安恒杯学到的新姿势

原创

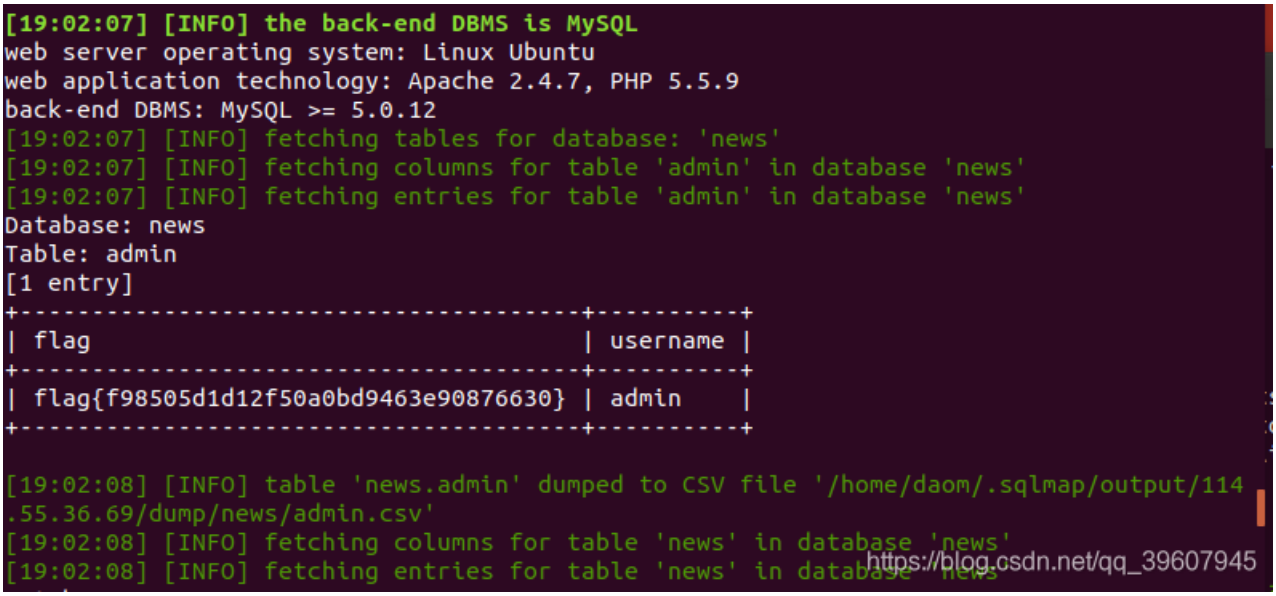
GG BON 于 2019-09-13 16:22:39 发布 218 收藏

新闻搜索

考点：POST注入

工具：BP、sqlmap

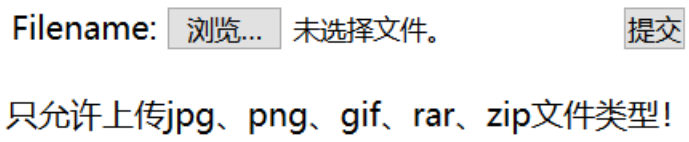
本题考查POST注入，一般的注入是GET型的，当用POST表单传参数的时候就不能起效，此时需要进行POST注入。而在本题中，通过截取请求包，然后利用sqlmap命令`sqlmap -r 文件名 -D news --dump`，news是本题中的数据库名。即可完成注入。



常规操作

考点：文件上传、phar://漏洞

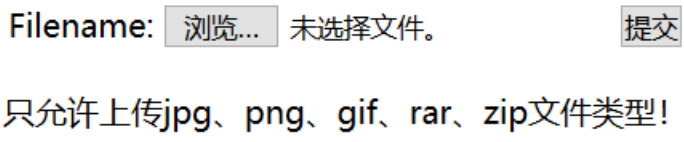
打开页面之后发现：



只允许上传jpg、png、gif、rar、zip文件类型!

提示了可以上传的文件的格式，里面有zip后缀的，查资料了解到可能域phar伪协议有关，phar伪协议主要是用来解析phar文件的，也即压缩文件，具体的作用见https://mp.csdn.net/mdeditor/100797979

我们在本地创建一个小马，然后压缩成.zip格式，上传上去



只允许上传jpg、png、gif、rar、zip文件类型!

文件保存路径为: /var/www/html/upload
/37b16dc4fd3112bee367527f57364ba9.zip

看到了文件的路径，然后访问url：`http://114.55.36.69:8009/index.php?url=phar://upload/37b16dc4fd3112bee367527f57364ba9.zip/south`实现对.zip的解析。然后我们用该链接连接小马即可。