3gcms的一次代码审计*（审一点发一点，有兴趣的可以跟上继续）

am0s / 2016-12-08 13:30:49 / 浏览数 3323 安全技术 漏洞分析 顶(0) 踩(0)

在源码之家发现这样一套源码http://guangzhou.mycodes.net/201410/3gcms2.0.rar
首先对框架目录大致了解一下。源码采用thinkphp2.1框架编写。

看了下网上公开的thinkphp的命令执行漏洞[size=;font-size:10.5000pt,10.5000pt]

```
$res = preg_replace('@(\w+)'.$depr.'([^'.$depr.'\/]+)@e', '$var[\'\1\']=\'\2\';', implode($depr,$paths));
```

这里已经被修复了，按照这个原理搜索文件
发现在\Core\Mode\Lite目录下的Dispatcher.class.php代码存在执行漏洞，但是本程序并没有开启lite模式。无法利用

查看install.php文件看到$lock_file = dirname(FILE).'/install.lck';
定义了防重复安装的文件，但是在下面并没有判断该文件。 导致重装漏洞。
下面的思路很明确了 。
重装进后台然后getshell
黑盒看了下后台，在后台模版处是可以修改模板后缀名的。。导致getshell

有兴趣的可以跟上继续，如果我挖到新洞还会继续接着发

上一篇：初探CSPBypass一些细节总结 下一篇：各种安全相关思维导图整理收集

1. 2 条回复


笑然 2016-12-09 01:54:34

加油~~

0 回复Ta


am0s 2016-12-09 11:59:34

小菜挖下去还是很吃力的 求大牛指点一下

0 回复Ta

目录