APP抓包心得

**方法一：使用模拟器，个人推荐夜神模拟器或者是网易的MuMu模拟器**

场景：需要抓取HTTPS的数据包

1、使用模拟器：夜神模拟器

第二步是最关键的一步，不管是Android系统还是IOS系统，抓APP数据包都比不可少

2、安装burp证书，burp设置好代理

Extender 
Dashboard 
Project options 
Target 
User options 
Proxy 
Passwe Scan Client 
Intruder 
captcha-killer 
Repeater 
Struts Finder 
Sequencer 
Fastjson scan 
Decoder 
Autonze 
Comparer 
Intercept HITP history WabSockats history O 
7 
0 
0 
Proxy Listeners 
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server _ 
Running Interface 
Invisible Redirect 
Certificate 
per-host 
Per-host 
Remove 
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another 
installation of aurp_ 
Import / export CA certificate 
Intercept Client Requests 
Regenerate CA certificate 
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab. 
Intercept requests based on the following rules: 
Master interception is tumed off 
Enabled 
Remove 
Operator Match type 
or 
or 
And 
File extension 
Request 
HITP method 
URL 
Relationship 
Does not match 
Contains parameters 
Does not match 
Is in target scope 
Condition 
(nglElnjpgSlnpngSlncssSlnjsSlmcoS) 
(getlpost) 

* 来到模拟器—>设置—>WALN—修改网络—>手动，如下图：主机名和端口与burp一致

Extender 
Dashboard 
Project options 
Target 
User options 
Passwe S 
Intruder 
7.0.0.6 
WLAN 
Android 7 
a 11:36 
Intercept HITP history WabSockats history Options 
Proxy Listeners 
0 
0 
Burp Proxy uses listeners to receive incoming HTTP requests from your browse 
Running Interface 
Invisible Redirect 
Edit 
Remove 
Each installation of Burp 
installation of aurp_ 
WiredSSl 
grates its own CA certificate that Proxy listeners c 
Import / ex 
certificate 
Regenerate CA certificate 
o 
Interce t Clien 
quests 
Use these settings to control wh ch requests are stalled for viewing and editing 
Intercept requests based on the following rules: 
Master interception is turne 
Enabled 
Up 
Operator Match type 
Relationship 
Does not match 
Contains parameters 
Does not match 
Is in target scope 
WiredSSlD 
HTTP 
192.168.100.2 
8088 
or 
or 
And 
File extension 
Request 
HI-rp method 
URL 

* 设置完成之后，需要导入burp证书，访问http://burp，下载证书。

rox 
7.0.0.6 
Android 7 
http://burp 
Burp Suite Professional 
Welcome to Burp Suite Professional. 
o 
o 
x 
• N a 11:39 
CA Certificate 
2 

* 下载完成后把证书改名：crt格式（**ps：模拟器或手机支持的格式**）
* 导入到模拟器中
* 设置->安全->SD卡安装证书，找到对应的证书

令 安 全 
凭 据 存 储 
存 储 类 型 
仅 限 软 件 
信 任 的 凭 据 
显 示 信 任 的 CA 证 书 
从 SD 卡 安 裝 
从 SD 卡 安 装 证 书 
清 除 凭 据 
删 除 所 有 证 书 

* 安装下一步，任意命名即可。

安 全 
用 户 凭 据 
查 看 和 修 改 存 储 的 凭 
从 SD 卡 安 装 
从 SD 卡 安 装 证 书 
清 除 凭 据 
删 除 所 有 证 书 
可 信 代 理 
查 看 或 停 用 可 信 代 理 
为 证 书 命 名 
凭 据 用 途 ： 
VPN 和 应 用 
该 数 据 包 包 含 ： 
1 个 CA 证 书 
取 消 
确 定 

3、burp抓包成功，如下图

22 一 Y 囗 囗 囗 K 一 L/ 囗 囗 > FS 一 2 = 囗 N 囗 囗 囗 囗 一 w 囗 囗 2 囗 囗 囗 A 囗 5 囗 f 囗 囗 囗 - 一 囗 囗 Eb 囗 
18 
17 
16 
12 
11 Content-Length: 40 旵 
10 
" Requestt 
4 
9 
8 
7 
1 
t 囗 囗 v 囗 囗 
囗 囗 Q DOI 囗 3 囗 W 
囗 ' g 囗 囗 囗 B 囗 囗 囗 一 T 囗 R 囗 ' 囗 囗 囗 一 N 囗 囗 一 囗 囗 HH 囗 X 囗 囗 + M 囗 囗 ' - M 囗 EED 囗 囗 囗 囗 ,_ 囗 一 5 囗 k 囗 囗 4 囗 囗 h " 囗 囗 E 囗 囗 囗 2 囗 一 囗 囗 囗 囗 一 囗 囗 囗 囗 囗 u 囗 2 囗 b 囗 囗 囗 ' | 囗 xvh 囗 囗 CR 囗 囗 囗 囗 - 囗 J … 囗 囗 = 囗 Y 囗 vxA 囗 囗 
Accept-Encoding gz 一 deflate 
X-IJmeng-Pro-Ver: 一 00 
X-Umeng-Sdk 20566 $ nd 乛 0 一 d/L ♂ , AN00-us 5 一 一 L ♂ , AN850020 一 一 2 一 release-keys/LlO-AN00E 一 一 4f309329D5d9C5d738bdd7dbb239297 
X-IJmeng-UTC 一 6 一 7545085046 
k 囗 囗 qq 一 sb 囗 N 囗 囗 ~ 囗 囗 囗 囗 囗 7 囗 囗 g 囗 q 囗 囗 囗 囗 X 囗 囗 囗 囗 囗 囗 囗 囗 L- - 囗 囗 g 囗 7W 囗 n 囗 >hH 囗 LIRi2 囗 囗 c 囗 囗 囗 囗 8 囗 囗 S 囗 - SSB < 囗 囗 囗 囗 一 囗 一 囗 囗 囗 … W 囗 囗 4 囗 囗 J 囗 一 囗 囗 " 囗 E 囗 囗 L3 囗 囗 囗 CAZ 
囗 - Af 囗 囗 囗 L < 囗 g6G 
7 囗 3 囗 7 囗 0 E 囗 J - E 囗 - 囗 囗 囗 u 囗 囗 一 囗 q P8 y 囗 囗 囗 囗 3 Ct R 囗 囗 囗 T 囗 一 3 囗 囗 U 囗 囗 一 囗 囗 B 囗 囗 囗 囗 囗 囗 囗 2 囗 囗 > 一 囗 囗 B : 囗 A 囗 囗 囗 囗 囗 囗 囗 D9 囗 「 H 囗 3 N 囗 囗 囗 囗 囗 囗 囗 
囗 囗 一 囗 - 囗 … K 囗 IV 囗 囗 J 囗 囗 - 囗 囗 囗 M 一 囗 囗 Z 囗 0 囗 . > 囗 囗 囗 囗 A 囗 6c - Y 囗 88Sh 囗 - 囗 3 囗 囗 yK 囗 囗 一 - 囗 m 囗 ' A 囗 乛 囗 囗 0 囗 囗 囗 囗 囗 R 下 囗 zuM 囗 囗 2 囗 囗 囗 囗 囗 Y 囗 囗 g 囗 s 《 囗 M 囗 k4 囗 囗 3 囗 囗 一 囗 - 囗 囗 囗 9 囗 囗 Z 囗 
h 囗 囗 9 囗 囗 囗 囗 C 一 囗 M 囗 囗 Z 囗 5 囗 囗 Z 囗 囗 >3 一 囗 囗 N 囗 囗 囗 囗 囗 y 囗 囗 囗 m 囗 bA 囗 k 囗 68 k 囗 囗 Z 囗 囗 8 囗 囗 囗 2 囗 囗 囗 囗 囗 囗 囗 囗 囗 囗 y 囗 囗 B 囗 囗 囗 囗 7 - 囗 一 囗 囗 囗 Y 囗 F 囗 囗 囗 M 囗 囗 囗 囗 囗 囗 囗 囗 囗 x 囗 囗 囗 囗 0 囗 囗 『 囗 囗 囗 囗 囗 一 囗 q 囗 X[ 囗 囗 
囗 S 囗 囗 k 囗 … 囗 囗 一 囗 0 4 囗 m 囗 S 囗 囗 7 囗 " 
囗 囗 囗 U >H 囗 囗 囗 」 - 囗 一 囗 囗 囗 囗 囗 囗 N 囗 囗 囗 - bg 囗 囗 囗 囗 囗 0 囗 y 囗 囗 Y 囗 y3 囗 = 囗 囗 囗 囗 Z Ph 囗 囗 ' 70 囗 UA 囗 囗 囗 2 囗 w 囗 囗 囗 M 
m 囗 囗 ~ 一 囗 囗 ?8 一 8 囗 M 囗 一 v 囗 囗 8 囗 囗 - 囗 6P 囗 = m 囗 N 囗 6 囗 囗 0 囗 囗 囗 k 囗 囗 囗 5 一 囗 囗 囗 囗 一 HY} 囗 囗 C 囗 h 囗 囗 囗 囗 一 一 囗 囗 j>y5k 
囗 囗 囗 囗 囗 囗 2 囗 囗 v 囗 一 囗 v 囗 M 囗 囗 囗 囗 囗 囗 囗 - 囗 囗 G 囗 囗 囗 囗 k 囗 囗 + 囗 2 囗 囗 囗 《 囗 囗 囗 囗 ' 囗 C c 囗 囗 囗 囗 囗 囗 囗 囗 < 囗 囗 囗 0 囗 一 囗 囗 囗 一 囗 y 囗 囗 c C 囗 囗 - 囗 e 囗 囗 囗 囗 g 囗 囗 囗 囗 c H N 一 囗 「 囗 6 囗 囗 X 囗 3 囗 - 囗 囗 囗 7 囗 囗 囗 囗 囗 JZJ CIW[ 囗 K 
d 囗 囗 6M 囗 囗 0 囗 囗 囗 囗 囗 囗 囗 囗 囗 一 m 囗 囗 囗 囗 h 囗 囗 囗 囗 kH 囗 囗 + 囗 W 囗 囗 一 ~ 5 囗 囗 囗 囗 so 囗 一 囗 囗 X 囗 < 囗 囗 ~ 囗 囗 囗 3 囗 囗 囗 Xc 囗 囗 囗 囗 w 囗 囗 囗 9 囗 囗 " SlJy 囗 C " 6 囗 ba 囗 囗 F 囗 囗 ' 7 囗 囗 亠 7 囗 囗 囗 x 囗 囗 - pvZM 囗 囗 囗 囗 囗 囗 
囗 - 囗 83 囗 囗 囗 H 囗 囗 +m 囗 S < 囗 囗 一 囗 囗 囗 一 囗 囗 囗 囗 囗 ev 囗 囗 u 囗 囗 Z5 m 囗 囗 囗 囗 囗 囗 囗 k 囗 v 囗 囗 囗 囗 囗 囗 囗 囗 M 囗 L 囗 W 囗 W 囗 囗 囗 囗 46 囗 囗 囗 = + 囗 7X 囗 囗 囗 囗 k 囗 囗 2 一 囗 囗 B 囗 囗 + 囗 k 囗 
一 EcA 囗 - 囗 囗 囗 6 囗 b 囗 工 囗 一 囗 G 囗 囗 = 囗 yN 囗 囗 Xq 囗 囗 囗 囗 囗 囗 bh 囗 N 囗 囗 K 一 囗 囗 囗 囗 一 一 囗 囗 囗 囗 8x 囗 囗 
囗 G 囗 囗 「 
囗 LN 囗 囗 D 「 囗 2 囗 囗 一 囗 一 u > 囗 > 囗 一 K' 囗 囗 
囗 J 囗 - 囗 囗 Q 囗 囗 囗 囗 囗 囗 囗 0 囗 《 囗 一 bJ 囗 囗 囗 Ub 囗 囗 、 K 囗 囗 囗 b 囗 … /O 囗 一 囗 W 囗 囗 囗 囗 囗 b 囗 囗 一 囗 ' 囗 囗 
R - 囗 囗 囗 C 囗 囗 囗 
囗 囗 囗 G 囗 囗 8 , 囗 3 囗 「 H 囗 囗 8 d 囗 囗 G 囗 囗 囗 + 囗 
囗 H 囗 8 囗 
囗 f 囗 囗 v 囗 - 囗 囗 囗 b 囗 囗 3 囗 囗 C 囗 
囗 囗 一 0 囗 囗 Sco 一 b465F6 一 9d0000 一 b 囗 cc03 一 665952E57C 一 02 一 8b98b4ec6bc8 一 0 一 6d3 一 dE6DfE7dbE4834b82563dC646D 囗 囗 囗 A 囗 囗 囗 囗 囗 囗 囗 x 囗 囗 Z 一 囗 囗 Hv 囗 + F?f 囗 囗 囗 U = 囗 一 囗 Z 囗 囗 囗 囗 囗 一 乛 囗 囗 囗 囗 c 
Host 
User-A.- 
Msg-Type envelope/Json 
Content-Type ut/i 
POST/unify logs HITP/I 一 
Forward 
Params Headers Hex 
HITP history WebSockets history Options 
2 囗 一 E 囗 囗 囗 囗 T 囗 囗 x 囗 囗 XA 囗 囗 
囗 囗 囗 囗 k D 囗 囗 W 囗 囗 - : 囗 8 囗 囗 囗 囗 囗 囗 M 囗 囗 囗 9 囗 囗 B 囗 
囗 囗 囗 r\C 亡 囗 - + 囗 M 囗 囗 
Typeasearchterm 
囗 囗 - 囗 囗 囗 Pc 一 6 
android5 一 一 … Ll 
3 < 囗 囗 q 囗 囗 3 一 囗 囗 囗 Fv 囗 一 囗 N 囗 囗 囗 囗 囗 囗 囗 2Dzh 囗 6 囗 E 囗 囗 「 囗 … 囗 一 3 囗 q 一 囗 囗 囗 囗 
囗 = 囗 囗 RK 囗 囗 mg 囗 囗 37 囗 bp 囗 - s 囗 囗 囗 囗 u 囗 囗 - 囗 囗 囗 囗 囗 F8/R 囗 D9 囗 6 囗 囗 囗 囗 R 囗 E 囗 En ' 囗 囗 囗 TE 囗 囗 囗 囗 Y 囗 · 囗 *BMir' 0 囗 2 囗 囗 
O-ANOO Build/LlO-AN00) 
n 一 5 囗 囗 2 囗 Ml 
《 23 囗 za 囗 5 囗 J 囗 囗 y 囗 K 囗 AQ 囗 78 囗 0 囗 2 囗 + h 囗 囗 4 囗 VR B 囗 囗 OH 囗 囗 2 一 W 一 囗 囗 囗 2 囗 " 
< 囗 Y 囗 一 乛 囗 E 囗 n m 囗 囗 囗 一 囗 囗 2 囗 囗 , - K 囗 囗 x 囗 囗 囗 囗 囗 •g k 、 囗 囗 囗 2 囗 囗 囗 囗 囗 > 囗 囗 囗 囗 RZ+ 囗 囗 , 囗 囗 0 囗 R N 囗 囗 囗 0 一 
囗 囗 囗 囗 囗 丁 - 囗 囗 囗 囗 囗 囗 囗 E 囗 囗 N 囗 8 囗 09 一 U 一 f + 囗 一 囗 uKE 囗 囗 囗 7x 囗 0 囗 囗 + 囗 h 囗 + n 囗 一 囗 「 c 囗 
U 囗 囗 = 囗 囗 
Commentthis item 
囗 囗 J 
Omatches 

**方法二（在安装有证书的前提下没有安装证书的回头看方法一）：Proxifier+burp**

场景：APP识别到模拟器开有代理，导致数据包错误或者hi不能正常打开访问APP，这种情况我们可以利用以代理的方式，达到绕过的效果。

1、burp设置好代理

Extender 
Dashboard 
Project options 
Target 
User options 
Passive Scan Client 
Intruder 
ca*cha-killer 
Repeater 
Struts Finder 
Sequencer 
Fastjson scan 
Decoder 
Autorize 
Comparer 
Intercept HTTP history WebSockets history Opuons 
? Proxy Listeners 
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one ofthe listeners as its proxy server 
Running Interface 
Invisible Redirect 
Certificate 
Per-host 
Per-host 
7 
0 
Each installation Of Burp generates its Own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in Other tools or another 
installation of Burp 
Intercept Client Requests 
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab. 
Intercept requests based on the following rules: Master interception is tumed off 
Add Enabled 
Remove 
Operator Match type 
or 
or 
And 
File extension 
Request 
HTTP method 
Relationship 
Does not match 
(AglfSlAjpgSlApngSlAcssSlAjsSlnicoS) 
Contains parameters 
Does not match (getlpost) 
Is in target scope 

2、关闭模拟器的代理，**不需要开启代理！**

夜 裤 幔 拟 嚣 7 ℃ ． 0 ． 6 了 
WLAN 
开 启 
WiredSSID 
已 迓 接 
添 加 网 络 
WiredSSID 
高 级 选 项 
代 理 
无 
| P 设 置 
DHCP 
取 消 
保 存 

3、下载Proxifier并打开修改完成，如下图：IP与端口需要对应BURP设置的IP和端口

proxifier 
文 件 〔 
配 置 文 1 
。 L) 视 認 (V) 
助 （ H 〕 
代 三 里 报 务 器 
应 用 程 序 
已 发 送 
已 接 牧 
地 址 
山 而 O 
类 型 
CNox.exe 
舔 加 ． 
0 
192 ． 10 & 100 ． 25 
移 除 
服 务 器 
地 址 ： 
囗 ： 
192 ． 10 & 100 ． 25 
协 议 
O O @ 
SOCKS 版 本 5 
SOCKS 版 本 
HTTPS 
连 接 
门 乙 门 乙 门 乙 门 乙 门 乙 门 乙 门 乙 门 乙 门 乙 门 乙 
输 证 
囗 
使 用 NTLM 
TPS 
用 F 名 ： 
& 100 ． 25 ： 日 0 日 日 HTTPS 
使 用 当 前 用 F 登 录 
1 4 字 壭 （ 1. 0 2 (B) 已 接 牧 ， 生 存 期 〈 1 秒 
密 码 ： 
& 100 ． 25 ： 日 0 日 日 HTTPS 
1 4 字 壭 （ 1. 0 2 (B) 已 接 牧 ， 生 存 期 〈 1 秒 
& 100 ． 25 ： 日 0 日 日 HTTPS 
选 项 
1 4 字 壭 （ 1. 0 2 (B) 已 接 牧 ， 生 存 期 〈 1 秒 
显 示 、 
Internet Explorer 0 
上 传 
就 绪 
1 个 活 动 连 接 

4、点击配置文件—>代理规则—>设置代理规则—>添加一条代理规则

代理的名称任意填，应用程序需要抓取模拟器程序的进程，这里用的夜神。

multiplayermanager.exe; nox.exe; noxrepair.exe; noxvmsvc.exe; noxvmhandle.exe

选取进程试最好是点击浏览，找到该进程的文件路径，并选取防止找不到路径导致找不到包

Proxifier 
žfț(F) 
103. 31 
[03. 31 
[03. 31 
[03. 31 
[03. 31 
[03. 31 
[03. 31 
[03. 31 
• 55:14] 
[03. 31 
• 55:14] 
Nox. exe 
Nox. exe 
Nox. exe 
(6. 21 
Nox. exe 
O 
Nox.exe 
Nox.exe 
Nox.exe 
LIII. 
23. 
23. 
Javaw. exe 
[auto—cre. 
Javaw. 
Nox. ex 
NoxVMS 
- 192 
- 192 
- 192 
- 192 
Nox. 
x 
Mul tiF1 ayerManager. exe ; NoxVMHand1e. exe 
exe;NoxVMSVC. exe, 
iexplore. exe, 
s om 
D 
ul 
pp. exe 
com 
fire*. exe, 
92. 168. 1. 
bin 
10. 1. o. 0-10. 5. 255. 255 
: 127. 
SfiďE (Direct— 
8000-9000 
example. 
3128 
ox 
an e. exe 
NoxVMHand1 e. 
exe 
NoxVMHand1 e. 
exe 
NoxVMHand1 e. 
exe 
NoxVMHand1 e. 
exe 
[04. 
[04. 
[04. 
[04. 
01 
01 
01 
01 
/ Block—Ë-Ë) : 
6368 
Proxy HTTFS 192. 168. 100. 25 
api—new. bignox. 
api—new. bignox. 
api—new. bignox. 
api¯new. bignox. : BO 
468 
500 

5、确定完成即可，运行APP可以看到模拟器的数据，如下图：

Proxifer 
О Nox.exe 
[04. 01 
х 
NoxVMHandle.exe *. 
О NoxVMHandle.exe 
* 
о 
NoxVMHandle.exe *. 
о 
NoxVMHandle.exe *. 
о 
NoxVMHandle.exe . 
о 
NoxVMHandle.exe *. 
о 
NoxVMHandle.exe *. 
о 
NoxVMHandle.exe *. 
о 
NoxVMHandle.exe *. 
о 
NoxVMHandle.exe *. 
127.0.0.1:61001 
„ 172.64.ЛЗО.Л4:8О 
. 172.64.1 30.14:443 
„ 172.64.ЛЗО.Л4:8О 
„ 192.168500.25:8088 
* . 175.25.50.81:7007 
„ 192.168500.25:8088 
„ 192.168500.25:8088 
„ 192.168500.25:8088 
„ 172.64.ЛЗО.Л4:8О 
08:14 
00:02 
00:01 
ЛЕЕВ? 
00:01 
00:01 
192.168.100.25:8088 н... 
• 68.100.25:8088 н... 
192.168.100.25:8088 н... 
• 68.100.25:8088 н... 
• 68.100.25:8088 н... 
192.168.100.25:8088 н... 
• 68.100.25:8088 н... 
• 68.100.25:8088 н... 
• 68.100.25:8088 н... 
• 68.100.25:8088 н... 
• 192.168500.25:8088 н... 
52 
83 
646 
л 40 
л 86 
л 40 
л 94 
2.18 кв 
2.33 кв 
863 
.62 кв 
.62 кв 
.62 кв 
867 
2.27 кв 
[04. 
[04. 
[04. 
[04. 
[04. 
[04. 
[04. 
[04. 
[04. 
[04. 
[04. 
[04. 
ijt% 
01 
01 
01 
01 
01 
01 
01 
01 
01 
01 
01 
01 
NoxVMHand1e. вхв — 
NoxVMHand1e. вхв 
NoxVMHand1e. вхв 
NoxVMHand1e. вхв 
172. 64. 130. 14:80 
Т-7], 140 
екнп, 00:01 
Nox. вхв — 
Nox. вхв — 
Nox. вхв — 
Nox. вхв — 
Nox. вхв — 
Nox. вхв — 
- 192.168.100. 25:вовв 192.168.100. 25:вовв нттњ 
- 192.168.100. 25:вовв 186 о $55 
- 172.64.130. 14:80 192.168.100. 25:вовв нттњ 
api-new. bignox. сот:во 192. 168. 100. 25:ВОВВ НТТЊ 
api-new. bignox. сот:во 192. 168. 100. 25:ВОВВ НТТЊ 
api-new. bignox. сот:во 192. 168. 100. 25:ВОВВ НТТЊ 
api-new. bignox. сот:во 223 3-Я 
api-new. bignox. сот:во 504 223 3-Я 
api-new. bignox. сот:во 171 3-Я 
NoxVMHand1e. вхв 
- 203.119.214. 125:443 192.168.100. 25:вовв нттњ 
203.119.214. 125:443 194 2329 $55 (2.27 кв) 
NoxVMHand1e. вхв — 
- 172. 64. 130. 140 3-Я 
NoxVMHand1e. вхв 
00:01 
15 
_ki? 500 ВА 
DNS 

6、burp抓包成功，如下图

Burp Project Intruder 
Repeater Window Help 
Extender 
Dashboard 
: 112 
Project options 
Target 
User options 
Passive Scan Client 
Intruder 
captcha-killer 
Repeater 
Struts Finder 
Sequencer 
Fastjson scan 
Decoder 
Autonze 
Comparer 
terc 
HITP history WabSockats history Options 
Request to httr 
Forward 
Drop 
Comment this item 
1 
2 
3 
4 
6 
7 
8 
9 
Params Headers Hex 
POST //wepoker/getUnreadMsgCount 
vi ajax HTTP/I I 
Accept-Encoding: gzip, deflate 
Content-Type: application/x-www-form-urlencoded 
User-A—mi 
Host 
Connecllu 
Content-Length: 212 
Android 51 1; Ll - 
O ANOO Build/LIO-ANOO) 
nRmmBUversion=5 6 6&appVersionCode— 
-27 Uang 
• ,zoä 
10 
• 75 
Hor 
O matches 
o' 

**方法三：夜神+xposed+JustTrustMe 可突破双向验证**

环境准备：

夜神模拟器（Android 5版本）、JustTrustMe、xposed

安装完成如下图：

* 安装xposed生成一个APP

0 
「 DC 亏 用 樘 拟 器 （ 1 ） 7 ℃ 05 
冒 
Android 5 
0 1013 
． 苗 戏 & 应 用 0 式 试 “ 逆 世 神 、 
0 
0 
0 
游 戏 中 心 
系 统 应 用 
游 推 荐 榜 单 
新 手 引 写 
谷 駭 安 鞍 器 
× 就 d 《 n 嗩 a 「 
WeChat 
0 币 
茉 飞 人 天 使 （ 高 版 ） 
世 神 -VIP 免 费 送 
战 玲 垅 2 （ 山 淘 异 兽 ） 
三 国 忑 飞 略 版 
力 宝 贝 归 采 
球 英 雄 

* 安装完成之后会打个绿√（踩坑点：xposed貌似不支持Android 7版本的）

roc 7.0.o.6 
Android 5 
a 10:15 
Xposed Installer 
Xposed Status 
Xposed Framework version 89 is active. 
INSTALL/UPDATE 
Version 89 
UNINSTALL 
Uninstaller (201 80117) 

* 安装完成后，可以专门绕过一些对模拟器有防护的APP，然后抓包方式与方法一一致。

**方法四：使用真机（Android and IOS）的方式**

场景：在实际的环境中，有很多的APP在模拟器中打开，会直接闪退，或者提示检测到使用模拟器打开。

1、安装burp证书，burp设置好代理（ps:设置的IP和端口要与真机的一致）

Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz 
Burp Project Intruder Repeater Window Help 
x 
Extender 
Dashboard 
Project options 
Target 
User options 
pro 
Passwe Scan Client 
Intruder 
captcha-killer 
Repeater 
Struts 
Finder 
Sequencer 
Fastjson scan 
Decoder 
Autorize 
Comparer 
Intercept HITP history WabSockats history O 
7 
0 
7 
0 
7 
0 
Proxy Listeners 
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server _ 
Running Interface 
Remove 
Invisible Redirect 
Certificate 
per-host 
Per-host 
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or 
another installation of aurp_ 
Import / export CA certificate 
Intercept Client Requests 
Regenerate CA certificate 
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab. 
ntercept requests based on the following rules: 
Master interception is tumed off 
Enabled 
Remove 
Up 
Operator Match type 
or 
or 
And 
File extension 
Request 
HITP method 
URL 
Relationship 
Does not match 
Contains parameters 
Does not match 
Is in target scope 
Condition 
(nglElnjpgSlnpngSlncssSlnjsSlmcoS) 
(getlpost) 
C] Automatically fix missing or superfluous new lines at end of request 
Automatically update Content-Length header when the request is edited 
Intercept Server Responses 
Use these settings to control which responses are stalled for viewing and editing in the Intercept tab. 

**Android 环境**

* 来到真机（本人的P20如下图）—>设置—>WALN—修改网络—>手动，如下图：主机名和端口与burp一致

O * 以 爷 10 ： 31 
令 GSWlFI_2BDO 
（ 未 更 改 ） 
显 示 高 级 选 项 
代 理 
该 浏 览 器 使 用 HTTP 代 理 ， 但 其 他 应 用 可 能 不 会 使 用 
服 务 器 主 机 名 
1 92 ． 1 68 主 129 
服 务 器 端 口 
8088 
对 以 下 对 象 绕 过 代 理 ： 
example ℃ om,mycomp.test ℃ om,localhost 
取 消 
DHCP > 
保 存 

* 设置完成之后真机也需要安装BURP的证书，如下图，访问http://burp,下载好证书

Q Burp Suite Professional 
Burp Suite Professional 
Welcorne to Burp Suite professional. 
10:34 
CA (Mificate 

* 下载完成后，回到设置—>安全—>更多安全设置—>加密和凭据—>从存储设备安装证书，找到下载的证书**（ps：证书的命名要以.crt的格式作为后缀名），如下图：**
* UCDownloads 
  config 
  novels 
  pictures 
  Screenshot 
  video 
  . 1.0.apk.1 
  cacert.crt 
  3B26a 
  content 
  2019iE7h14E 
  0.97 KB 
  66 47 
  Android 
  CRT 
  BIN 
* 点击安装，默认安装，安装完成即可。

**IOS 环境**

* 来到真机（本人的IOS如下图）—>设置—>WALN—点击网络—>配置代理—>自动修改为手动，如下图：主机名和端口与burp一致

无 SIM 
下 午 10 ． 46 
< 返 回 
配 置 代 理 
关 手 自 
闭 动 动 
服 端 鉴 
务 囗 定 
器 
192 ． 168 ． 1 ， 129 
8088 

* 设置完成之后真机也需要安装BURP的证书，如下图，访问http://burp,点击右上角的证书，并安装，出现相关提示

0 
已 下 载 描 述 文 件 
安 裝 ． 谘 卉 在 " 谖 " 应 00 嵘 
还 文 件 。 
关 闭 
甴 
m 

* 根据提示，回到设置—>通用—>关于本机—>证书信任设置—>针对根证书启用完全信任，把PortSwigger CA选择即可安装完成**，如下图：**

〈 + 机 书 值 任 设 0 
受 倌 任 证 书 存 傭 区 版 本 2m8 口 m00 
PortSwigger CA 
讲 一 7 00r0 