

Include Page

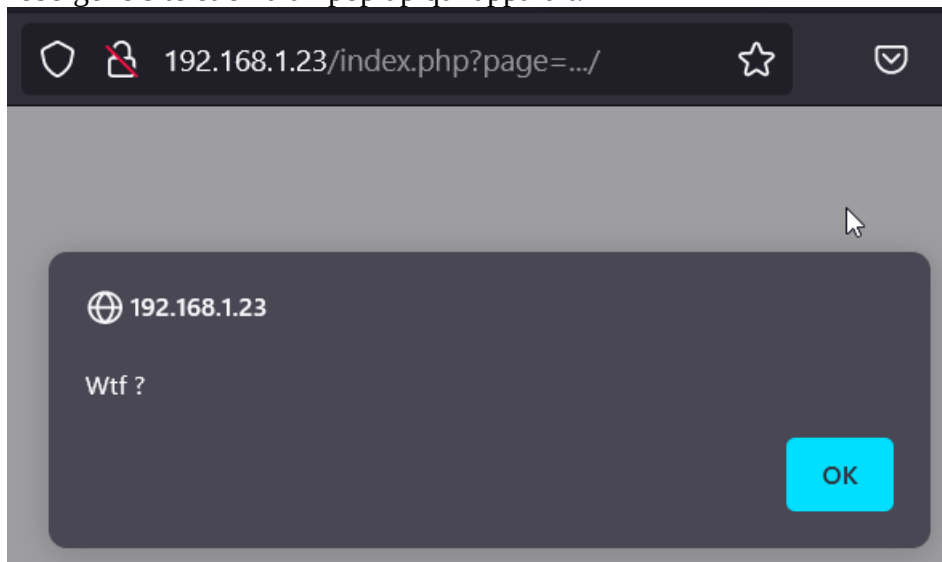
Il s'agit de se balader dans la machine qui héberge le site...

Exploration

Quand on navigue sur le site on remarque très vite que les adresses commencent toutes par `http://192.168.1.23/index.php?page=`

Offensive

On termine `http://192.168.1.23/index.php?page=` par « `../` » pour tenter de naviguer dans la machine qui héberge le site et on a un pop up qui apparaît.



Il suffit alors d'ajouter « `../` » un certain nombre de fois puis « `etc/passwd` » dossier où sont stockés les mots de passes

Faible

Navigation écrite dans l'adresse par système de page équivalente à la navigation dans une machine

Mitigation

Utiliser des routes