Crushing crumbs of information to eat a whole cake.

Felipe Pr0teus

Who am I?

- Felipe Espósito (Pr0teus).
- 10+ years of experience.
- Father of a girl.
- Bug bounty when the above item allows.
- Blue team instructor when the above item allows as well.
- Security Researcher at Tenchi Security

Motivation

We as a society rely in each other, not only governments but services. That's create a huge supply chain of trust?! and relationships.

ALICE IN SUPPLY CHAINS

THIRD-PARTY CYBER RISK MANAGEMENT NEWSLETTER

Electricity company has to know:
Your name, where you live, how much you spend in energy, if you are paying...

Police find marijuana plantation in Santo Antônio de Pádua

A marijuana plantation was found inside a residence in the Gabri neighborhood late Tuesday morning in Santo Antônio de Pádua.

The same can occur in a lot of other services that we use...
Internet Provider, Water, Gas,

How can we exploit this relationships?

- Hack every single company. (Hack the planet!)
- Wait for the company be hacked and get the leak (boring!)

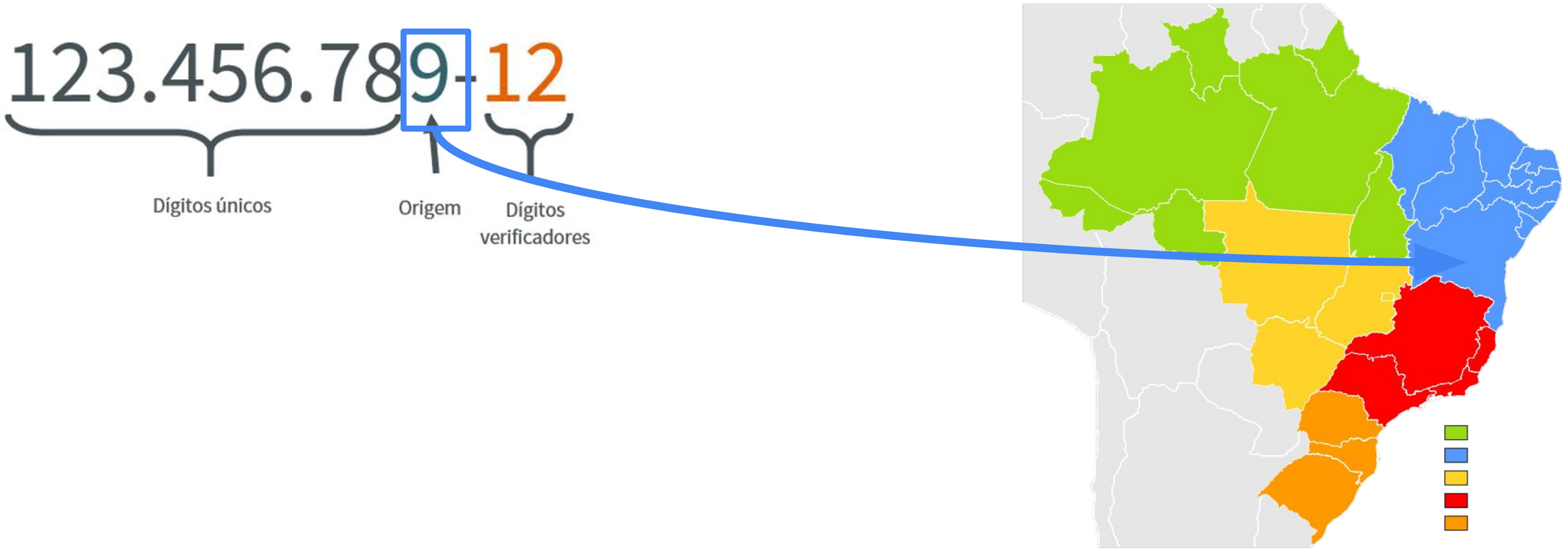
Then i start to wonder:
What **is the minimum** crumb of information do i need to get access to anyone electricity bill for example ?

CPF

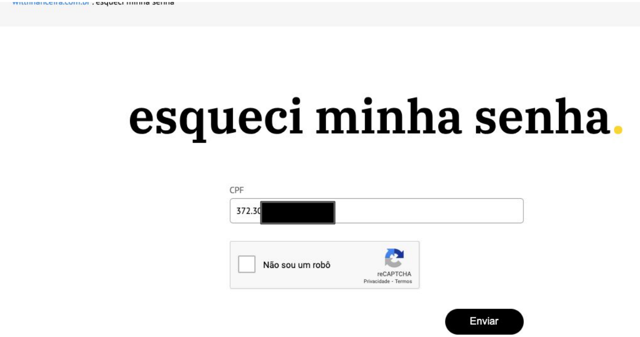
Its similar the Social Security Number in United States of America.

Every single brazilian has (at least) one.

That makes a **awesome** Primary Key in databases.



Every single piece of information, is a good intel



witfinanceira.com.br / esqueci minha senha

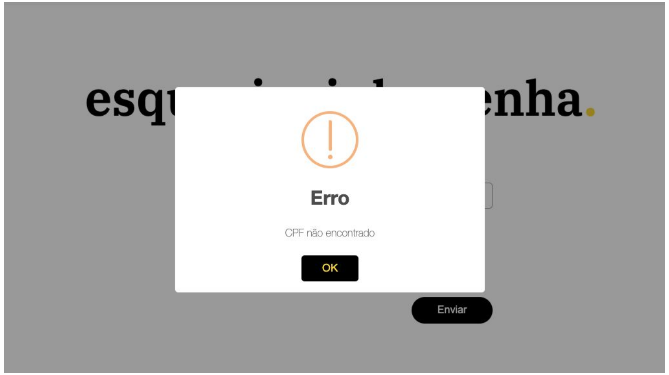
esqueci minha senha.

CPF

372.30[redacted]

□ Não sou um robô

Enviar



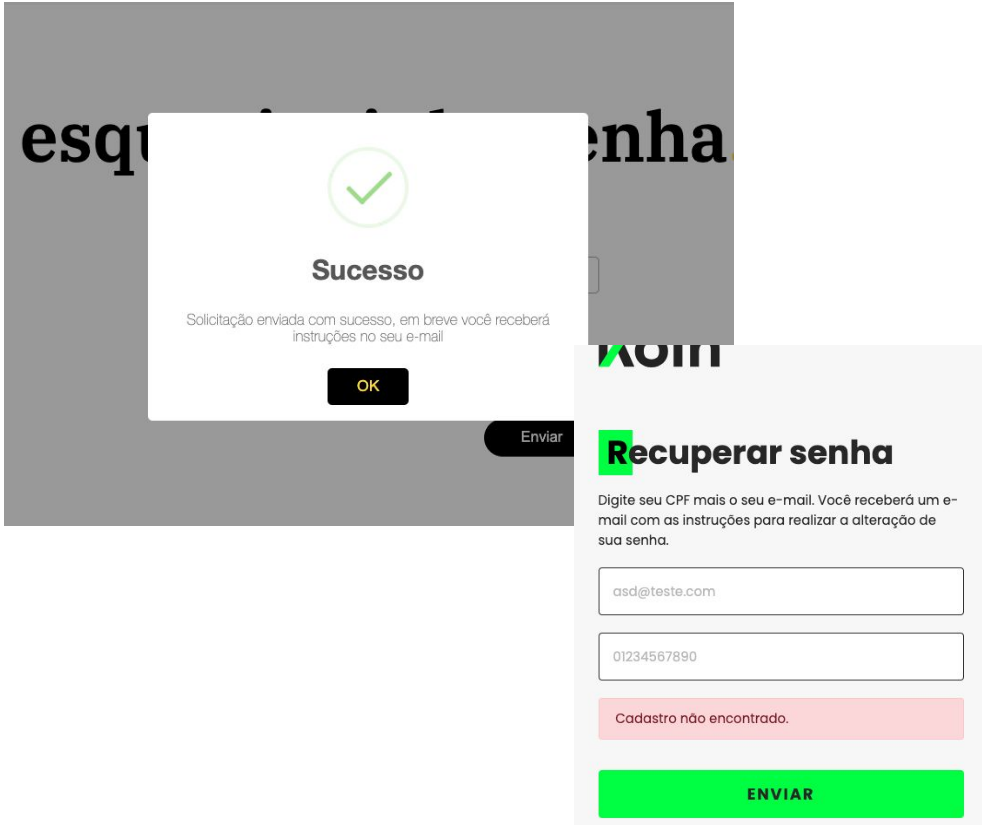
esqu enha.

Erro

CPF não encontrado

OK

Enviar



esqu enha.

Sucesso

Solicitação enviada com sucesso, em breve você receberá instruções no seu e-mail

OK

Enviar

Koin

Recuperar senha

Digite seu CPF mais o seu e-mail. Você receberá um e-mail com as instruções para realizar a alteração de sua senha.

asd@teste.com

01234567890

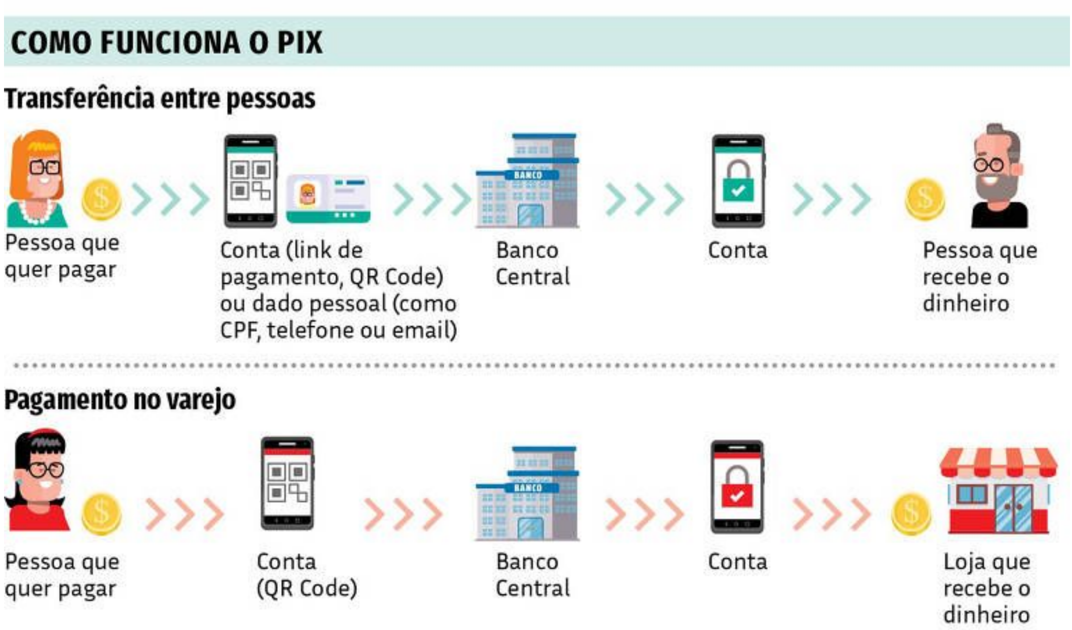
Cadastro não encontrado.

ENVIAR

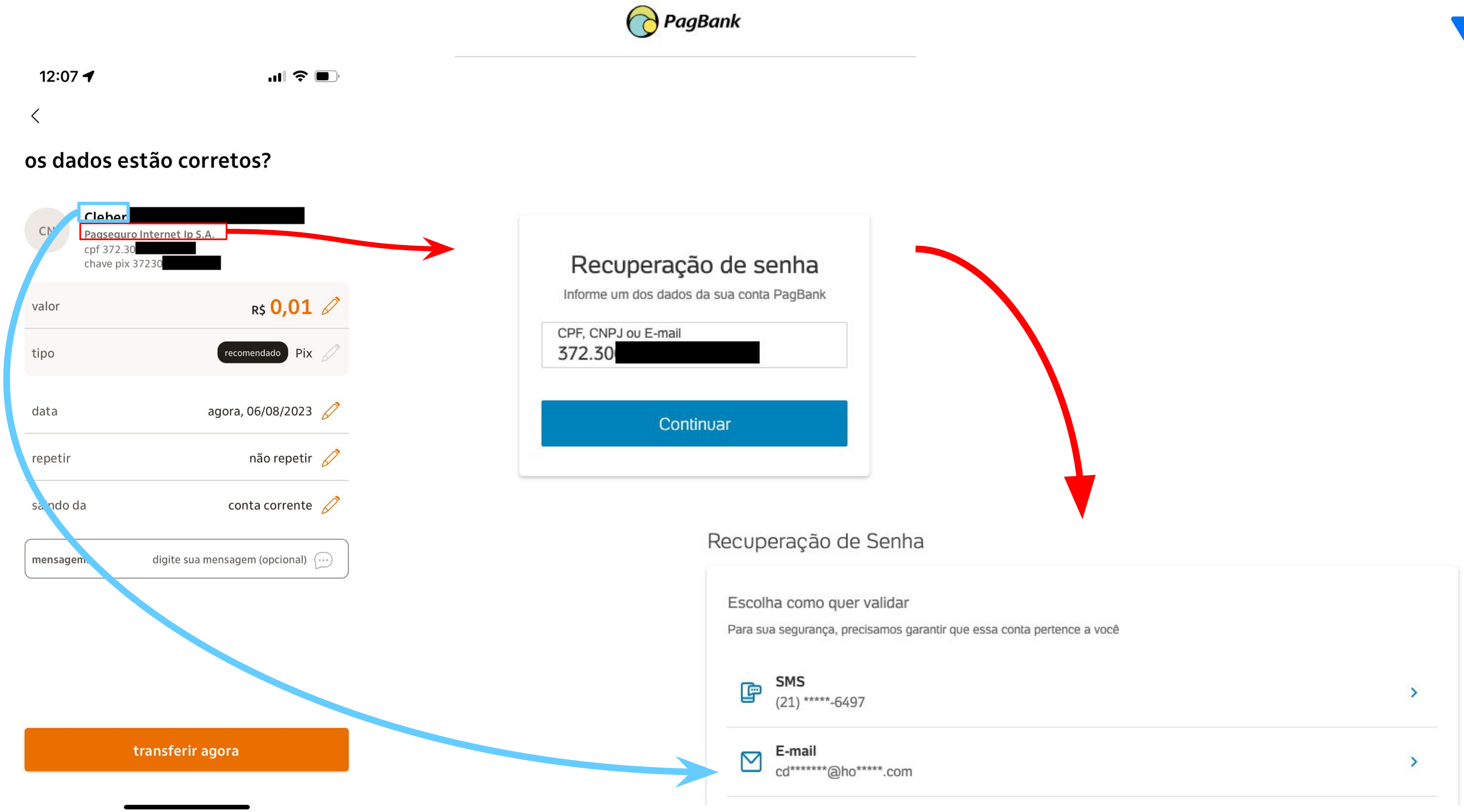
PIX

Its an instant payment system created in Brazil. Currently the main form of payment, like nobody carry cash anymore. You can have 4 PIX keys:

- Cellphone (98,7KK)
- CPF (107,8KK)
- E-MAIL (68,8KK)
- RandomKey (QRcode)


COMO FUNCIONA O PIX
Transferência entre pessoas
Pessoa que quer pagar
Conta (link de pagamento, QR Code) ou dado pessoal (como CPF, telefone ou email)
Banco Central
BANCO
Conta
Pessoa que recebe o dinheiro
Pagamento no varejo
Pessoa que quer pagar
Conta (QR Code)
Banco Central
BANCO
Conta
Loja que recebe o dinheiro

- 469 kk active Pix keys: Data from july 2022
  https://www.metropoles.com/brasil/economia-br/brasileiro-se-rende-ao-pix-e-total-de-chaves-ja-supera-o-dobro-da-populacao



PagBank

12:07

os dados estão corretos?

CN

Cleber [redacted]

Pagseguro Internet Ip S.A.

cpf 372.30[redacted]

chave pix 37230[redacted]

valor	R$ 0,01
tipo	recomendado Pix
data	agora, 06/08/2023
repetir	não repetir
saindo da	conta corrente

mensagem: digite sua mensagem (opcional)

transferir agora

Recuperação de senha

Informe um dos dados da sua conta PagBank

CPF, CNPJ ou E-mail

372.30[redacted]

Continuar

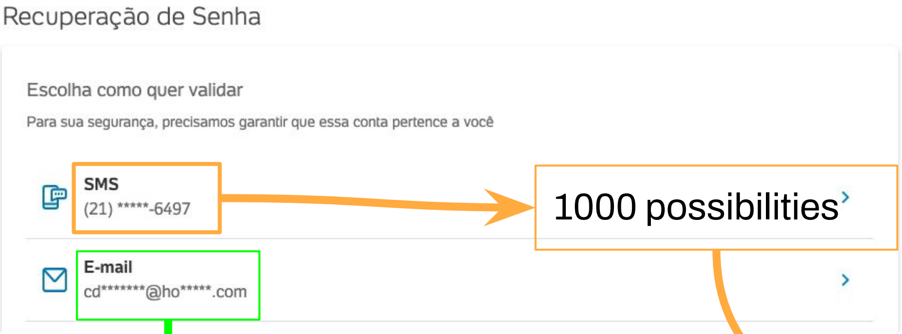
Recuperação de Senha

Escolha como quer validar

Para sua segurança, precisamos garantir que essa conta pertence a você

SMS
(21) *****-6497

E-mail
cd*******@ho*****.com



Recuperação de Senha

Escolha como quer validar

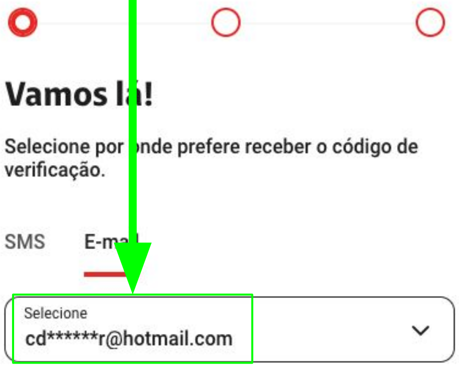
Para sua segurança, precisamos garantir que essa conta pertence a você

SMS
(21) *****-6497

E-mail
cd*******@ho*****.com

1000 possibilities

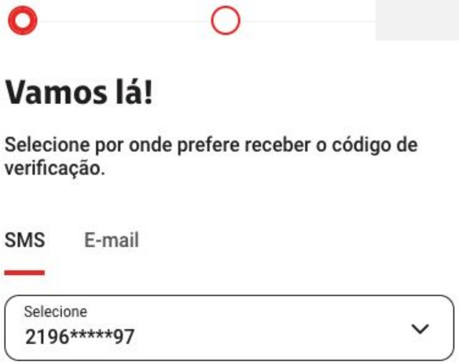
Not only the R and TLD.
Matching numbers of *



Vamos lá!

Selecione por onde prefere receber o código de verificação.

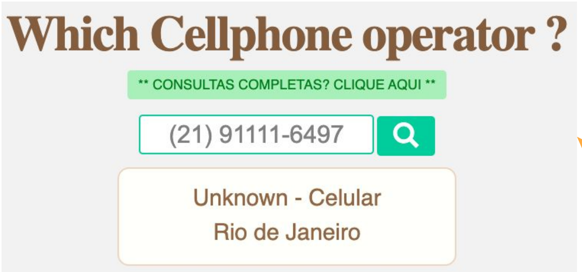
Selecione
cd******r@hotmail.com



Vamos lá!

Selecione por onde prefere receber o código de verificação.

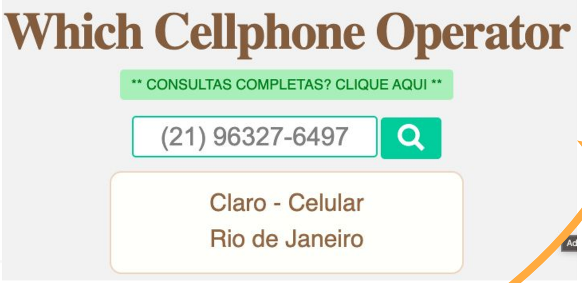
Selecione
2196*****97



Which Cellphone operator ?

(21) 91111-6497

Unknown - Celular
Rio de Janeiro

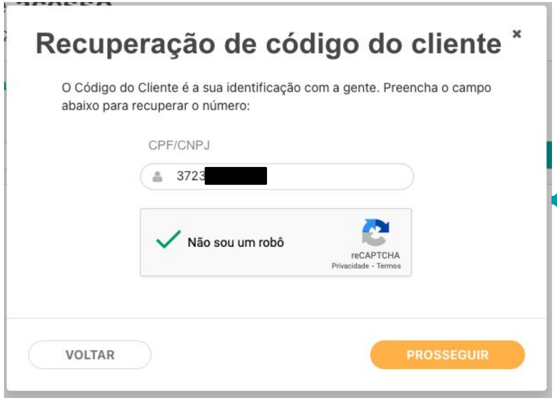


Which Cellphone Operator

(21) 96327-6497

Claro - Celular
Rio de Janeiro

99 possibilities



Recuperação de código do cliente ×

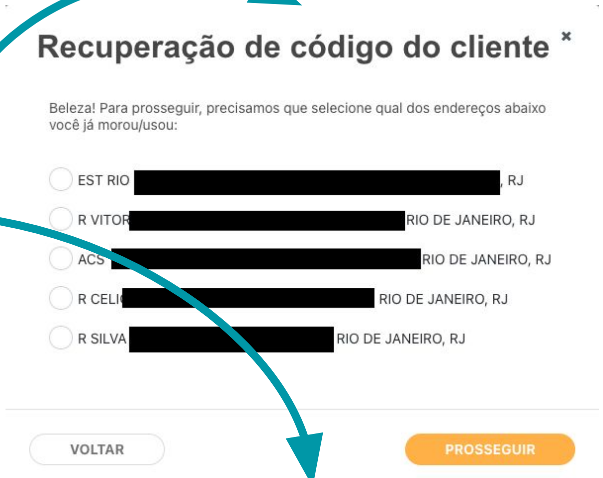
O Código do Cliente é a sua identificação com a gente. Preencha o campo abaixo para recuperar o número:

CPF/CNPJ

3723[redacted]

✓ Não sou um robô

VOLTAR PROSSEGUIR



Recuperação de código do cliente ×

Beleza! Para prosseguir, precisamos que selecione qual dos endereços abaixo você já morou/usou:

○ EST RIO [redacted], RJ

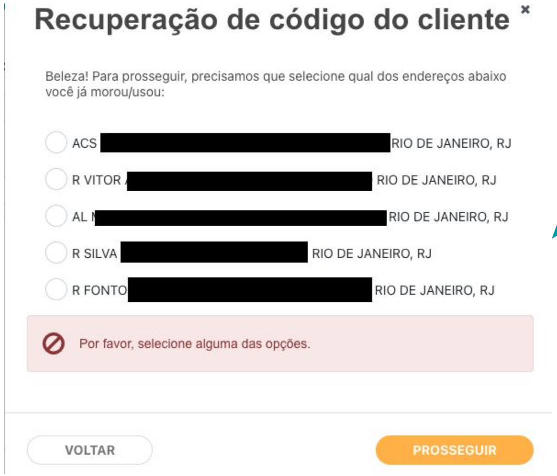
○ R VITOR[redacted]RIO DE JANEIRO, RJ

○ ACS [redacted]RIO DE JANEIRO, RJ

○ R CELI[redacted] RIO DE JANEIRO, RJ

○ R SILVA [redacted]RIO DE JANEIRO, RJ

VOLTAR PROSSEGUIR



Recuperação de código do cliente ×

Beleza! Para prosseguir, precisamos que selecione qual dos endereços abaixo você já morou/usou:

○ ACS [redacted]RIO DE JANEIRO, RJ

○ R VITOR [redacted] RIO DE JANEIRO, RJ

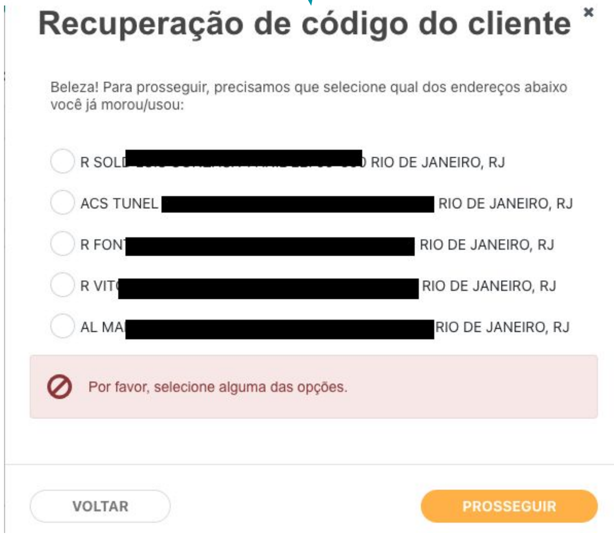
○ AL [redacted]RIO DE JANEIRO, RJ

○ R SILVA [redacted] RIO DE JANEIRO, RJ

○ R FONTO[redacted]RIO DE JANEIRO, RJ

Por favor, selecione alguma das opções.

VOLTAR PROSSEGUIR



Recuperação de código do cliente ×

Beleza! Para prosseguir, precisamos que selecione qual dos endereços abaixo você já morou/usou:

○ R SOLD[redacted] RIO DE JANEIRO, RJ

○ ACS TUNEL [redacted] RIO DE JANEIRO, RJ

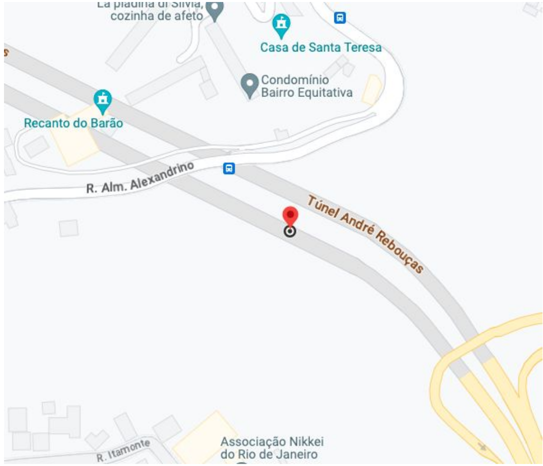
○ R FON[redacted] RIO DE JANEIRO, RJ

○ R VIT[redacted] RIO DE JANEIRO, RJ

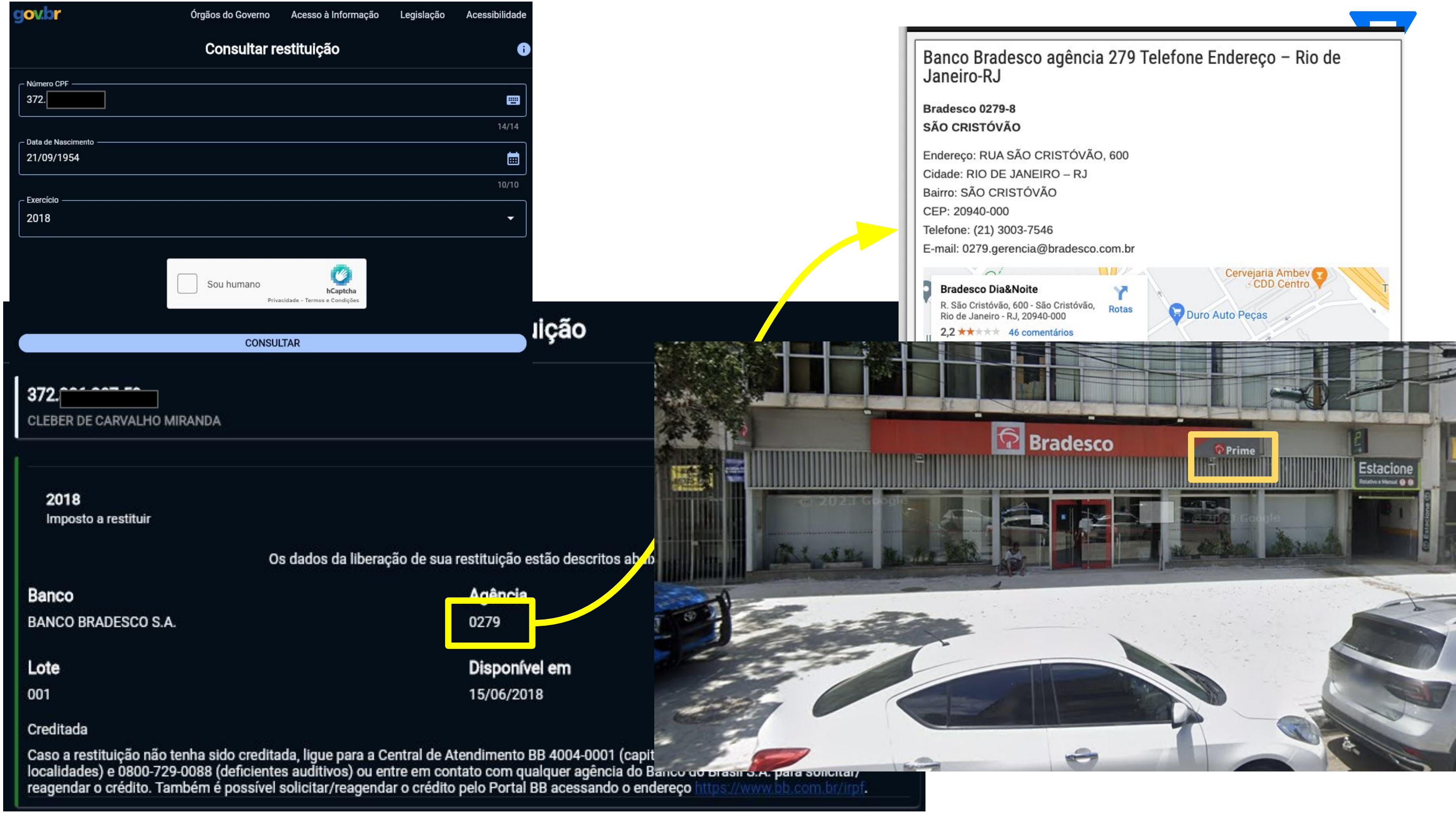
○ AL MA[redacted]RIO DE JANEIRO, RJ

Por favor, selecione alguma das opções.

VOLTAR PROSSEGUIR



La piadina di Silvia, cozinha de afeto
Casa de Santa Teresa
Condomínio Bairro Equitativa
Recanto do Barão
R. Alm. Alexandrino
Túnel André Rebouças
R. Itamonte
Associação Nikkei do Rio de Janeiro



Consultar restituição

Número CPF
372.[redacted]
14/14

Data de Nascimento
21/09/1954
10/10

Exercício
2018

□ Sou humano

CONSULTAR

ição

372.[redacted]
CLEBER DE CARVALHO MIRANDA

2018
Imposto a restituir

Os dados da liberação de sua restituição estão descritos ab

Banco	Agência
BANCO BRADESCO S.A.	0279
Lote	Disponível em
001	15/06/2018

Creditada

Caso a restituição não tenha sido creditada, ligue para a Central de Atendimento BB 4004-0001 (capit localidades) e 0800-729-0088 (deficientes auditivos) ou entre em contato com qualquer agência do Banco do Brasil S.A. para solicitar/ reagendar o crédito. Também é possível solicitar/reagendar o crédito pelo Portal BB acessando o endereço https://www.bb.com.br/irpf.

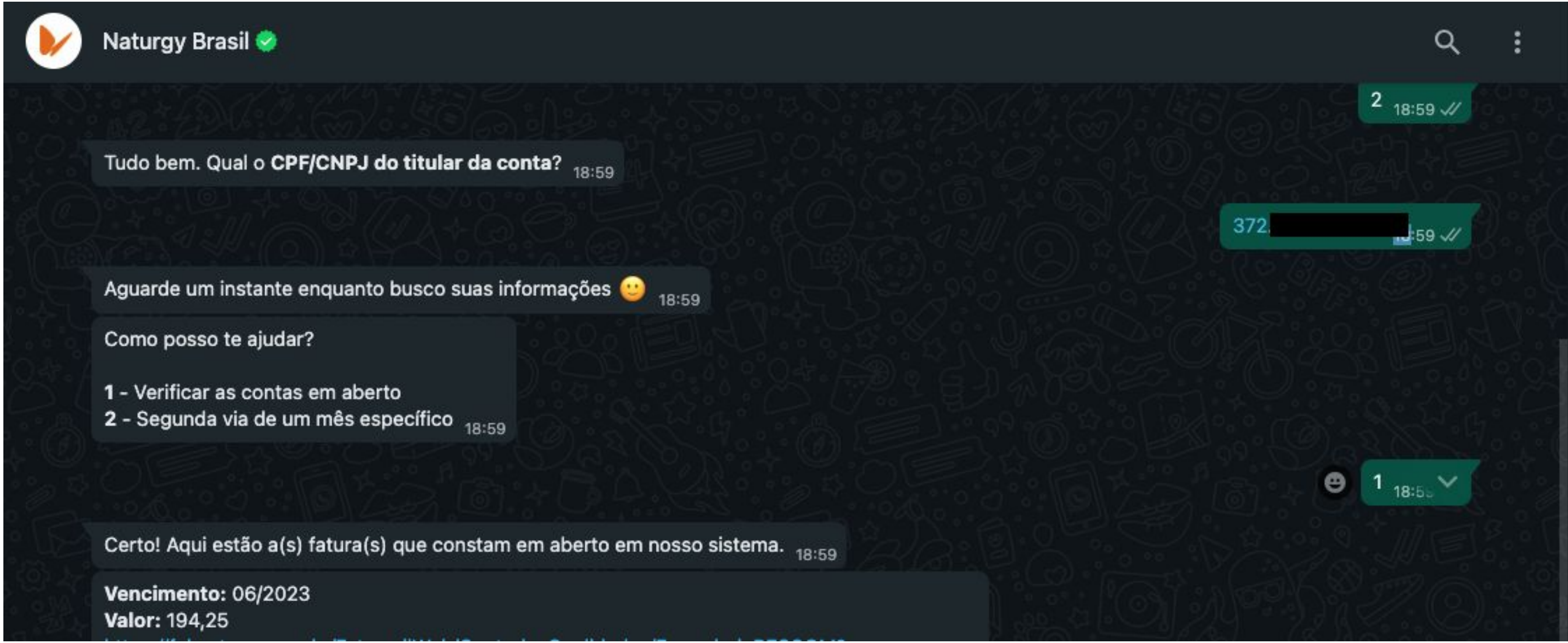
Banco Bradesco agência 279 Telefone Endereço – Rio de Janeiro-RJ

Bradesco 0279-8
SÃO CRISTÓVÃO

Endereço: RUA SÃO CRISTÓVÃO, 600
Cidade: RIO DE JANEIRO – RJ
Bairro: SÃO CRISTÓVÃO
CEP: 20940-000
Telefone: (21) 3003-7546
E-mail: 0279.gerencia@bradesco.com.br

Bradesco Dia&Noite
R. São Cristóvão, 600 - São Cristóvão, Rio de Janeiro - RJ, 20940-000
2,2 ★★★★★ 46 comentários
Rotas
Cervejaria Ambev - CDD Centro
Duro Auto Peças
Bradesco
Prime
Estacione
© 2023 Google

Not only websites:



Naturgy Brasil

2 18:59

Tudo bem. Qual o **CPF/CNPJ do titular da conta?** 18:59

372[redacted]:59

Aguarde um instante enquanto busco suas informações 🙂 18:59

Como posso te ajudar?

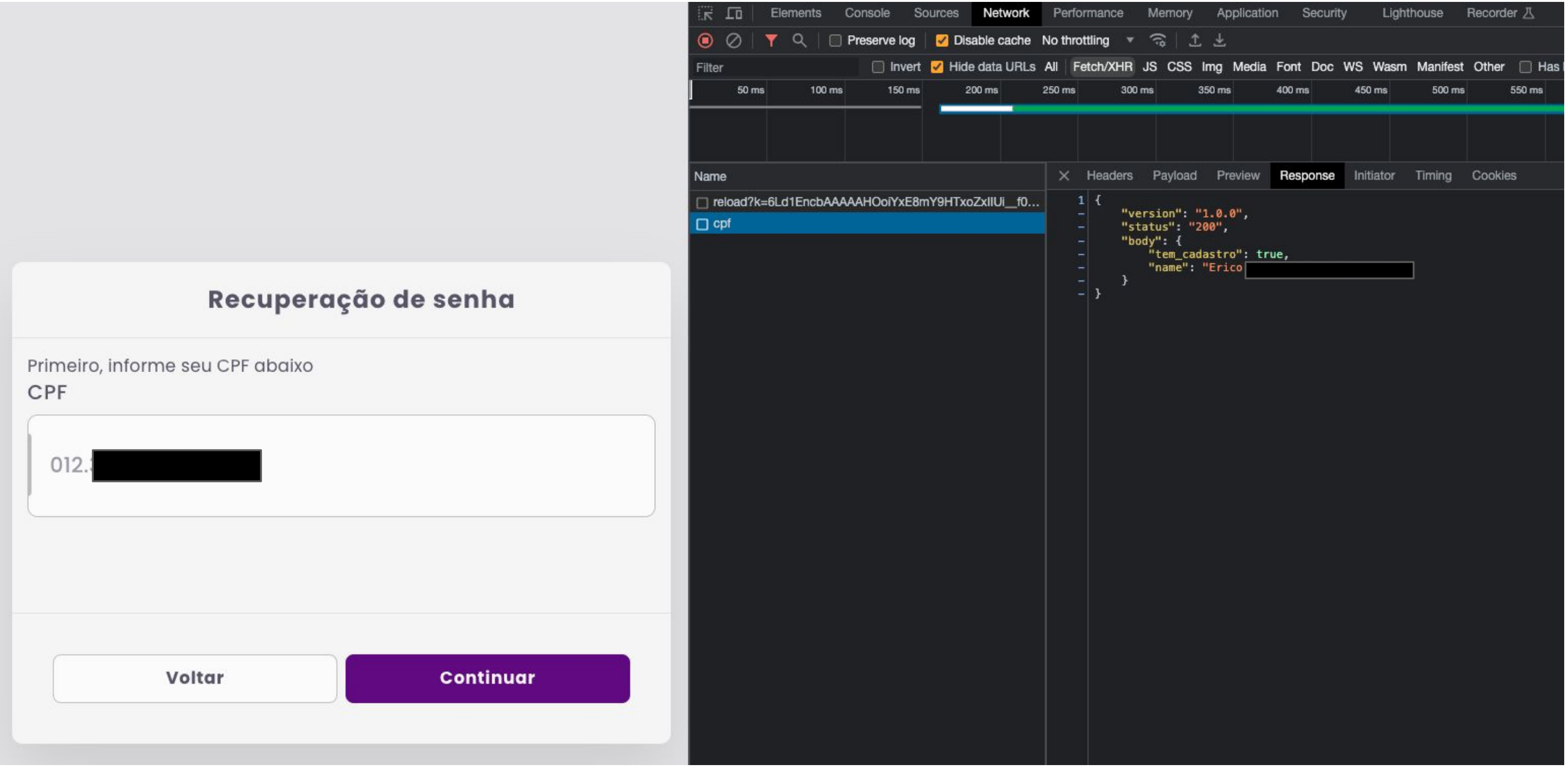
1 - Verificar as contas em aberto
2 - Segunda via de um mês específico 18:59

1 18:5

Certo! Aqui estão a(s) fatura(s) que constam em aberto em nosso sistema. 18:59

Vencimento: 06/2023
Valor: 194,25

Sometimes we have to look further



Recuperação de senha

Primeiro, informe seu CPF abaixo

CPF

012.[redacted]

□ Preserve log ☑ Disable cache

□ Invert ☑ Hide data URLs

□ reload?k=6Ld1EncbAAAAAHOoiYxE8mY9HTxoZxIIUi__f0...

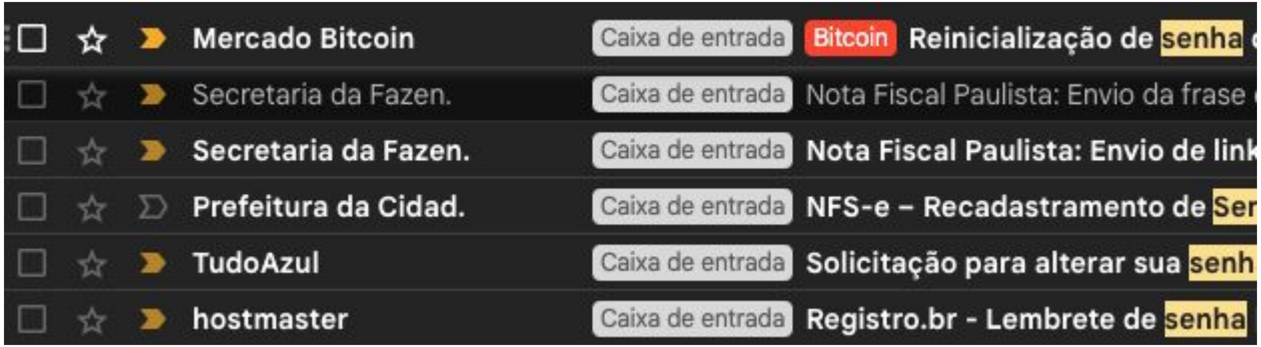
□ cpf

```
{
    "version": "1.0.0",
    "status": "200",
    "body": {
        "tem_cadastro": true,
        "name": "Erico [redacted]
    }
}
```

There are side effects ? sometimes!

Some services will send an email to the target.

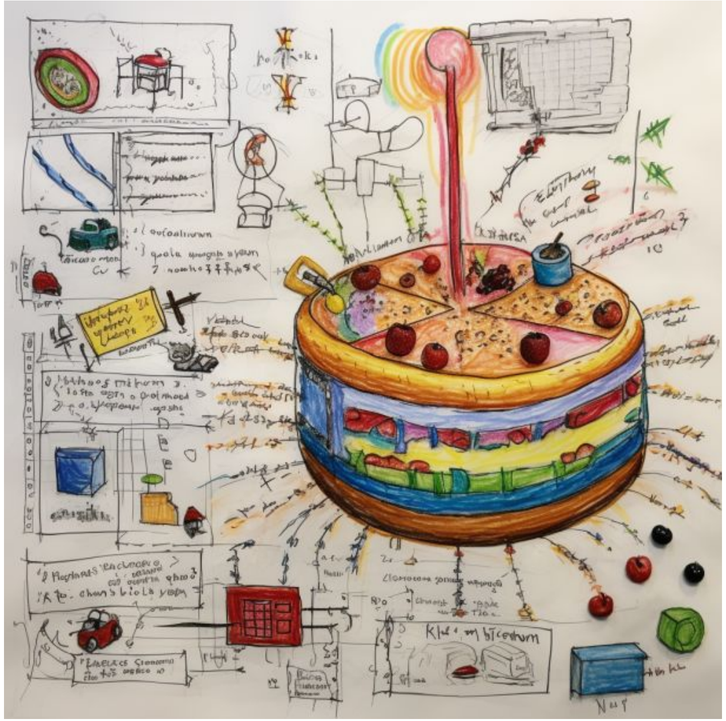
Letting him know that he is being targeted by someone.



Mercado Bitcoin	Caixa de entrada	Bitcoin Reinicialização de senha
Secretaria da Fazen.	Caixa de entrada	Nota Fiscal Paulista: Envio da frase
Secretaria da Fazen.	Caixa de entrada	Nota Fiscal Paulista: Envio de lin
Prefeitura da Cidad.	Caixa de entrada	NFS-e – Recadastramento de Se
TudoAzul	Caixa de entrada	Solicitação para alterar sua senh
hostmaster	Caixa de entrada	Registro.br - Lembrete de senha

The main problem:

If i only know the just one piece of information about the target, how do i pivot and found other pieces to get the whole cake ?

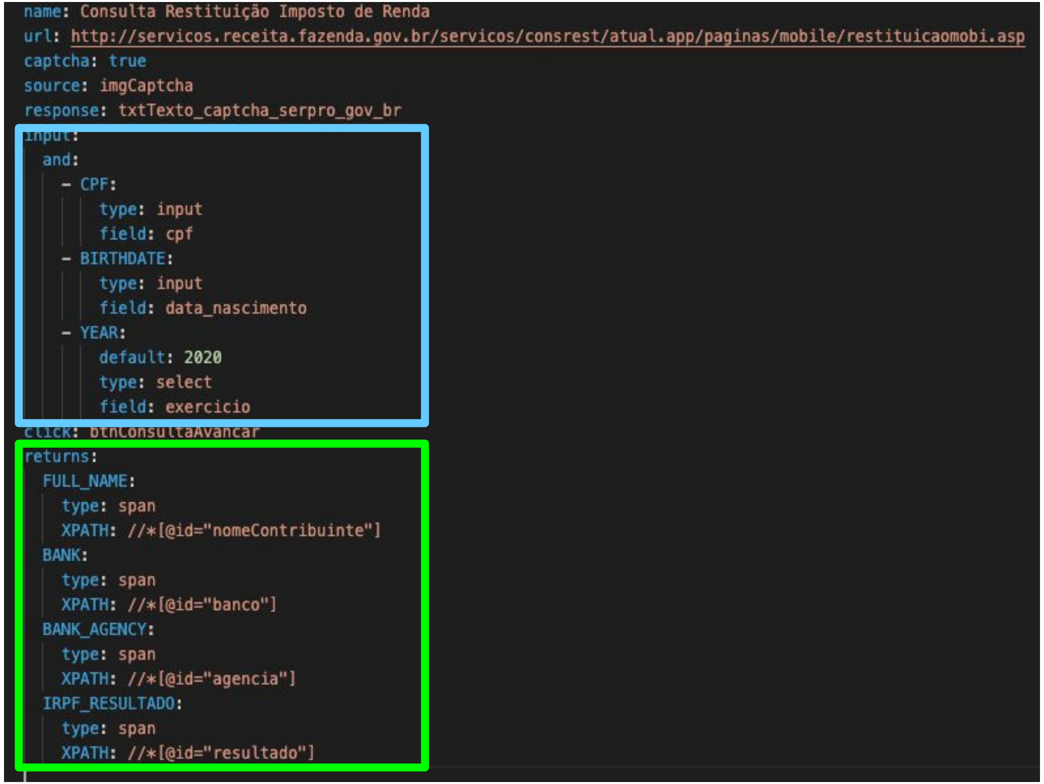


Generated by midjourney

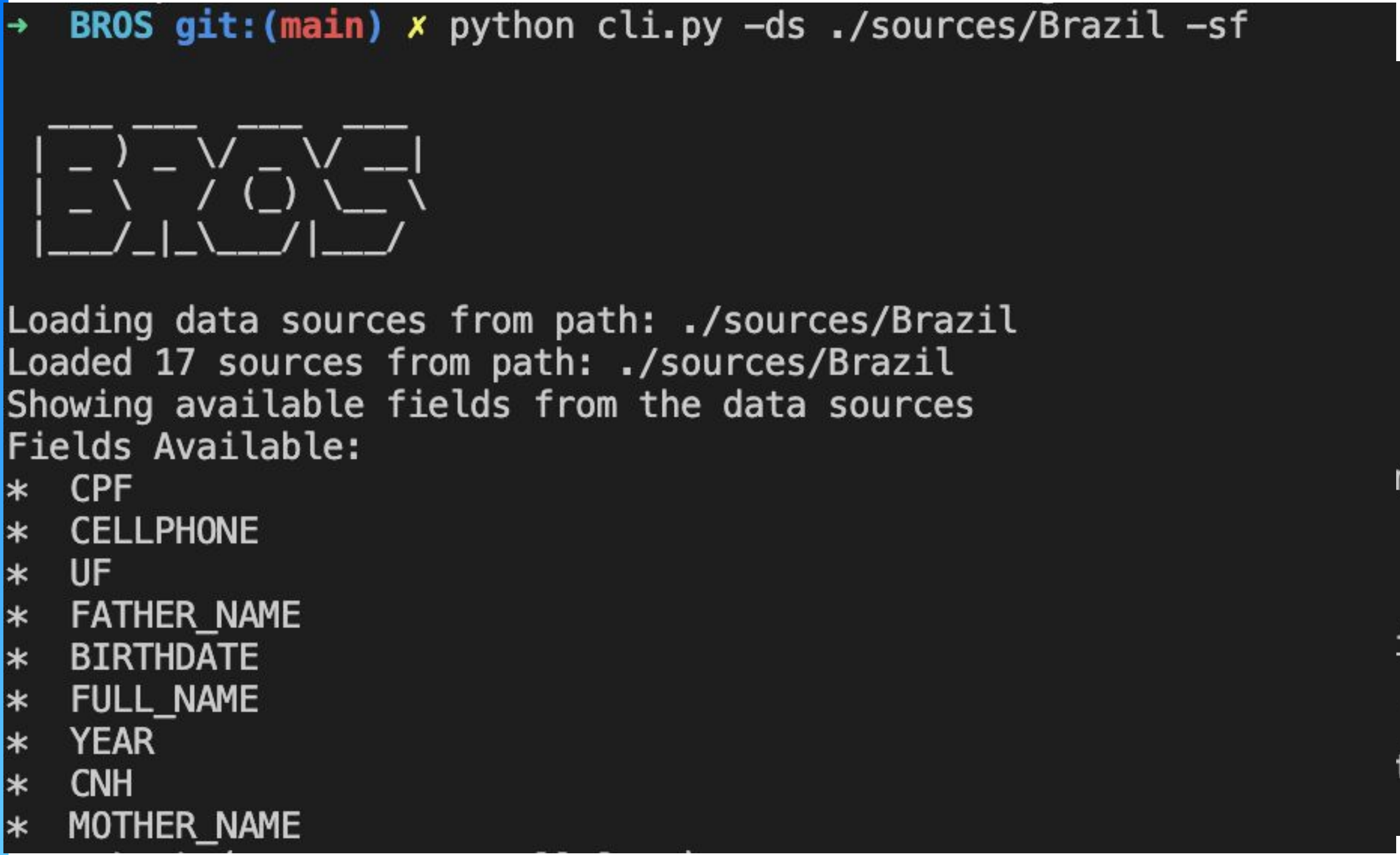
Catalog all the info:

Designed YAML files:

- Easy to write/read & parse.
- AND & OR relationship between input data



```
name: Consulta Restituição Imposto de Renda
url: http://servicos.receita.fazenda.gov.br/servicos/consrest/atual.app/paginas/mobile/restituicaomobi.asp
captcha: true
source: imgCaptcha
response: txtTexto_captcha_serpro_gov_br
input:
  and:
    - CPF:
        type: input
        field: cpf
    - BIRTHDATE:
        type: input
        field: data_nascimento
    - YEAR:
        default: 2020
        type: select
        field: exercicio
click: btnConsultaAvancar
returns:
  FULL_NAME:
    type: span
    XPATH: //*[@id="nomeContribuinte"]
  BANK:
    type: span
    XPATH: //*[@id="banco"]
  BANK_AGENCY:
    type: span
    XPATH: //*[@id="agencia"]
  IRPF_RESULTADO:
    type: span
    XPATH: //*[@id="resultado"]
```



```
→  BROS git:(main) ✗ python cli.py -ds ./sources/Brazil -sf

 ___ ___  ___  ___
| _ ) _ \/ _ \/ __|
| _ \   / (_) \__ \
|___/_|_\\___/|___/

Loading data sources from path: ./sources/Brazil
Loaded 17 sources from path: ./sources/Brazil
Showing available fields from the data sources
Fields Available:
*  CPF
*  CELLPHONE
*  UF
*  FATHER_NAME
*  BIRTHDATE
*  FULL_NAME
*  YEAR
*  CNH
*  MOTHER_NAME
```

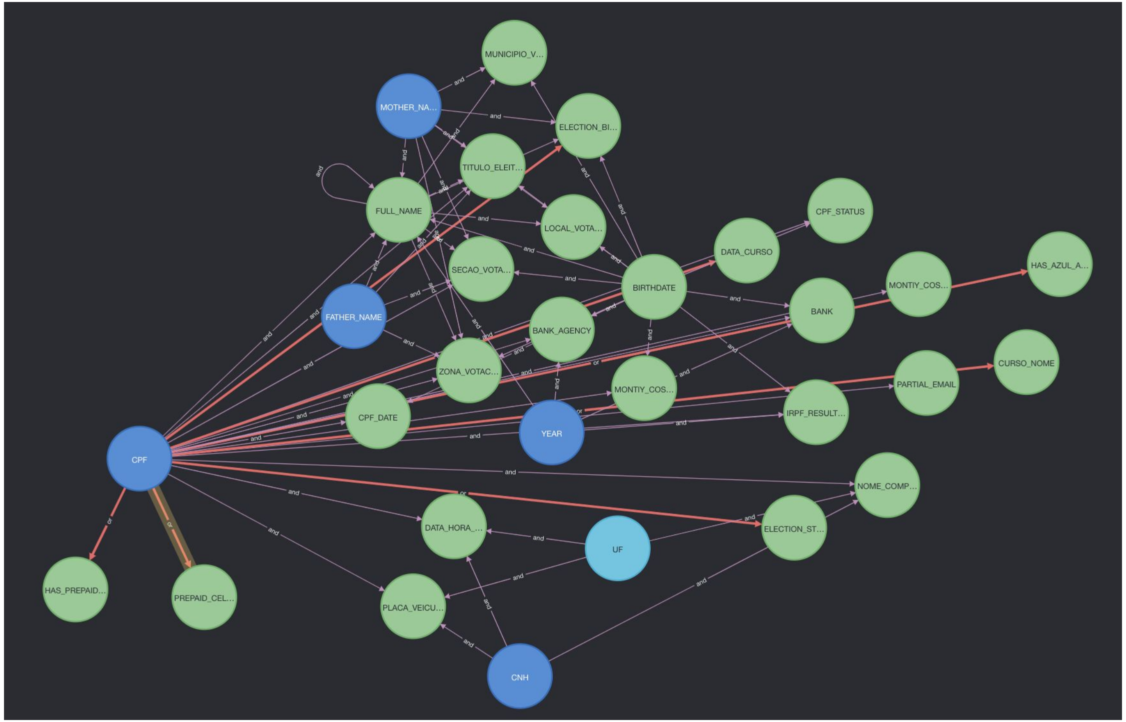
```
n get from

ied shell.

 shell, to
tion.
```

Parse all the information and graph it.

Because everybody loves graphs right?



TENCHI DOWN-TO-EARTH CLOUD SECURITY

Demo time

Future Work

- Uniform the input fields and output fields (avoid confusion), with regex!
- Add more sources ! Contribute to the project!
- Add some kind of filters for context.
    - Ex: if the CPF is from SP only look for datasources in SP.
- Add Browsing Automation

Conclusion

- **User interface** and **User Experience** must take security into account.
- There isn’t some sort of norm or regulation on this, so till there you have room to exploit.
- The same can be applicable to several countries and different contexts. Go for it!

THAT'S *LL FOLKS !
Thanks!

- Any Questions ?!
- Special Thanks for:
    - Corvolino
    - Thiago Bordini
    - Alexandre Sieira
    - Rodrigo Montoro
- The code and data-sources are available at: https://github.com/pr0teus/bros