THCON 2025

WOCSA

Worlwide Open Cyber Security Association

DVID

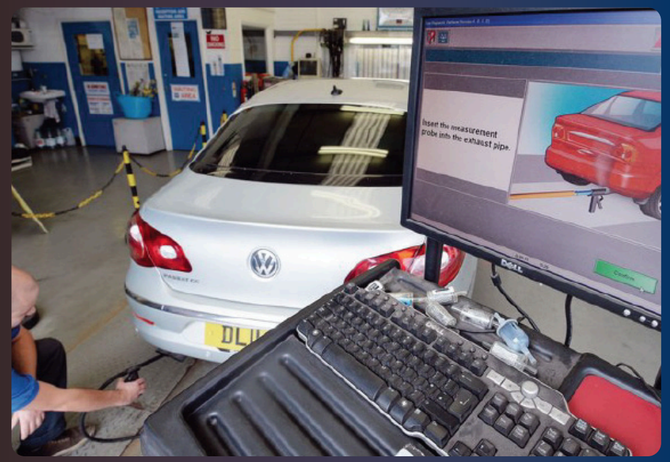
CYBLEX

Consulting

BATTLEFIELD

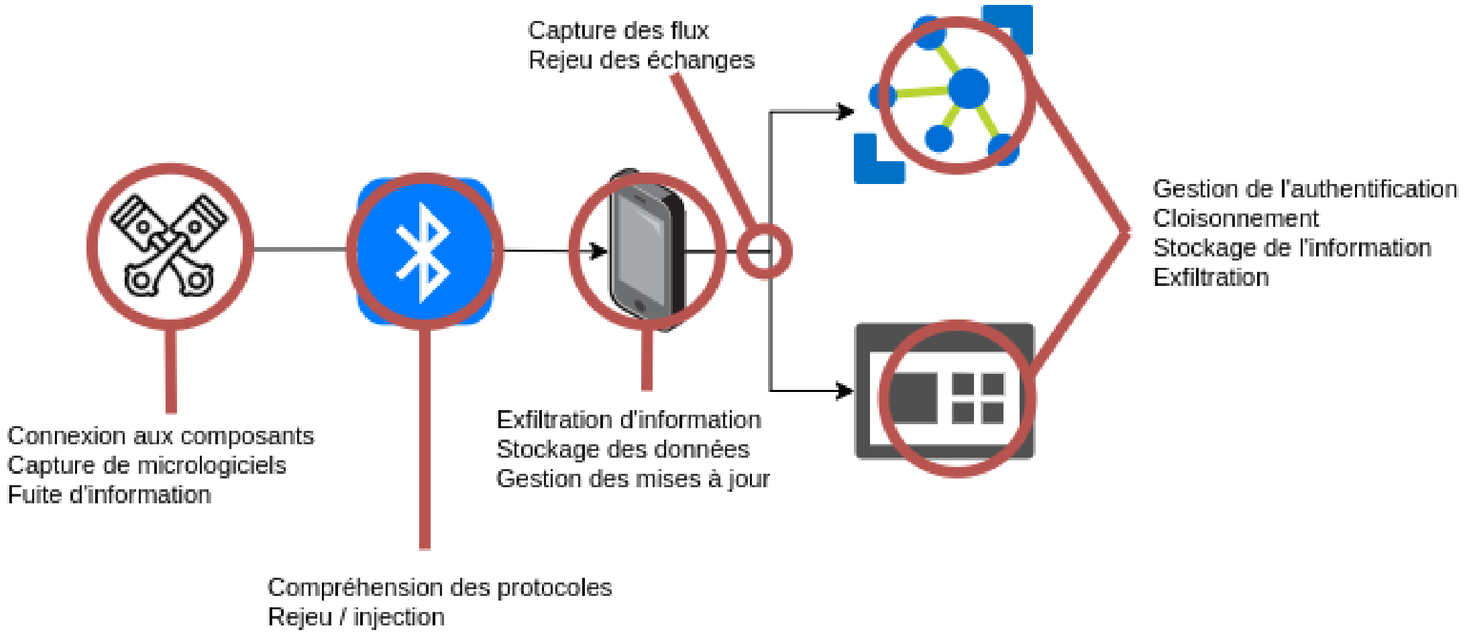
Pacemarker (2017)

LG SmartThinQ (2016)



Volkswagen (2015)

ECOSYSTEM



30%
of hardware

20%
of cloud computing

20%
of data transport

30%
of only data

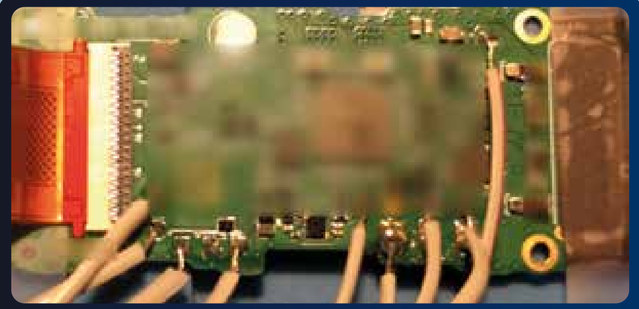
PRACTICAL

- Debug ports are opened
- Bootloader memory readable bytes per bytes
- Firmware reconstruction from exact
- Binary analysis
- Remote Code Execution finding

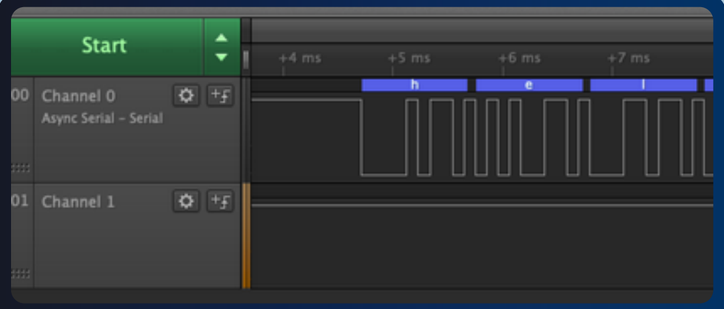
```
[ ] crc32 (NEW)
[*] md (NEW)
[*] memcmp (NEW)
[*] memcpy (NEW)
[*] memset (NEW)
[ ] memtest (NEW)
[ ] memtester (NEW)
[ ] memory modify (mm) (NEW)
[*] mw (NEW)
```

```
=> md.b 0x4000000 0x50
04000000: de ad be ef de
04000010: de ad be ef de
04000020: de ad be ef de
04000030: de ad be ef de
04000040: de ad be ef de
=>
```

IRL



Soldering on PCB



Probing of signals

UART

```
=> md.b 0x4000000 0x50
04000000: de ad be ef de
04000010: de ad be ef de
04000020: de ad be ef de
04000030: de ad be ef de
04000040: de ad be ef de
=>
```

Memory display

gmbnomis/**uboot-mdb-dump**

1 3 92 24

Firmware recovery

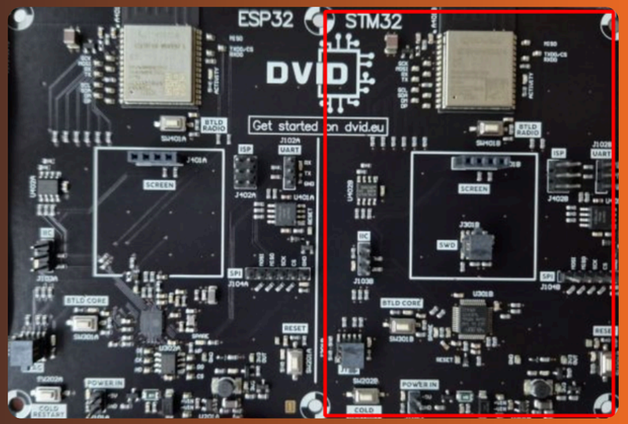
Firmware emulation

```
memset(acStack152,0x0200);
sprintf(acStrack152,"echo input:%s>/tmp",pcVar1);
system(acStrack152)
```

Firmware disassembly

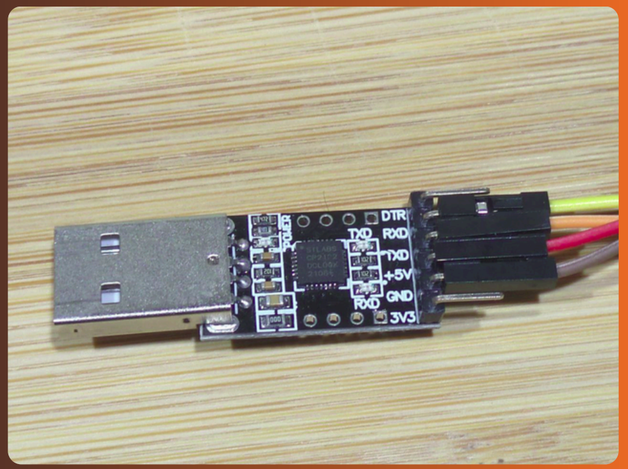
LET'S PLAY YOURSELF

This workshop will focus on STM32 side (right) of the DVID board and explore UART protocol.



OBJECTIVE :

- Wire correctly UART to the STM32 MCU
- Dump firmware to local computer
- Analyze the firmware to find useful information
- Pass the password through UART dongle

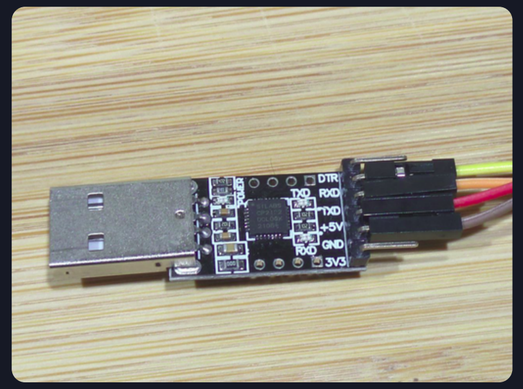


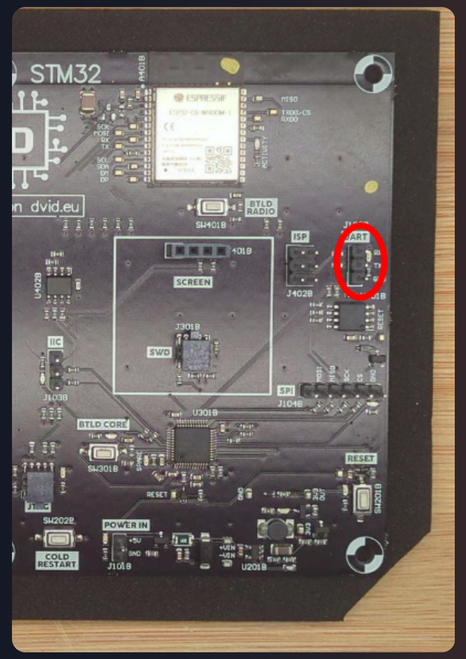
YOUR TURN - WIRE THE BOARD

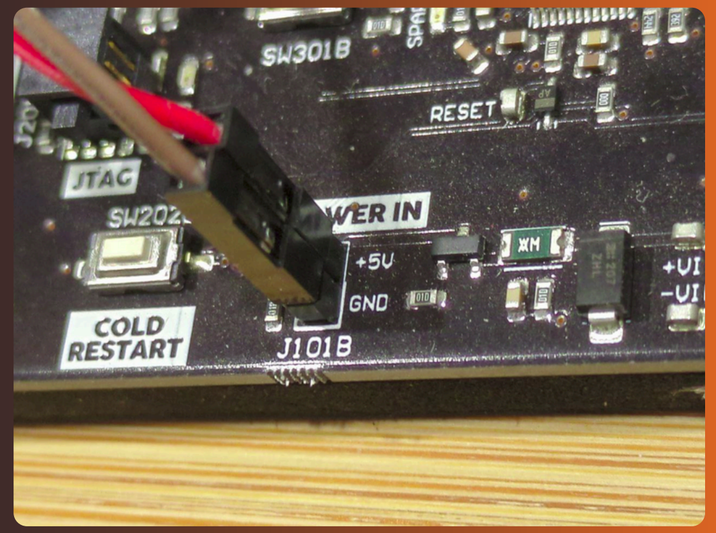
Locate the UART pins on DVID Board (STM32 side)

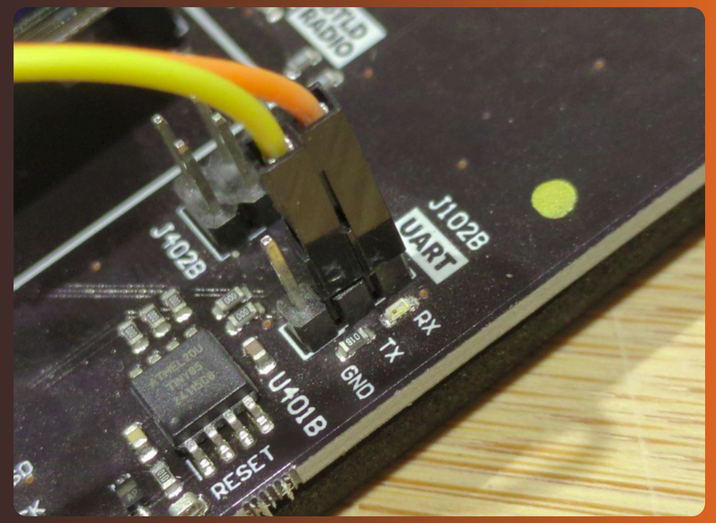
Remember : TX & RX are crossed wired

Press RESET button to start the board.

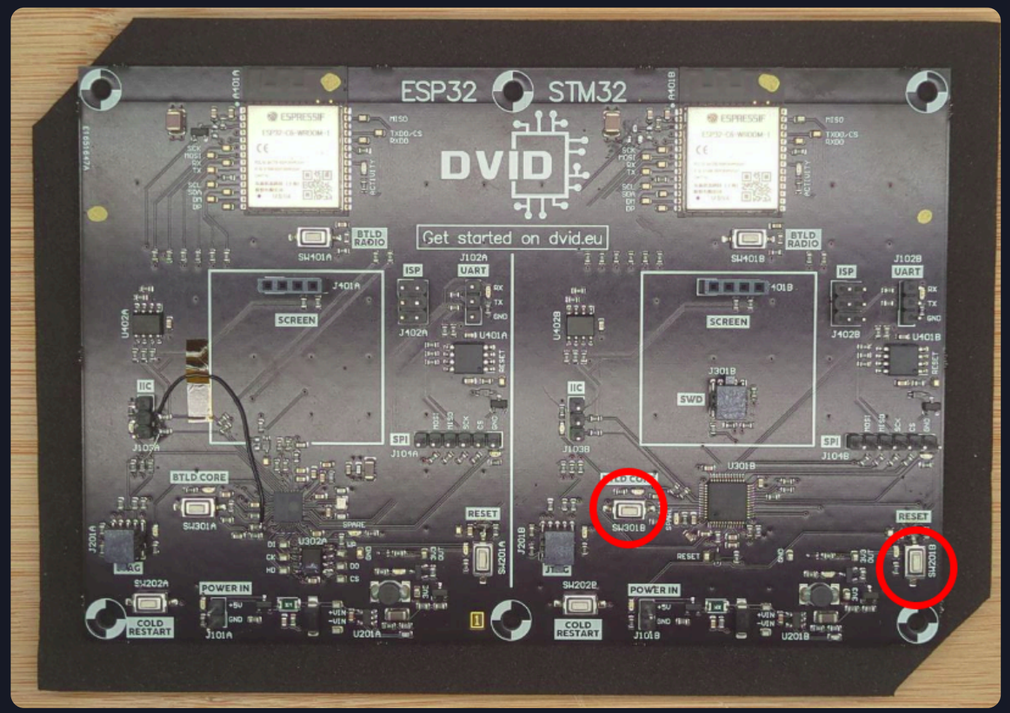








YOUR TURN - READ THE FLASH



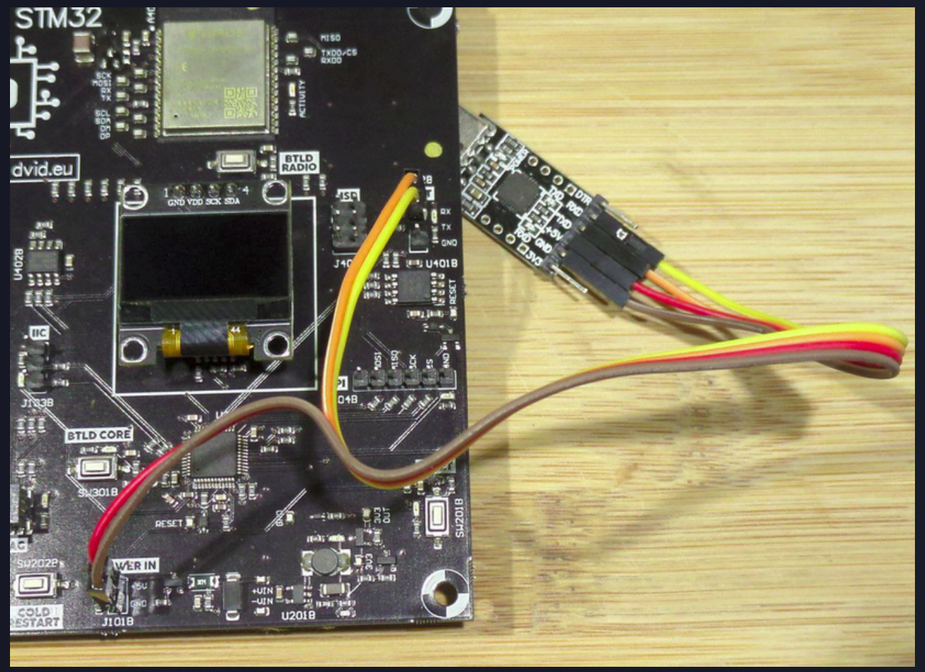
HOLD BTLDCORE
HOLD & RELEASE RESET

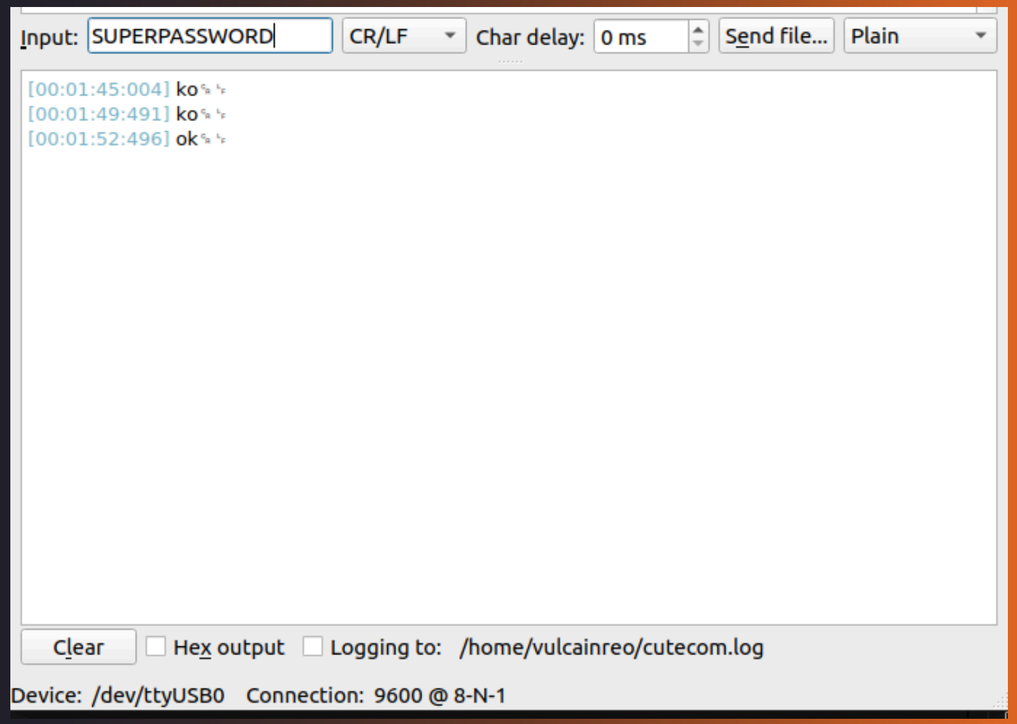
strings test.bin | grep -i pass

Pass from UART ?
SUPERPASSWORD

Arduino_STM32/tools/linux64/stm32flash/stm32flash -b 115200 -r test.bin /dev/ttyUSB0

YOUR TURN - TALKING IN UART



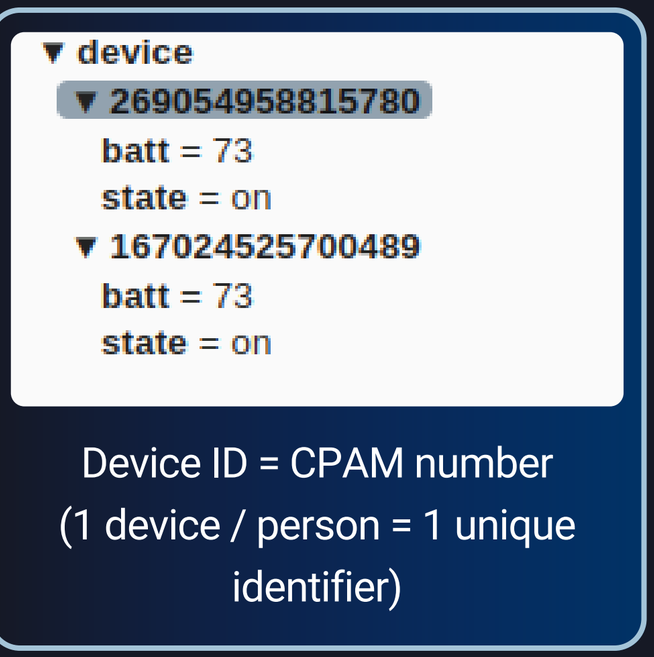


https://packages.debian.org/fr/sid/amd64/cutecom

PRACTICAL

- MQTT server accessible with certificate (clientID)
- jokers (#) usage is allowed
- Illegitimate access to other devices data
- llegitimate access to $SYS
- GPDR data leakage

IRL



Device ID = CPAM number
(1 device / person = 1 unique identifier)

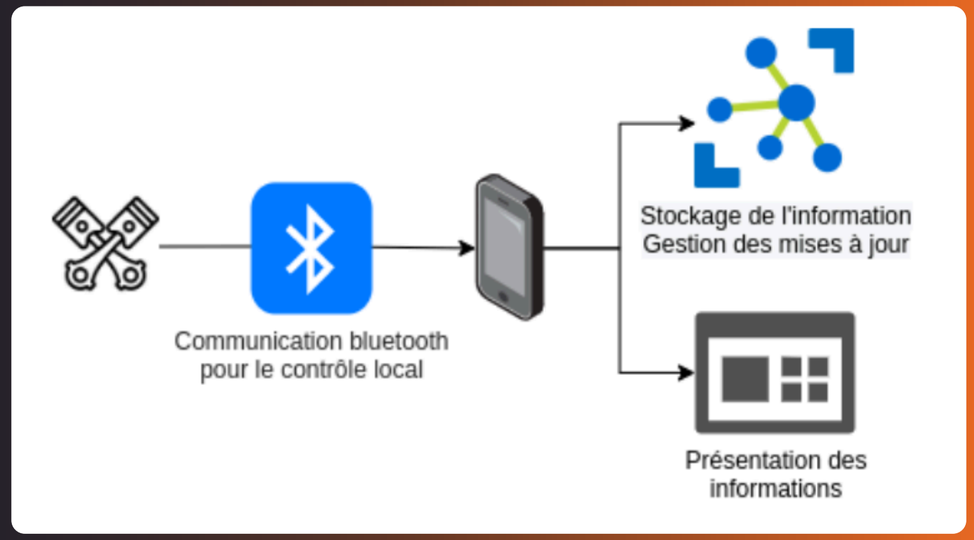
Let's do some quick OSINT

PRACTICAL

- Enroll the device using OTP
- Access to all devices on /devices endpoint
- Convert URL from /me to /device/UUID
- Combine /device/UUID with all devices UUID
- Impersonate device

PRACTICAL

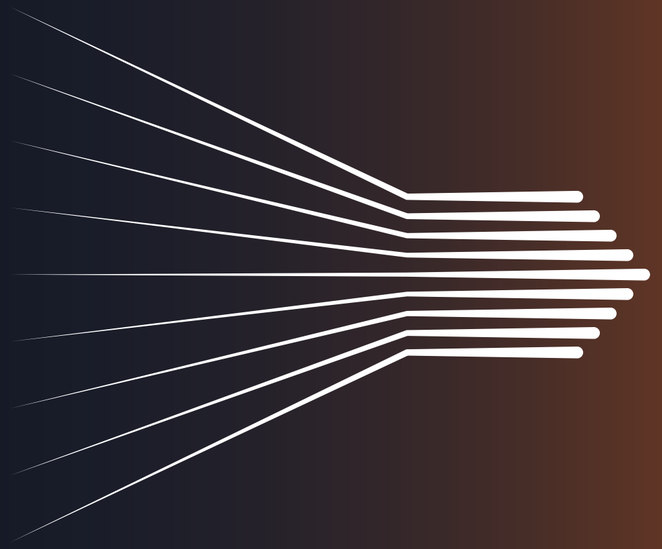
- Unit analysis of equipment
- No injection endpoint on Web app
- Discover how XSS can be injected
- MQTT enrollment allows custom data
- XSS exploit is executed on dashboard UI



Injection of an XSS load in the proprietary field during device enrollment, the payload is executed when the device proprietary is printed on the dashboard

SUMMARY

- Data produced on one side of the chain may only be consumed at the other side
- Debug code VS Production code
- Least privilege principle / features limits flexibility
- Unique identifiers can be personal and require protection
- Default passwords need to be updated

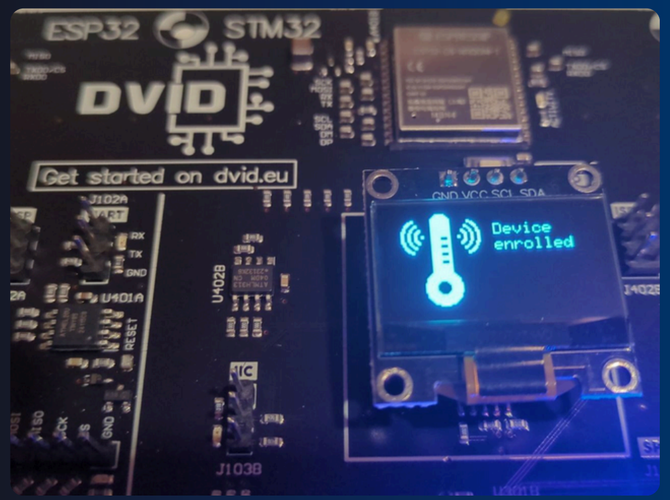


How to anticipate vulnerabilities and learn how to correct them right from the design phase

WHAT IF GOING MORE FURTHER ?

- Immersive experience directly inspired by the IoT world
- Tools and techniques that can be reused directly in co

STAY "OPEN SOURCED"



Community trainings

CTF challenges

DVID Battle (school battle)

https://github.com/dvid-security/dvidv2-opensource

WOCSA

Worlwide Open Cyber Security Association

- WOCSA (Worldwide Open Cyber Security Association) is a federation of **non profit association** with its HQ based in France and exists right now on **5 continents.**
- Cybersecurity is a public affair in which **everyone has to take a part**.
- WOCSA joins experts with other people **to take care of our digital life.**
- WOCSA mixes **international projects** with **local actions** based on:
  - a permanent work to develop proximity network,
  - focused on local actions,
  - unbounded collaboration as core way of work.

CYBER JUTSU

WOCS'HACK

WOCSA ETHICAL HACKING WORKSHOPS

DEFCON

Toulouse Hacking Convention_

CAMPUS CYBER

cité des sciences & de l'industrie

WOCSA

Worlwide Open Cyber Security Association

DVID

CYBLEX
Consulting