

安卓逆向——dy急速版设备抓包分析补充

原创

[含笑](#) 于 2021-07-16 18:04:15 发布 241 收藏

分类专栏: [安卓逆向](#)

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/qq_39551311/article/details/118813390

版权



[安卓爬虫](#) 同时被 2 个专栏收录

3 篇文章 0 订阅 ¥99.90 ¥99.00

订阅专栏



[安卓逆向](#)

33 篇文章 15 订阅

订阅专栏

URL 参数分析

26	26
27- BaseUrl="https://aweme.snssdk.com/aweme/v1/challenge/search/	27+ BaseUrl="https://aweme.snssdk.com/aweme/v1/challenge/search/?os_api=22,
28 params_dict = url_to_dict(BaseUrl)	28 params_dict = url_to_dict(BaseUrl)
29 print(json.dumps(params_dict))	29 print(json.dumps(params_dict))
30	30
31 # {	31 # {
32 # "os_api": "22",	32 # "os_api": "22",
33 # "device_type": "PCRT00",	33 # "device_type": "PCRT00",
34 # "ssmix": "a",	34 # "ssmix": "a",
35 # "manifest_version_code": "140401",	35 # "manifest_version_code": "140401",
36- # "dpi": "270",	36+ # "dpi": "240",
37- # "uuid": "860946023464137",	37+ # "uuid": "861322275115182",
38 # "app_name": "aweme",	38 # "app_name": "aweme",
39 # "version_name": "14.4.0",	39 # "version_name": "14.4.0",
40 # "ts": "{}",	40 # "ts": "{}",
41 # "cpu_support64": "false",	41 # "cpu_support64": "false",
42 # "app_type": "normal",	42 # "app_type": "normal",
43 # "appTheme": "dark",	43 # "appTheme": "dark",
44 # "ac": "wifi",	44 # "ac": "wifi",
45 # "host_abi": "armeabi",	45 # "host_abi": "armeabi",
46 # "update_version_code": "14409900",	46 # "update_version_code": "14409900",
47 # "channel": "tengxun_1128_0112",	47 # "channel": "tengxun_1128_0112",
48 # "_rticket": "{}",	48 # "_rticket": "{}",
49 # "device_platform": "android",	49 # "device_platform": "android",
50- # "iid": "2375422181901277",	50+ # "iid": "334728601798093",
51 # "version_code": "140400",	51 # "version_code": "140400",
52- # "cdid": "12e98a74-ed25-491b-b546-dd0ff2fcc2e8",	52+ # "cdid": "456b77aa-b445-4881-bd0c-8917a89223c6",
53- # "openudid": "46101091d3dadeac",	53+ # "openudid": "32179c3d31702c5b",
54- # "device_id": "2463383096665719",	54+ # "device_id": "2058710736716423",
55- # "resolution": "810*1440",	55+ # "resolution": "720*1280",
56 # "os_version": "5.1.1",	56 # "os_version": "5.1.1",
57 # "language": "zh",	57 # "language": "zh",
58 # "device_brand": "OPPO",	58 # "device_brand": "OPPO",
59 # "aid": "1128",	59 # "aid": "1128",
60 # "mcc_mnc": "46000"	60 # "mcc_mnc": "46000"
61 # }	61 # }

https://blog.csdn.net/qq_39551311

发起请求的data参数对比分析

16	17
"sdk_version": "2.13.0-rc.2",	"sdk_version": "2.13.0-rc.2",
"sdk_target_version": 29,	"sdk_target_version": 29,
"git_hash": "a74dfele",	"git_hash": "a74dfele",
"os": "Android",	"os": "Android",
"os_version": "6.0.1",	"os_version": "6.0.1",
"os_api": 23,	"os_api": 23,
"device_model": "Nexus 6P",	"device_model": "Nexus 6P",
"device_brand": "google",	"device_brand": "google",
"device_manufacturer": "Huawei",	"device_manufacturer": "Huawei",
"cpu_abi": "armeabi-v7a",	"cpu_abi": "armeabi-v7a",
"build_serial": "8485T16111000553",	"build_serial": "8485T16111000553",
"release_build": "cl7f5d1_20200720",	"release_build": "cl7f5d1_20200720",
"density_dpi": 560,	"density_dpi": 560,
"display_density": "mdpi",	"display_density": "mdpi",
"resolution": "2392x1440",	"resolution": "2392x1440",
"language": "zh",	"language": "zh",
"mc": "DC:EE:06:17:77:E6",	"mc": "DC:EE:06:17:77:E6",
"timezone": 8,	"timezone": 8,
"access": "wifi",	"access": "wifi",
"not_request_sender": 0,	"not_request_sender": 0,
"rom": "EMUI-3230295",	"rom": "EMUI-3230295",
"rom_version": "MTC20L",	"rom_version": "MTC20L",
"cdid": "899f8a7f-ae6d-49cd-b910-48114ca8f701",	"cdid": "6d5f7210-e1dd-4918-9cd0-db764c5319a7",
"sig_hash": "aea615ab910015038f73c47e45d2146b",	"sig_hash": "aea615ab910015038f73c47e45d21466",
"openudid": "1bfa1339f238c042",	"openudid": "1bfa1339f238c042",
"clientudid": "dc924d67-5dad-45bc-b541-57253e1cd31a",	"clientudid": "be137676-fec6-4c17-a780-cdb715f64471",
"serial_number": "8485T16111000553",	"serial_number": "8485T16111000553",
"sim_serial_number": [],	"sim_serial_number": [],
],],
"region": "CN",	"region": "CN",
"tz_name": "Asia/Shanghai",	"tz_name": "Asia/Shanghai",
"tz_offset": 28800,	"tz_offset": 28800,
"oaid_may_support": false,	"oaid_may_support": false,
"req_id": "23db36c1-df6b-4ada-9600-c9f7053bffc",	"req_id": "cead522b-adfe-4424-9939-c43aaa6cb8ed",
"custom": {	"custom": {
"filter_warn": 0,	"filter_warn": 0,
"web_ua": "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 6P Build/V/MTC20L",	"web_ua": "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 6P Build/V/MTC20L; wv) AppleWebKit",
},	},
"apk_first_install_time": 1623744772648,	"apk_first_install_time": 1623744772648,
"is_system_app": 0,	"is_system_app": 0,
"sdk_flavor": "china"	"sdk_flavor": "china"
},	},
"gen_time": 1623838351891	"gen_time": 1625817620443
}	}

https://blog.csdn.net/qq_39551311

对比需求的请求的包，发现cookie还多了一个odin_tt的参数

The screenshot displays the WinConfig application window with a list of network requests on the left and the Fiddler interface on the right. The Fiddler interface shows the details of a selected request, including the Request Headers, Client information, Cookies, and Response Headers. A red box highlights a cookie value in the Cookies section: `odin_tt=fad0977d5f5e3741ccab587f52f0942fa84480c33436fd889b0ce1f6d43069e295571661e0fbedfa518a08e2c290ac02cda6779e463e28e7b34589865ff9b9308treq=1f3d2a2ab047c6dde5b199c92b3f1b753861a64ff3`. A red arrow points to this value with the text "需求的请求, 还少了一个 odin_tt 的 cookie".

模拟请求激活设备，得到 odin_tt