

OSINT for Pentest

HackBahia

whoami

André Luís

Formado em Gestão de TI pela FIPP [Unoeste]

Consultor de Segurança pela PRIDE Security

disclaimer

As informações e opiniões apresentadas nesta apresentação são de responsabilidade exclusiva do autor e não representam necessariamente as opiniões ou posições da PRIDE Security.

o que é OSINT

OSINT (Open Source Intelligence) é a coleta e análise de informações de fontes abertas disponíveis ao público.

É usado em diferentes áreas para obter insights úteis a partir de dados acessíveis, como sites, redes sociais e documentos governamentais.

tópicos

- case01 - Dados bancários via Reclame Aqui
- case02 - Subdomínio não indexado pelo Google porém encontrado via Duckduckgo
- case03 - Login e senha via Reclame Aqui
- case04 - Dados de acesso via Vimeo
- case05 - Dados de acesso via YouTube [CVE]
- ...
- ...
- E quando algumas informação vêm anonimizada [Reclame Aqui começou a ocultar informações sensíveis]

case 01

The background features a dark blue field on the left, transitioning into a large, overlapping circular shape on the right. This shape is divided into two main color sections: a dark purple section on the left and a medium blue section on the right. The overall composition is minimalist and modern.

case 01

- Dados bancários via Reclame Aqui

Contexto: Para realizar um cadastro em um determinada instituição era necessário dados bancários válidos, porém para serem válidos, seria necessário realizar contato formal com a instituição pelo ambiente de cadastro [FORA DO ESCOPO].



case 01

- Dados bancários via Reclame Aqui

Contexto: Para realizar um cadastro em um determinada instituição era necessário dados bancários válidos, porém para serem válidos, seria necessário realizar contato formal com a instituição pelo ambiente de cadastro [FORA DO ESCOPO].



case 01

- Dados bancários via Reclame Aqui

Contexto: Para realizar um cadastro em um determinada instituição era necessário dados bancários válidos, porém para serem válidos, seria necessário realizar contato formal com a instituição pelo ambiente de cadastro [FORA DO ESCOPO].



case 01

- Dados bancários via Reclame Aqui

Contexto: Para realizar um cadastro em um determinada instituição era necessário dados bancários válidos, porém para serem válidos, seria necessário realizar contato formal com a instituição pelo ambiente de cadastro [FORA DO ESCOPO].

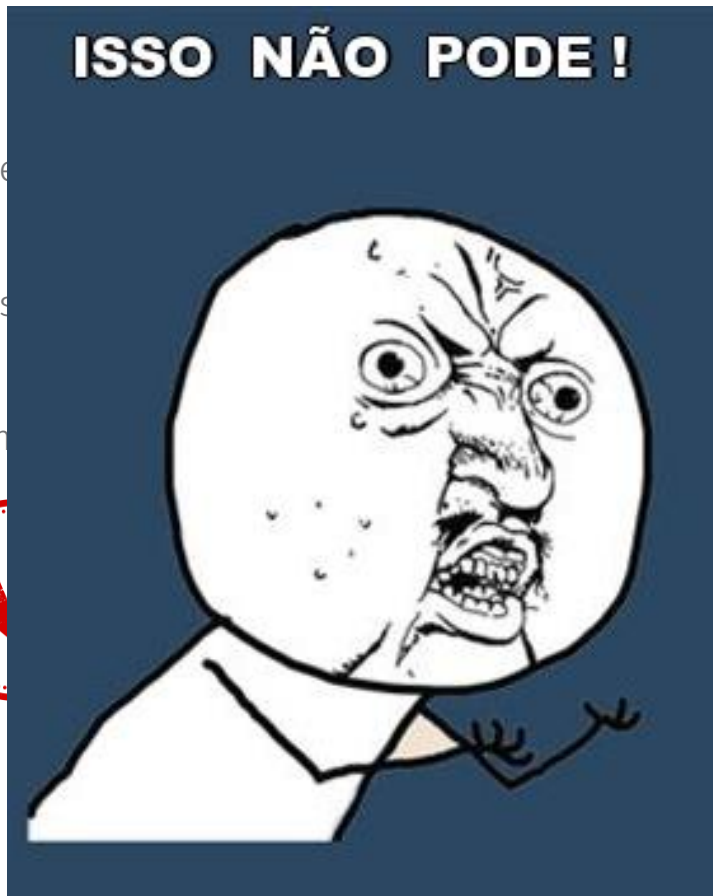


case 01

- Dados bancários via Reclame

Contexto: Para realizar um cadas
dados bancários válidos, porém
formal com a instituição pelo an

cessário
ar contato



case 01

- Dados bancários via Reclame Aqui

Dork utilizada -> site:reclameaqui.com.br “exemplo.com” “conta corrente”



case 01

- Dados bancários via Reclame Aqui

Dork utilizada -> site:reclameaqui.com.br “exemplo.com” “conta corrente”



Réplica do consumidor

Olá, boa tarde!

Segue abaixo os dados da conta PJ no banco conveniado:

Ag: 1 [REDACTED]

CC: 130 [REDACTED]

CNPJ:*****1 [REDACTED]

RAZÃO SOCIAL: ***** T [REDACTED] S*****

case 01

- Dados bancários via Reclame Aqui
Dork utilizada -> site:reclameaqui.com.br “exemplo”



Réplica do consumidor

Olá, boa tarde!

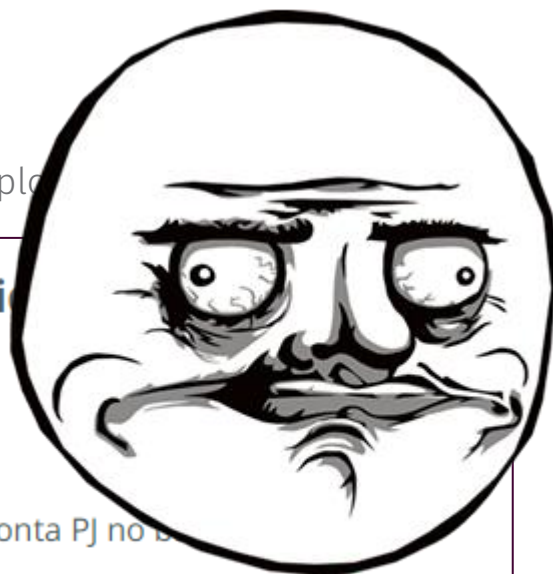
Segue abaixo os dados da conta PJ no B

Ag: 1 [REDACTED]

CC: 130 [REDACTED]

CNPJ:*****1 [REDACTED]

RAZÃO SOCIAL: ***** T [REDACTED] S*****



ME GUSTA

case 02

The background features a dark blue field on the left, transitioning into a large, overlapping circular shape on the right. This circle is divided into two main color sections: a darker, purplish-blue on the left and a lighter, sky-blue on the right. The overall composition is minimalist and modern.

case 02

- Subdomínio não indexado pelo Google porém encontrado via Duckduckgo

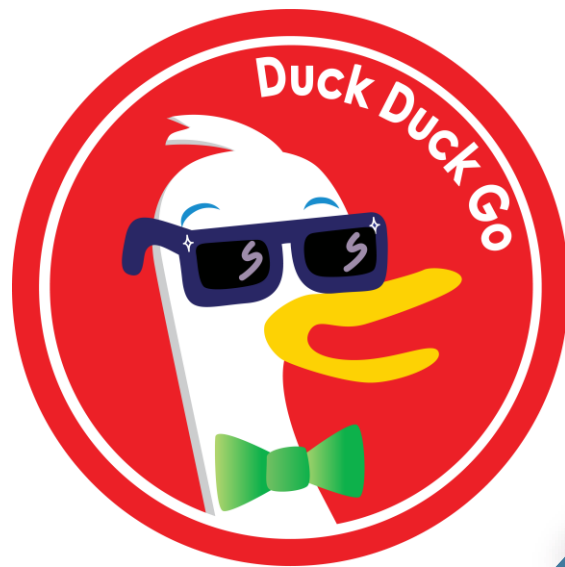
Contexto: Ao realizar pesquisas pelo domínio principal da instituição via Google nada era encontrado, o que pareceu o fim do caminho [nesse momento, parece que as coisas estão perdidas, afinal, se não tem no Google...]



case 02

- Subdomínio não indexado pelo Google porém encontrado via Duckduckgo

Contexto: Ao realizar pesquisas pelo domínio principal da instituição via Google nada era encontrado, o que pareceu o fim do caminho [nesse momento, parece que as coisas estão perdidas, afinal, se não tem no Google...]

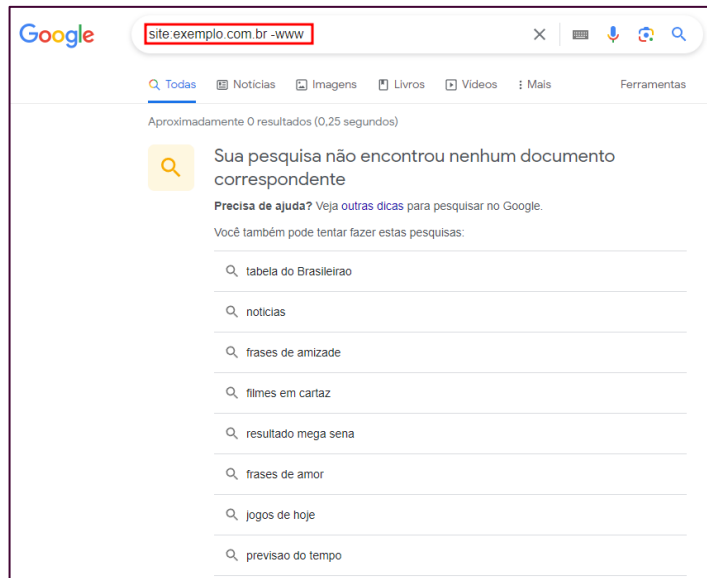


case 02

- Subdomínio não indexado pelo Google porém encontrado via Duckduckgo
Dork utilizada -> site:exemplo.com.br -www

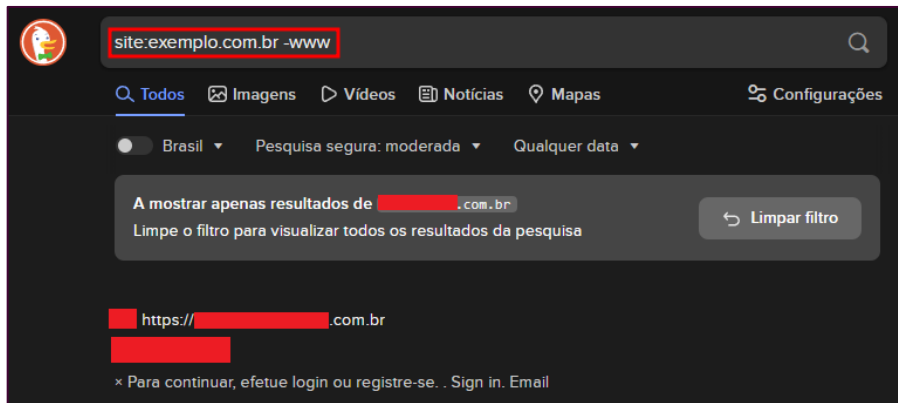
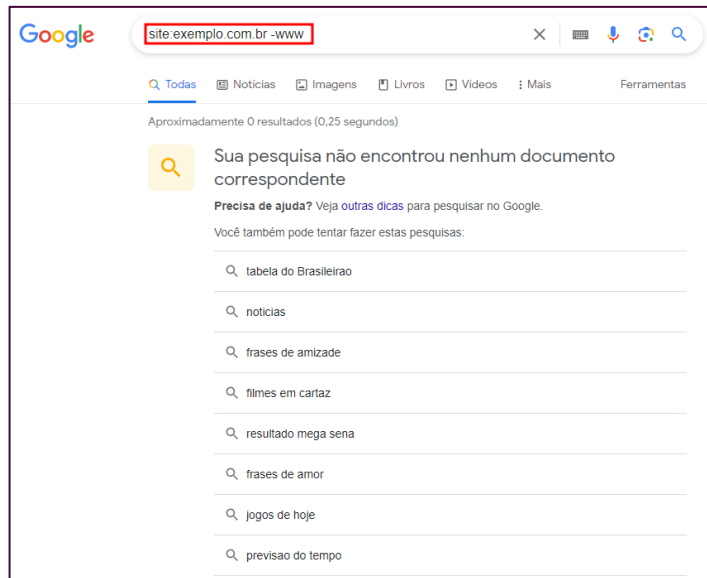
case 02

- Subdomínio não indexado pelo Google porém encontrado via Duckduckgo
Dork utilizada -> site:exemplo.com.br -www



case 02

- Subdomínio não indexado pelo Google porém encontrado via Duckduckgo
Dork utilizada -> site:exemplo.com.br -www



case 03

The background features a large, dark blue circle on the left side, which overlaps with a lighter blue circle on the right. The overlapping area creates a gradient effect, transitioning from dark blue to light blue. The text 'case 03' is positioned on the left side, within the dark blue circle.

case 03

- Login e senha via Reclame Aqui

Contexto: Acessar um painel de consulta de exames com dados reais, uma vez que não havia formas de realizar um cadastro na plataforma.

case 03

- Login e senha via Reclame Aqui

Contexto: Acessar um painel de consulta de exames com dados reais, uma vez que não havia formas de realizar um cadastro na plataforma.



quando nada é
permitido: phishing,
engenharia social...



...mas ainda assim
a própria empresa
nos ajuda

case 03

- Login e senha via Reclame Aqui

Dork utilizada -> site:reclameaqui.com.br "exemplo.com.br" "senha"

Resposta da empresa

06/05/2022 às 15:00

Prezada Carolina! Boa tarde, tudo bem?

Conforme suas manifestações em nossos canais, primeiramente peço pela sua experiência, onde levamos seu relato ao conhecimento de nossa Gestão para análise e providências necessárias, e agradeço também pela sua sinalização pois só assim conseguimos resolver esses fluxos internos, para que isso não volte acontecer com nenhum de nossos beneficiários. Segue abaixo chave e senha de acesso [REDACTED]

Chave de acesso: K [REDACTED] 2 Senha: F [REDACTED] 9

case 03

- Login e senha via Reclame Aqui

Dork utilizada -> site:reclameaqui.com.br "exemplo.com.br" "senha"

Podemos aqui auxiliar a empresa a educar seus colaboradores a não compartilhar dados sensíveis, mesmo que a intenção seja boa!

Resposta da empresa

06/05/2022 às 15:00

Prezada Carolina! Boa tarde, tudo bem?

Conforme suas manifestações em nossos canais, primeiramente peço pela sua experiência, onde levamos seu relato ao conhecimento de nossa Gestão para análise e providências necessárias, e agradeço também pela sua sinalização pois só assim conseguimos resolver esses fluxos internos, para que isso não volte acontecer com nenhum de nossos beneficiários. Segue abaixo chave e senha de acesso [REDACTED]

Chave de acesso: K [REDACTED] 2 Senha: F [REDACTED] 9

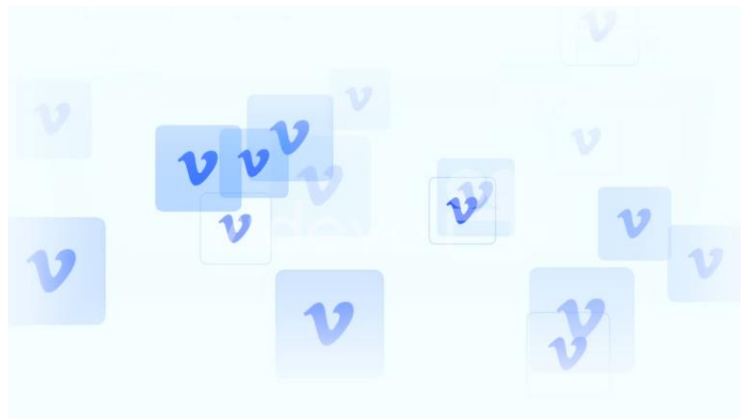
case 04

The background features a large, dark blue circle on the left side, which overlaps with a lighter blue circle on the right. The overlapping area creates a gradient effect, transitioning from dark blue to a medium blue. The rightmost part of the image is a solid light blue color.

case 04

- Dados de acesso via Vimeo

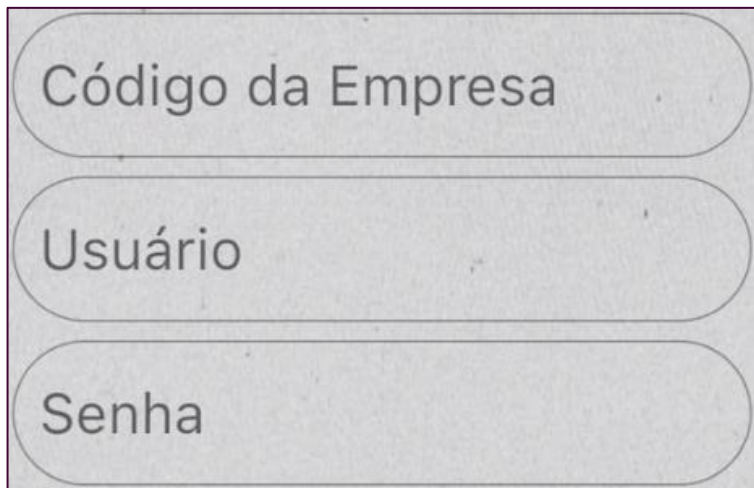
Contexto: Encontrar dados de acesso para um ambiente com acesso diferente, pois necessitava de dados como empresa, login e senha e esse padrão não era conhecido [a diversificação na busca pode trazer resultados interessantes]



case 04

- Dados de acesso via Vimeo

Dork utilizada -> site:exemplo.com.br "exemplo.com.br" "senha"

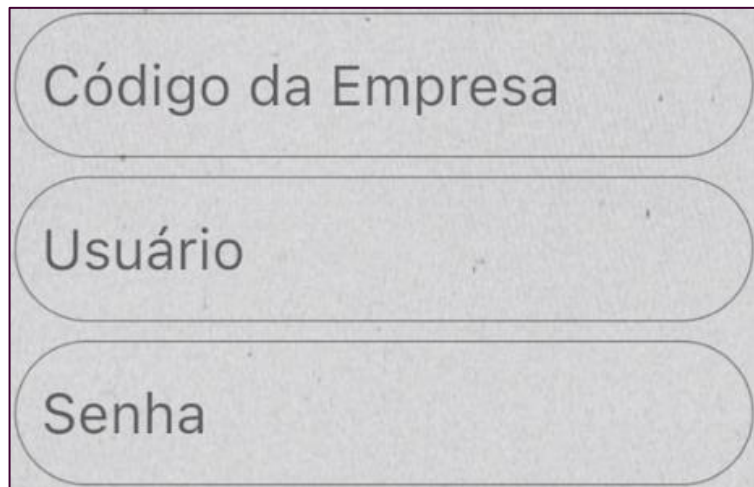


A screenshot of a login form with three input fields, each with a light gray background and rounded corners. The fields are stacked vertically and labeled in a dark gray font. The top field is labeled 'Código da Empresa', the middle field is labeled 'Usuário', and the bottom field is labeled 'Senha'.

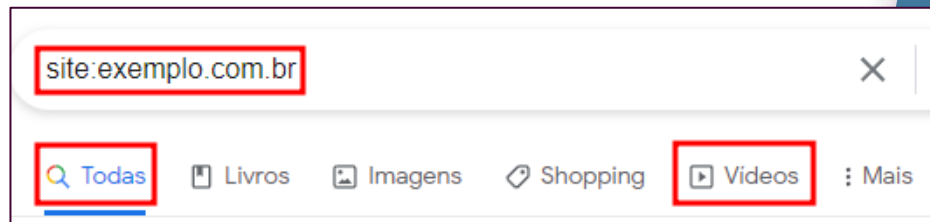
case 04

- Dados de acesso via Vimeo

Dork utilizada -> site:exemplo.com.br "exemplo.com.br" "senha"



A screenshot of a login form with three rounded rectangular input fields stacked vertically. The top field is labeled 'Código da Empresa', the middle field is labeled 'Usuário', and the bottom field is labeled 'Senha'.



case 04

- Dados de acesso via Vimeo
O que foi possível encontrar nesse vídeo?
Padrões de acesso



case 04

- Dados de acesso via Vimeo
O que foi possível encontrar nesse vídeo?
Padrões de acesso



Código da Empresa:

1 [REDACTED] 1

Insira o **número do seu ID do RH** nos campos **USUÁRIO** e **SENHA**.

Se você for um **terceiro**, informe os **6 primeiros dígitos do seu CPF** nos dois campos.

case 05

The background features a large, dark blue circle on the left side, which overlaps with a lighter blue circle on the right. The overlapping area creates a gradient effect, transitioning from dark blue to light blue. The text 'case 05' is positioned on the left side, within the dark blue circle.

case 05

- Dados de acesso via YouTube [CVE]

Contexto: Após criar um cadastro na plataforma foi encontrada uma falha de *Account Takeover*. Na busca por um impacto maior, realizamos a busca por algum usuário com maior privilégio dentro da plataforma [a busca por vídeos novamente nos trouxe bons resultados]



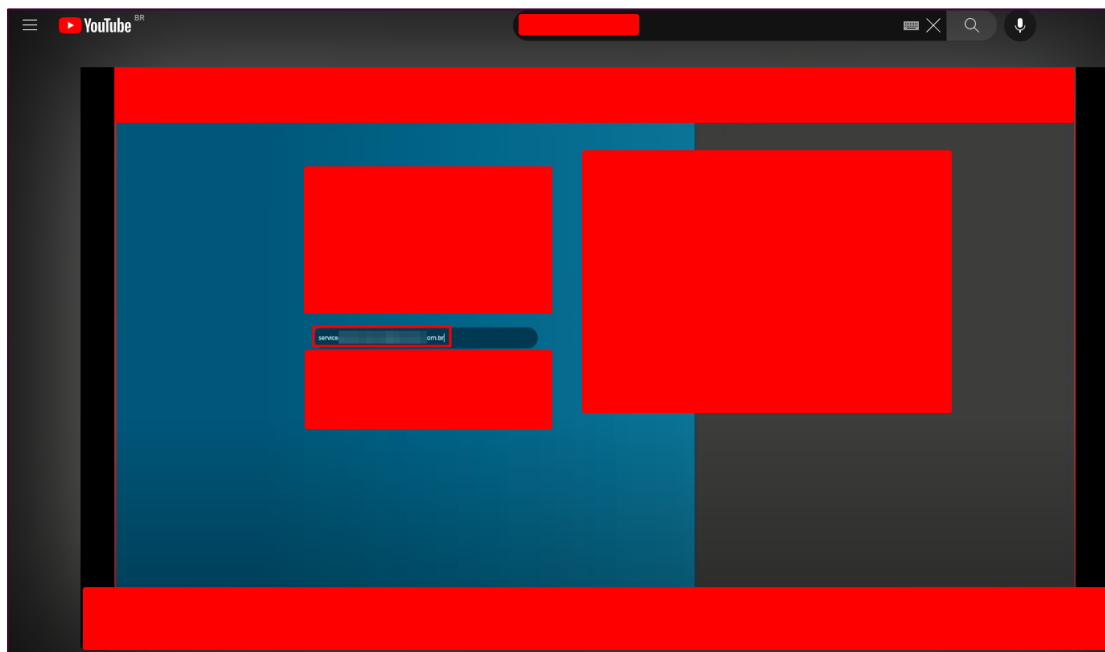
case 05

- Dados de acesso via YouTube [CVE]
Dork utilizada -> site:exemplo.com.br

case 05

- Dados de acesso via YouTube [CVE]

Dork utilizada -> site:exemplo.com.br



case 05

- Dados de acesso via YouTube [CVE]

A partir da exploração do *Account Takeover*, existia uma URL vulnerável a IDOR [*Insecure Direct Object Reference*] que ainda não havia sido reportado ao fabricante, o que rendeu uma CVE.



case 05

- Dados de acesso via YouTube [CVE]

A partir da exploração do *Account Takeover*, existia uma URL vulnerável a IDOR [*Insecure Direct Object Reference*] que ainda não havia sido reportado ao fabricante, o que rendeu uma CVE.



case 05

- Dados de acesso via YouTube [CVE]

A partir da exploração do *Account Takeover*, existia uma URL vulnerável a IDOR [*Insecure Direct Object Reference*] que ainda não havia sido reportado ao fabricante, o que rendeu uma CVE.



mudando o mindset

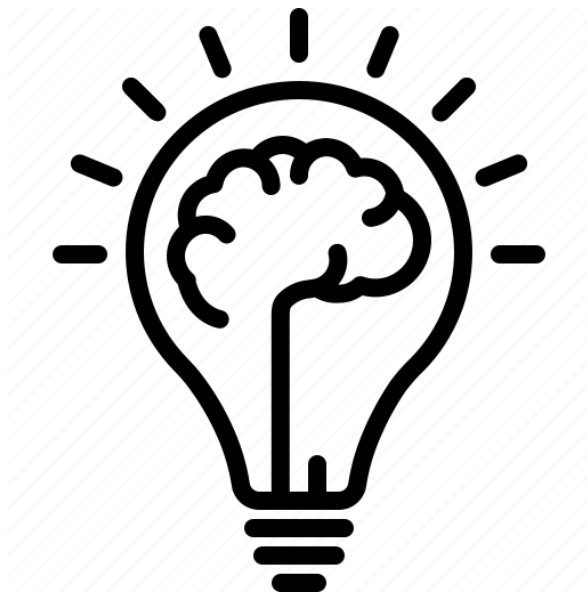
insights

insights

- Alguns dados sensíveis o Reclame Aqui tem anonimizado como CPF, nomes de pessoas, endereços ... porém outros dados ainda continuam disponíveis na plataforma como dados bancários, números de telefones, entre outros.

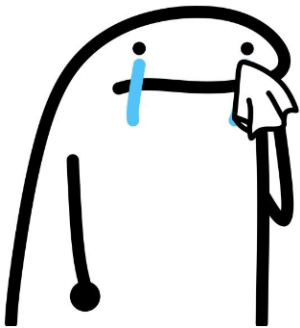
insights

- Alguns dados sensíveis o Reclame Aqui tem anonimizado como CPF, nomes de pessoas, endereços ... porém outros dados ainda continuam disponíveis na plataforma como dados bancários, números de telefones, entre outros.



insights

- Sendo assim, podemos selecionar esses dados disponíveis e buscar outras formas de obter os dados anonimizados pela plataforma. E de que formas podemos realizar essa busca?



insights

- Sendo assim, podemos selecionar esses dados disponíveis e buscar outras formas de obter os dados anonimizados pela plataforma. E de que formas podemos realizar essa busca?

NOME: *****

CPF: *****

CONTATO: 11 9. [REDACTED] 2

EMAIL: *****

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



insights

- Alguns serviços que utilizamos no nosso dia a dia podem ser extremamente importantes para nos auxiliar nessa busca que tal um PIX?

insights

- Alguns serviços que utilizamos no nosso dia a dia podem ser extremamente importantes para nos auxiliar nessa busca que tal um PIX?



insights

- Alguns serviços que utilizamos no nosso dia a dia podem ser extremamente importantes para nos auxiliar nessa busca que tal um PIX?



Você vai pagar para

LAR [REDACTED] DIAS

CPF: ***,325.858-**- NU PAGAMENTOS - IP

Chave: +55 (**) *****3372

☐ Salvar contato

Valor a pagar

R\$ 0,00

newsletters, cursos e livros

- Existem diversas newsletters, githubs e afins que podem auxiliar na busca por novos *insights*:



The OSINT Newsletter



mensagemem final

- *Remember #OSINT != tools. Tools help you plan and collect data but the end result of that tool is not OSINT. You have to analyze, verify, receive feedback, refine, and produce a final, actionable product of value before it can be called intelligence.*

Jake Creps

obrigado!