

htpasswd w htaccess robots

Exploration

Quand on cherche "robots.txt" dans google on tombe sur ce lien :
<https://developers.google.com/search/docs/crawling-indexing/robots/create-robots-txt?hl=fr>
dans <http://192.168.1.16/robots.txt> on voit qu'il y a un disallow sur deux dossiers : whatever et .hidden
Dans <http://192.168.1.16/whatever> il y a fichier htpasswd et <http://192.168.1.16/admin/> donne une possibilité d'accès via username et mdp a une zone sécurisée

Offensive

Le username est très certainement root, le mot de passe doit être la partie cryptée après les ":". D'après <https://md5.gromweb.com/?string=qwerty123@> le mot de passe serait "qwerty123@"

Faible

Une adresse évidente pour accéder à la partie administration du site.
Le username et le mot de passe écrits dans un fichier accessible.

Mitigation

Ne pas écrire le username et le mot de passe administrateur dans un fichier accessible du site

Sources

- <https://developers.google.com/search/docs/crawling-indexing/robots/create-robots-txt?hl=fr>
- <https://md5.gromweb.com/?string=qwerty123@>