phpok 4.8.338版本存在 任意文件上传漏洞

漏洞描述

phpok是深圳市锟铻科技有限公司一套采用PHP+MYSQL语言开发的企业网站系统。 phpok 4.8.338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。

漏洞分析

在 www/framework/admin/rescate_control.php 第 53行

```
public function save_f()
    {
        $id = $this->get('id','int');
        if(!$id){
            if(!$this->popedom['add']){
                $this->json(P_Lang('您没有权限执行此操作'));
            }
        }else{
            if(!$this->popedom['modify']){
                $this->json(P_Lang('您没有权限执行此操作'));
            }
        }
        $title = $this->get('title');
        if(!$title){
            $this->json(P_Lang('附件分类名称不能为空'));
        }
        $root = $this->get('root');
        if(!$root){
            $this->json(P_Lang('附件存储目录不能为空'));
        }
        if($root == '/'){
            $this->json(P_Lang('不支持使用/作为根目录'));
        }
        if(!preg_match("/[a-z0-9\_\/]+/",$root)){
            $this->json(P_Lang('文件夹不符合系统要求，只支持：小写字母、数字、下划线及斜
杠'));
        }
        if(substr($root,0,1) == "/"){
            $root = substr($root,1);
        }
        if(!file_exists($this->dir_root.$root)){
            $this->lib('file')->make($this->dir_root.$root);
        }
        $filetypes = $this->get('filetypes');
        if(!$filetypes){
            $this->json(P_Lang('附件类型不能为空'));
        }
        $list_filetypes = explode(",",$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'));
            }
        }
        $filetypes = implode(",",$list_filetypes);
        $typeinfo = $this->get('typeinfo');
        if(!$typeinfo){
            $this->json(P_Lang('附件类型说明不能为空'));
        }
        $maxinfo =
str_replace(array('K','M','KB','MB','GB','G'),'',get_cfg_var('upload_max_filesiz
e')) * 1024;
        $filemax = $this->get('filemax','int');
        if(!$filemax || ($filemax && $filemax>$maxinfo)){
            $filemax = $maxinfo;
        }
        $data =
array('title'=>$title,'root'=>$root,'filetypes'=>$filetypes,'typeinfo'=>$typeinf
o,'filemax'=>$filemax);
        $data['folder'] = $this->get('folder');
        $data['gdall'] = $this->get('gdall','int');
        if(!$data['gdall']){
            $gdtypes = $this->get('gdtypes');
            $data['gdtypes'] = $gdtypes ? implode(',',$gdtypes) : '';
        }else{
            $data['gdtypes'] = '';
        }
        $data['ico'] = $this->get('ico','int');
        $data['is_default'] = $this->get('is_default','int');
        $this->model('rescate')->save($data,$id);
        $this->json(true);
    }
```

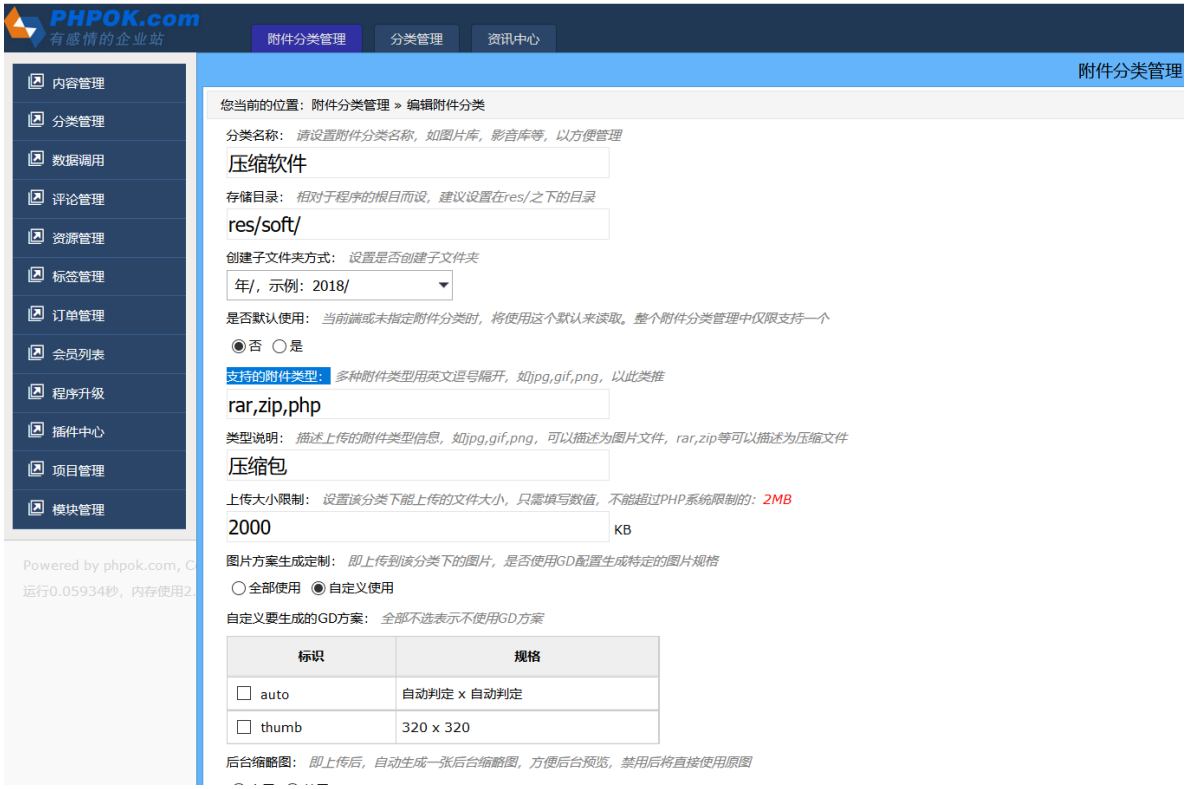
这段代码是设置 可以上传的附件类型的代码。重点看下段代码

```
$list_filetypes = explode(",",$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'));
    }
}
$filetypes = implode(",",$list_filetypes);
```

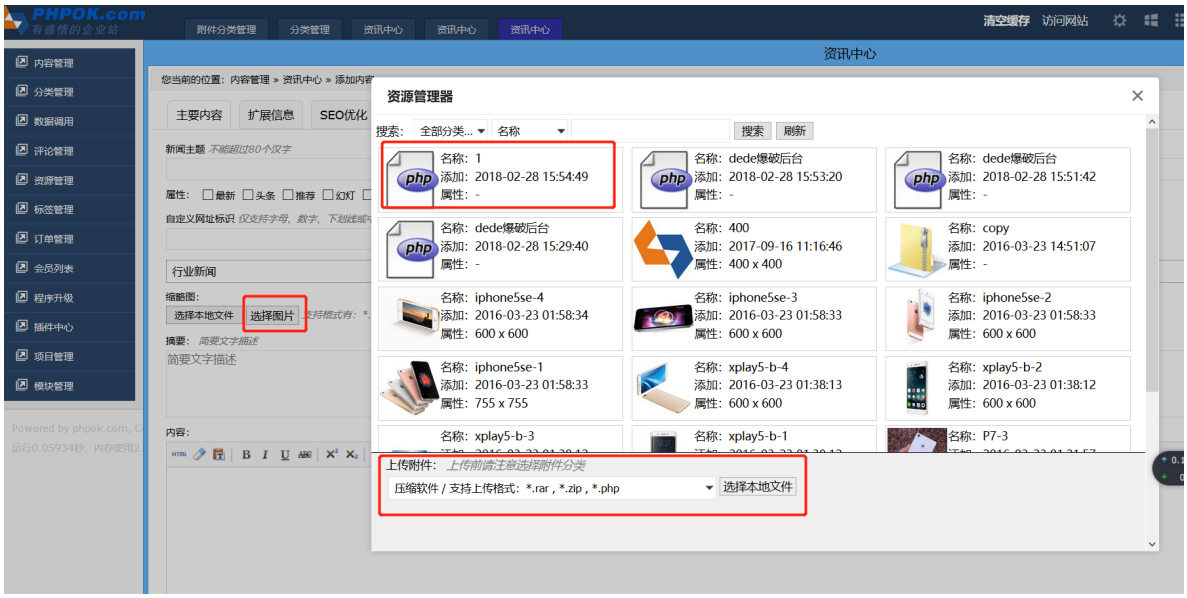
这里只判断附件类型是否为空，并没有限制后缀，导致可以自行添加php后缀，进而执行上传文件操作，获取网站shell。

漏洞复现：

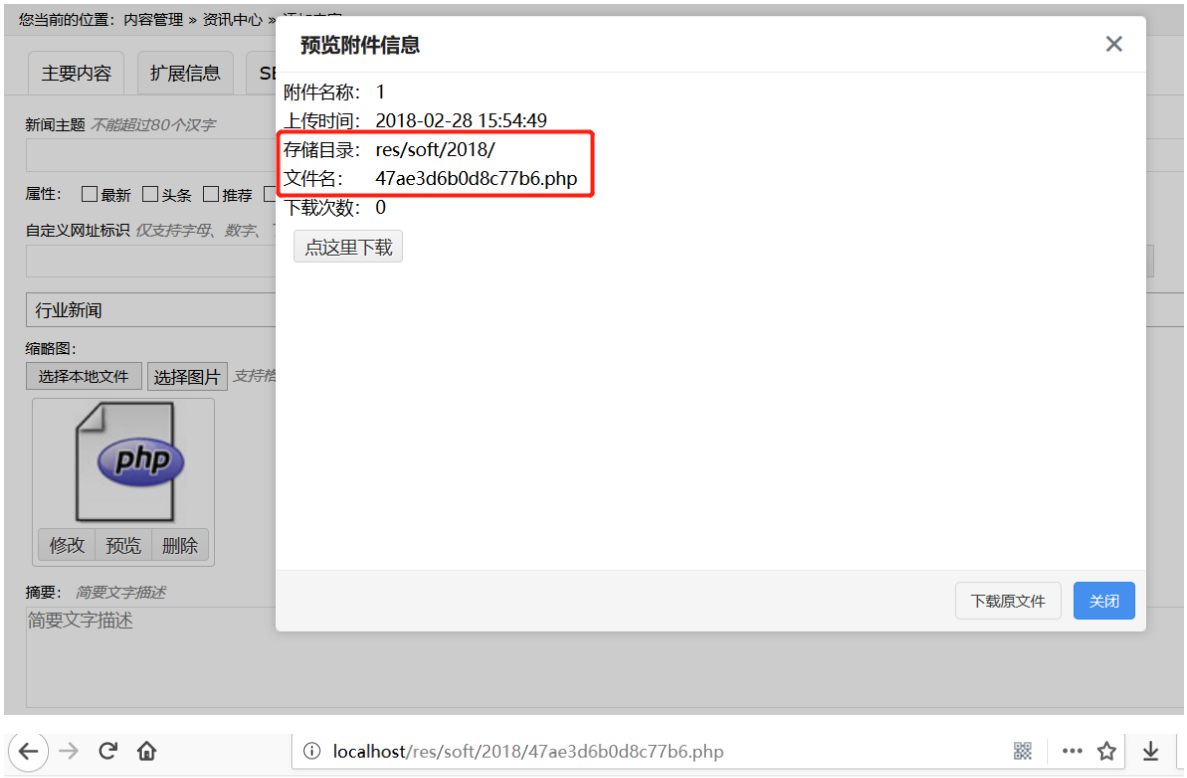
在phpok 管理员后台，选择 工具 > 附件分类管理 编辑分类列表。在 支持的附件类型： 中添加php。



然后再内容管理>行业新闻 添加新的文章。在选择图片，资源管理器中上传新的附件。



上传成功之后，点击预览，即可看到上传的附件的地址。



php shell

修复方案：

对上传类型后缀进行过滤