# PHPWind\_9.0.2漏洞披露

## 后台getshell

利用方式：远程

用户交互：不需要登录/需登录

权限要求：普通用户/功能管理员/

利用接口：/phpwind/admin.php?\_json=1&m=appcenter&c=app&a=upload

### 漏洞分析

漏洞位置出现在插件模板上传安装位置对应的源码位置为applications\appcenter\admin\AppController.php

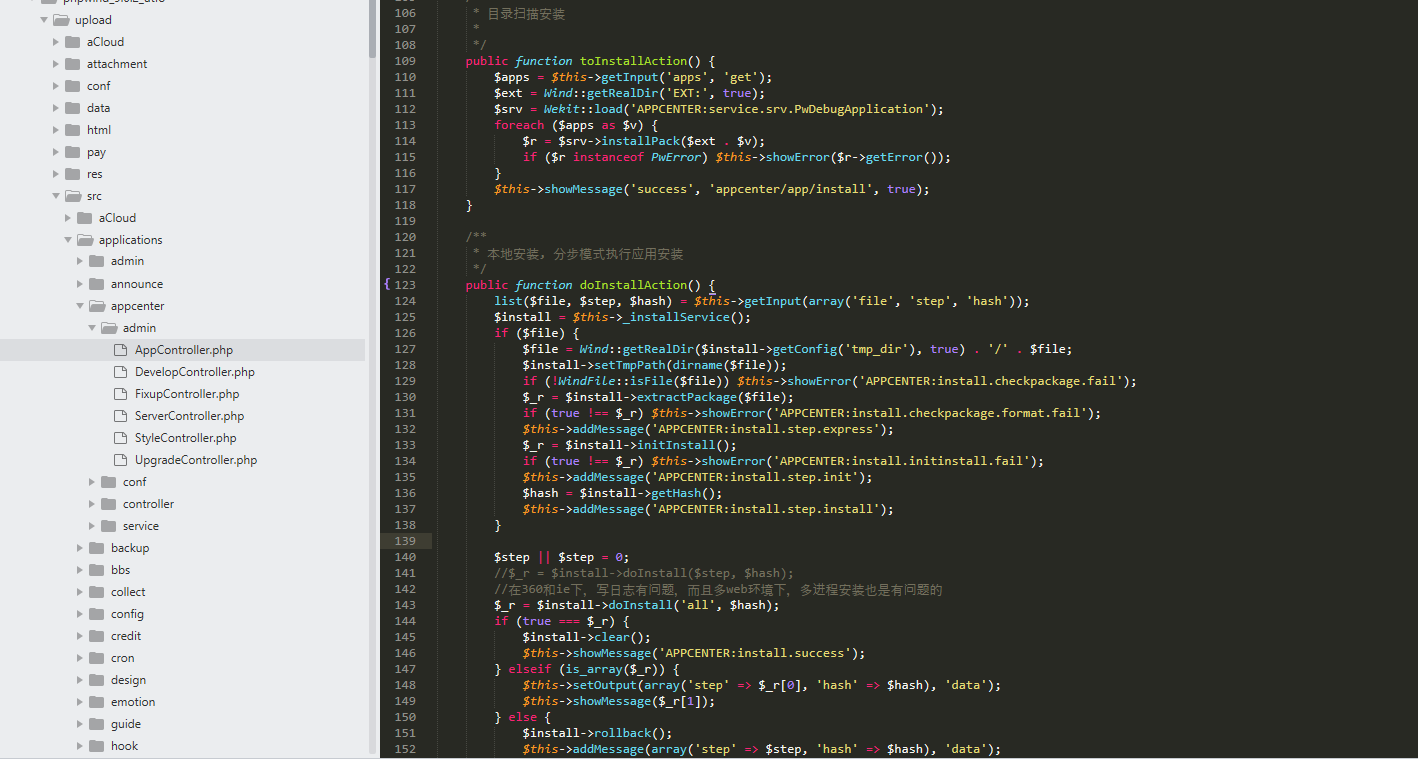


图1

跟踪代码执行当本地上传时会进入uploadAction函数，先进行了用户验证然后新建一个文件上传的PwApplicationUpload类开始执行上传



图2

跟进PwApplicationUpload此类的主要作用为队上传文件先进行文件类型（后缀）校验上传的文件是否为zip,并根据时间戳生死临时目录和hash后生成一个临时文件名返回保存



图3

上传后执行本地应该安装时进入doinstallAction



图4

根据时间戳获取到刚刚上传的文件信息进行解压，跟进extractPackage

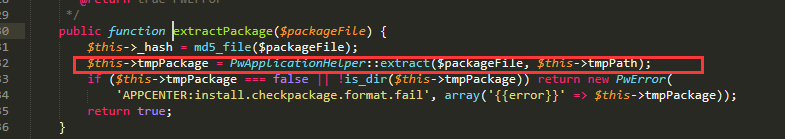


图5

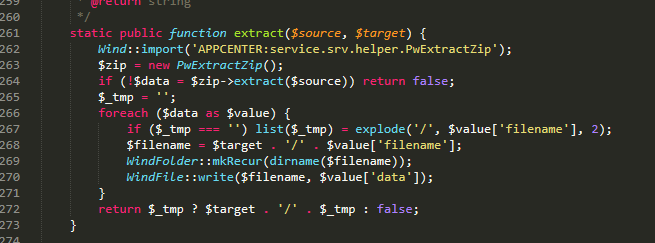


图6

phpwind\_9.0.2\_utf8\upload\src\applications\appcenter\admin\

\PwApplicationHelper.php

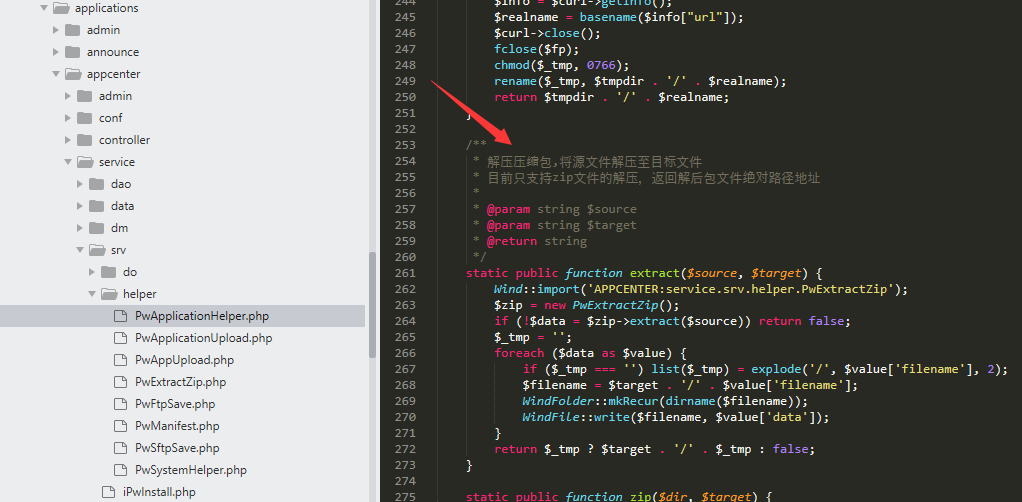


图7

解压后进行初始化安装包信息校验manifest

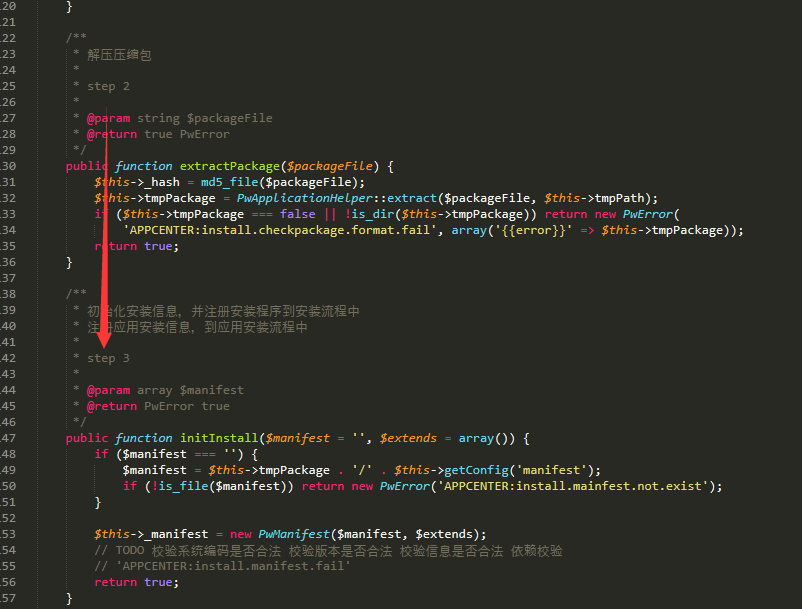


图8

getConfig解析manifest的配置信息

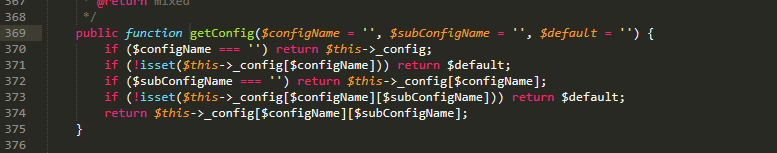


图9

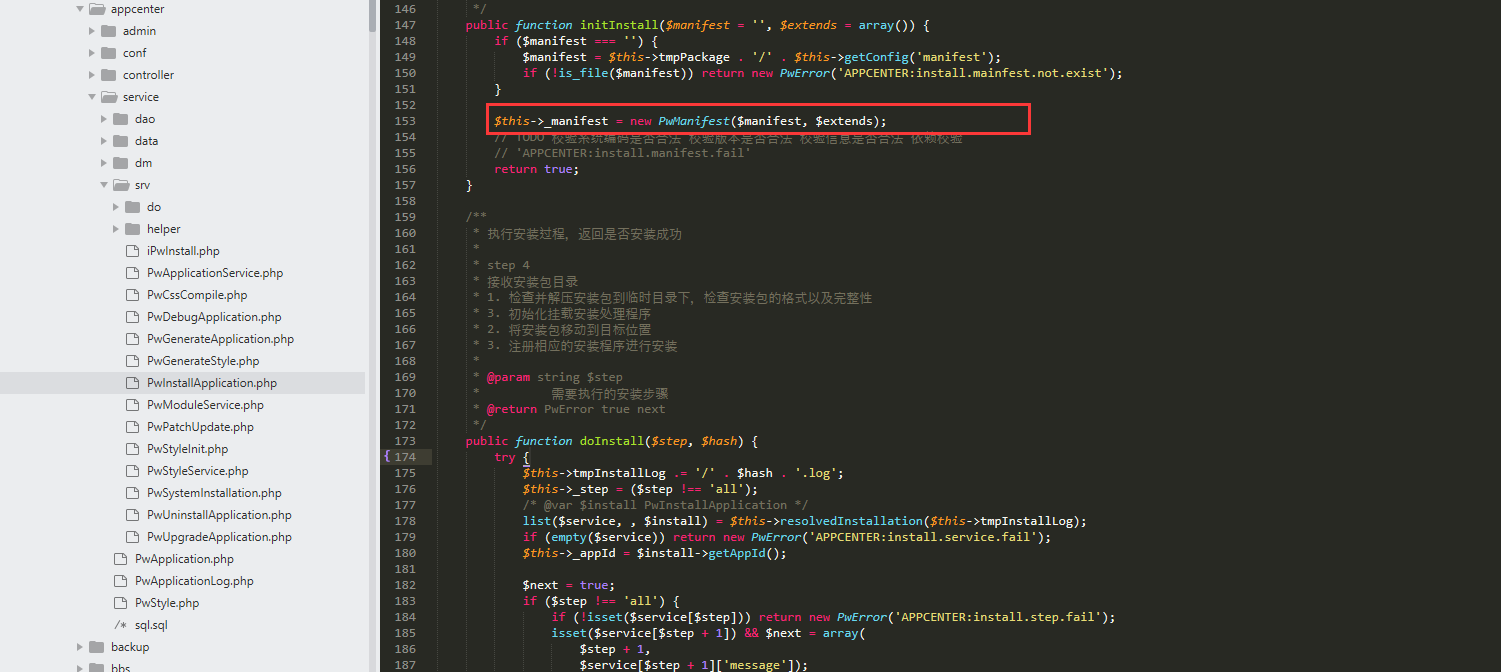


图10



图11

最后执行安装，若安装过程出现错误进行回滚。具体代码如下

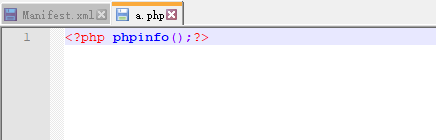


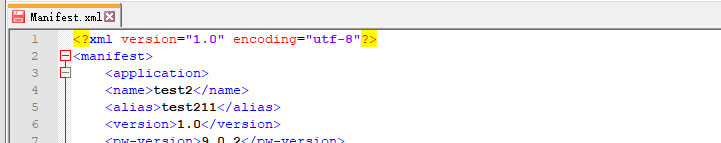
图11

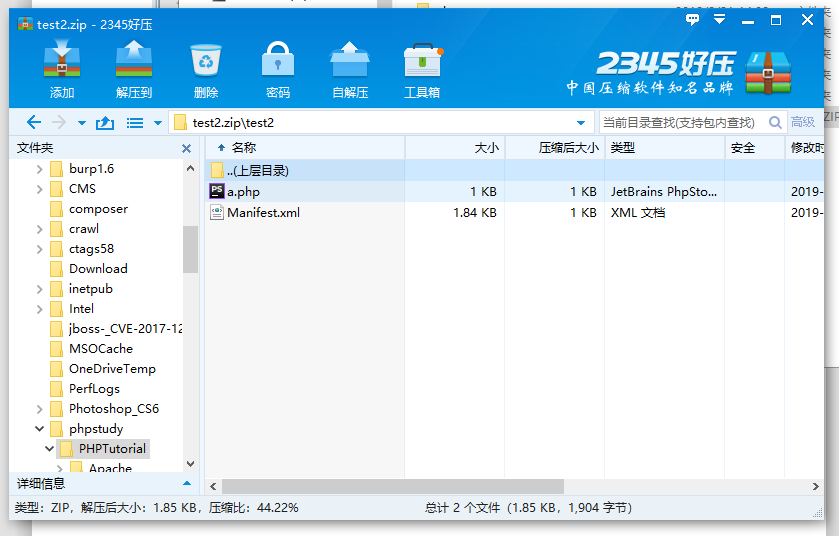
通过以上整个上传及解压流程可知，在对安装包的校验时主要在第三步此过程中主要校验了manifest的配置信息，只要压缩包中存在manifest.xml文件且配置信息中的alias名称不和之前重复即可解压安装成功，因此攻击者可以伪造包含manifest.xml文件的zip包，zip包除了伪造的manifest.xml还包含php后面文件，安装成功后木马即存在自解压的模板目录下，直接getshell。

### 复现

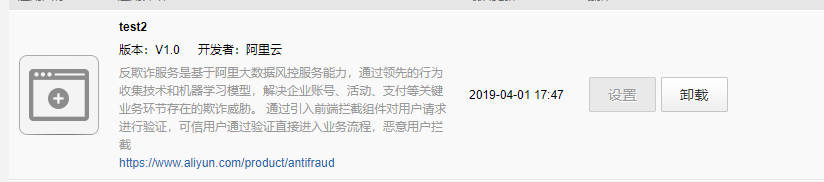
构造payload





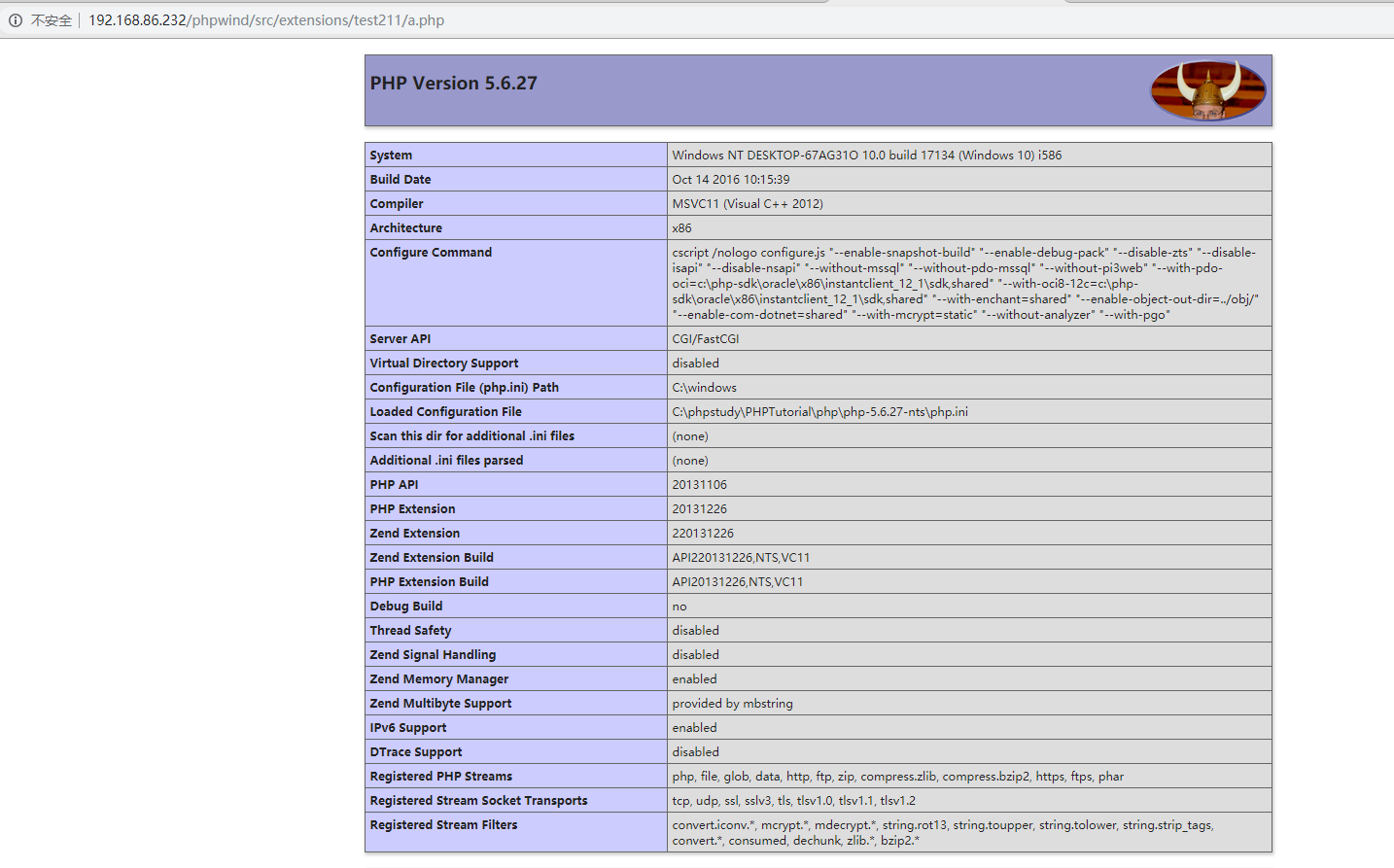






根据分析安装成功后的目录名为alias名称，最后访问a.php getshell

<http://192.168.86.232/phpwind/src/extensions/test211/a.php>



### 修复建议

严格验证下载的模板文件或manifest.xml的MD5值保证不可被伪造。

## 任意目录/文件删除

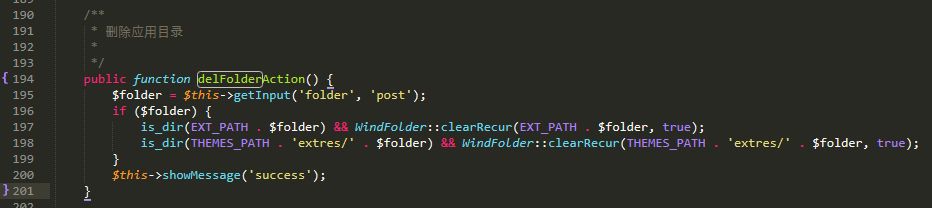
版本：phpwind先进版v 9.0.2

### 漏洞分析

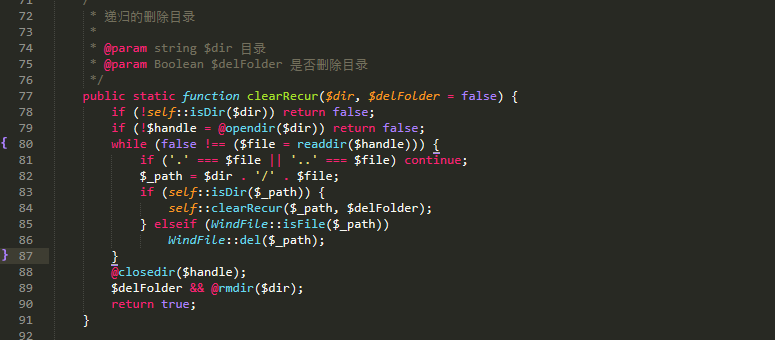
在程序代码位置phpwind\src\applications\appcenter\admin\AppController.php删除目录处代码194行处可以看到delFolderAction的对应功能为删除应用目录，先通过getInput方法获取了前台post的目录名，查看下此函数



直接获取&name并返回了&value,比较简单然后将返回的值直接给了$folder,接着连带$folder调用了clearRecur目录删除函数,



跟踪到此函数的定义在代码位置\phpwind\wind\utility\WindFolder.php 77行



此函数的功能是根据之前&folder值递归删除，整个删除过程folder并未进行任何过滤,直接造成任意目录删除。

再来看

\* 删除已上传压缩包

\*/

public function delFileAction() {

$file = $this->getInput('file', 'post');

if ($file && file\_exists(ATTACH\_PATH . $file)) {

WindFile::del(ATTACH\_PATH . $file);

}

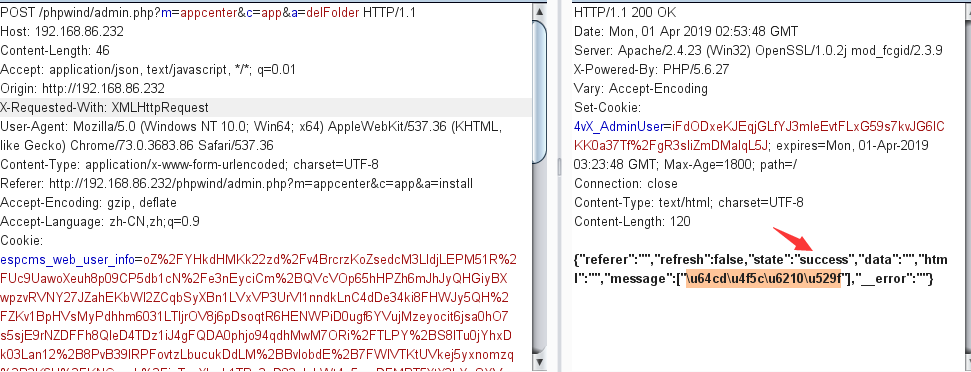
$this->showMessage('success');

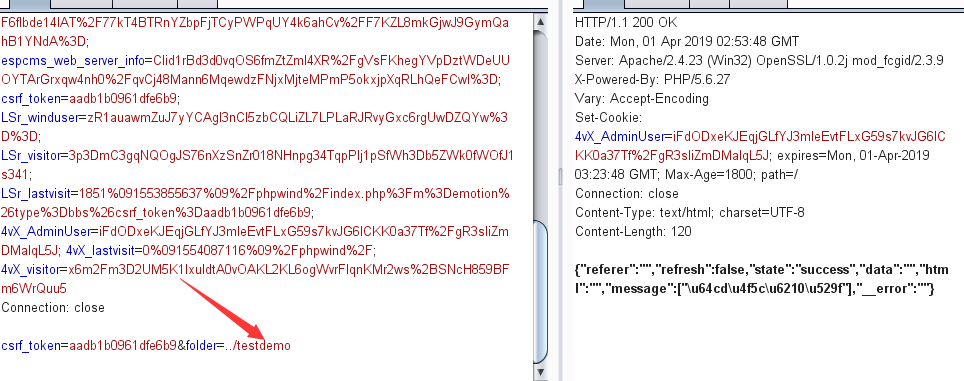
}

很明显File直接可控。

### 复现

任意目录删除





任意文件删除

