登录

ZZCMS任意删除漏洞(CVE-2019-8411)分析

此生已尽我温柔 / 2019-02-27 09:48:00 / 浏览数 1185 安全技术 漏洞分析 顶(0) 踩(0)

---

zzcms 任意删除文件漏洞(CVE-2019-8411) 分析

Payload：

```
action = del■filename = .. / 1.php
```

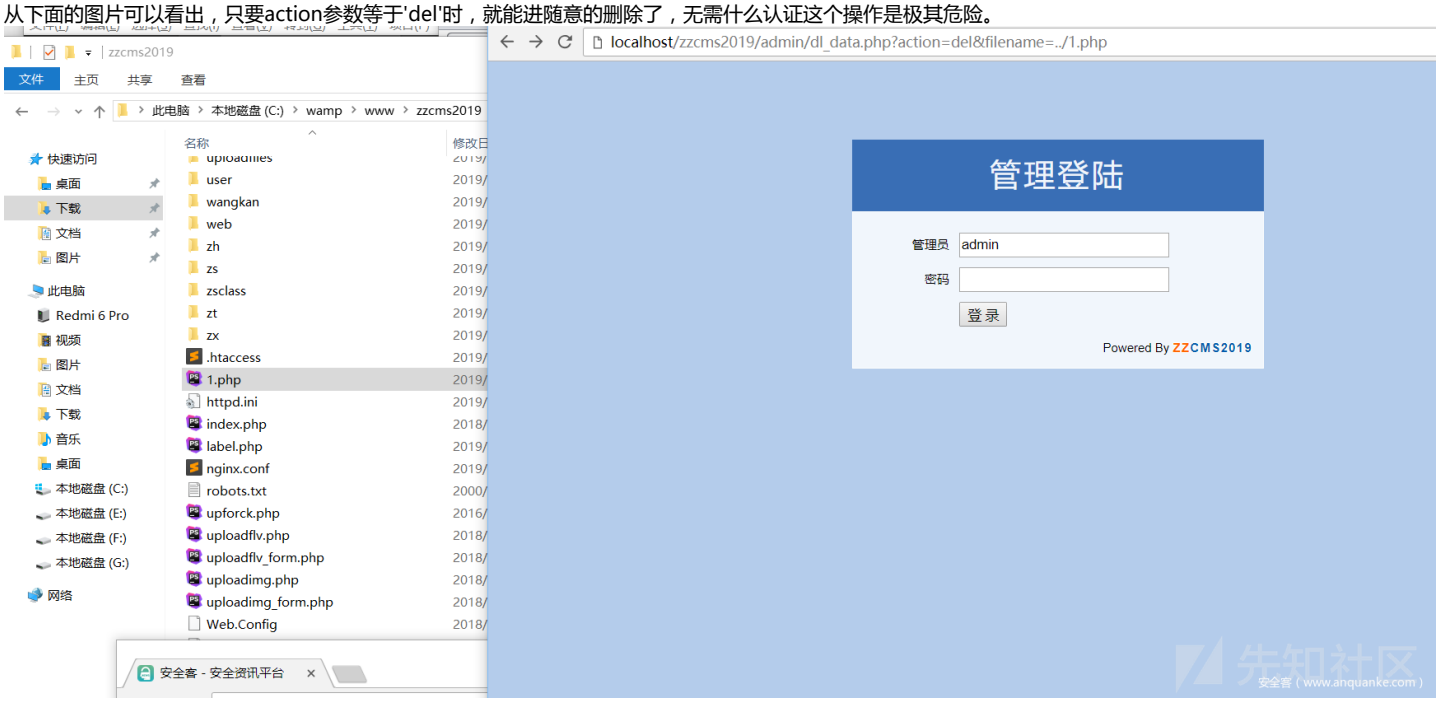
漏洞分析

这个漏洞产生的很大原因是开发者没有按照正确的安全开发，对敏感操作没有进行认证。

打开admin/dl_data.php，发现只要把del赋值action参数，然后添加需要删除的文件，就可以删除了，没有进行任何的认证。

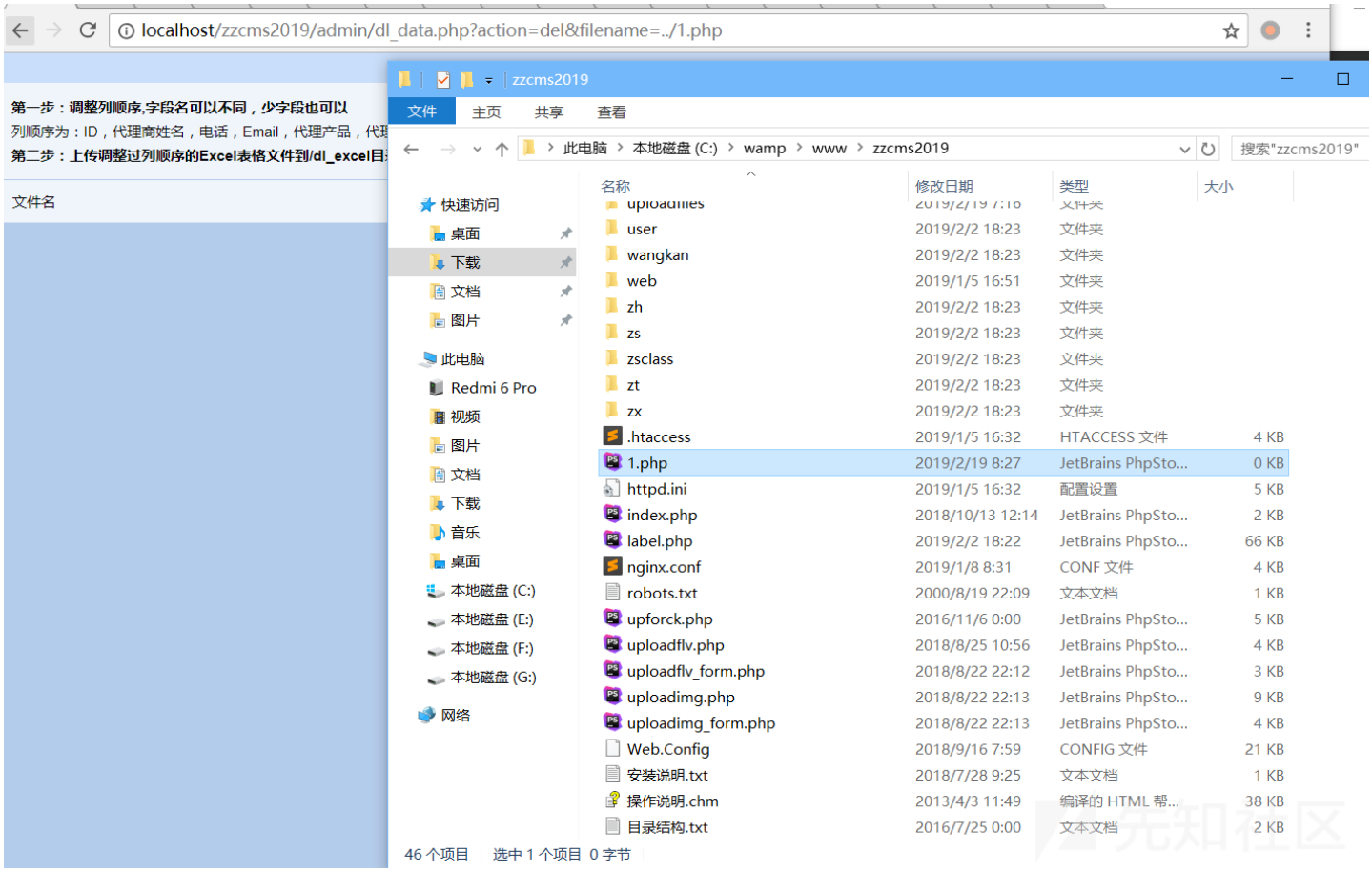
```
if ($action=="del") {
$fp="../dl_excel/".$_GET["filename"];
    if (file_exists($fp)){
    unlink($fp);
    }else{
    echo "<script>alert('请选择要删除的标签');history.back()</script>";
    }
}
```


从下面的图片可以看出，只要action参数等于'del'时，就能进随意的删除了，无需什么认证这个操作是极其危险。



进行简单的添加认证后，这个Payload 就失效了，当然这个认证只是我个人的随意添加的，更多细节需要开发者团队自己增加。

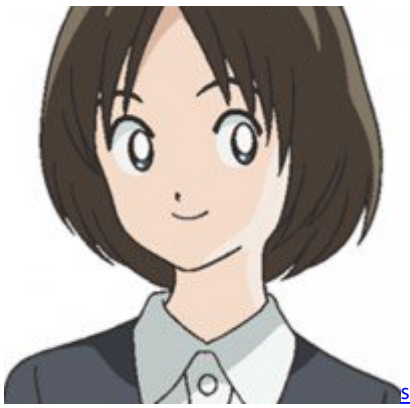
```php
if (isset($_COOKIE["admin"]) && isset($_COOKIE["pass"])){
    $sql="select * from zzcms_admin where admin='".addslashes($_COOKIE["admin"])."'";
    $rs=query($sql) or showmsg('查寻管理员信息出错');
    $ok=is_array($row=fetch_array($rs));
    if($ok){
        if ($_COOKIE["pass"]!=$row['pass']){
        showmsg('管理员密码不正确，你无权进入该页面','../admin/login.php');
        }
    }else{
    showmsg('管理员已不存在，你无权进入该页面','../admin/login.php');
    }
}else{
if ($action=="del") {
$fp="../dl_excel/".$_GET["filename"];
    if (file_exists($fp)){
    unlink($fp);
    }else{
    echo "<script>alert('请选择要删除的标签');history.back()</script>";
    }
}
}
```



点击收藏 | 1 关注 | 1

上一篇：深入分析恶意软件 Emotet 的... 下一篇：浅析区块链共识机制

1. 1 条回复



sera 2019-02-27 15:12:54

。。

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板