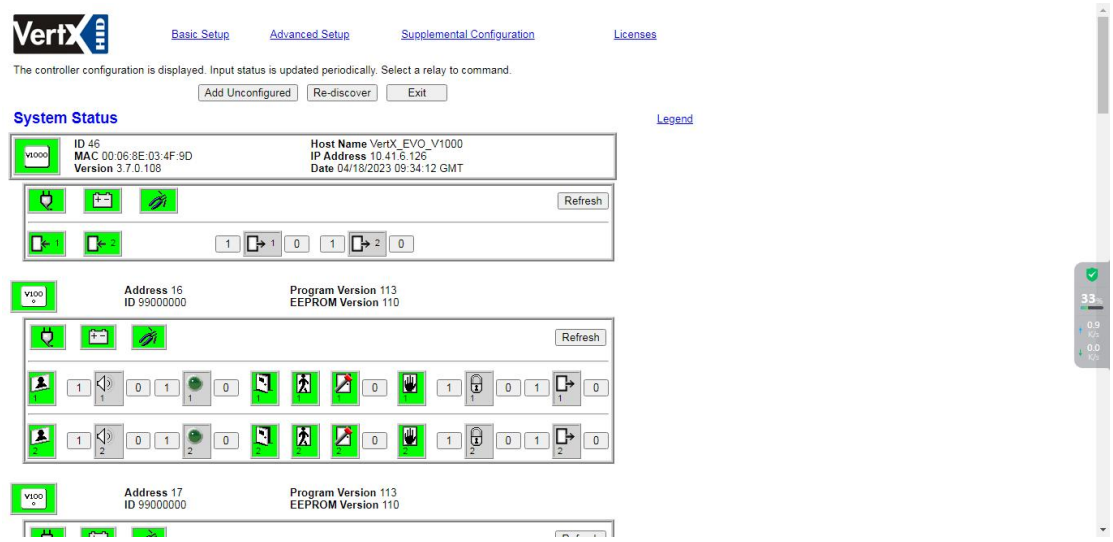
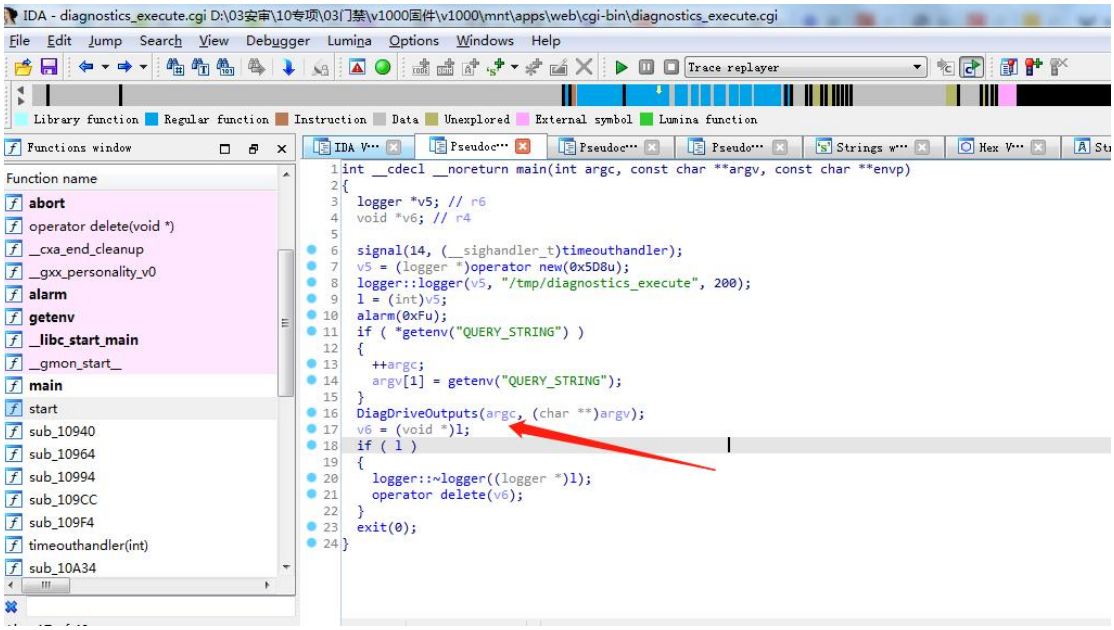
1. BoardType, Description, and Relay parameters overflow

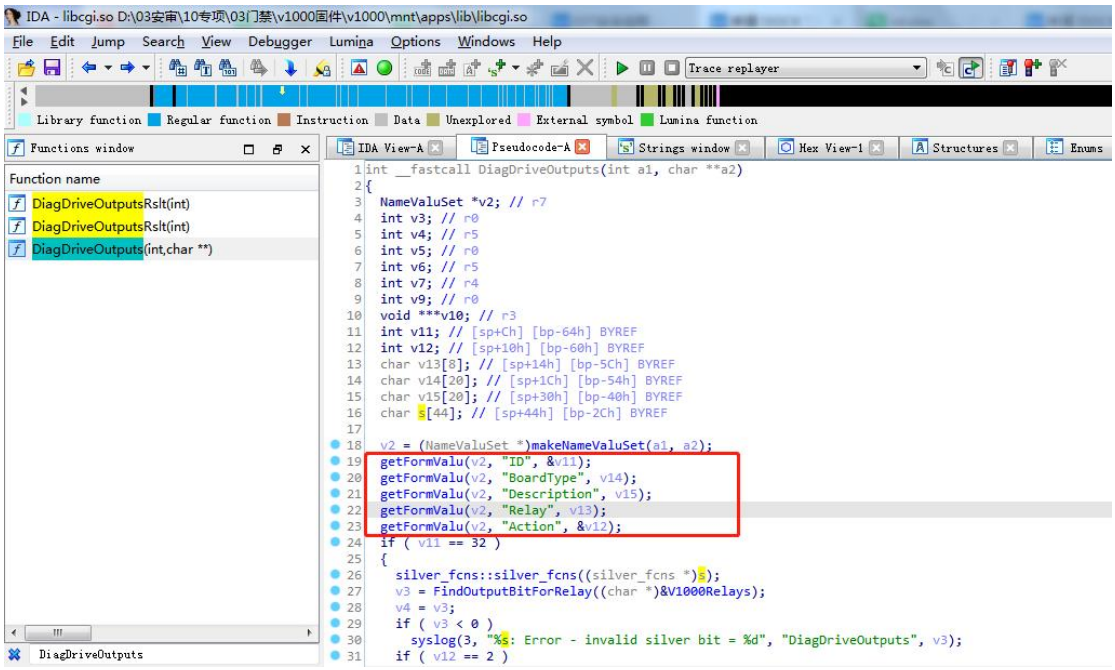
This is the front-end control interface, which can control the opening and closing of the door, etc.
https://xx.xx.xx.xx/cgi-bin/diagnostics.cgi?Category=status



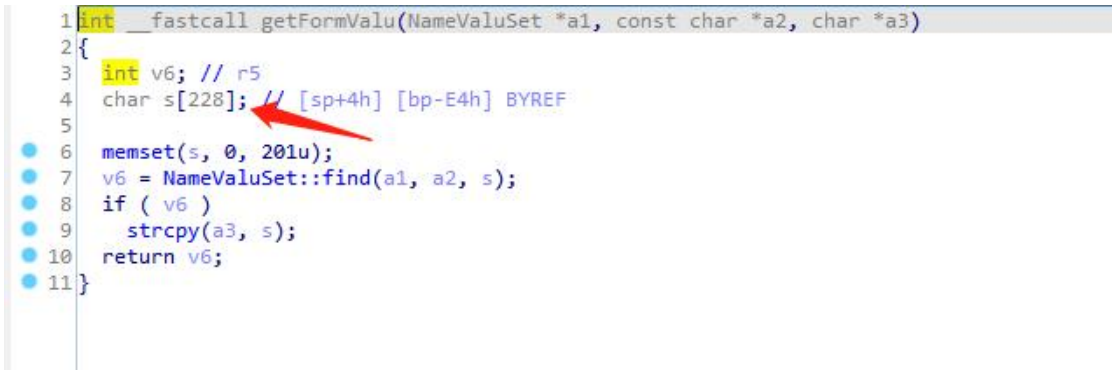
The program entry of the backend, the following DiagDriveOutputs is to parse the parameters passed in by the front end, there is a buffer overflow vulnerability in the parsing process of the interface parameters, in which DiagDriveOutputs is implemented by libcgi.so, so the vulnerability exists in libcgi.so



Open Libcgi.so, the buffer sizes of the three parameters of BoardType, Description, and Relay are 20, 20, and 8 respectively, and the function for parsing the three parameters of BoardType, Description, and Relay is getFormValu



Open getFormValu, you can see that the length of the buffer is 228, far exceeding the buffer length of the three parameters of BoardType, Description, and Relay, so these are the three buffer overflow points.



2. The secondary overflow caused by the overflow of the Description parameter

The maximum length of the Description buffer is 228, and the length of v7 is 20, so strcpy may also cause secondary overflow.

```
16  char v16[20]; // [sp+1Ch] [bp-54h] BYREF
17  char v17[20]; // [sp+30h] [bp-40h] BYREF
18  char s[44]; // [sp+44h] [bp-2Ch] BYREF
19
20  v2 = (NameValuSet *)makeNameValuSet(a1, a2);
21  getFormValu(v2, "ID", &v13);
22  getFormValu(v2, "BoardType", v16);
23  getFormValu(v2, "Description", v17);
24  getFormValu(v2, "Relay", v15);
25  getFormValu(v2, "Action", &v14);
26  if ( v13 == 32 )
27  {
28    silver_fcns::silver_fcns((silver_fcns *)s);
29    v3 = FindOutputBitForRelay((char *)&V1000Relays);
30    v4 = v3;
31    if ( v3 < 0 )
32      syslog(3, "%s: Error - invalid silver bit = %d", "DiagDriveOutputs", v3);
33    if ( v14 == 2 )
34      v5 = silver_fcns::set_timed_silver_bit((silver_fcns *)s, v4);
35    else
36      v5 = silver_fcns::set_silver_bit((silver_fcns *)s, v4, v14);
37    v6 = v5;
38    silver_fcns::~silver_fcns((silver_fcns *)s);
39    goto LABEL_8;
40  }
41  if ( !strcmp(v16, "V100") )
42  {
43    v7 = (char *)memset(s, 0, 0x14u);
44    v8 = strcpy(v7, v17);
45    strcat(v8, v15);
46    v9 = FindOutputBitForRelay(V100Relays);
47    if ( !strcmp(v17, "ForcedDoor") )
```