PHPSecInfo

1) Informations générales

Rubrique	Outil d'audit de la configuration PHP (5.2.x et antérieur)
Public	Administrateurs Systèmes et Réseaux
Editeur	PHP Security Consortium
Licence	New BSD
Fonctionnalités	PHPSecInfo évalue la sécurité de la configuration PHP. Il effectue une série de tests de l'environnement PHP pour identifier des problèmes possibles de sécurité. Il contrôle les valeurs données aux directives PHP dans le fichier php.ini et suggère des modifications pour ces directives.

2) Installation

L'outil s'installe facilement et rapidement :

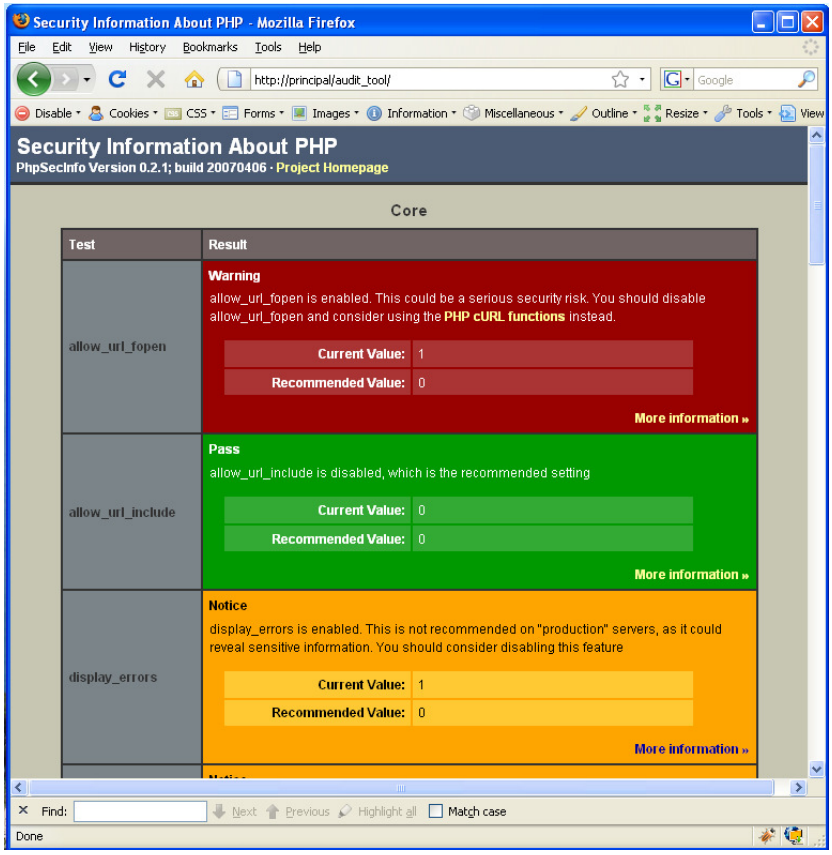
- ✓ télécharger phpsecinfo.zip version 0.2.1 20070406
  http://phpsec.org/projects/phpsecinfo
- ✓ décompresser l'archive
- ✓ mesures de sécurité :
  - renommer le répertoire audit_tool
  - mettre un .htaccess dans le répertoire afin d'en restreindre l'accès
- ✓ placer le répertoire audit_tool à la racine du site web

3) Utilisation

3.1) Lancer les tests

Ouvrir un navigateur et entrer l'URL :
http://.../audit_tool/index.php

Le fichier index.php du répertoire audit_tool réalise les tests et affiche les résultats.



Liste des tests :

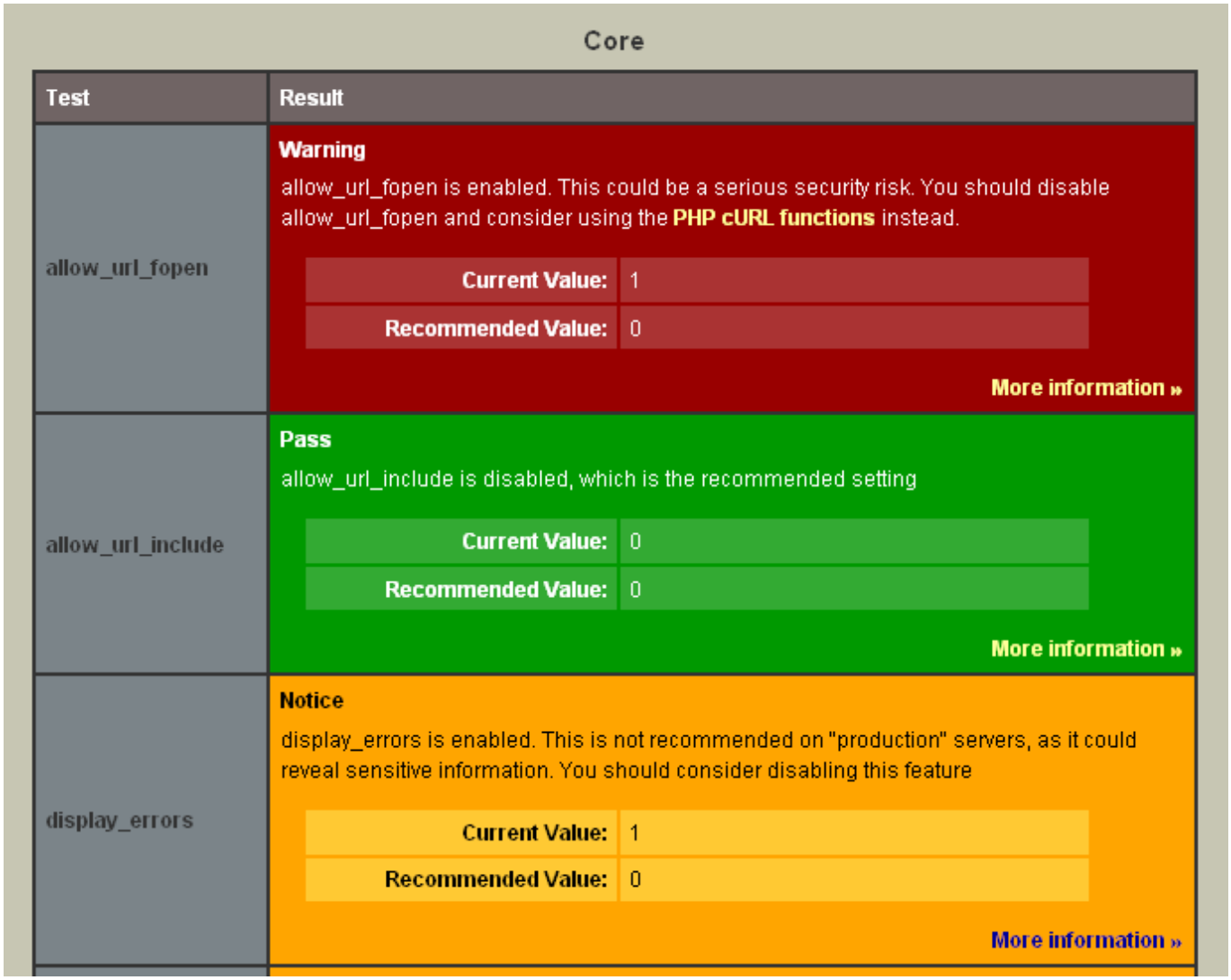
- Core :
  - Directives :
    allow_url_fopen,
    allow_url_include,
    display_errors,
    expose_php,
    file_uploads,
    magic_quotes_gpc,
    memory_limit,
    open_basedir,
    post_max_size,
    register_globals,
    upload_max_filesize,
    upload_tmp_dir.
  - Autres tests :
    user_id , group_id,
- curl : file_support
- Directive CGI : force_redirect
- Directives de session : save_path, use_trans_sid

3.2) Analyser les résultats

Les résultats sont affichés dans plusieurs tableaux :

- Section des tests exécutés :
  - core
  - CGI
  - Session
  - Curl
- Section des tests non exécutés
- Section Résumé

a) Section des tests exécutés



Affiche pour chaque test :

- un code couleur + un statut :
  - warning (rouge) = risque important de sécurité
  - notice (orange) = risque de sécurité
  - pass (vert) = OK

- un message

- un lien "More information >>" vers le site phpsecinfo qui explique les implications de sécurité pour ce test

Par exemple, un clic sur le lien "More information >>" pour le test allow_url_fopen affiche la page web ci-contre

http://phpsec.org/projects/phpsecinfo/tests/allow_url_fopen.html

Test	Result
allow_url_fopen	**Warning** allow_url_fopen is enabled. This could be a serious security risk. You should disable allow_url_fopen and consider using the **PHP cURL functions** instead. **Current Value:** 1 **Recommended Value:** 0 **More information »**

PhpSecInfo Test Information

allow_url_fopen

Test Description

This test checks to see if allow_url_fopen is enabled.

Security Implications

If enabled, allow_url_fopen allows PHP's file functions -- such as `file_get_contents()` and the `include` and `require` statements -- can retrieve data from remote locations, like an FTP or web site. Programmers frequently forget this and don't do proper input filtering when passing user-provided data to these functions, opening them up to code injection vulnerabilities. A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is *on* by default.

Recommendations

You should disable allow_url_fopen in the php.ini file:

```
; Disable allow_url_fopen for security reasons
allow_url_fopen = 'off'
```

b) Section des tests non exécutés

Des tests peuvent ne pas être exécutés si :

- une fonctionnalité n'est pas activée (ex : PHP pas compilé en CGI, extension curl non activée)

Tests Not Run

Test	Result
CGI::force_redirect	**Not Run** You don't seem to be using the CGI SAPI **More information »**
Curl::file_support	**Not Run** CURL support is not enabled in your PHP install **More information »**

- la directive à tester n'est pas présente dans la version de PHP sur le serveur (PHP < 5.2.x)

Core::allow_url_include	**Not Run** You are running a version of PHP older than 5.2, and allow_url_include is not available **More information »**

c) Section résumé

Test Results Summary

Test	Result
Notice	7 out of 12 (58.33%)
Pass	4 out of 12 (33.33%)
Warning	1 out of 12 (8.33%)

4) Conclusion

PHPSecInfo :

- Ne remplace pas les bonnes pratiques de sécurisation des applications.
- Identifie des problèmes potentiels mais certains réglages déconseillés peuvent être nécessaires à l'environnement de production (par exemple file_uploads pour les sites permettant le dépôt de fichiers).
- Certains réglages ou conseils de sécurité ne sont pas pris en compte (activer use_only_cookies, placer des fonctions comme phpinfo, phpversion, php_uname, etc. dans disable_functions).

5) Sur Internet

Partie sécurité du manuel PHP	http://www.php.net/manual/en/security.php
PHP Security consortium	http://phpsec.org
Outil PHPSecInfo	http://phpsec.org/projects/phpsecinfo