Phpcms_V9任意文件上传 -临时解决方案

potato / 2017-04-11 07:34:57 / 浏览数 4353 安全技术 漏洞分析 顶(0) 踩(0)

很简单，在download函数中我们可以看到，`$remotefileurls``数组，中，$k是未经过滤去除#.jps的恶意url，而$file是经过过滤处理的恶意url。并且保存的后缀，将会使用
修改 phpcms/libs/classes/attachement.class.php 文件中的download函数
在

```
foreach($remotefileurls as $k=>$file)
```

循环中，大约是167行左右的位置，将

```
            if(strpos($file, '://') === false || strpos($file, $upload_url) !== false) continue;
$filename = fileext($file);
```

修改成

```
            $filename = fileext($k);
```

我们再使用poc测试一下
如图

图中的两个jpg文件，就是我测试的结果。这样就可以防御住任意文件上传攻击了。

正在写具体分析，所以呢大家等一下吧

上一篇：Metasploit、Powers... 下一篇：phpcms v9.6.0 wap...
1. 0 条回复
   - 动动手指，沙发就是你的了！