ctf-wp-第三届“百越杯”福建省高校网络空间安全大赛 Do you know upload?

原创

zc01@ 于 2018-09-28 14:17:16 发布 1092 收藏

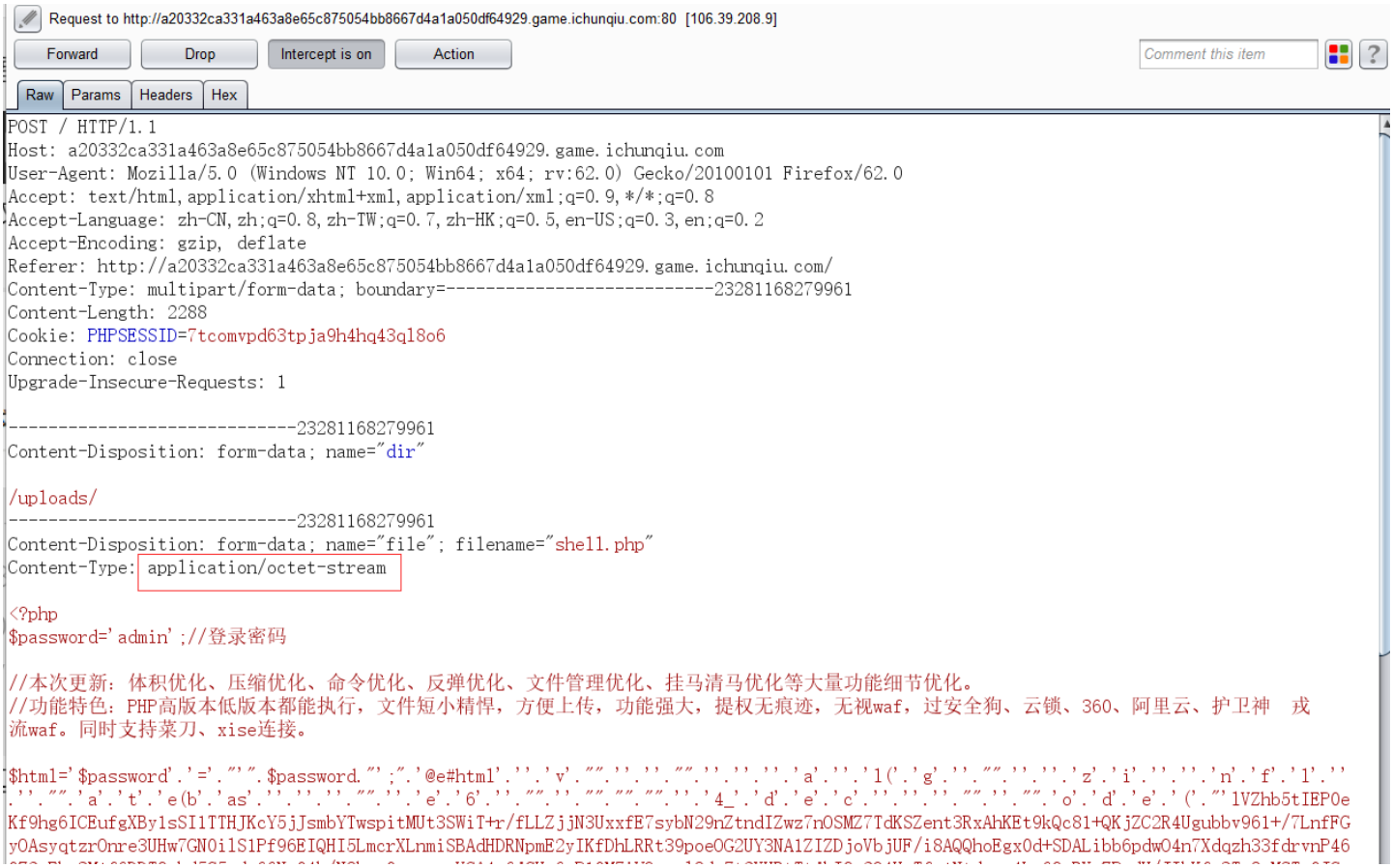
分类专栏： ctf-wp 文章标签： ctf wp web 文件上传

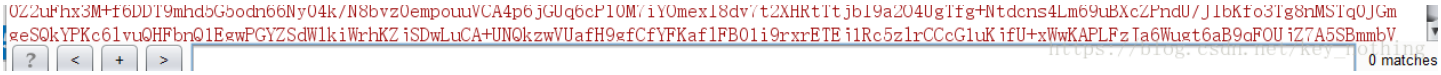
本文链接：https://blog.csdn.net/key_nothing/article/details/82882582

考察：文件上传漏洞、数据库基本操作

访问url ：只能上传图片文件

试着上传大马，burp抓包：





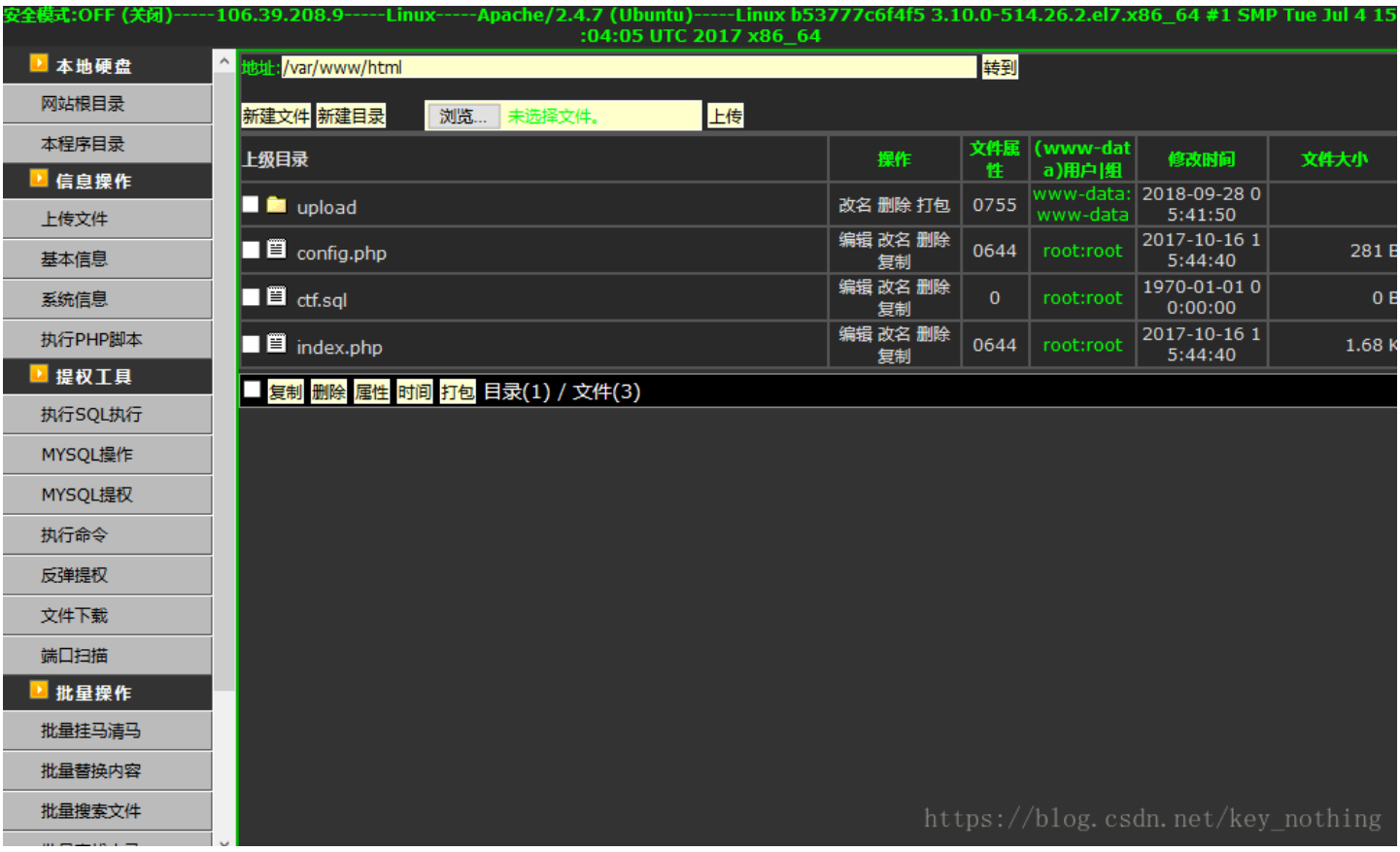
尝试修改文件类型为：image/jpeg
结果上传成功：

图片上传

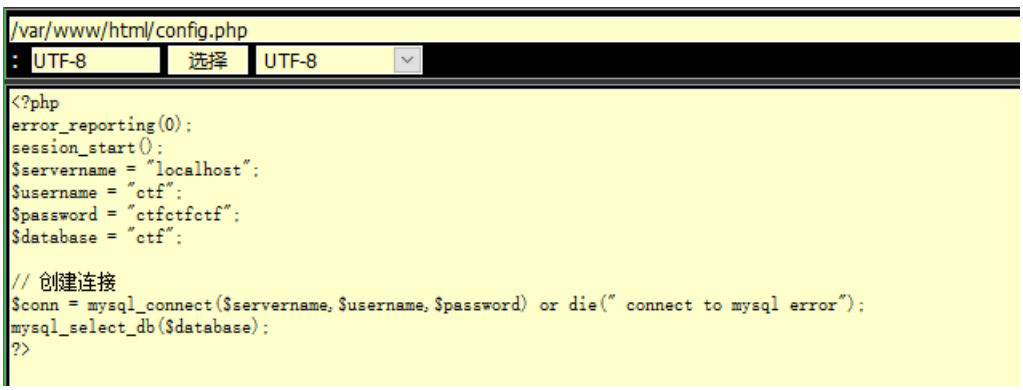
Filename: 浏览... shell.php
Submit

Upload: shell.php
Type: image/jpeg
Size: 1.8369140625 Kb
Stored in: upload/shell.php

访问大马：



发现有个ctf.sql 。flag应该在数据库中，看看config.php，找到数据库连接方法：



执行一下sql语句：看看都有那些表

存在flag表，看看内容：

bingo