0x01 前言

PHPYun是一款国内流行的人才网站管理系统，做了一些测试，发现了一点问题，做个记录，未深入。

0x02 环境搭建

PHPYun官网：https://www.phpyun.com

网站源码版本：PHPYUN人才招聘系统v4.3Beta

程序源码下载：链接: https://pan.baidu.com/s/1pMQ58Np 密码: je4n

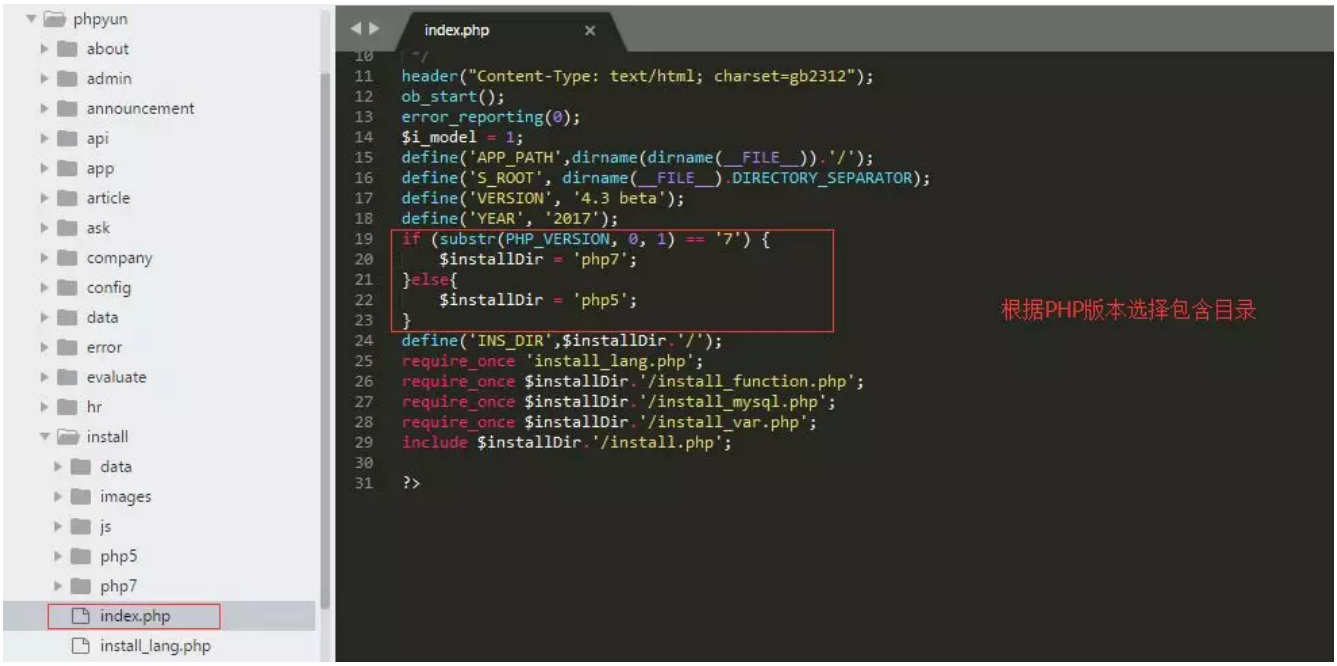
默认后台地址：http://127.0.0.1/admin/index.php

默认账号密码：admin/admin

0x03 CMS重装漏洞

代码分析：

1、漏洞文件位置：/install/index.php



在index.php中，根据PHP版本来选择包含目录，我们的环境包含的PHP5目录，进一步跟进PHP5目录查看代码

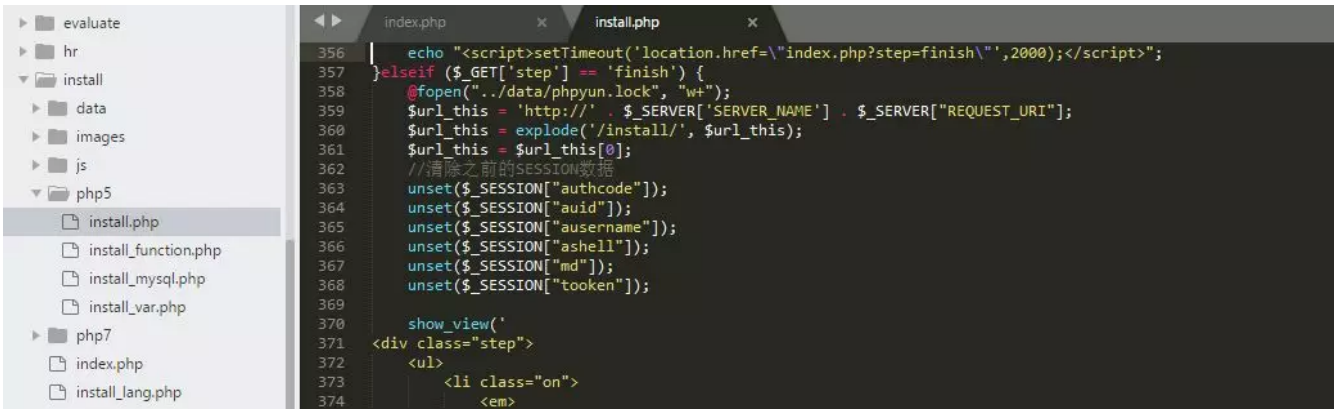
2、漏洞文件位置：/install/php5/install.php

可以看到，这边是有有做lock文件判断的，那么问题出在哪呢？ 我们再来看一下常量S_ROOT的定义：

define('S_ROOT', dirname(**FILE**).DIRECTORY_SEPARATOR);

也就是S_ROOT等价于 \install\，而不是根目录\;所以这边的判断是判断/install//data/phpyun.lock文件是否存在。

我们再来看一下同文件install.php下的第357-368行：



代码逻辑上，/install/index.php文件包含/install/php5/install.php文件，这边使用相对路径，那么生成的phpyun.lock文件在根目录下/data/phpyun.lock。

综上，在php5/install.php中判断/install/data/phpyun.lock文件是否存在，然而实际上phpyun.lock在/data/phpyun.lock中，导致程序在实现上存在CMS重装漏洞。

漏洞利用：

代码分析主要在代码逻辑上，利用却很简单，直接访问http://127.0.0.1/install/index.php 直接进入重装界面。

0x04 后台Getshell

代码分析:

漏洞文件位置：/admin/model/config.class.php 第88-114行中：

config.class.php

```
88    function save_action(){
89        if($_POST['config']){
90            unset($_POST['config']);
91            if($_POST['map_key']){
92                if(strpos($this->config['sy_weburl'],'https')!==false){
93
94                    $_POST['mapurl'] = 'https://api.map.baidu.com/api?v=2.0&ak='.$_POST['map_key'].'&s=1';
95
96                }else{
97                    $_POST['mapurl'] = 'http://api.map.baidu.com/api?v=2.0&ak='.$_POST['map_key'];
98                }
99            }
100           foreach($_POST as $key=>$v){
101               $config=$this->obj->DB_select_num("admin_config","`name`='$key'");
102               if($config==false){
103                $this->obj->DB_insert_once("admin_config","`name`='$key',`config`='".iconv("utf-8", "gbk", $v)."'");
104               }else{
105                $this->obj->DB_update_all("admin_config","`config`='".iconv("utf-8", "gbk", $v)."'","`name`='$key'");
106               }
107           }
108           if($_POST['code_strlength']<5){
109               $this->web_config();
110               $this->layer_msg("网站配置设置成功！",9,1);
111           }else{
112               $this->layer_msg("验证码字符数不要大于4！",8,1,'');
113           }
114       }
```

save_action函数对用户提交的参数写入数据库中，并调用web_config()函数进行写入到配置文件，我们继续跟进web_config()函数

漏洞文件位置：/app/public/common.php 第513-529行：

```php
function web_config(){
    $config=$this->obj->DB_select_all('admin_config');
    if(is_array($config)){
        foreach($config as $v){
            $configarr[$v['name']]=$v['config'];
        }
    }
    made_web(PLUS_PATH.'config.php',ArrayToString($configarr),'config');
    if(!file_exists(PLUS_PATH.'pimg_cache.php')){
        $this->advertise_cache();
    }
    if(!file_exists(PLUS_PATH.'dbstruct.cache.php')){
        include_once(LIB_PATH."cache.class.php");
        $cacheclass= new cache(PLUS_PATH,$this->obj);
        $cacheclass->database_cache("dbstruct.cache.php");
    }
}
```

这段代码从数据库中读取数据，并写入到配置文件config.php中，并未经任何处理，导致攻击者可以构造脚本代码写入配置文件，从而导致程序在实现上存在代码执行漏洞。

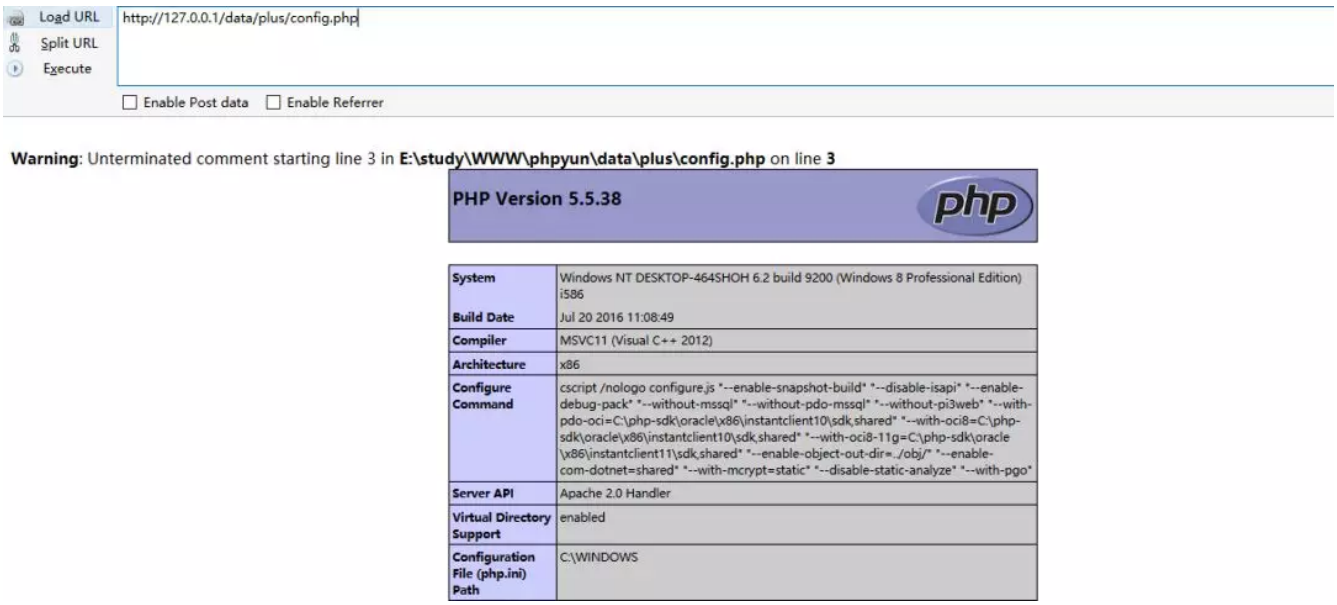
漏洞利用：

登录系统--网站设置--安全设置--填写Payload：

5.2版本： ");phpinfo();$config=array("

5.4版本：");phpinfo();/*

通过直接访问http://127.0.0.1/data/plus/config.php，成功触发代码执行漏洞



0x05 总结

像PHPYun这样的人才网站管理系统，相对功能会复杂些，但仍有很多可以挖掘的点，黑盒结合白盒进行测试，发现的两个问题，并未深入，欢迎志同道合的朋友来相互探讨，交流。

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。