

**NOUVEAU AU RAYON INFORMATIQUE - NOUVEAU AU RAYON INFORMATIQUE**

THE HACKADEMY PRESENTE

# SPECIAL WIRELESS

5,90 € - JANVIER 2004

LES MAGAZINES INFORMATIQUES NOUVELLE GÉNÉRATION



L 19168 - 3 H - F: 5,90 € - RD



**EN 2004 ON ARRACHE LES FILS !**

the HACKADEMY JOURNAL - the HACKADEMY JOURNAL - the HACKADEMY JOURNAL - the HACKADEMY JOURNAL - the HACKADEMY JOURNAL

# the HACKADEMY JOURNAL

N°12 3.20€



100% white hat hacking

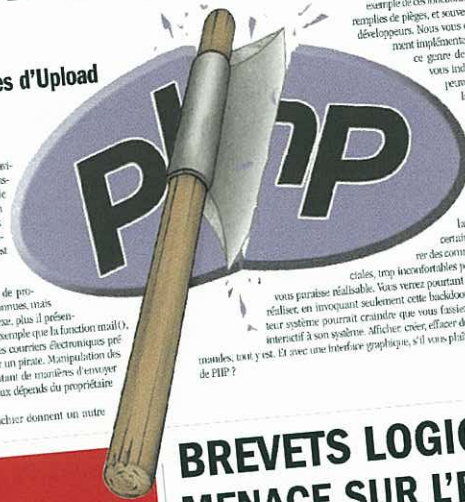
# PHP HACKING PARTY

- Détourner les mails
- Exploiter les formulaires d'Upload
- Backdoor en PHP

La plupart des bugs PHP est exploitables avec un simple navigateur web. Nous revenons du monde du développement sur les plus classiques, comme les SQL injections (page 4) et la faille include (page 14), dans des cas concrets et inédits. L'injection de code peut cependant éviter ces problèmes en réalisant correctement les paramètres donnés par l'utilisateur. La filtrage excessif pour corriger ces failles est d'ailleurs très facile à mettre en oeuvre.

Nous vous dévoilons ce mois-ci d'autres erreurs de programmation PHP, plus difficiles à exploiter, moins connues, mais néanmoins fréquentes. Plus un site web est complexe, plus il présente de vulnérabilités potentielles. Nous verrons par exemple que la fonction mail(), qui reste la manière la plus élégante d'envoyer des courriers électroniques, offre des possibilités intéressantes... pour un pirate. Manipulation des formulaires, décodage de l'encodage MIME : autant de manières d'envoyer des mails anonymes ou de jouer au spammeur sans dépendre du propriétaire du site vulnérable.

Les formulaires qui permettent l'envoi d'un fichier ont un autre



exemple de ces fonctionnalités, nous les avons remplis de pièges, et souvent mal utilisés par les développeurs. Nous vous expliquons donc comment implémenter, de manière sécurisée, ce genre de formulaires, non sans vous indiquer quelles méthodes peuvent se révéler fatales pour la sécurité du serveur.

Pour ceux qui ne mesurent toujours pas la gravité des problèmes liés à PHP, nous vous présentons enfin une backdoor écrite dans ce langage. L'exploitation de certaines failles demande d'insérer des commandes sous des formes spéciales, très inconfortables pour qu'une attaque puisse vous paraître réalisable. Vous verrez pourtant avec quelle facilité on peut réaliser, en invoquant seulement cette backdoor, tout ce qu'un administrateur système pourrait craindre que vous fassiez s'il vous donnait un accès interactif à son système. Afficher, créer, effacer des fichiers, exécuter des commandes, tout y est. Et avec une interface graphique, s'il vous plaît ! Est-ce là toute la puissance de PHP ?

Lire pages 9-11

## Sites gouvernementaux

### Les informations personnelles des citoyens bien mal protégées



## BREVETS LOGICIELS : MENACE SUR L'EUROPE

Les projets de lois de la commission qui rendent brevetables de simples méthodes pourrait asphyxier la création. Lire pages 6

### SOCIAL ENGINEERING REPORTAGE : Le Vidéo club donnait le numéro de CB de ses clients!

## C'EST L'HIVER DEVENEZ PINGOUIN LISEZ NOTRE NUMÉRO SPÉCIAL DÉBUTANT POUR PASSER A LINUX

### CRYPTOGRAPHIE

#### Notre nouvelle rubrique

Lire p.28

### TRAVAUX PRATIQUES

#### mail anonyme

Lire p.11

#### Programmer un Key logger

Lire p.12

#### TCHAT : attention au troyen mIRC

Lire p.6



#### Installer un serveur web sécurisé

Lire p.13

### SURF SESSION

#### La face cachée de Google

Lire p.16

#### IPcop : la solution routeur/firewall

Lire p.17

#### Adore : un rootkit surprenant

Lire p.26

#### ArenHack : la sécurité pour tous

Lire p.18

### FAILLE DU MOIS

#### Apache : un nouvel exploit sur les logs

Lire p.24



DOM 3,5€ - BEL 4€ - CH 6,40frs - CAN 5,95 \$CAN - MAR 35Dh - MAY 4,30€

# THE HACKADEMY JOURNAL FAIT BOUGER LES CHOSES

## EN CE MOMENT CHEZ VOTRE MARCHAND DE JOURNAUX