Principes de la Sécurité Web

1

Comment protéger votre site des tentatives de piratage?

1) Si vous utilisez un script de management de contenu (blog, forum, galerie, etc.), soyez sûr d'avoir toujours la dernière version.

Dès qu'un faille est détectée dans un script, l'auteur du script publie une version qui corrige la faille. Mais en même temps la faille est largement commentée sur de nombreux sites et donc des pirates essayent immédiatement de l'exploiter sur des sites qui n'ont pas encore fait la mise à jour.

2

2) Si vous programmez vous même vos scripts, ne faites jamais confiance à une entrée extérieure.

Toutes les entrées ($_POST, $_GET) doivent être vérifiées et/ou traitées avant utilisation, sinon vous prenez de gros risques **d'injection de code** ou de **Cross Site Scripting**. Une recherche sur Google vous donnera beaucoup plus de détail sur ce type d'attaques.

3

3) Toujours échapper ses entrées extérieures dans une requête SQL.

Pour éviter le risque **d'injection sql**, vous devez traiter toutes vos entrées extérieures avant de les utiliser dans une requête. En php, renseignez vous sur la fonction mysql_real_escape_string().

4

4) Sécuriser votre base de données

Créer des usagers et lui affecter les bon privilèges. À voir dans un prochain cours.

5

5) Ne laissez pas votre répertoire web avec un CHMOD777.

Avec un CHMOD 777 tout le monde à tous les droits sur votre répertoire, c'est courir un grand risque. Un CHMOD 705 est normalement suffisant. À voir dans un prochain cours.

6

6) Choisissez bien vos mots de passe.

N'utilisez jamais le même login et mot de passe pour votre connexion ftp et votre connexion à la base de donnée, si il était découvert, ça donnerai accès à tout!!!

Choisissez un mot de passe suffisamment long, qui soit une combinaison de lettres, chiffres et signes et qui n'a pas de signification.

7

7) Si vous utilisez votre propre serveur, soyez sûr qu'il soit bien paramétré.

Vous devez être sûr d'avoir les versions à jour d'Apache, PHP, MySQl, etc..

Paramétrer correctement un serveur nécessite de bonne connaissances, vous trouverez de nombreux sites ou livres pour vous aider.

Soyez sûre de ce que vous faites, de nombreux serveurs deviennent des relais de spam suite à un mauvais paramétrage.

8

8) Toujours se tenir informé.

Il y a de nombreux sites donnant des alertes sécurités ou des conseils pour protéger votre site.

Le mieux est de régulièrement vérifier sur ces sites les dernières nouvelles pour ne pas laisser une faille sur son site.

Les pirates ont de nouvelles idées tous les jours. Il faut donc toujours se tenir au courant.

9

TESTER SA CONFIGURATION SERVEUR AVEC PHPSECINFO

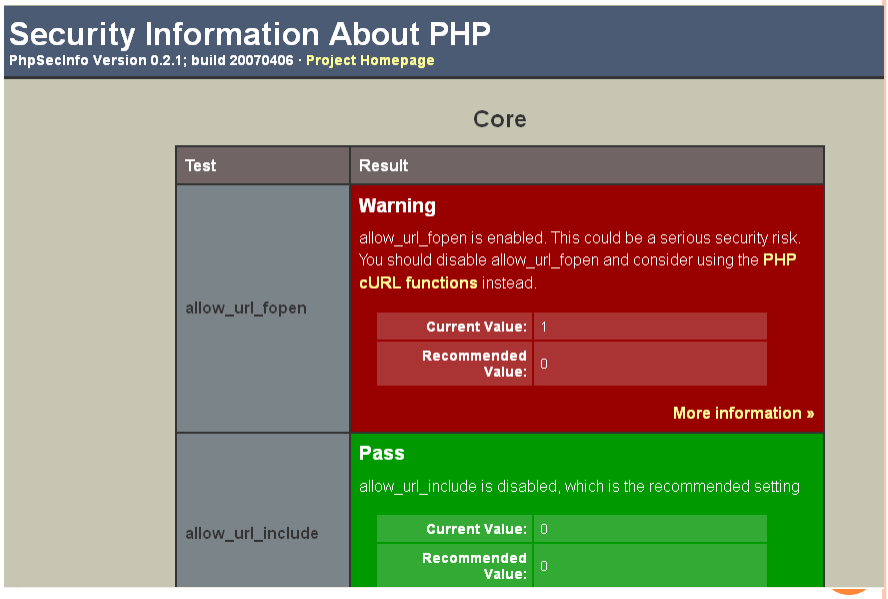
PHPSecInfo, un outil d'évaluation de la configuration PHP d'un serveur Web, adopté officiellement par le PHP Security Consortium.

Sous la forme d'un script PHP disposant de nombreux tests l'utilisateur pouvant en fournir d'autres au besoin, PHPSecInfo affiche pour chaque réglage de php.ini, un commentaire sur sa sécurité, avec conseils et suggestions, le tout accompagné de codes de couleur pour discerner rapidement les besoins pressants.
http://phpsec.org/projects/phpsecinfo/

Le télécharger, le copier dans votre répertoire www et y accéder par le Web.

10

EXEMPLE



Exercice :

- Installer **PHPSecInfo**
- Tester **PHPSecInfo**