# hook从未如此丝滑

原创海岸线突击队 酒仙桥六号部队 2020-12-29原文

> 这是 **酒仙桥六号部队** 的第 **138** 篇文章。 全文共计2143个字,预计阅读时长7分钟。

## 朋友们好啊

我是葫芦兄弟掌门人铁头娃!

刚才有个朋友问我:"铁老师,发生甚么事了?"

我说怎么回事?

给我发了几张截图,我一看!

奥!原来是昨天有个app,54多兆。

不仅有壳抓包还加密。

塔门说:

有一个说是我对这个app做测试,脱壳脱的头发都没了。

铁老师你能不能教教我简单的测法?

帮我缓解下我的工作量。

我说可以~

我说你一个一个脱壳练死劲不好用,他不服气。

我说小朋友,你用脱壳来比我hook。

他说比不过,

他说你这个没用,

我说我这个有用。

这是化劲, app测试是讲化劲的, 四两拨千斤。

他非要和我试试!

## 我啪一下就站起来,上来就先搭建环境

本次测试采用模拟器环境。

frida环境搭建略过,\*度资料很多。

使用的是mumu模拟器(adb连接比\*神模拟器方便很多)。

以及httpdecrypt

(https://github.com/lyxhh/lxhToolHTTPDecrypt)

首先连接adb并运行frida-server;

C:\Users\xxx>adb connect 127.0.0.1:7555

connected to 127.0.0.1:7555

C:\Users\xxx>adb shell

root@x86:/ #

启动httpdecrypt;

#### python3 app.py

在运行时可能遇到报错;

#### [ERROR] device not found, please wait for few seconds and retry.

解决: 全局搜索get\_usb\_device, 修改为get\_usb\_device (tim eout=1000)即可。

下载 burp 插件 HTTPDecrpyt 并进行安装。 https://github.com/lyxhh/lxhToolHTTPDecrypt/releases

## 这个app不讲武德

首先正常对app抓包;



可以看到app对所有参数都进行了加密,不论是请求包还是返回包;

用神器jadx对app进行逆向试试;

🚳 *New Project - jadx-gui
文件 视图 导航 工具 帮助
🖻 🖻 🕼 🕸 🏕 🎾 🔍 🗢 🔿 🎯 📳 🥕
<pre>comapk comapk comapk comapk com com com com com com com com com com</pre>

有壳,还有加密。

# 他上来就是一个加壳,一个加密,我全都防出去了敷

浏览器访问http://127.0.0.1:8088/

o /	×
-----	---

A Home Hooks ■ Stack Q Finds ● UIDump	🏭 toBurp 💄 Custom 🛛 🗮 Decoder	
Identifier: com.		
com. Confirm		
Identifier	ApplicationName	Pid
com.android.providers.telephony	移动网络配置	0
com.android.providers.calendar	日历存储	1141
com.netease.nemu_vinput.nemu	nemu-vinput	825
com.android.providers.media	媒体存储	971
com.android.wallpapercropper	com.android.wallpapercropper	0
com.android.documentsui	文档	0
com.android.galaxy4	Black Hole	0
com.android.externalstorage	外部存储设备	0
com.android.htmlviewer	HTML 查看程序	0
com.		1283
com.frida.lxh.fridademo	fridademo	0
com.android.quicksearchbox	搜索	0
com.android.mms.service	MmsService	0
com.android.providers.downloads	下载管理程序	971
com.android.browser	浏览器	0

找到目标app,将app包名com.xxx.xxx填入框中并点击Confirm;

然后点击Hooks功能;

在Match中输入刚才的包名,点击Confirm。

C:1.	C:\Window	/s\Systen	n32\cmd.exe - python_app	.pv		-		$\times$
[16:	08:20]	[INFO]	HooksMatch: ['com.		], Options:			^
LTP.			pt failed to 1	oad, Keason is am	biguous name, it matches: com	(pid:	1755),	co
m. Filos			(pid: 1783), I	ry restarting the	app to continue loading the script.			
10:	08:34	LINFUL	create_script					
110:	08:34	LINPUL	HOOK App: com					
[10:	00.04]	[INFO]	script_on					
110:	00.04]	[INFO]	hooks running		White 1:			
110:	00:34]	[INFO]	hooks class cor		Not and the set of the			
[16:	00:34]	[INFO]	hooks class con		IbbApplicationDelegategz all method			
[10.	00.341	[INFO]	hooks class com		ippoppiicationDelegateus all methou			
[10.	00.34]		hooks class com		login uiew WolComoActivity all mothed			
[16.	00.041	TNROL	hooks class com		road comm IDynamicUnPoadTool all mothod			
[16.	00.041		hooke class com		comm bridge OpgoingNotification all method			
16.	08.34]	TNFOL	hooks class com		bhwidget bridge BridgeOneCodeWainActivity all me	thod		
16:	08:341	Î ÎNFOÎ	hooks class com		bbwidget, bridge, BridgeTrendsMainActivity all me	:hod		
16:	08:341	INFO	hooks class com		bbApplicationDelegate all method			
16:	08:34	INFO	hooks class com		bblibrary.comm.commTools.tool.EncryptionTool all	method	1	
[16:	08:34	INFO	hooks class com		.ogin.view.WelComeActivity\$1 all method			
[16:	08:34]	[INFO]	hooks class com		comm. appApplication. LoveNanNingApplication all ma	ethod		
[16:	08:34]	[INFO]	hooks class com		ybblogin.interfaces.ILoginView all method			
[16:	08:34]	[INFO]	hooks class com		ybblibrary.comm.commTools.tool.EncryptionTool\$AES	5 all me	ethod	
[16:	08:34]	[INFO]	hooks class com		ybbwidget.bridge.BridgeShareActivity all method			
[16:	08:34	[INFO]	hooks class com		comm. appApplication. LoveNanNingApplication\$1 a11	method		
[16:	08:34	[INFO]	hooks class com		base.moduleInjector.AppModuleService all method			
[16:	08:34]	[INFO]	hooks class com		comm.appApplication.LoveNanNingApplication\$2 all	method		
[16:	08:34]	[INFO]	hooks class com.		bwidget.bridge.BridgeCustomScanActivity all me	hod		
[16:	08:34	[INFO]	hooks class com.		pblibrary.comm.commTools.tool.BaseEncryptionTool	. all me	ethod	
[16:	08:34]	[INFO]	hooks class enum					

等待输出:

### [INFO] hooks class enum done...

此时,已经将该app所有方法进行了hook。

0 / ×		🛓 Download App
★ Home Hooks Stack Q, Finds Hooks Z Castan	● UCump III tellurp L Custon # Decoder	
Match 3 control	Optices 3 ("startsMass") ***	
	2 [Proved action/01179] 3 [Proved action/01177]	
Output Console X		
MethodName	Args Dursp	Return Value
com bilbrary comm.commTools. tool Encryption (ool gerContext))		(android content Context): com gin view WelComeActivity@feddut
com bölkbrary.comm.commTools. tool.tt.ncryphonTool.keyPhomJNI()		(ave.lang.8tring):: yto-CC '#CP#%P\$%%(58(1%)' +((1,-)+,-(+,-0-/12
con	argti ==	(vold) : undefined
com stillbrary commicommillada. topi Electrotion (socianave Electrotion Tabil	arge **	(com biblionary comminment Tool a tool & us rotion Tool) : com biblio
argType0 : object)		rary comm.commTools.tool.Els.rypewritoolges40064
com. jtöliterary comm.commTools. tool.ExcryptionTool.getRawKey( argType0:object)	$agir_{[22],33,34,46,36,11,32,34,35,31,33,34,35,37,33,36,37,35,36,37,39,46,34,34,34,34,34,34,44,44,44,44,44,44,44,$	([9):[-09.12,-29.71,79,-123,-12,-114,63,-23.59,126,-07,- 123,33,39]

我们重复刚才的操作。

根据数据包中加密后的数据,找到相应的方法。

C, KullaOSHEmE2WPEUNjMOvi 171 V A	×		
Output Console X arg ryper - oojeca)			
com jóbilsny comit comit Tools. tool:EncrystonTool&ES encryst[ argType1::object argType1::sting)	nega	""""""""""""""""""""""""""""""""""""""	KUUNOSUEHEZVIPEUNJUOVOOLIII IIIXXIIIISEDEVICEUTJIJNENJAATALIIN ZUHQAESIAATHOOVIVISIJUOJAESI ESOTTIVOgoekiesiinetviviojaesi Noovivioodukuunikosatoosojaesi Noovivioodukuunikosatoosojaesi
comto/ibrary.comm.comm?oos. tool.Encryption?ool6AE8.decrypt( argType0 : object argType1 : string)	Burp Suite Professional v2020.2.1 - Temporary Project - Ecensed to surf Burp Project Intuder Repeater Window Help Danhbard Target Prove Introder Repeater Sequence Decoder Compare 1	lenyy – O X Extender   Project options   User sptims   PidE	
com	1	Target https://	2465e25018211048791e02773644
com. bolibrary.comm.commTools. tool.EncryptionTool.catchRuleStr( argType0:object)	Request Raw Headers Hex	Response           Raw         Headen         Hea         Rander	0d8jd88=%3kd0jAE8/EC8/PKC85
com	1 POST /uc/gl/norr/hD/nglatehe8bory HTP/1.1 2 Context (anglh, 216 4 Context (anglh, 216 4 Context (anglh, 216 4 Context (anglh, 216 5 Decempt formaling, gala, off late 6 Decempt - Address, 21.6 6 Decempt - Address, 21.6 6 Decempt - Address, 21.6 6 Decempt - Address, 21.6 7 Decempt	1         HTDP:/.1.200           2         Intro. Nov. 20: Nov. 20:20: 40: 00: 30: 601           2         Intro. Nov. 20: Nov. 20:20: 40: 00: 30: 601           4         Intro. Nov. 40: 401           4         Intro. Nov. 20: 80: 40: 40: 40: 40: 40: 40: 40: 40: 40: 4	* pder:socoo,messager:18(2888 roatsr:null)
comVbbApplicationDelegate\$3.in tercept.son( argType0 : string)	T (Content-Type: application/jown.charact=0TF-8 8 classramp: 1000723350025 9 colum: 10 exeruity/Code: 90(20400-25000211048/91c002713644o	7 Set-Cookie: SUN NELE-LESI NELEONATION/LOOPANO/Beck/2014/10/1004/201710 [100320370.httls/     8 Cookie: Langth: 308     9     9     10 SetAnt-Langth: 308     10 SetAnt-	pde".90000,"message":"85(24)(3 "0ata":null)
com YbbAppicationDelegate52.s howEnxor( argType0: object) argType1: object)	(c) on AN 31 data (1.1.6) (c) data (1.1.6) (c) data (1.1.6) (c) data (1.1.6) (c) data (1.1.6)(c) data (1.1.6)(c) data (1.1.6)(c) data (1.1.6)(c) data (1.1.6)(c) data (1.1.6)(c) data (1.1.6)(c) data (1.1.6)(c) data (1.1.6)(c) data (1.1.6)(c) data (1.1.6)(c) data (1.1.6.		

com.xxx.xxx.ybblibrary.comm.commTools.tool.EncryptionTool\$AES.en
crypt(argType0 : object argType1 : string)

可以看到是这个函数将请求包的数据进行了加密。

Q 6uA7eLVXK355559M45QAELm 1775 ∨ ∧ X Burp Suite Professional V3220.21 - Temporary Project - Iconsed to us Days Physic Hindre Expansive Hindre Hindre Hindre Hindre Expansive Hindre Hindre Expansive Hindre Dispatial Sequencer Decoder Compare	Herryz – C X Extender [Physics options [1962]	
Sed Cool < + >+ Request Bay Paulos Inc	Target I	(Jana Jang Seing) : Kuluko SulEm 62W/FGUNgki Ovo2016 11 1989 12 11 11 11 10 10 10 10 10 10 10 10 10 10
POIT Androph Learn's (* registrationalisery #1757.1.1 Contract Learn's LPA Contract Learn's LPA Contract Learn's LPA Contract Learning and Learning LPA Contract LPA Cont	Intervi 1: 200         Physics Res	(jensiling Sing): null (jensiling Sing): :962489c2891621164891c62773644 e
C + D Type a search term 0 matche	Image:	(java lang String) : ej30d5/5&=%3kd0(AES/ECB/PXCS8 Padding(AES)
cont	pelant wellen kanstende besette (neel meleksete) (sin anderen anderen er men geneten en en en syntheme	(jawa lang 88mg): ("code", 90000; "message", "銀石和弓 9587, 國際新研究(1,"code", nunj
com 'YbbApplicationDelegateG3 in arget (*coa**;*eeee,*e tercepLison( argT(pe0: sting)	mp**%23858.25 ####80:********11	(maxiang.String): ("code" 90000, "maxaage","他已转已 先初,如重时获取1 ","data",nul)
con		(inid) : undefined

com.xxx.xxx.ybblibrary.comm.commTools.tool.EncryptionTool\$AES.de
crypt(argType0 : object argType1 : string)

是返回包的解密函数。

我们看下加密函数:

com.xxx.xxx.ybblibrary.comm.commTools.tool.EncryptionTool\$AES.en crypt(argType0 : object argType1 : string)

可以看到加密函数需要两个参数,分别是对象和字符串。

但是我们需要知道对象参数的具体类型。

现在转到Finds功能中,搜索函数的类名。

com.xxx.xxx.ybblibrary.comm.commTools.tool

点击Confirm。

找到方法名EncryptionTool\$AES.encrypt。



可以看到加密函数参数中,对象类型的参数具体类型为static。

选择到encrypt,然后右键发送到toBurp功能。



转到toBurp功能。

点击Confirm。

Artone ■ Hooks ■ Stack Q, Finds	
toBurp 🖌 Control	
input	Output
com a successory to the committee second contract of the second sec	("classrame": "conytblibrary.com.com/fools.tool.troryptionTool545", "methodrame": "encrypt", "classing":
info:	
1	Overloads:
	("Argt", "jandroki, content, Context, Java, Jang, Shing)", "Return Value", "Java, Jang, Shing", "Tength", 25 *
	add hosk expert static expert instance toDurp Generate •
Ovipet Console X	
Info	Call

点击add。

由于这个加密函数有两个参数,所以需要自己编辑代码(默认为一 个参数)。

there ■ Hooks ■ Stack Q. Finds ● UDump ■ toBurp ▲ Custom ■ Decoder	
x8up / Contem	
input	Output
com c	("classes": "com/
Info:	"PALTNELLATIONATION TRACAMMENT" }
1 ("Classes" * Con. philling con conficts tool (Proyetonios1645", "arthouse" * Proyet", "Look * 4, "Loopt")	CMarger "gavatorial content: Content_ava.tang.Strang", "Return Value", "pixa.tang.String", "Return Value", "pixa.tang.tang.tang.tang.tang.tang.tang.tan
Dulput Console 🗙	Generate export instance script
into	Generate toBurp script

由于对象参数类型为static,所以我们选择Generate export static script。

如果参数为动态, 那我们选择Generate export instance script。

现在可以看到,在custom中会生成代码。

<pre>     set strict;     war rpc_result = sull;     war rpc_result_los = null;     set_set/set/set/set/set/set/set/set/set/set/</pre>
Cutput Console X

代码中, arg0是传过来的加密字符串, arg1是Android的Context 对象。

添加代码:

```
var context =
```

```
Java.use('android.app.ActivityThread').currentApplication().getA
pplicationContext();
```

再用同样的方法生成decrypt的代码。

最终代码为:

Custom	💉 loadScript - ScriptManage SaveScript
1 2 3 4 5 6 7 8 4 9 10 ▲ 11 ▲ 12 13 14 15 16 17	<pre>'use strict'; 'use strict'; 'use strict'; 'use rec_result = null; 'use rec_result = null; 'rec.exports = {     tag24239=10fd5sfd01s5459978c4306b1f02; function(arg0, arg1){         Java.perform(function () {             try{</pre>
18	
19 28 - 21 - 22 - 23 24 25 26 27 28 29 30 31 32 33 1 32 33 1 32	<pre>// Amake Function tag#00f123tad4835abBase6e02346p447d02; function(arg0, arg1){     Java.perform(function () {         try{             var context = Java.use('android.app.ActivityThread').currentApplication().getApplicationContext();             var EncryptionTool5AE5ret509488cc1050170935865d6bc478 = Java.use("com</pre>
Output C	Console 🗙
Info	

### 点击左上角loadScript 将脚本发送到burp。



在burpsutie中进行配置。

Request					
Raw Hex	Raw Hex				
1	Scan				
	Do passive scan				
	Do active scan				
	Send to Intruder	Ctrl+I			
	Send to Repeater	Ctrl+R			
	Send to Sequencer				
	Send to Comparer				
	Send to Decoder				
	Request in browser	►			
	Send to HTTPDecrypt				
	Custom Request functions1				
	Custom Request functions2				
	Engagement tools	►			
	Change request method				
	Change body encoding				
	Copy URL				
	Copy as curl command				
	Copy to file				
	Paste from file				
	Save item				
	Save entire history				
	Paste URL as request				
	Add to site map				
	Convert selection	►			
	URL-encode as you type				
	Cut	Ctrl+X			
	Сору	Ctrl+C			

点击send to HttpDecrypt 打开配置界面。

0 / ×	HTTPDecrypt Config		×	
	HTTPDecrypt WebServer URL	http://127.0.0.1:8088/	Body Auto	
	Custom Request functional	tag24239e10fd5afd01a5459978c4306b1f02	Test	
A Home Hooks E Stack Q Ein	Custom Request enctions2:	tagf0f1c91ca14d835ab8ae6e62346a447d02		
Custom / InadScript - ScriptManage SaveScript	Custon Response function 3:	tag24239e10fd5afd01a5459978c4306b1f02		
1 'use strict';	Custom Response Mictions4:	tagf0f1c91ca14d835ab8ae6e62346a447d02		
2 3 var rpc_result = null; 4 var rpc result ins = null;	OK ancel	Notice: Terminald will be copied to the clipboard. Paste it into Terminal!		
▲ 5 - rpc.exports = {				
7 8 - tag24239e10fd5afd01a5459978c4306b1f02: f	unction(arg0, arg1)			
18 - tryf				
A 11 var context = Java.use('	angroid.app_ctivityThr	ead').currentApplication().getApplicationContext();		
A 12 var EncryptionTool\$AES68	3/ae8a10e76a7052b218c70	bcaf88e = Java.use("comybblibra	y.comm.commTool:	.tool.EncryptionTool\$AES");
13 rpc_result = Encryption]	ool\$AE563bae8a10e76a70	52b218c70bcaf80e.encrypt(arg0, arg1);		
14 // send(JSON.stringify)	"aa" 'bb", "aal": "bbb"))	+'-cusataBaamBscBriBpt-')		
A 15 }catch(e){send("tag24239e707	d5 d8185459978c438601t	02, " + e + "-eraarooaaar-")}		
17 return rpc result:				
18 },				
19 // Added Function				
20 - tagf0f1c91ca14d835ab8ae6e62346a447d02: f	unction(arg0, arg1){			
A 21 - Java.perform(function () {				
A 22 try{		and') currenthenlication() estimalization(estevt())		
A 24 var EncryptionTool\$AFS7e	589488cc1b5817b9835876	Sdbc4f8 = lava_use("com.	v.com.comTool	.tool.EncryptionToolSAES"):
25 rpc_result = EncryptionT	oo1\$AES7ec589488cc1b581	7b98358765dbc4f8.decrypt(arg0, arg1);		
26 // send(JSON.stringify({				
▲ 27 }catch(e){send("tagf0f1c91ca	14d835ab8ae6e62346a447d	82, " + <b>e</b> + "-er88roo888r-")}		
28 });				
29 return rpc_result;				
31 // Added Function				
32				
33				
i 34 )				

Outnut Console 🕱

## 然后就可以对加密后的数据进行加解密了。

Custom	nvocation response X								
("code": 10000, "message": "", "data": {"count": "1	Peode"-10000 "manages"-"" "date"- "sount"-"100" "time"-		Params	Edited	Status	Length	MIME t	Extension	Title
	{ code : 10000; message : , data .{ codit : 100 ; time : "600000"3	2.10	~		200	176	JSON		
	555555 JJ	2.10	$\checkmark$		200	176	JSON		
		pRu	$\checkmark$		200	602	script		
					200	218	HTML		
					200	865	script		
i i					200	970	script		
		Y			200	862	text		
					200	457	script		
		lotS			200	626	text		
					000	0004			
	确定				_				
Raw	leaders Hex Render								

- 3
- 4
- 5
- HTTP/1.1 200 Date: Mon, 30 Nov 2020 10:12:51 GMT Content-Type: application/json;charset=UTF-8 Connection: close X-Application-Context: apiGateway:prod:38080 Set-Cookie: loginAccount=106745944; Max-Age=2592000; Expires=Wed, 30-Dec=2020 10:12:51 GMT; Path=/ Set-Cookie: SERVERID=13e8232e99649a22ac219777bf656af9 1606731171 1606731171;Path=/ 6 7
- 8 Content-Length: 108 9
- k3an97uHPZKo/Zsr5gn3d1Nbvo5qs48K0B3hTcD4JThRMg1aRFBY1RI1hF907k47rJ8xrY144WcOyjGr5pOSfHi9dZprHR9HzOue7Yb8z1E= 10

## 耗子为知,好好反思

app测试的时候,hook的难点在于定位所需要hook的函数和参数。 然后就是根据函数名和参数名进行hook代码的编写。

httpDecrypt提供了较为方便的集成的环境。相比脱壳看代码,这种调试的方法会省下我们大量的时间。







精选留言

用户设置不下载评论