## 1. Injection dans le fichier cœur `index.php` (racine du site)

Le fichier `index.php` officiel de Joomla a été modifié : une variable `$__payload` (base64+gzip) a été ajoutée en tête de fichier, puis le code d'origine l'écrit dans un fichier temporaire et l'exécute (`include`) à **chaque affichage de page**, avant même que Joomla ne démarre.

## 2. Dizaines de « web shells » déposés dans `images/`

Le dossier `images/` (qui ne devrait contenir que des médias) contient plus d'une cinquantaine de fichiers `.php`/`.phtml`/`.pht`/`.php3`/`.php4`/`.php5` aux noms aléatoires (`up_XXXX.*`, `cmd_XXXX.*`, `jce_*.php`, `32o10hql.php`, `6282f87cc6d109c5.php`, `xeivos.php`, `class-template-provider.php`, etc.). Exemples de contenu :

## 3. Backdoor « auto-réparateur » + gestionnaire de fichiers caché

Le fichier `media/403.php` est un script de persistance très sophistiqué : protégé par un paramètre secret (`?bhca8373`), il compare la somme SHA1 de 4 fichiers précis à une valeur attendue et, en cas de différence (donc si un administrateur les nettoie), **re-télécharge automatiquement** la version piégée depuis un serveur externe (`dd.mega888my.info` — nom de domaine lié à un réseau de spam « casino/mega888 »). Les 4 fichiers surveillés :

- **`components/com_ajax/link.php`** : n'est PAS un fichier Joomla légitime. C'est un web shell obfusqué, littéralement nommé dans ses commentaires « WonderfulWebshell » (un shell PoC public).

- **`components/com_ajax/restorer.php`** (70 Ko) : un gestionnaire de fichiers web complet en chinois (« 文件管理器 »), protégé par le mot de passe `bhca@8373` (le même que le paramètre secret ci-dessus) — c'est le panneau d'administration caché de l'attaquant, lui donnant un accès total au système de fichiers du site à tout moment.