

## No Hack Allowed

Afin d'éviter l'exploitation des bugs de sécurité sur quelques logiciels comme phpnuke, nous avons mis une redirection de toutes les pages admin.php vers no.hack.allowed.ovh.com

### **Et qu'est-ce qu'on fait maintenant ?**

Vous pouvez bien sûr continuer à faire fonctionner votre site en changeant tout simplement admin.php en un autre fichier. Appelez le vraiment autrement pour éviter un éventuel hack. admin-a-moi.php ou mon-admin.php etc.

Vous pouvez utiliser ce freeware <http://www.orbit.org/replace/> qui va vous permettre de changer admin.php en autre chose sur toutes vos pages html/php. Sous Mac vous avez BBEdit (version lite gratuite) <http://www.barebones.com/products/bbedit/>.

N'oubliez pas de protéger ensuite cette page (vous trouverez tout ce dont vous avez besoin dans ces guides) :  
HtaccessProtection,  
HtaccessProtectIP,  
HtaccessAutre.

### **Cette mesure est-elle définitive ?**

C'est fort probable... Si nous trouvons une autre solution, plus souple nous la mettrons alors en place. En attendant les problèmes générés par le trou de sécurité portant sur ce fichier sont susceptibles de vous causer et de nous causer trop d'ennuis pour rester sans rien faire. Nous sommes conscients de la gêne occasionnée mais nous ne pouvons pas laisser les choses en l'état pour l'instant.

### **C'est quoi cette histoire de hack ?**

admin.php est le nom du script utilisé par pas mal de softs opensource (entre autres) qui permet de les administrer. Il ne s'agit pas du même script d'un logiciel à l'autre, mais de nombreux projets ont eu des bugs de sécurité en rapport avec un fichier portant ce nom. Voici quelques pages qui traitent de ce sujet. Allez y jeter un oeil pour vous rendre compte de l'ampleur et de la fréquence de ces problèmes.

Dans un monde parfait, tous les webmasters devraient mettre à jour immédiatement la version du soft qu'ils utilisent lorsqu'il y a un problème de sécurité.

Malheureusement, nous ne vivons pas dans un monde parfait et beaucoup de sites ont ces problèmes de sécurité. Et généralement, aucune restriction d'accès n'est installée pour ce script. Pourtant, il est relativement simple de mettre en place un .htaccess

Le hackeur n'a donc qu'à chercher si la page existe en testant tout simplement les liens standards :  
<http://votresite/admin.php> par exemple.

Si la page existe, il teste si admin.php est vulnérable. Si c'est le cas, sa fête commence. Il a un contrôle total sur le site. Il peut donc effacer les fichiers, modifier le contenu du site ou simplement installer un backdoor qui lui permettra de revenir un autre jour même si vous aviez bien sécurisé votre admin.php.

Cette prise de contrôle se finit souvent en effacement de la page d'index ou de tout le site. Même si vous disposez de 5 backups accessibles en lecture seule BackupsSurPlan, c'est quand même très embêtant pour vous.

## OVH

Il faut souligner que le hackeur ne peut pas accéder aux autres sites hébergés sur nos machines. Nous avons un niveau de sécurité basé sur un chroot qui permet de garantir cette option.

Mais il y a pire.

Le hackeur peut aussi lancer une attaque à partir de nos machines sur des IP sur Internet. Notre réseau est très important et nous pouvons sans aucun problème déborder 100Mbps ou 200Mbps de plus. C'est ce qui s'est passé à plusieurs reprises. Le résultat : une indisponibilité du service d'hébergement pendant une dizaine de minutes.

```
cccvalden 3685 0.0 0.8 12704 4516 ? S 03:23 0:00 php admin.php Çúÿ¿
cccvalden 3687 0.0 0.1 1644 752 ? S 03:23 0:00 sh -c /tmp/. " /s 200.217.189.100 65535 9999 1>
/tmp/4843output 2>&1;
cccvalden 3688 1.9 0.0 1152 404 ? R 03:23 1:52 /tmp/. /s 200.217.189.100 65535 9999
```

ou encore

```
mmoreva 25081 0.0 0.8 12704 4516 ? S 18:48 0:00 php admin.php ýüÿ¿
mmoreva 25083 0.0 0.1 1644 752 ? S 18:48 0:00 sh -c ./s 200.241.255.83 65535 9999 1> /tmp/4843output
2>&1; cat /tmp
mmoreva 25084 6.5 0.0 1152 404 ? S 18:48 2:11 ./s 200.241.255.83 65535 9999
```

Le hackeur a pu télécharger un code source et le compiler, puis lancer une attaque DoS sur 200.217.189.100 dans le but de rendre cette IP inaccessible. Sauf qu'en même temps il a aussi rendu indisponibles certaines machines critiques sur notre réseau.

Concernant ce admin.php, il s'agit d'un bête script php qui fait un exec :

```
# grep exec ./www/concom/admin.php
@ $changedir = exec("pwd");
@ $changedir = exec("pwd");
$changedir = exec("$temp[0]; pwd");
```

dans \$temp[0] on peut tout passer comme commande Unix. On peut donc télécharger les fichiers, les compiler et les exécuter.

De plus, on peut voir chez ce client qu'il en possède plusieurs !

```
# find -name admin.php
./www/concom/admin.php
./www/admin/actumedia/admin/admin.php
./www/arno24/actumedia/ben25/admin.php
./www/rando/admin.php
./www/gallerie/admin.php
./www/gallerie/ /admin.php
```

Vous pouvez aussi voir que le dernier est un script probablement copié par le hackeur dans un répertoire avec des espaces. Le hackeur a donc mis en place un backdoor en espérant que personne ne va voir que le répertoire avec des espaces existe !!

```
# cd ./www/gallerie
```

```
1. ls -al
```

```
total 92
drwxr-xr-x 2 cccvalden users 4096 nov 24 23:28
drwxr-xr-x 8 cccvalden users 4096 nov 24 23:29 .
drwx
r-x 20 cccvalden users 8192 nov 27 11:32 ..
-rw-r--r-- 1 cccvalden users 2762 oct 23 18:40 admin.php
```

Il faut avoir un ?il d'expert pour voir ce répertoire. Est-ce que le hackeur a installé un autre backdoor (avec un nom de fichier différent) ?

```
# fgrep "exec(" * -r
www/concom/admin.php: @ $changedir = exec("pwd");
www/concom/admin.php: @ $changedir = exec("pwd");
www/concom/admin.php: $changedir = exec("$temp0; pwd");
www/readme.php: $work_dir = exec("pwd");
www/rando/admin.php: @ $changedir = exec("pwd");
www/rando/admin.php: @ $changedir = exec("pwd");
www/rando/admin.php: $changedir = exec("$temp0; pwd");
www/gallerie/admin.php: @ $changedir = exec("pwd");
www/gallerie/admin.php: @ $changedir = exec("pwd");
www/gallerie/admin.php: $changedir = exec("$temp0; pwd");
www/gallerie/ /admin.php: @ $changedir = exec("pwd");
www/gallerie/ /admin.php: @ $changedir = exec("pwd");
www/gallerie/ /admin.php: $changedir = exec("$temp0; pwd");
```

Apparemment non, mais il faut rester vigilant.

Nous avons eu en tout 7 attaques :

Vous pouvez voir 3 attaques entre 3h et 5h du matin. 2 attaques entre 6h et 7h. une petite coupure à 14h30 dûe à une attaque qui est resté en interne, puis 1 attaque vers 19h, puis une petite coupure. La taille de l'attaque est entre 100Mbs et 200Mbs sur 800Mbs du total.