## 极路由 ssh close 的情况下强行开启极路由 ssh 进行代码执行

首先我们认识几个页面来了解这个利用链的方式。

`http://192.168.199.1/local-ssh/`
这个页面会下发一个 `local_token` 供服务器验证，每次请求完都会刷新。同时提供校验服务和执行作用。

路由默认指向 `http://www.4006024680.com`，实则解析 `192.168.199.1` 如果不是请手动解析至 路由管理 `ip+uri`


*Figure 1:*

`http://192.168.199.1/cgi-bin/turbo/proxy/router_info`
访问后会返回一串 `json` 的数据，其中 `debug_info` 中会显示你访问来源 `ip` 和路由的网关 `ip` 并会返还一个时间戳，以及路由型号 `UUID`，我们记住这个 `UUID`，一会要用。

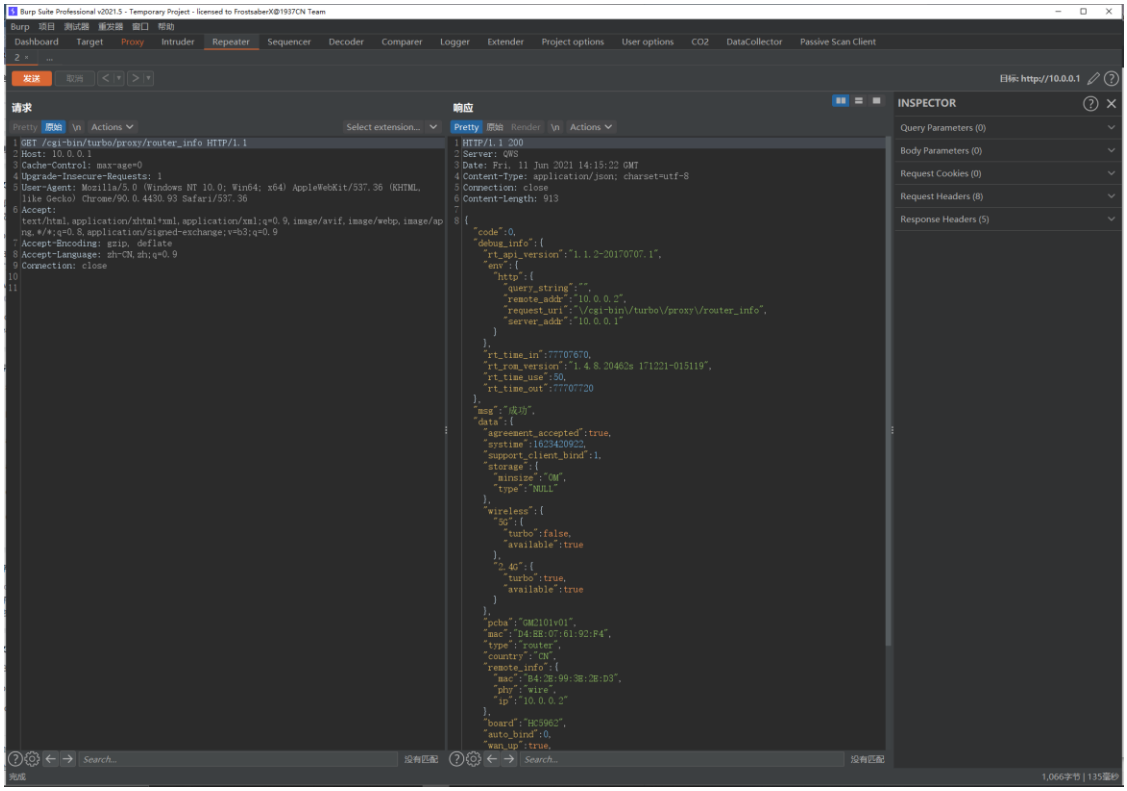


*Figure 2:*

漏洞原理是一个官方的后门，用来给客服强制临时开启 SSH 进行远程调试。其简单原理就是随机 token 来和 UUID 生成一串 cloud token 然后进行验算，目前使用一个接口来给各位提供验算生成服务。

然后记录下 local_token 和 UUID，打开

```
www.hiwifi.wtf  //hiwifi what fuck ?
```

输入 获取 `cloud token` ，提交后就可以打开 `ssh`

ssh 密码为 WiFi 密码 用户名 root 通过以上方式就可以进行 RCE 远程代码执行，因为是 root 权限，所以可以进行固件替换后门等 持久化操作为所欲为

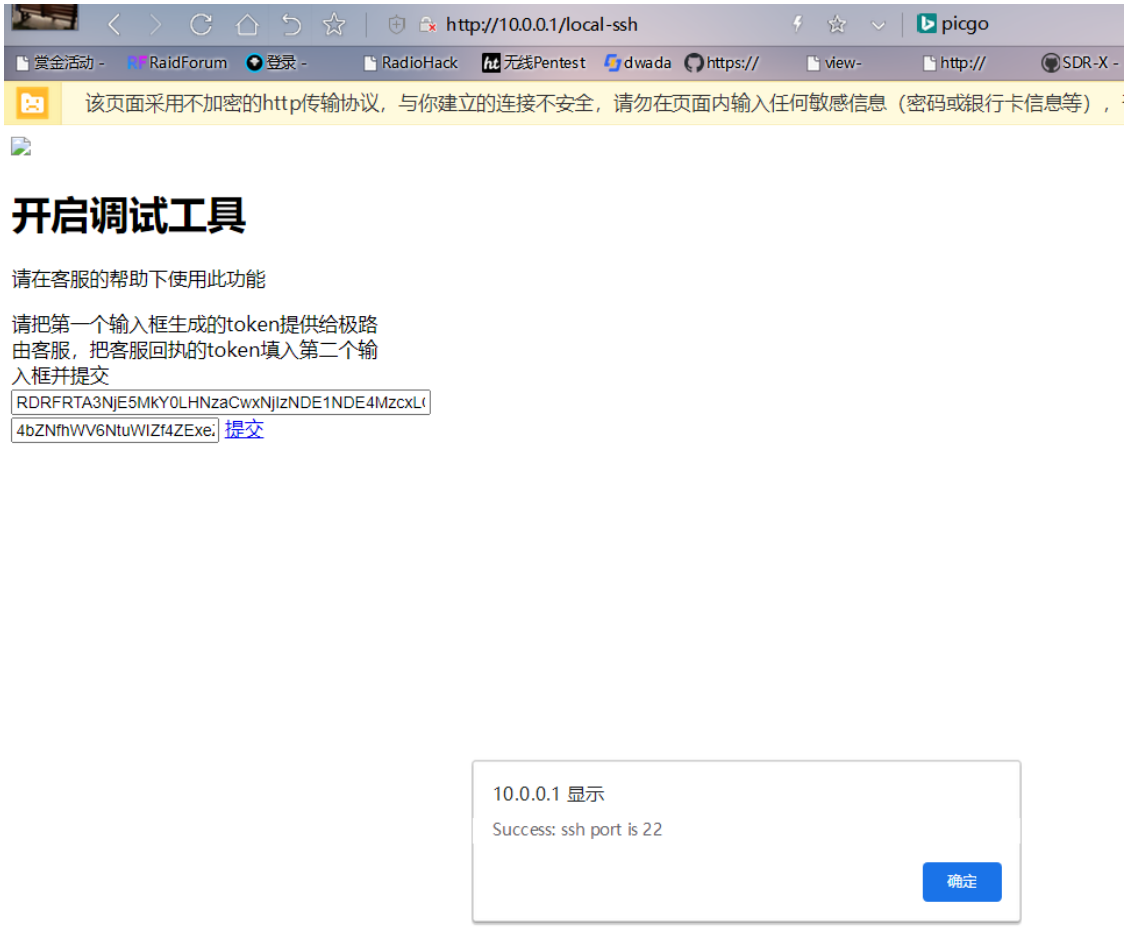
http://10.0.0.1/local-ssh
picgo
该页面采用不加密的http传输协议，与你建立的连接不安全，请勿在页面内输入任何敏感信息（密码或银行卡信息等），
开启调试工具
请在客服的帮助下使用此功能
请把第一个输入框生成的token提供给极路由客服，把客服回执的token填入第二个输入框并提交
RDRFRTA3NjE5MkY0LHNzaCwxNjIzNDE1NDE4MzcxL
4bZNfhWV6NtuWIZf4ZExe.
提交
10.0.0.1 显示
Success: ssh port is 22
确定

*Figure 3:*

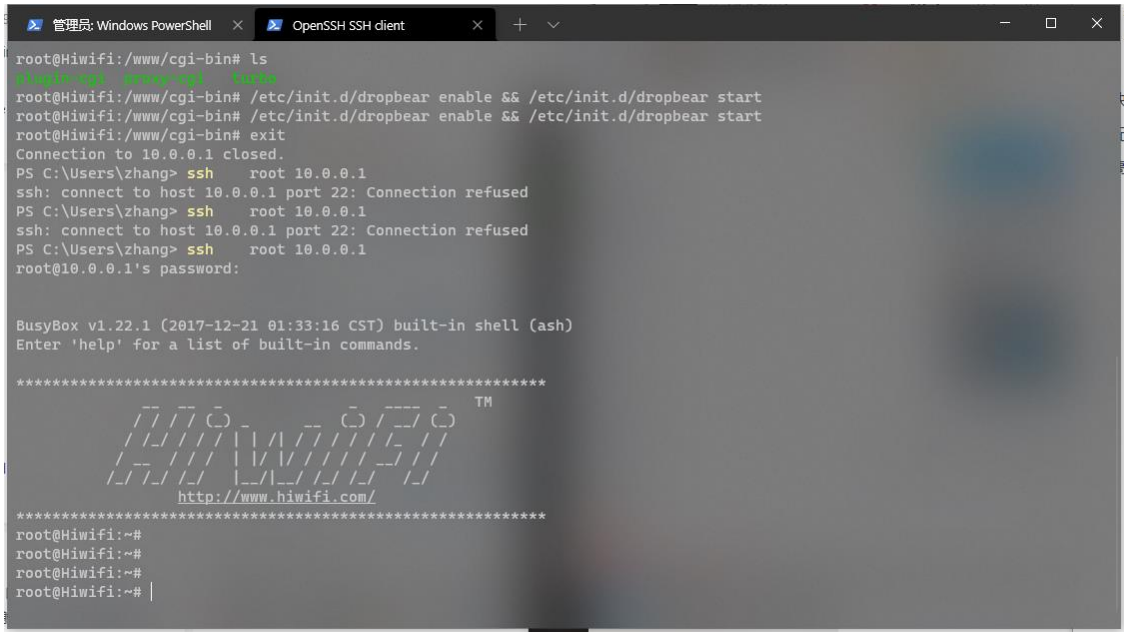


*Figure 4:*

这里我们如果要使用官方固件的话，我们就需要输入以下命令

`vim /etc/init.d/dropbear`

删掉以下一行

`'SSHKeepAlive:uinteger:300' \`

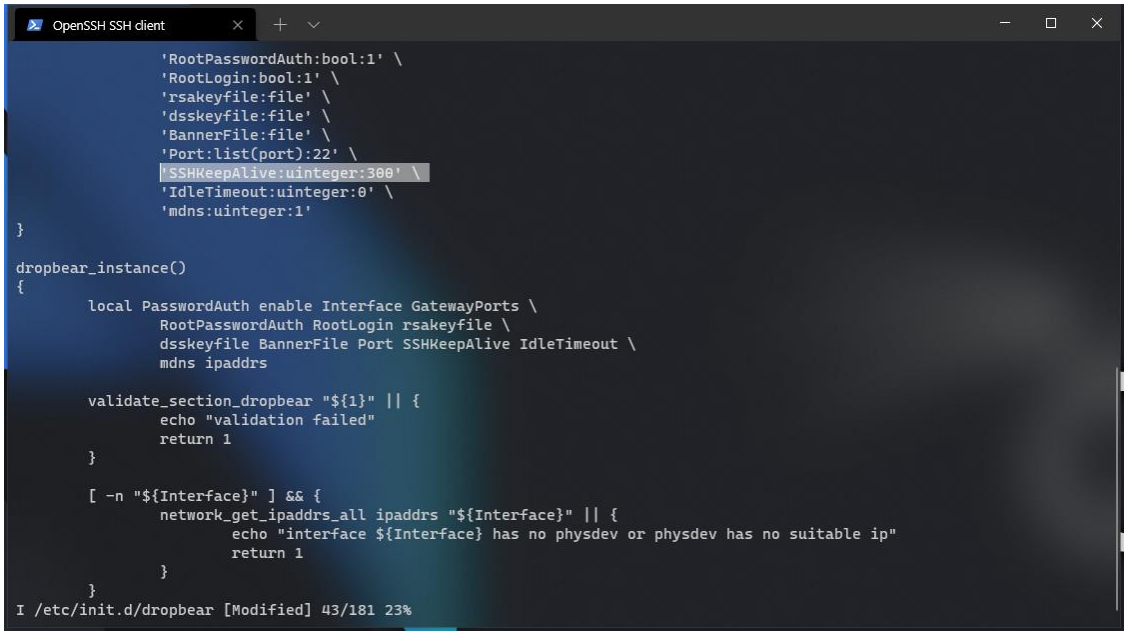


*Figure 5:*

然后在命令行执行

```
/etc/init.d/dropbear enable
```

即可永久打开