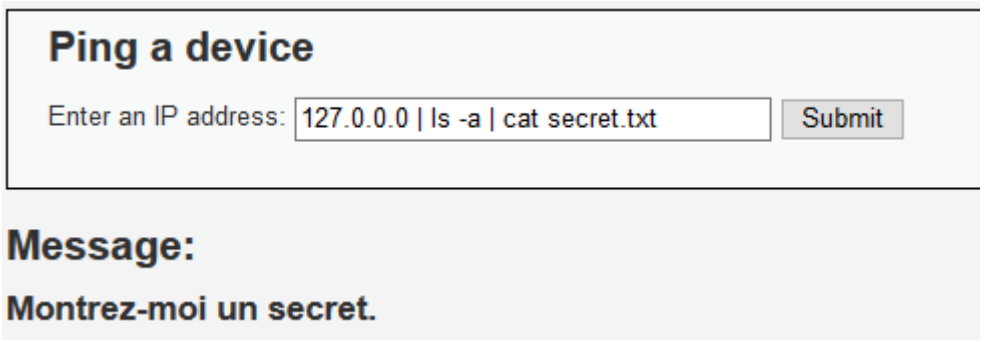
Audit Sécurité Informatique

Command Injection :

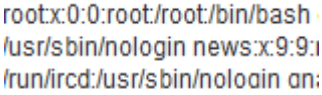


Comme on peut le voir sur cette image à l'aide du champ de texte et de 2 commandes j'ai pu rentrer dans le fichier secret.txt(même si sur l'image on ne me voit pas encore dedans).

Pour en arriver là j'ai d'abord mis une commande et ensuite j'ai fait un pipe suivit d'un ls, j'ai vu qu'il y avait un retour avec le nom du fichier qui m'intéressait, alors j'ai refais cette manip en y ajoutant « cat secret.txt ».

Pour éviter ce genre de problème il faudrait s'assurer qu'il n y ait rien d'autre après le ping et si il y a quoi que ce soit après l'adresse IP renvoyer une erreur.

File Inclusion :



Pour avoir ce bout du contenu du fichier passwd j'ai regardé l'url dans circulant dans les 2 dossiers proposer, ensuite j'ai décidé de modifier le contenu de l'url après « ? » page=file'quelque chose' par une autre valeur. Ça m'a affiché un fichier caché me disant que j'étais sur la bonne voie, alors j'ai

décidé d’essayer en mettant à la place de file2 ou 1 de mettre le chemin de la racine jusqu’au fichier rechercher. Ce qui ma permit d’avoir le contenu du fichier.

Pour éviter de telles intrusions il est important de ne pas informer l’utilisation sur sa position dans l’arborescence, de plus il ne faut pas utiliser des variables transmises dans l’url pour ce déplacé dans les différents fichiers du site web.