Whoami – Quem sou eu ?

- Estudante da Fatec Bauru – Redes
- DevOps – EZ devs
- Estudante de segurança da informação

Historia – Onde se iniciou

- Tudo começou no Foreign Broadcast Information Service (FBIS)
- Jornais
- Revistas
- Televisão
- Pioneiro no uso de Open Source Intelligence (OSINT)
- Deram início ao projeto na década de 1930 na Universidade de Princeton

Historia – Segunda guerra e o FBI

- Sua função era analisar os noticiários por rádio e monitorar publicações oficiais da União das repúblicas Socialistas Soviéticas
- Já em 8 de novembro de 2005 foi anunciado por John Negroponte o Open Source Center (OSC) que é um braço da CIA (depois do 11 de setembro de 2001)
- Coletar , reunir e trabalhar as informações
- Foi ai que deu inicio ao termo OSINT

Leis – O que eu posso e não posso

- Invasão de dispositivos
- Violar mecanismos de segurança para obter vantagem indevida
- Obter informações
- Adulterar
- Destruir
- Graças às técnicas de buscas usando OSINT podemos começar a procura de informações válidas e falhas em possíveis clientes.

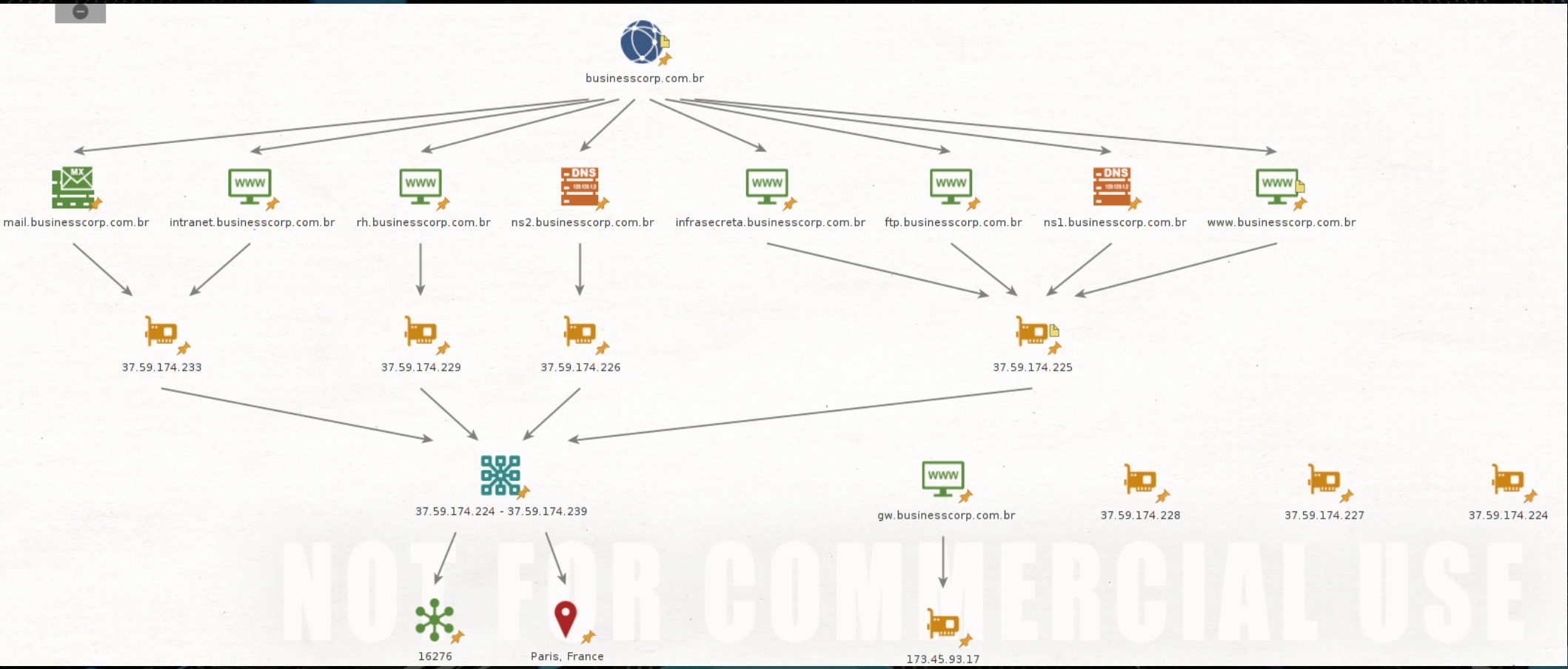
Motivação

- Problemas com leis
- Problemas com permissão das empresas
- Problemas com logs
- Buscar por determinada vulnerabilidade
- Buscar por arquivos importantes
- Buscar por informações sensíveis
- Monitorar vazamentos

OSINT – Buscando informações públicas

- Informações sobre infraestruturas

Um pouco da meta ....



Whois - Quem é?

Buscando por informações sobre domínios

- Nome do domínio , quem registrou o domínio
- Quando foi criado e até quando é valido
- Servidores DNS e País
- email de contato ,Nome do responsável ,CPF/CNPJ
- Protocolo TCP que funciona por padrão na porta 43

Whois - Quem é?

Example

Summary | Attachments (0) | Notes | Properties (2)

Notes

```
domain:      businesscorp.com.br
owner:       Desec Security
ownerid:     23.019.510/0001-06
responsible: Ricardo Longatto
country:     BR
owner-c:     JORL047
admin-c:     JORL047
tech-c:      JORL047
billing-c:   JORL047
nserver:     ns1.businesscorp.com.br 37.59.174.225
nsstat:      20190520 AA
nslastaa:    20190520
nserver:     ns2.businesscorp.com.br 37.59.174.226
nsstat:      20190520 AA
nslastaa:    20190520
saci:        yes
created:     20170904 #17416766
changed:     20180912
expires:     20190904
status:      published

nic-hdl-br:  JORL047
person:      José Ricardo Longatto
e-mail:      ricardolongatto@gmail.com
country:     BR
```

Perform an **Online Whois Lookup** of a domain or IP address to fi

businesscorp.com.br

GET WHOIS DATA

Whois - Quem é?

Buscando por informações de IPS

- Range de rede
- CIDR
- Organização responsável
- Endereço
- Cidade
- País

Whois - Quem é?

Buscando por informações de IPS

```
inetnum:        37.59.174.224 - 37.59.174.239
netname:        OVH_1341873 62
country:        PT
descr:          Failover Ips
```

Whois - Quem é?

Buscando por informações de IPS

```
role:           OVH PT Technical Contact
address:        OVH Hosting LDA
address:        Avenida Miguel Bombarda, 133 - 6ºA
address:        1050-164 Lisboa
address:        Portugal
admin-c:        OK217-RIPE
tech-c:         GM84-RIPE
nic-hdl:        OTC6-RIPE
abuse-mailbox:  abuse@ovh.net
mnt-by:         OVH-MNT
created:        2008-12-23T17:48:44Z
last-modified:  2008-12-23T17:48:44Z
source:         RIPE # Filtered
```

Whois - Quem é?

Buscando por informações de IPS

```
route:          37.59.0.0/16
descr:          OVH ISP
descr:          Paris, France
origin:         AS16276
mnt-by:         OVH-MNT
created:        2012-01-25T17:04:21Z
last-modified:  2012-01-25T17:04:21Z
source:         RIPE # Filtered
```

Whois - Quem é?

Realizando consulta com Python3 + API

```
python3 whois-url.py
```

```
200

% Copyright (c) Nic.br
%  The use of the data below is only permitted as de
%  full by the terms of use at https://registro.br/1
%  being prohibited its distribution, commercializat
%  reproduction, in particular, to use it for adverti
%  any similar purpose.
%  2019-05-25T12:36:24-03:00

domain:      businesscorp.com.br
owner:       Desec Security
ownerid:     23.019.510/0001-06
responsible: Ricardo Longatto
country:     BR
owner-c:     JORL047
admin-c:     JORL047
tech-c:      JORL047
billing-c:   JORL047
nserver:     ns1.businesscorp.com.br 37.59.174.225
nsstat:      20190524 AA
nslastaa:    20190524
nserver:     ns2.businesscorp.com.br 37.59.174.226
```

Whois - Quem é?

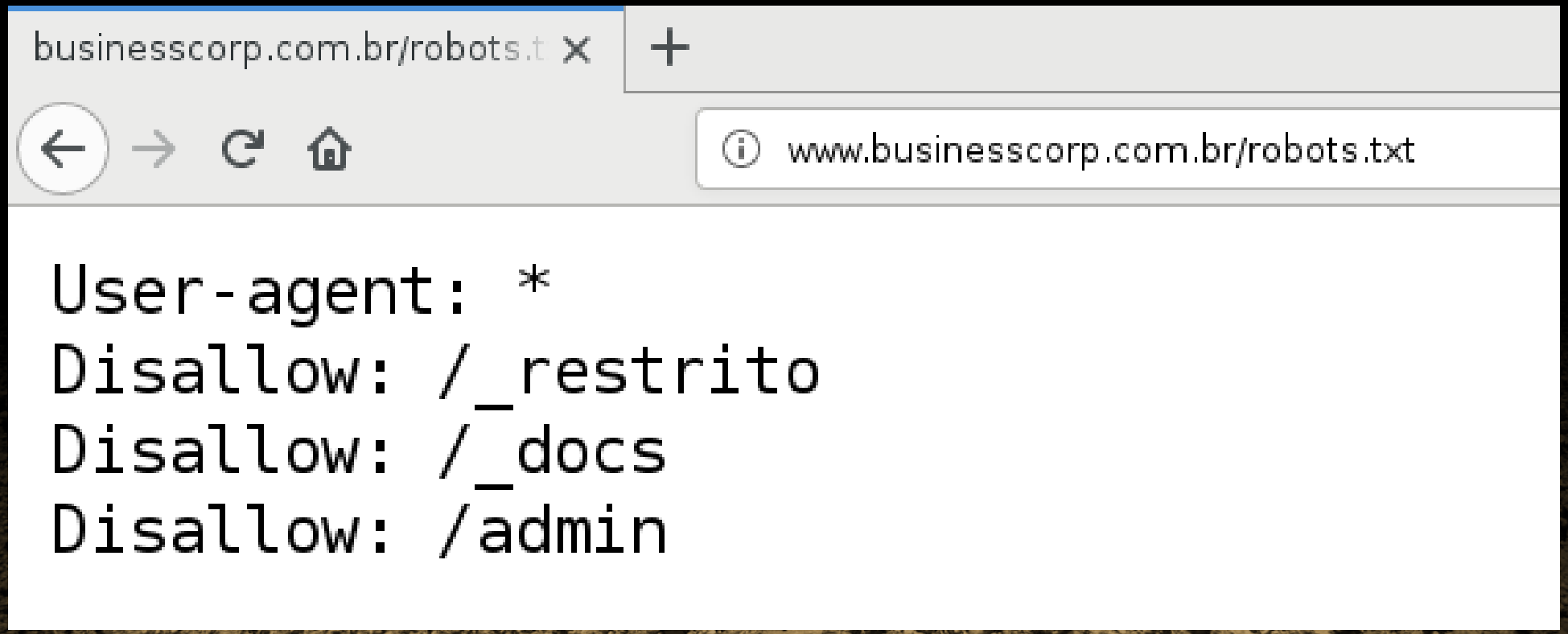
Realizando consulta com Python3 + API

```
 % python3 whois-ip.py
200
inetnum:     186.192.80.0/20
aut-num:     AS28604
abuse-c:     CSGLO
owner:       Globo Comunicação e Participaçoes SA
ownerid:     27.865.757/0024-90
responsible: Regina Sampaio
country:     BR
       c:    RES59
       :     CTG6
       v:    186.192.80.0/20
       r:    ns01.oghost.com.br
       :     20190524 AA
      aa:    20190524
       r:    ns04.oghost.com.br
       :     20190524 AA
      aa:    20190524
       r:    ns03.oghost.com.br

nic-hdl-br:  RES59
person:      Regina Sampaio
e-mail:      fapesp@corp.globo.com
country:     BR
created:     19991110
changed:     20180917

nic-hdl-br:  CSGLO
person:      CSIRT Globo.com
e-mail:      csirt@csirt.globo
country:     BR
created:     20150903
changed:     20160104

nic-hdl-br:  CTG6
person:      Contato Técnico - Globo.com
e-mail:      fapesp@corp.globo.com
```

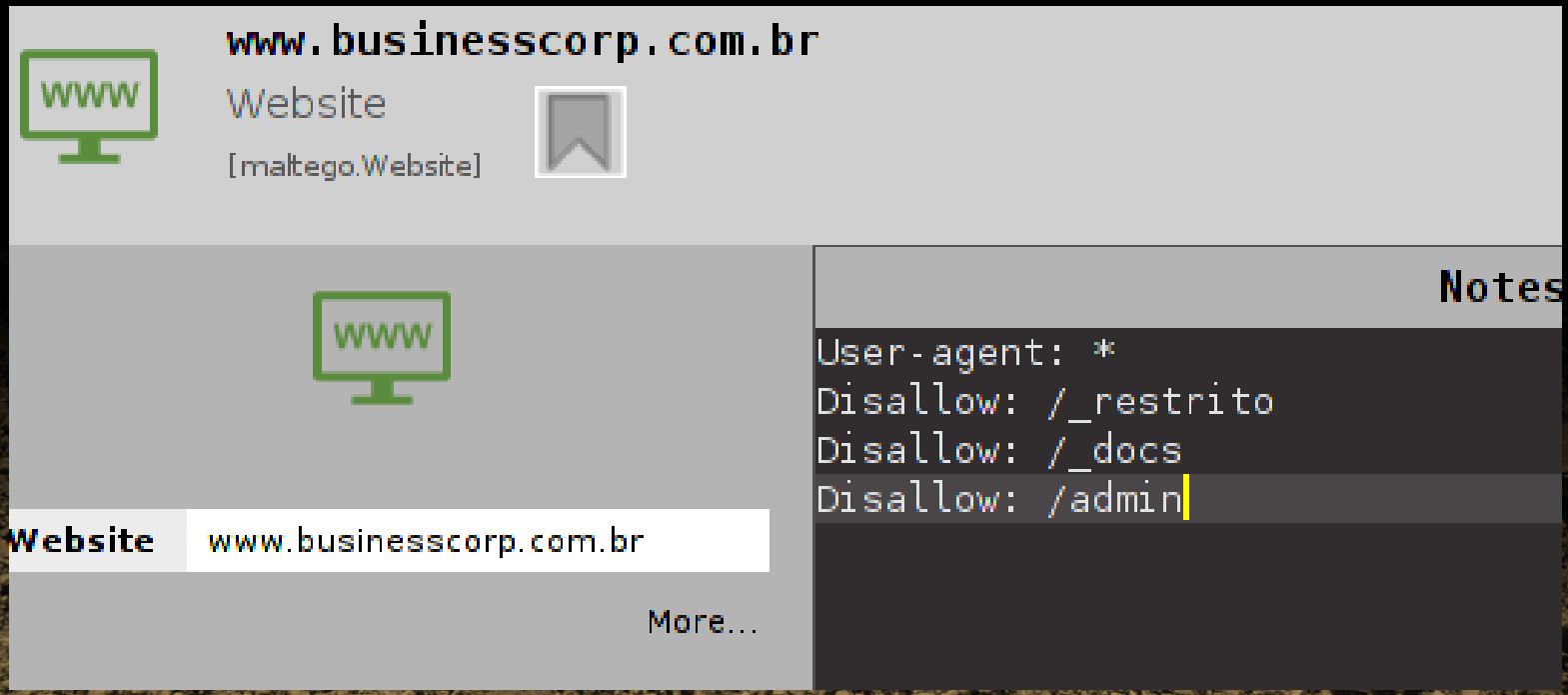
Robots.txt – O que não deve ser achado

- Não querem que sejam indexados pelos Web Crawlers
- Arquivos
- Diretórios
- Clean URLS
- No Clean URLS
- Sempre tenha um arquivo robots.txt na raiz do seu servidor web

Robots.txt – O que não deve ser achado



Robots.txt – O que não deve ser achado



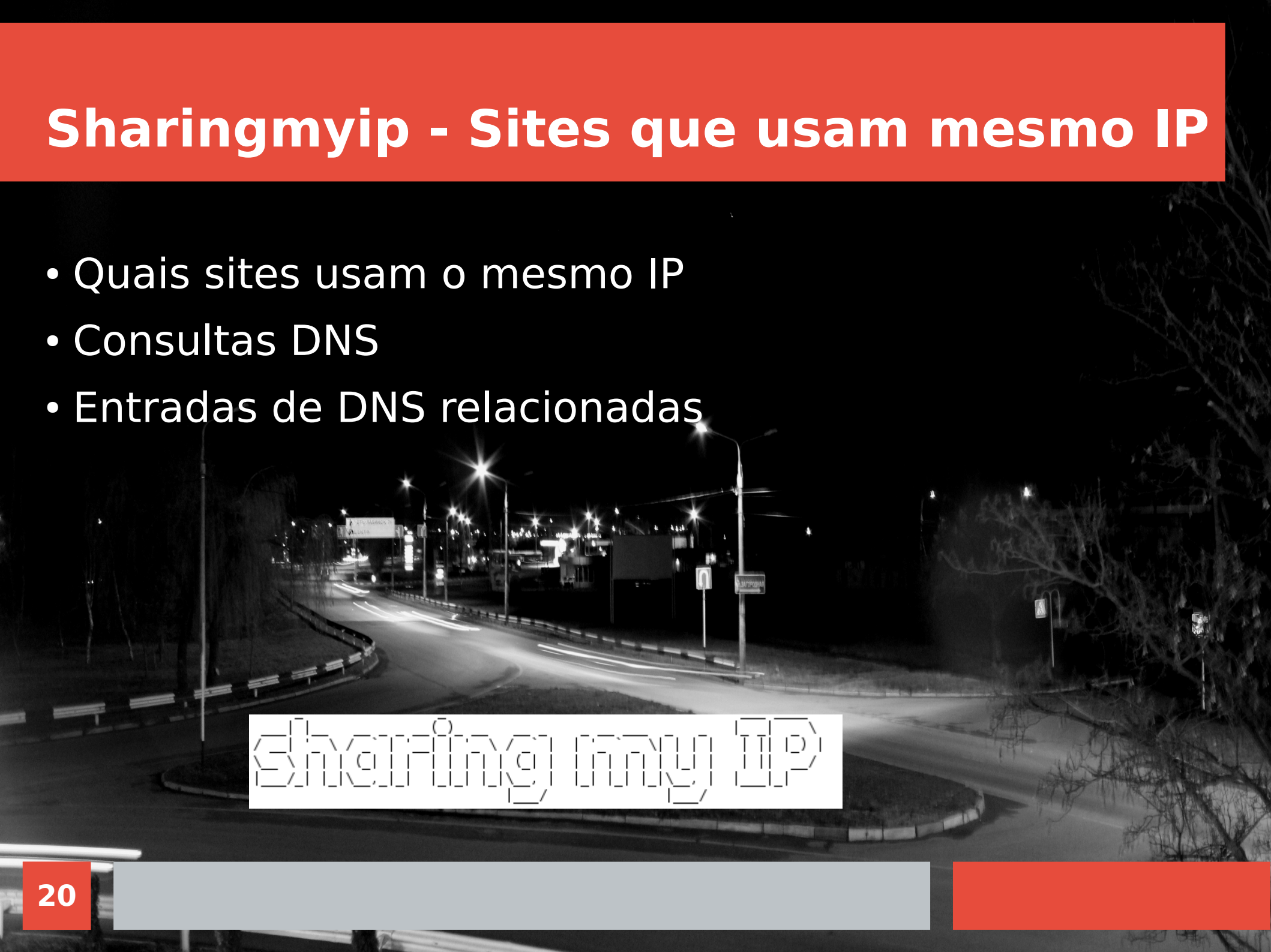
Robots.txt – O que não deve ser achado

Realizando consulta com Python3 + API

```
 % python3 check-robots.py www.businesscorp.com.br
User-agent: *
Disallow: /_restrito
Disallow: /_docs
Disallow: /admin
```

Sharingmyip - Sites que usam mesmo IP

- Quais sites usam o mesmo IP
- Consultas DNS
- Entradas de DNS relacionadas



Sharingmyip - Sites que usam mesmo IP

http:// www.businesscorp.com.br Check this s

Tweet

== Site(s) at this IP address (37.59.174.225) ==

www.businesscorp.com.br
ns1.businesscorp.com.br
ftp.businesscorp.com.br
businesscorp.com.br

Sharingmyip - Sites que usam mesmo IP

```
== DNS for www.businesscorp.com.br ==
businesscorp.com.br name server ns2.businesscorp.com.br.
businesscorp.com.br name server ns1.businesscorp.com.br.
businesscorp.com.br mail is handled by 10 mail.businesscorp.com.br.
businesscorp.com.br has address 37.59.174.225
www.businesscorp.com.br has address 37.59.174.225
www.businesscorp.com.br has no AAAA record
```

Sharingmyip - Sites que usam mesmo IP

```
== Related DNS entries for www.businesscorp.com.br ==
www.businesscorp.com.br - 37.59.174.225
mail.businesscorp.com.br - 37.59.174.233
ns1.businesscorp.com.br - 37.59.174.225
ns2.businesscorp.com.br - 37.59.174.226
gw.businesscorp.com.br - 173.45.93.17
ftp.businesscorp.com.br - 37.59.174.225
rh.businesscorp.com.br - 37.59.174.229
intranet.businesscorp.com.br - 37.59.174.233
```

Sharingmyip - Sites que usam mesmo IP

Coleta de dados com Python3

```
 % python3 sharingmyip.py
Site (s) neste endereço 8.8.8.8
www.businesscorp.com.br
ns1.businesscorp.com.br
ftp.businesscorp.com.br
businesscorp.com.br

DNS para  businesscorp.com.br
businesscorp.com.br name server ns2.businesscorp.com.br.
businesscorp.com.br name server ns1.businesscorp.com.br.
businesscorp.com.br mail is handled by 10 mail.businesscorp.com.br.
businesscorp.com.br has address 37.59.174.225
businesscorp.com.br has no AAAA record

Entradas de DNS relacionadas para businesscorp.com.br
www.businesscorp.com.br - 37.59.174.225
mail.businesscorp.com.br - 37.59.174.233
ns1.businesscorp.com.br - 37.59.174.225
ns2.businesscorp.com.br - 37.59.174.226
ftp.businesscorp.com.br - 37.59.174.225
rh.businesscorp.com.br - 37.59.174.229
intranet.businesscorp.com.br - 37.59.174.233
```

DNSDumpster – Informações sobre DNS

- DNS Servers
- Servidores de email
- Registros de DNS
- Possível localização
- Proprietários de blocos de IP

DNSDumpster – Informações sobre DNS

DNSDumpster – Informações sobre DNS

AS16276 OVH SAS

DNS Servers

ns2.businesscorp.com.br.

ns1.businesscorp.com.br.

DNSDumpster – Informações sobre DNS

37.59.174.226 ip226.ip-37-59-174.eu	AS16276 OVH SAS France
37.59.174.225 ip225.ip-37-59-174.eu	AS16276 OVH SAS France

HACKER TARGET

DNSDumpster – Informações sobre DNS

businesscorp.com.br

FTP: 220 ProFTPD 1.3.4a Server (FTP)
[::ffff:37.59.174.225]//

SSH: SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u2

HACKER TARGET

Netcraft -

A Netcraft é uma empresa com sede em Bath na Ingraterra , ela é uma empresa que presta serviços

- Anti fraud
- Anti Phishing
- Testes em aplicativos
- Revisão de código
- Pentests

Netcraft -

- Encontrar subdomínios
- Sistema operacional
- Informações sobre o bloco de rede
- Titulo do site , Rank do site , Descrição , Palavras chaves , Linguagem primaria ,analise de Risco e etc..
- Site , Domínio, IP , IPv6, Domínio Registrador , Organização responsável , Hospedado em qual país , Empresa que hospeda , DNS reverso ,Email do DNS admin e NameServer

Netcraft -

What's that site running?

Find out what technologies are powering any website:

www.businesscorp.com.br

Site title	Business Corp	**Date first seen**	November 2017
Site rank	829612	**Primary language**	Portuguese
Description	""		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	1/10		

Netcraft -

Network

Site	http://www.businesscorp.com.br
Domain	businesscorp.com.br
IP address	37.59.174.225 (VirusTotal)
IPv6 address	*Not Present*
Domain registrar	nic.br
Organisation	Desec Security, Brazil
Top Level Domain	Brazil (.com.br)
Hosting country	PT

Netcraft -

Netblock Owner	Failover Ips
Nameserver	ns1.businesscorp.com.br
DNS admin	hostmaster@businesscorp.com.br
Reverse DNS	ip225.ip-37-59-174.eu
Nameserver organisation	whois.nic.br
Hosting company	OVH
DNS Security Extensions	*unknown*

Netcraft -

Hosting History

Netblock owner	IP address	OS	Web server
Failover Ips	37.59.174.225	Linux	Apache/2.2.22 Debian

Site Technology

Application Servers

An application server is a server that provides software applicati
management of large distributed systems.

Technology	Description
Apache	Web server software
Debian	*No description*

Netcraft -

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier develop
developing.

Technology	Description
jQuery	A JavaScript libr
Modernizr	*No description*

Client-Side

Includes all the main technolo

Technology
JavaScript

Server-Side

Includes all the main technologi

Technology
PHP

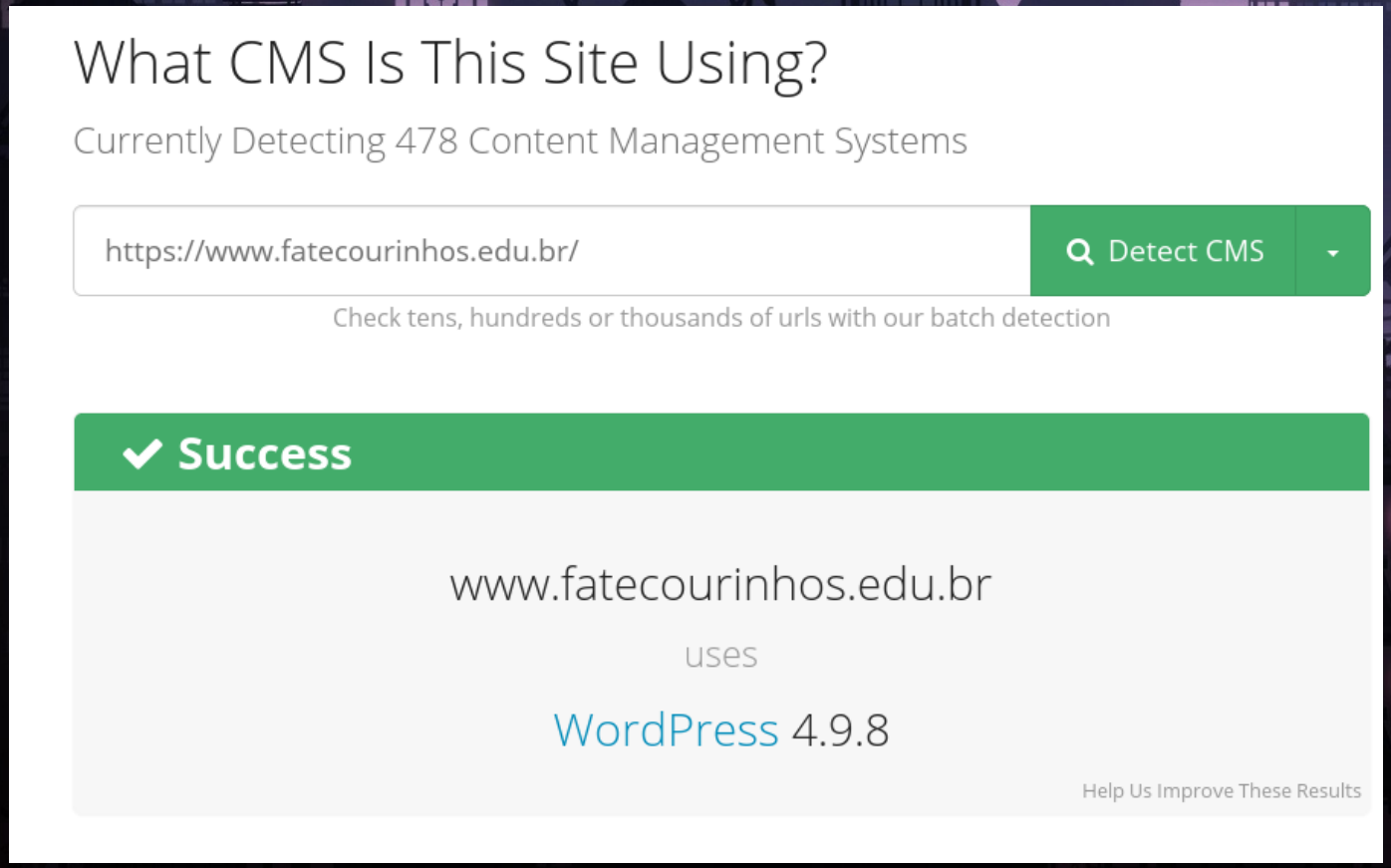
WhatCMS – Reconhecendo CMS

- Conseguem reconhecer mas de 422 CMS’s
- Lançado em Dezembro de 2011
- Wordpress, Joomla, Moodle, Drupal, PhpBB
- Meta, Headers, Javascript
- https://whatcms.org/Tech_Reports

WhatCMS – Reconhecendo CMS + API

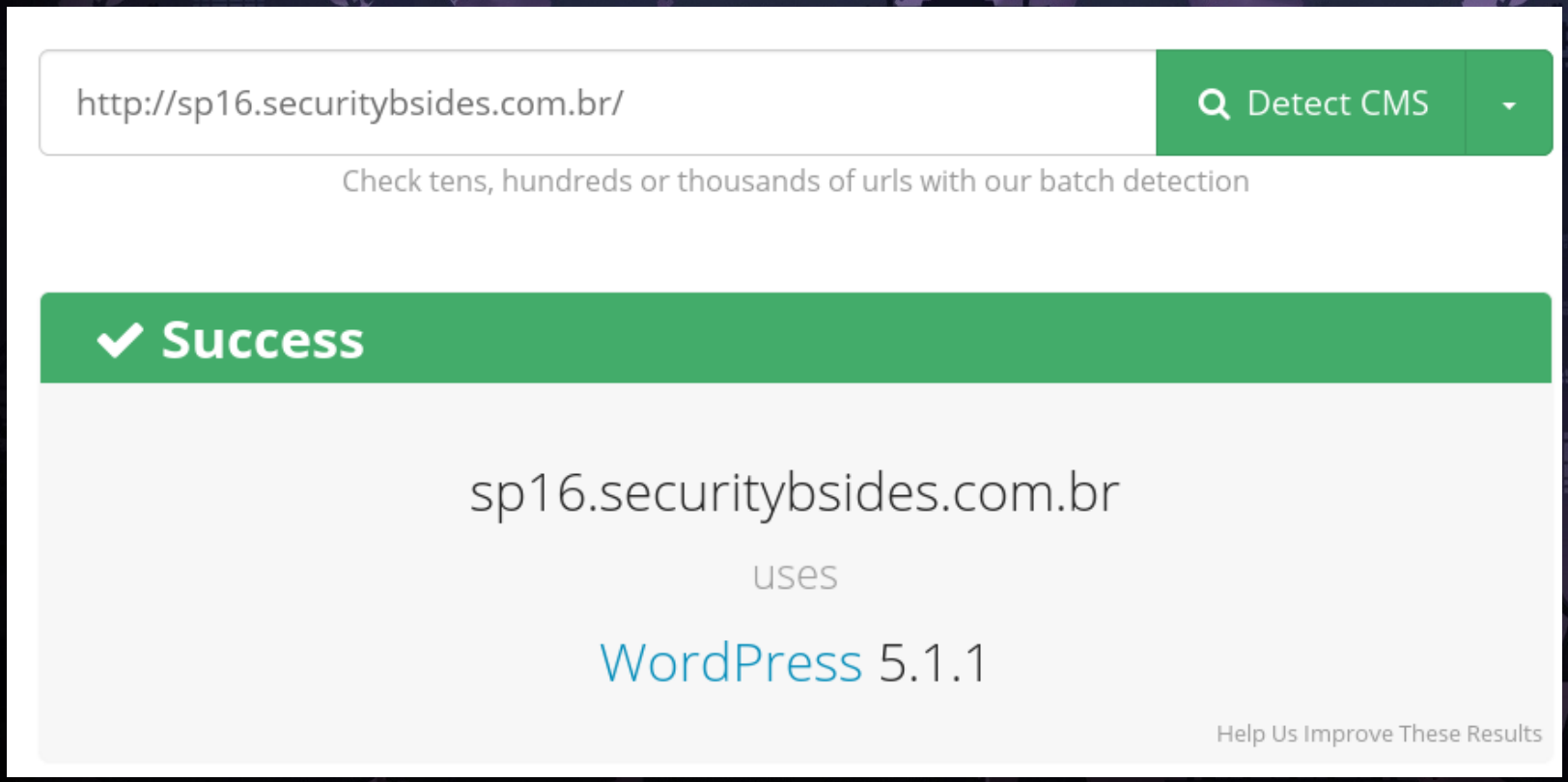
- Realizar 1000 (mil) requisições por mês
- 1 requisição a cada 10 segundos
- https://whatcms.org/Documentation
- https://github.com/HA71/pywhatcms

WhatCMS – Reconhecendo CMS + API



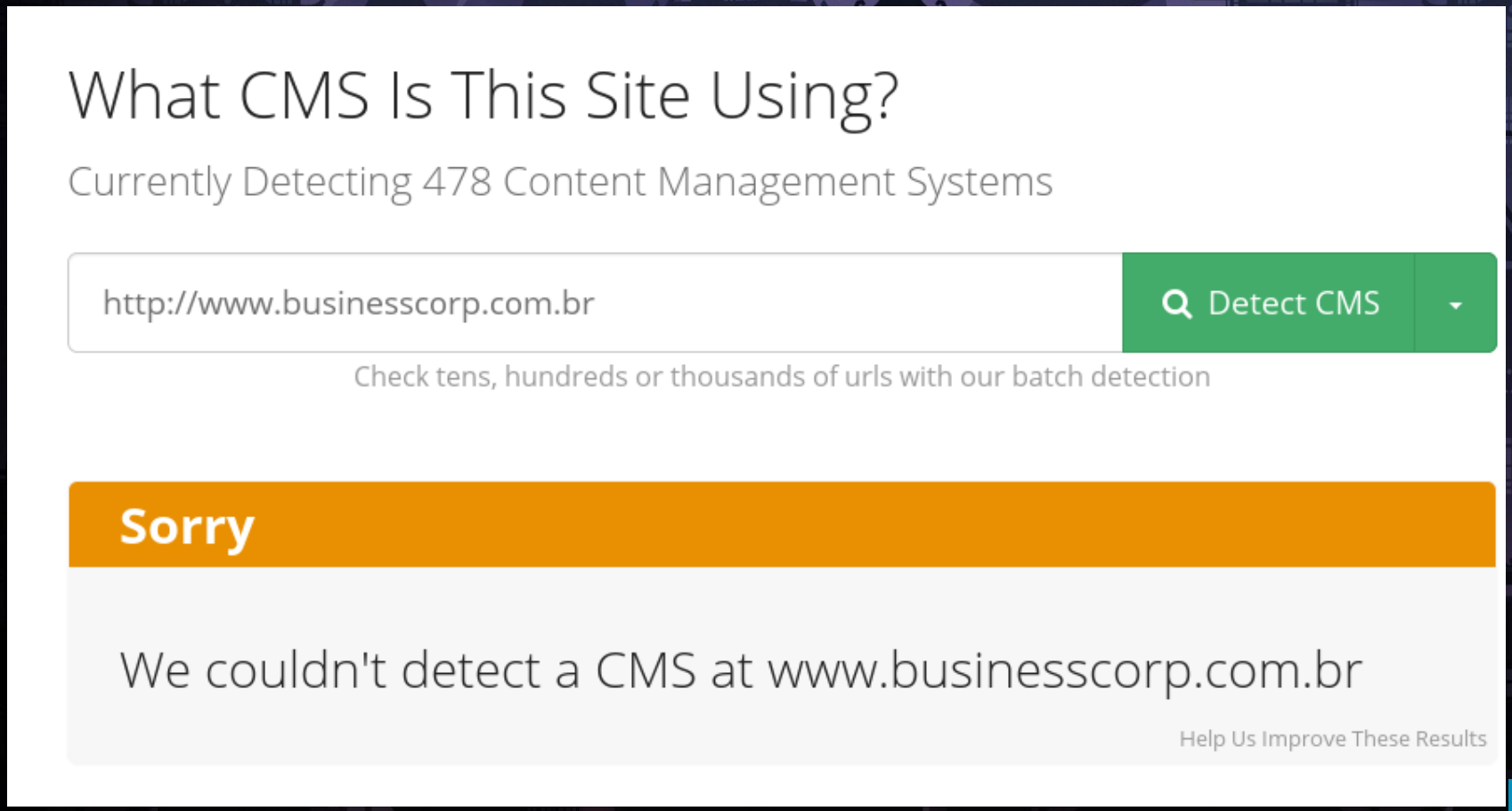
WhatCMS

WhatCMS – Reconhecendo CMS + API



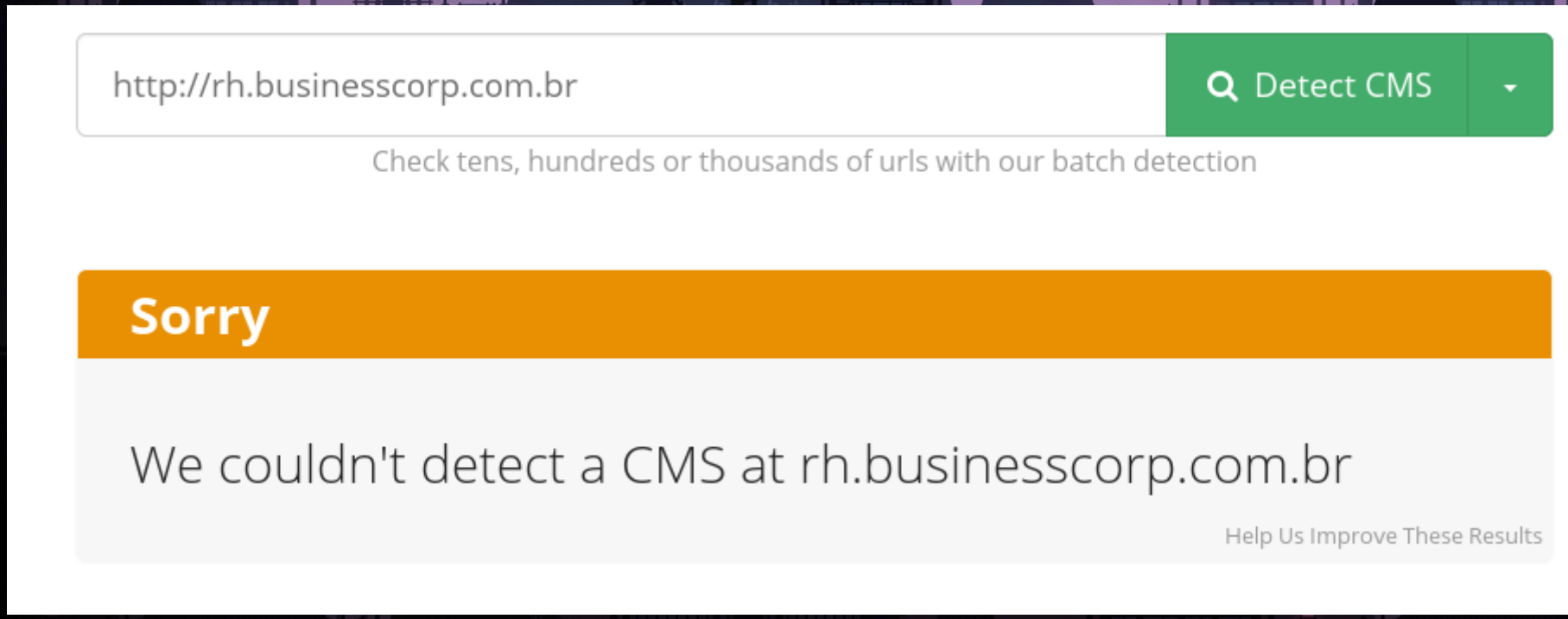
WhatCMS

WhatCMS – Reconhecendo CMS + API



WhatCMS

WhatCMS – Reconhecendo CMS + API



WhatCMS – Reconhecendo CMS + API

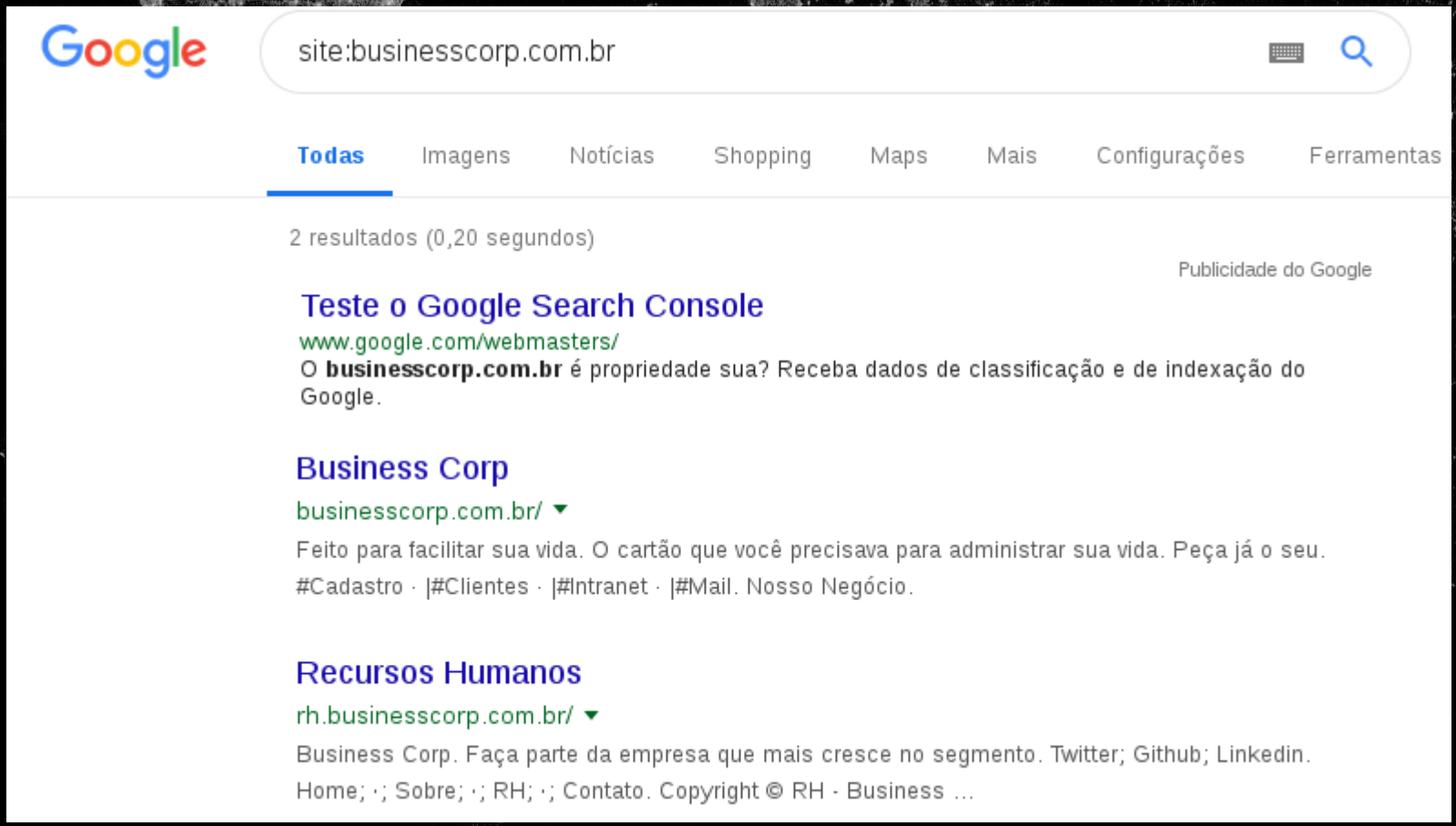
Reconhecimento com Python + API

```
 % python script-whatcms.py
WordPress
200
high
https://whatcms.org/c/WordPress
4.9.8
Success
1
https://whatcms.org/APIEndpoint/Detect?key=92
https://whatcms.org/?s=fatecourinhos.edu.br
```

Google Hacking -

- Fundada por Larry Page e Serget Brin em 2005.
- Operadores
- Docks
- Exploit DB
- Versões específicas vulneráveis
- Localizar todas as páginas
- Paginas de administração
- Backups de arquivos
- E tudo que pode estar sendo indexado pelo Google.

Google Hacking -



Google Hacking -

Bing -

- É um motor de busca desenvolvido pela Microsoft
- Infelizmente pouco usado
- **Operadores**
- Contains
- Filetype
- Url
- Site

Bing -

site:businesscorp.com.br

Recursos Humanos

rh.**businesscorp.com.br** ▾

Business Corp Faça parte da empresa que mais cresce no segmento. Twitter; Github; Linkedin; Home · Sobre · RH · Contato; Copyright © RH - Business Corp S.A 2017.

Recursos Humanos

rh.**businesscorp.com.br**/?page=submit ▾

Envie seu curriculo: ... PDF do curriculo

Business Corp

businesscorp.com.br ▾

Cartões Empresariais. Crie uma cartão personalizado para sua empresa, assim seus cliente podem pagar com o cartão do seu proprio negocios e obter descontos.

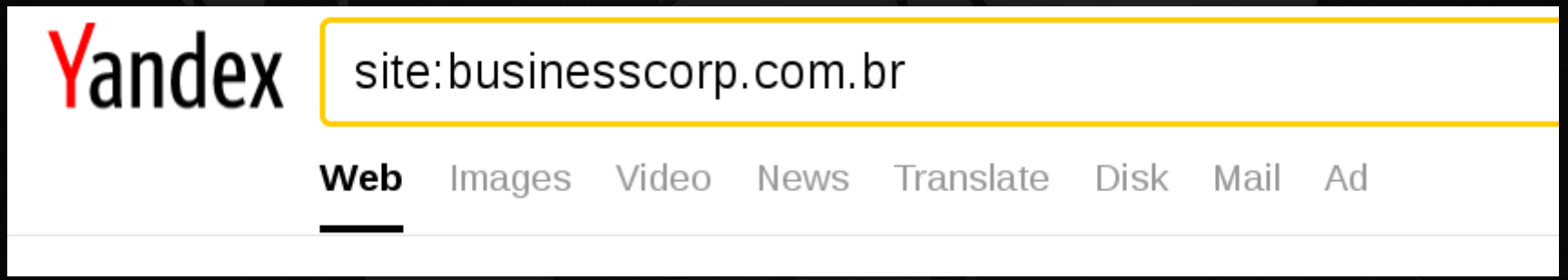
Bing -

Coletando informações com Python

Yandex -

- Motor de busca russo
- Lançado em 1997
- Em janeiro de 2015, o Yandex Search gerou 51,2% de todo o tráfego de pesquisa na Rússia
- Podemos usar **Operadores**
- site

Yandex -


Yandex
site:businesscorp.com.br
Web
Images
Video
News
Translate
Disk
Mail
Ad

Yandex -

Business Corp
businesscorp.com.br
Cartões Empresariais. Crie uma cartão personalizado para sua empresa, assim seus cliente podem pagar com o cartão do seu proprio negocios e obter descontos.

Business Corp
ftp.businesscorp.com.br
Cartões Empresariais. Crie uma cartão personalizado para sua empresa, assim seus cliente podem pagar com o cartão do seu proprio negocios e obter descontos.

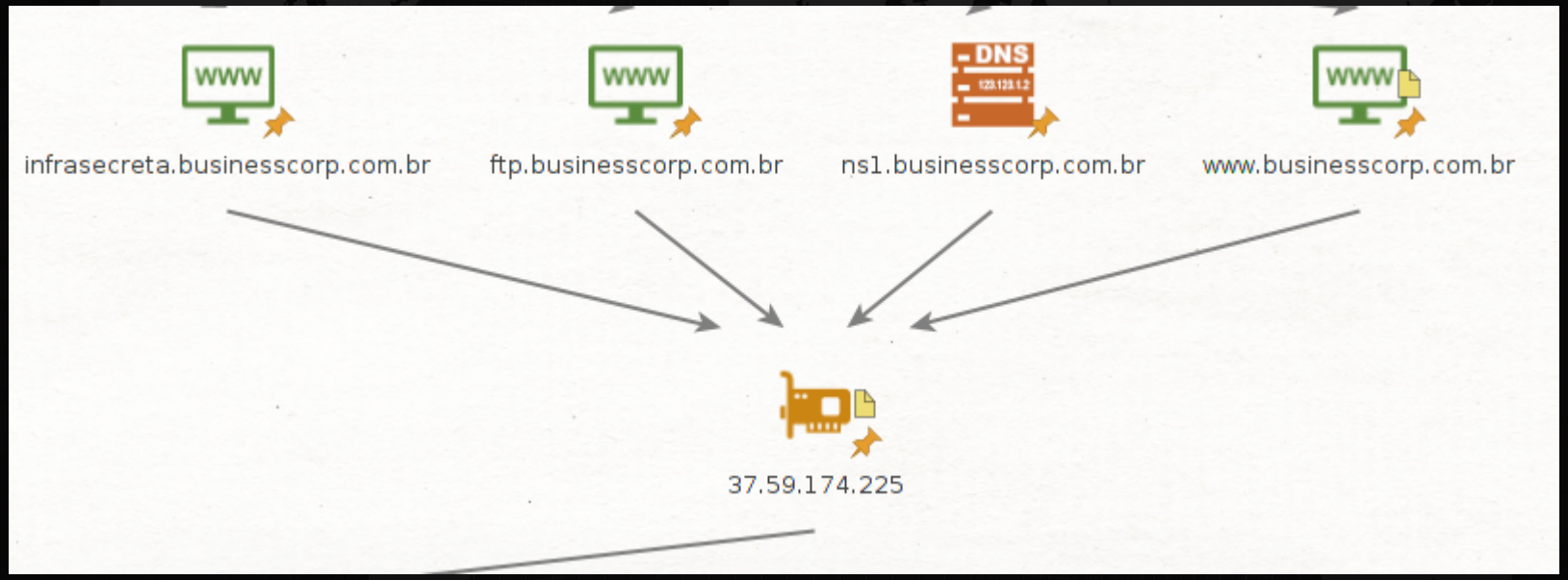
Business Corp
infrasecreta.businesscorp.com.br
Cartões Empresariais. Crie uma cartão personalizado para sua empresa, assim seus cliente podem pagar com o cartão do seu proprio negocios e obter descontos.

Business Corp
ns1.businesscorp.com.br
Cartões Empresariais. Crie uma cartão personalizado para sua empresa, assim seus cliente podem pagar com o cartão do seu proprio negocios e obter descontos.

Recursos Humanos
rh.businesscorp.com.br
Business Corp...

Recursos Humanos
rh.businesscorp.com.br › ?page=submit
Envie seu curriculo...

Yandex -


www
www
DNS
www
infrasecreta.businesscorp.com.br
ftp.businesscorp.com.br
ns1.businesscorp.com.br
www.businesscorp.com.br
37.59.174.225

Shodan -

- Lançado em 2009 por John Matherly
- Encontrar por dispositivos conectados na internet
- Webcam ,Banco de dados,Servidores,Roteadores etc
- Banners de serviço
- Metadados
- Mensagens de boas vindas
- Versões de serviço
- Common Vulnerabilities and Exposures (CVE)

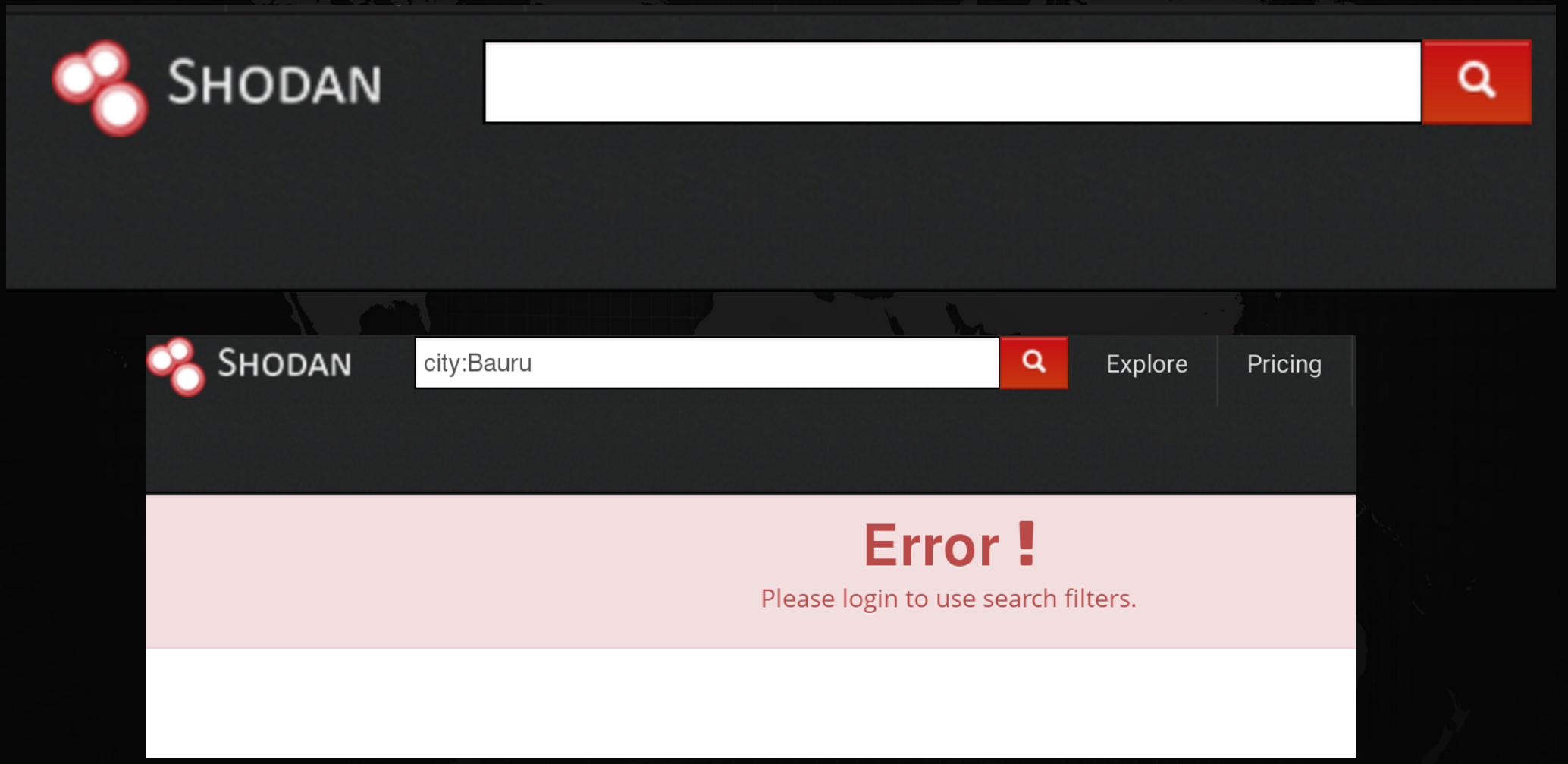
Shodan –

- Cidade
- País
- Organização
- Hostnames
- ASN
- Serviços
- Portas
- Localização do servidor
- CVE

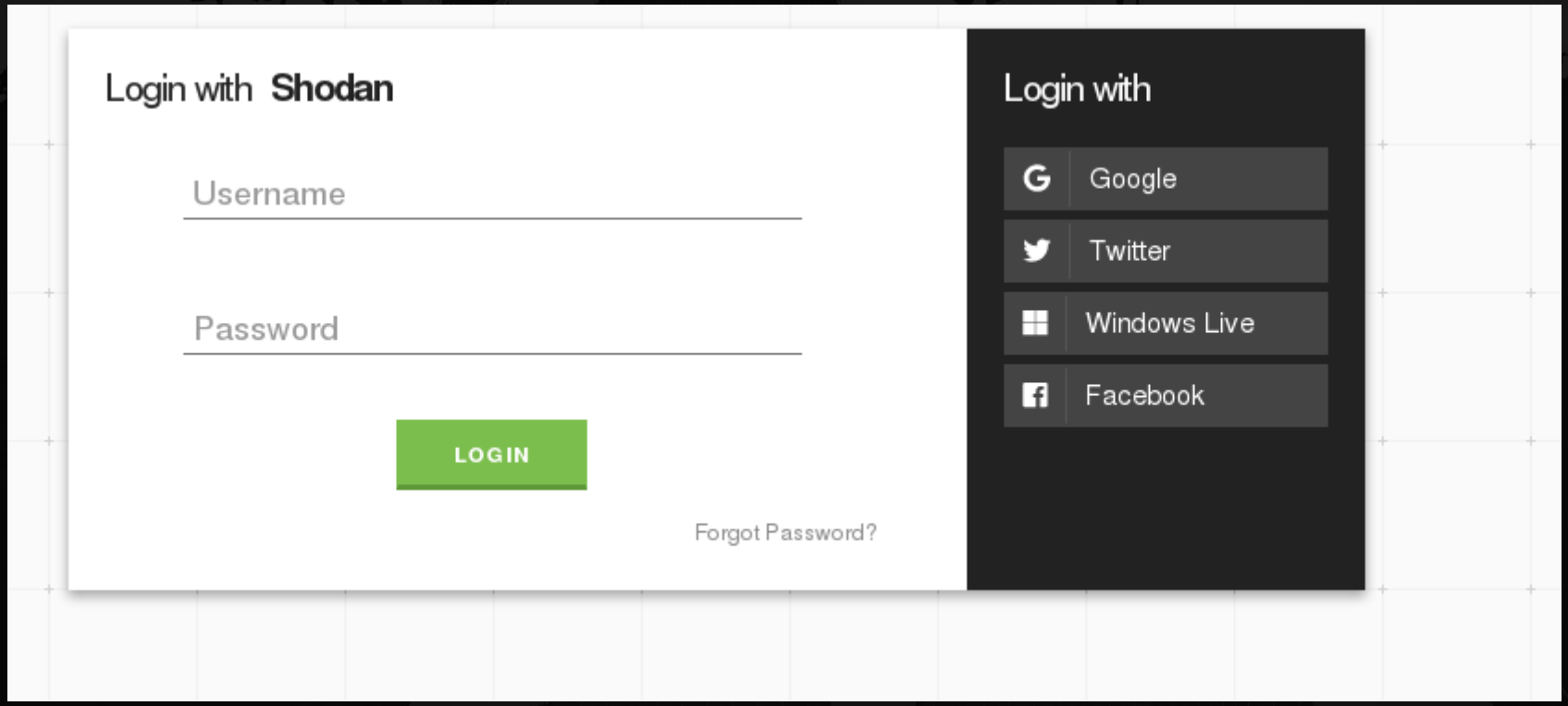
Shodan – Operadores

- city
- OS
- port
- IP
- NET
- hostname
- Server
- Palavras chaves
- Dorks complexas

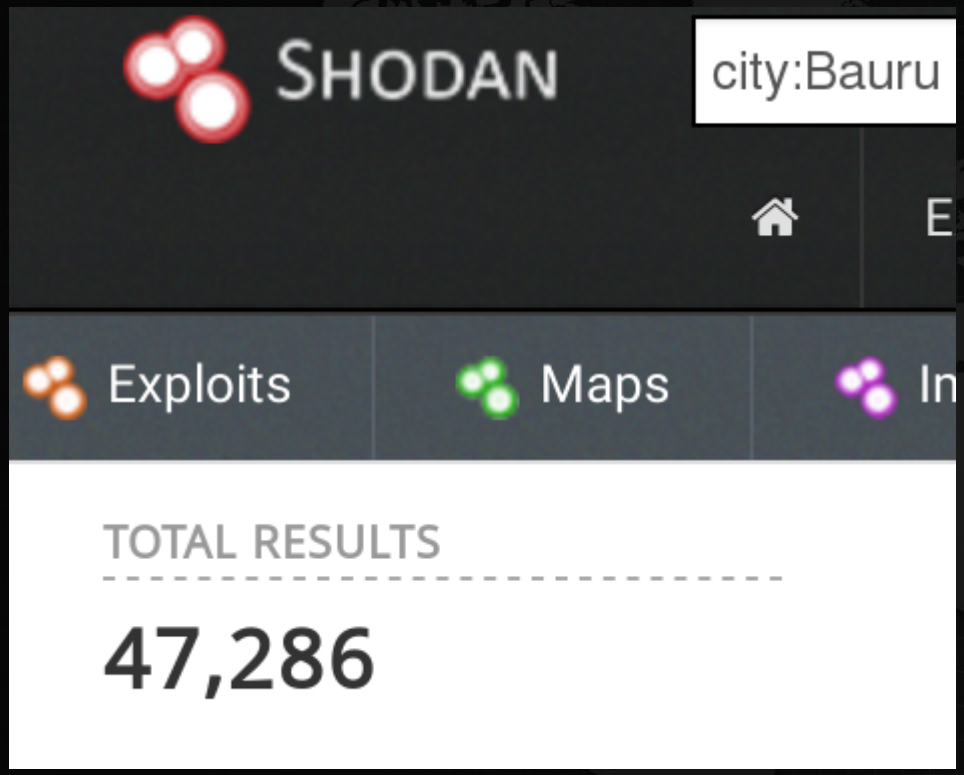
Shodan – Operadores

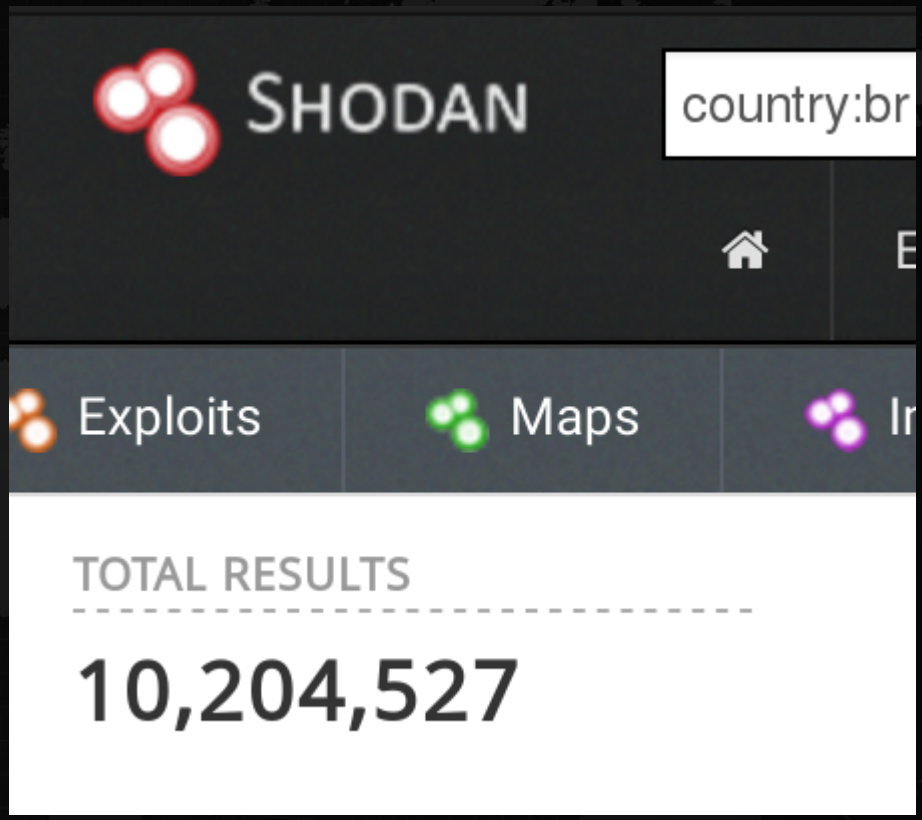


Shodan – Operadores

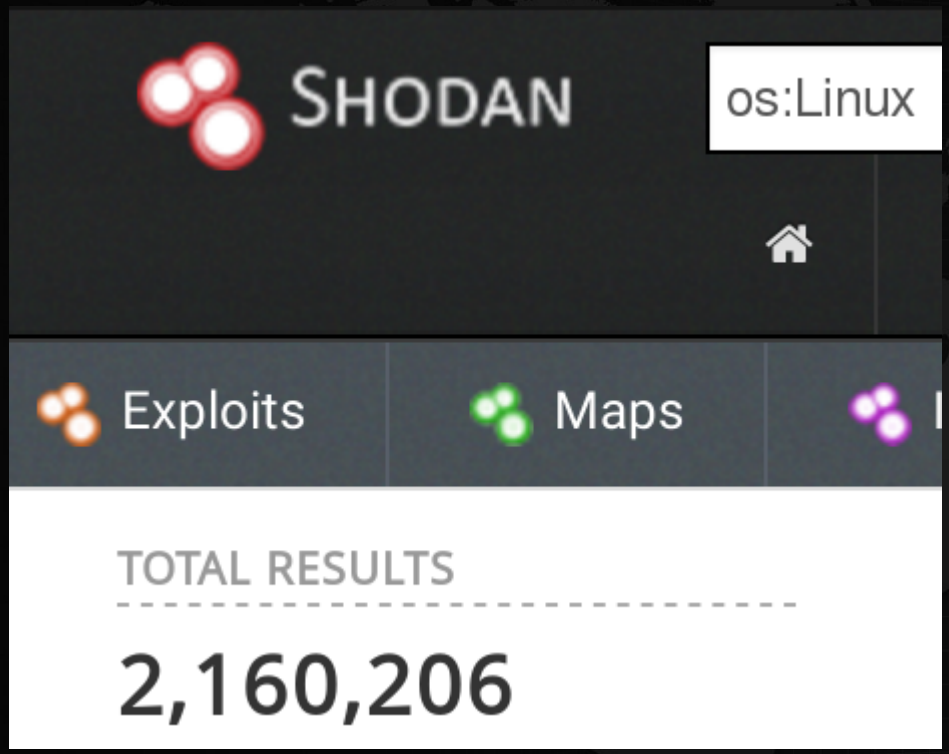


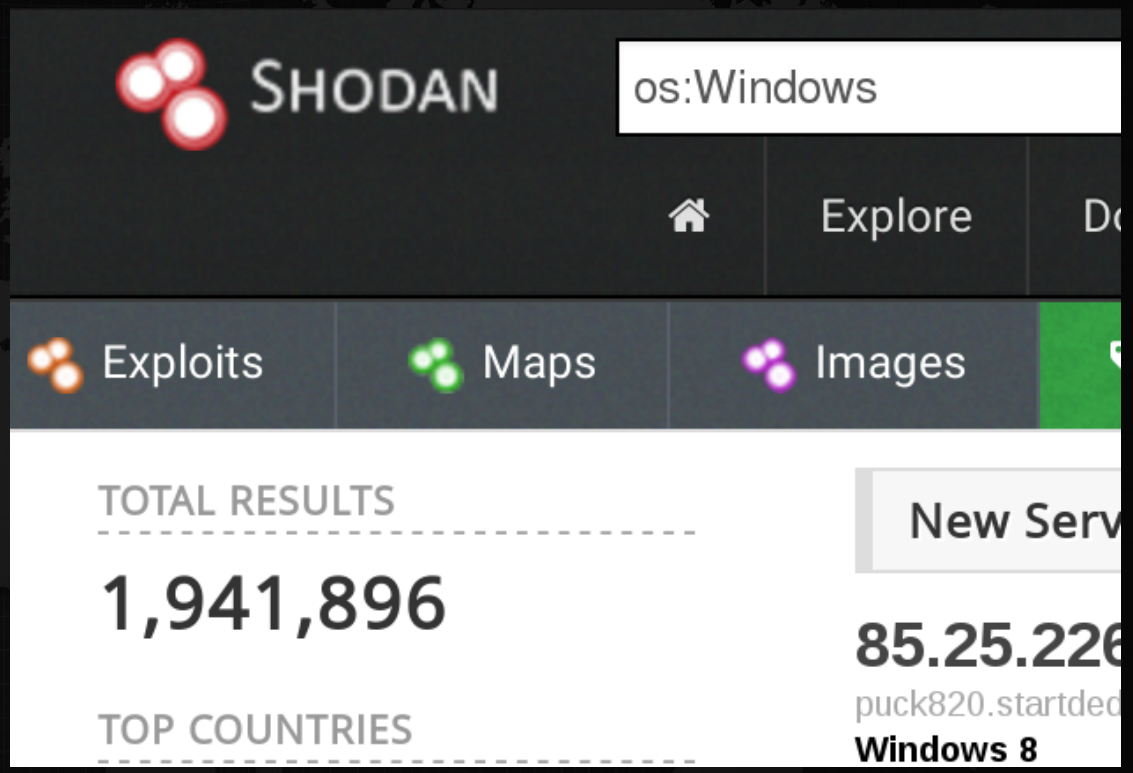
Shodan – Operadores



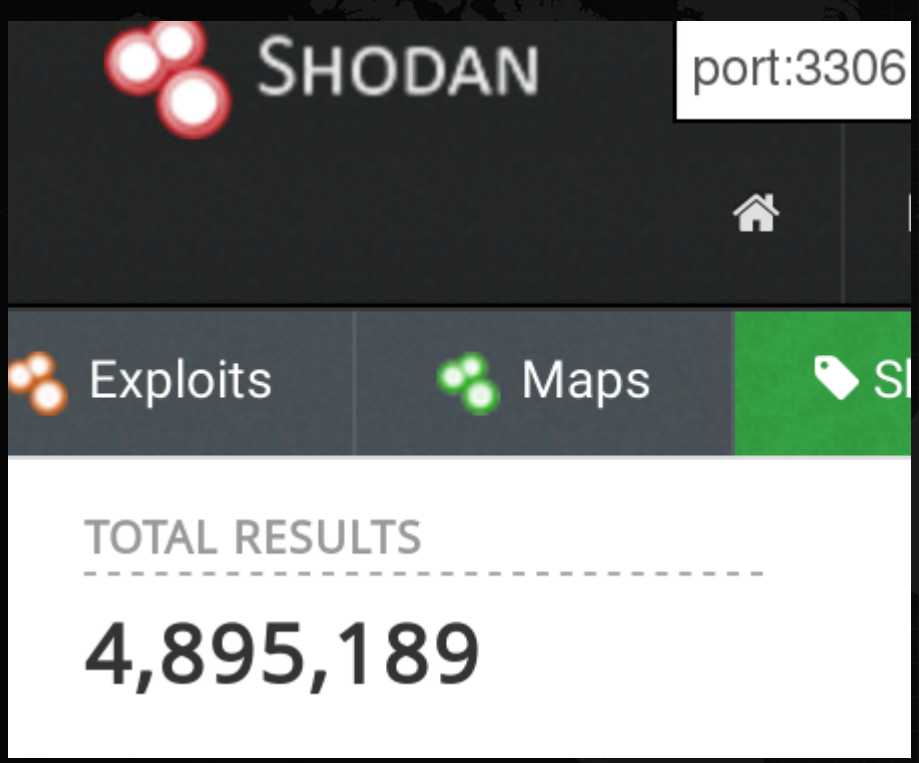


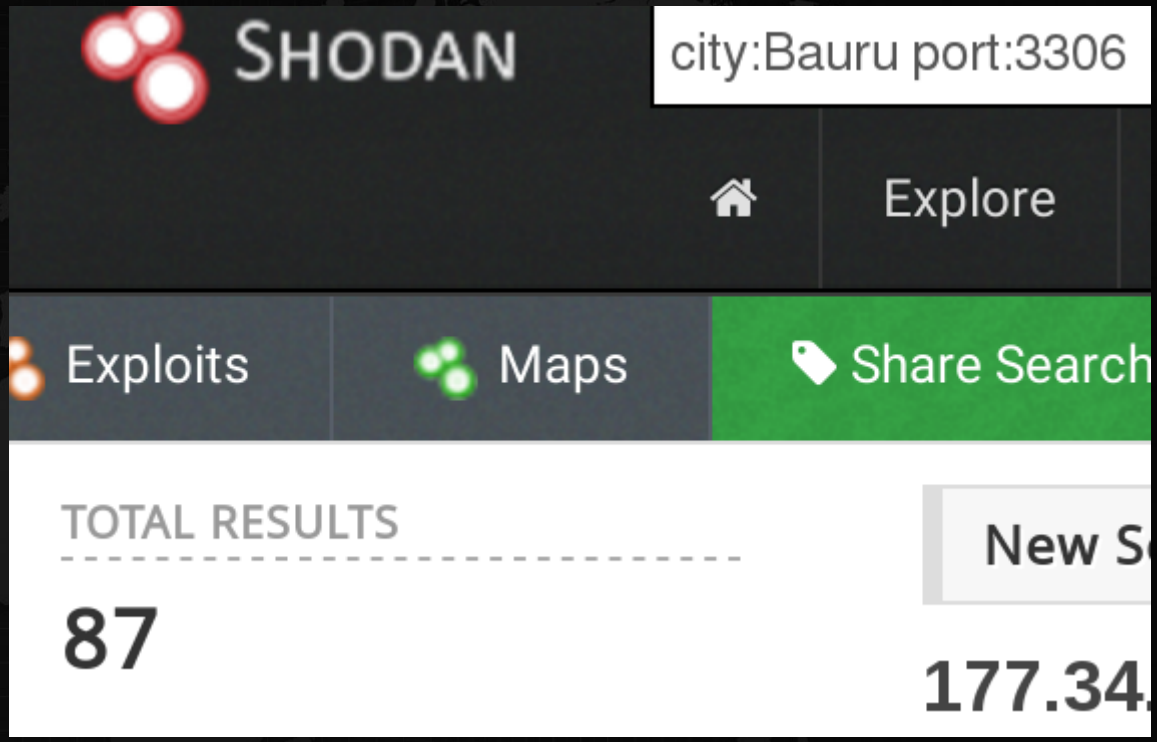
Shodan – Operadores



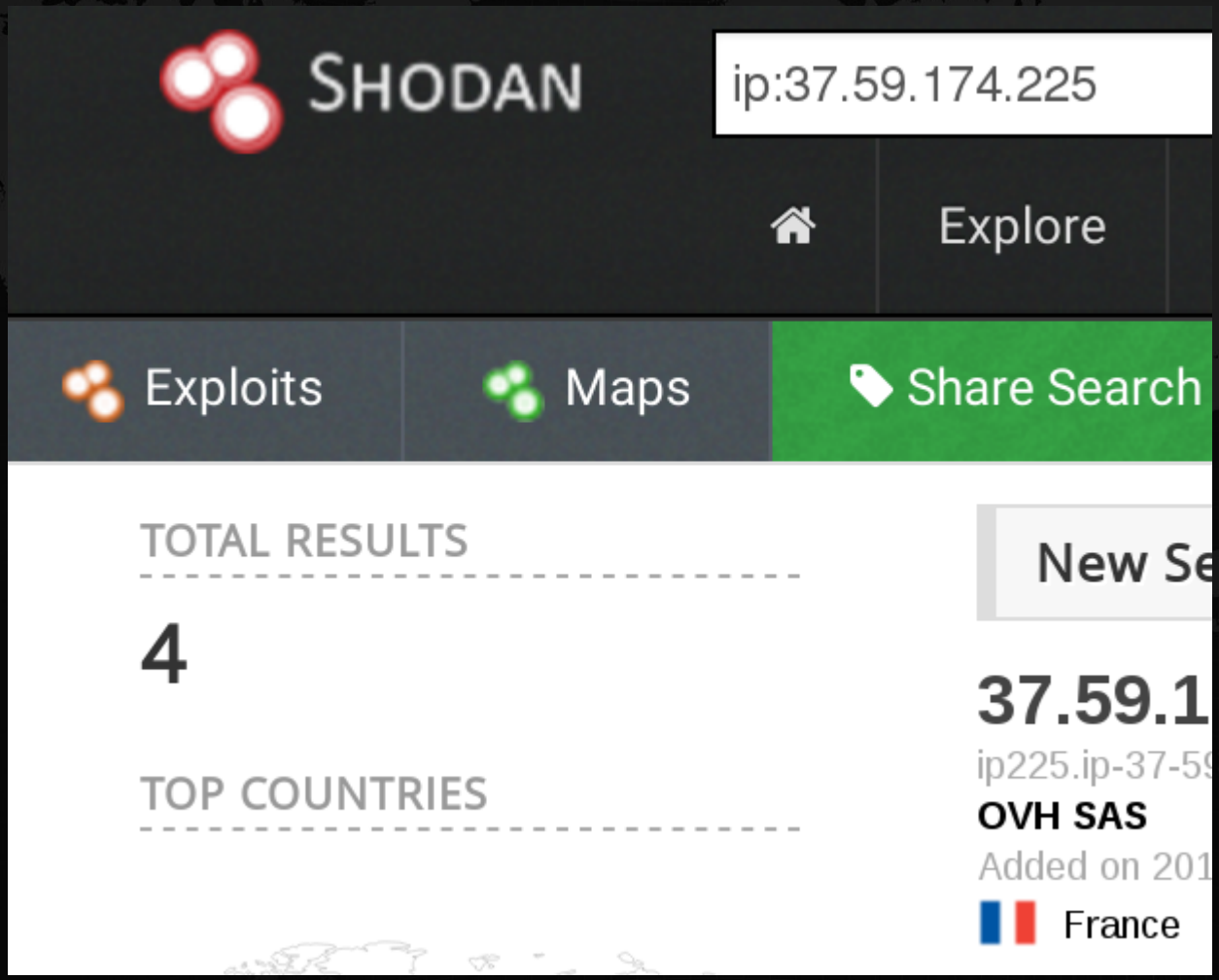


Shodan – Operadores





Shodan – Operadores



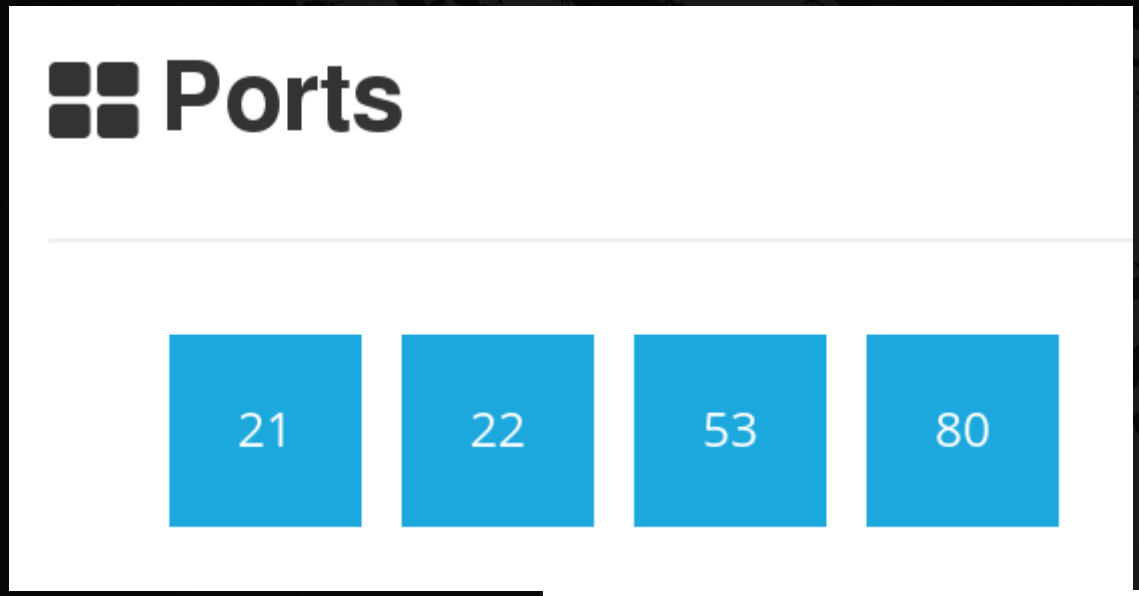
Shodan – Operadores

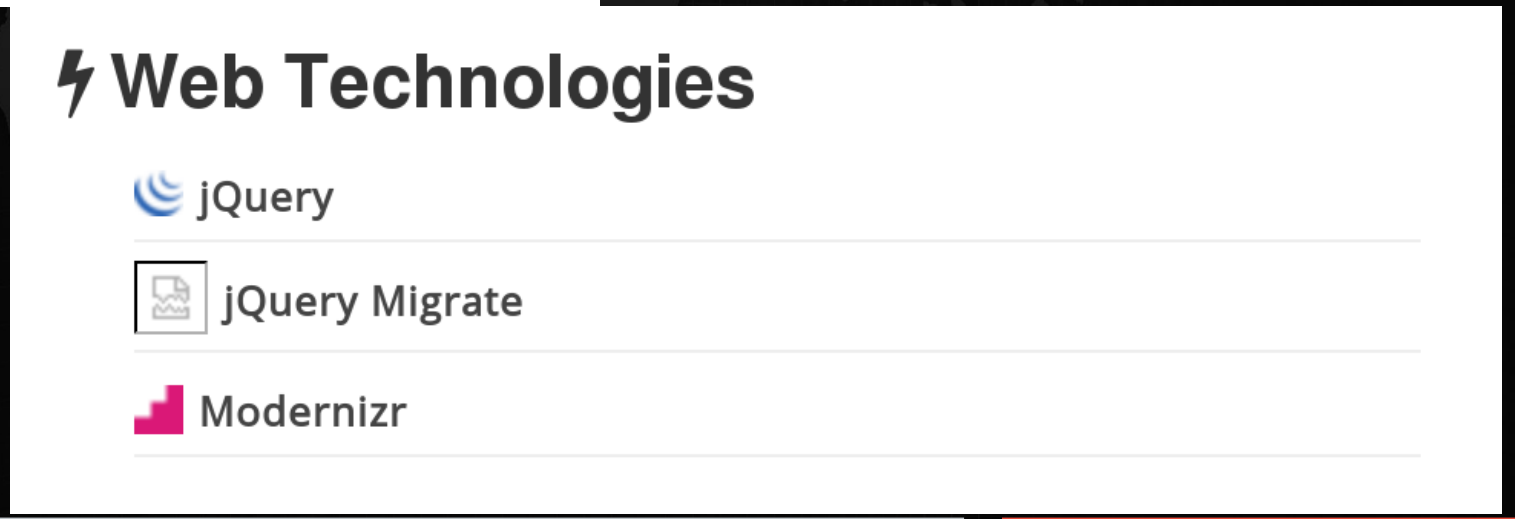
37.59.174.225 ip225.ip-37-59-174.eu View Raw

Data

Country	France
Organization	OVH SAS
ISP	OVH SAS
Last Update	2019-05-22T11:55:08.436283
Hostnames	ip225.ip-37-59-174.eu
ASN	AS16276

Shodan – Operadores





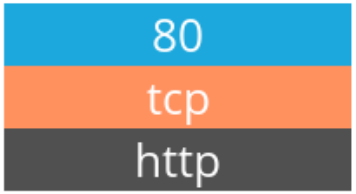
Shodan – Operadores

⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2012-4558	Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.
CVE-2013-1896	mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.

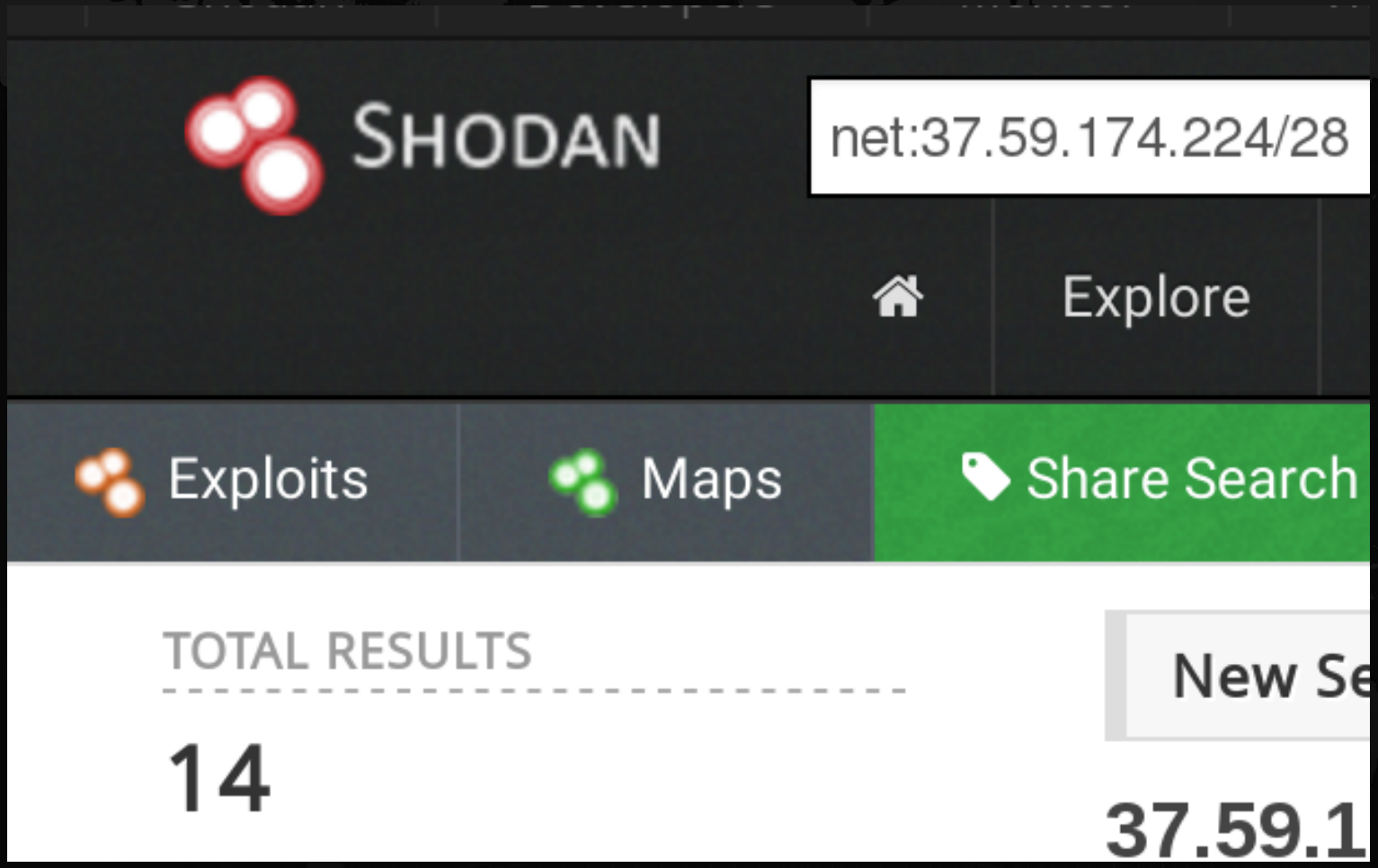
Shodan – Operadores



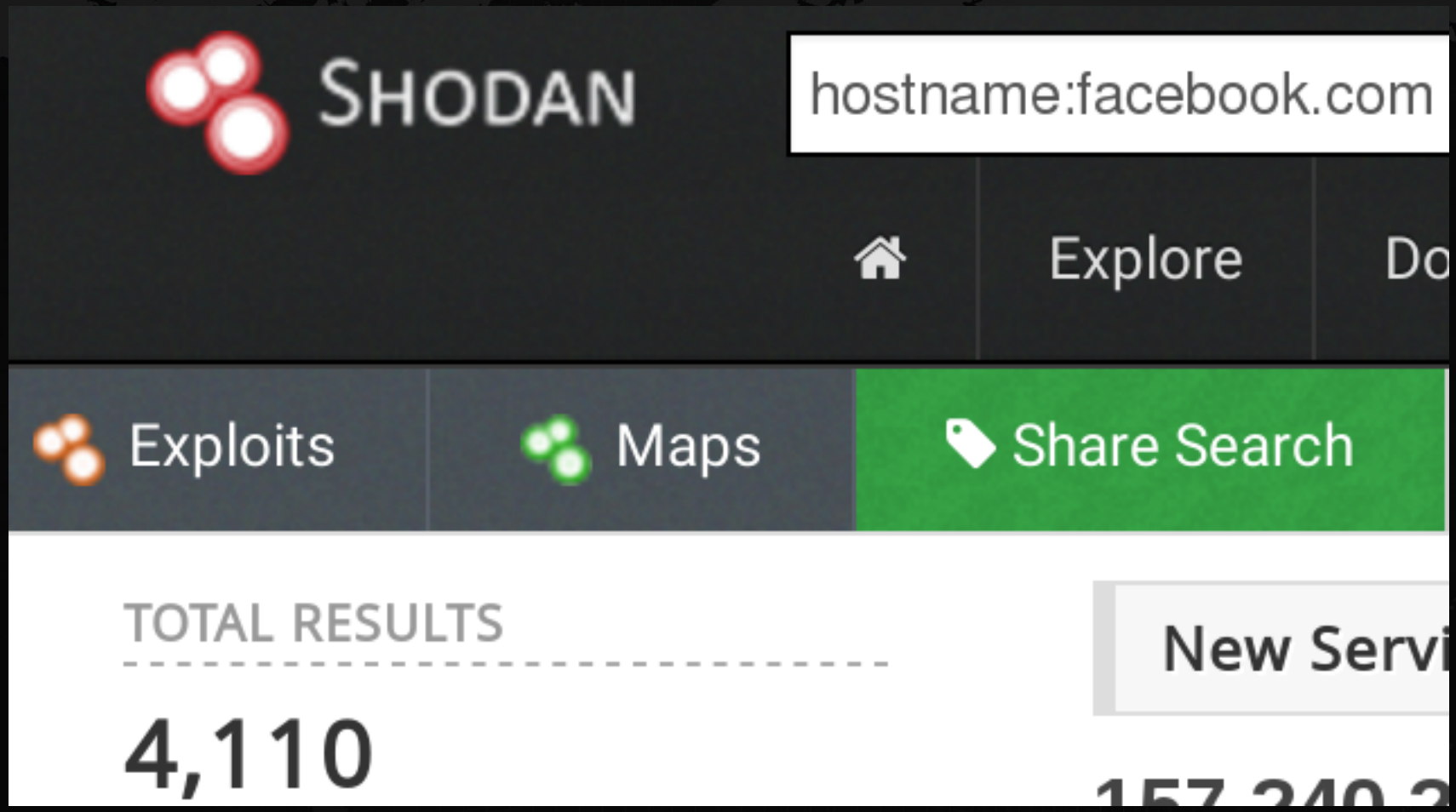
Apache httpd Version: 2.2.22

```
HTTP/1.1 200 OK
Date: Wed, 14 Oct 2015 11:35:58 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Tue, 13 Oct 2015 18:27:58 GMT
ETag: "20463-1b79-522009aede4a5"
Accept-Ranges: bytes
Content-Length: 7033
Vary: Accept-Encoding
Content-Type: text/html
```

Shodan – Operadores



Shodan – Operadores



Shodan – Via linha de comando CLI

- Usamos Python s2
- https://account.shodan.io
- Documentação https://shodan.readthedocs.io
- Apenas a versão via linha de comando apresenta CVE

Shodan – Via linha de comando CLI

```
pip3 install shodan
```

```
Commands:
  alert        Manage the network alerts for your account
  convert      Convert the given input data file into a different format.
  count        Returns the number of results for a search
  data         Bulk data access to Shodan
  domain       View all available information for a domain
  download     Download search results and save them in a compressed JSON...
  honeyscore   Check whether the IP is a honeypot or not.
  host         View all available information for an IP address
  info         Shows general information about your account
  init         Initialize the Shodan command-line
  myip         Print your external IP address
  org          Manage your organization's access to Shodan
  parse        Extract information out of compressed JSON files.
  radar        Real-Time Map of some results as Shodan finds them.
  scan         Scan an IP/ netblock using Shodan.
  search       Search the Shodan database
  stats        Provide summary information about a search query
```

Shodan – Via linha de comando CLI

```
shodan init su
```

```
Successfully initialized
```

```
shodan host 37.59.174.225
```

SHODAN

Shodan – Via linha de comando CLI

```
root@57b6bb7d46be:/# shodan host 37.59.174.225
37.59.174.225
Hostnames:                ip225.ip-37-59-174.eu
Country:                  France
Operating System:         Linux 3.x
Organization:             OVH SAS
Updated:                  2019-05-21T09:43:48.284755
Number of open ports:     4
Vulnerabilities:          CVE-2012-4558  CVE-2013-1896   CVE-2012-3499   CVE-20
-0231   CVE-2017-7679   CVE-2013-2249   CVE-2016-4975   CVE-2013-5704   CVE-20
-7668   CVE-2013-6438   CVE-2012-2687   CVE-2017-3167   CVE-2017-3169   CVE-20
-0098   CVE-2013-1862   CVE-2016-8612

Ports:
     21/tcp ProFTPD (1.3.4a)
     22/tcp OpenSSH (6.0p1 Debian 4+deb7u2)
     53/udp
     80/tcp Apache httpd (2.2.22)
```

Shodan – Via linha de comando CLI

```
shodan host 200.211.154.140
```

```
Vulnerabilities:          CVE-2018-10549 CVE-2018-10548  CVE-2018-10
545      CVE-2018-10547  CVE-2018-10546  CVE-2019-9638   CVE-2010-12
56       CVE-2014-4721   CVE-2014-5459   CVE-2018-19520  CVE-2018-19
396      CVE-2018-19395  CVE-2018-19935  CVE-2018-17082  CVE-2019-96
39       CVE-2010-3972   CVE-2019-9021   CVE-2019-9637   CVE-2015-89
94       CVE-2017-16642  CVE-2018-14883  CVE-2010-1899   CVE-2010-27
30       CVE-2018-20783  CVE-2016-7478   CVE-2019-6977   CVE-2014-99
12       CVE-2014-0237   CVE-2014-9427   CVE-2014-0238   CVE-2019-90
23       CVE-2019-9020   CVE-2019-9641   CVE-2012-2531   CVE-2019-90
24       CVE-2018-15132
```

Shodan – Via linha de comando CLI

Coletando informações com Python + API

```
 % python3 shodan-recon.py

IP: 37.59.174.225
Organization: OVH SAS
Operating System: None


Port: 80


Port: 53


Port: 22


Port: 21
```

Censys -

- Censys criado em 2015 na universidade de Michigan
- Busca de dispositivos , redes e infraestruturas
- 45 das Fortune 500 usa dados do Censys
- Latitude/Longitude ,País , Rota , Portas abertas e protocolos
- Podemos ver o tipo de servidor usado
- Status do teste
- Titulo do IP usado
- Nome da rede de sites e IPS.

Censys -

O resultado nos formatos

- Table ,JSON , Raw WHOIS

Informações básicas

- Informações básicas do domínio
- Contato para relatar algum abuso
- Informações de Contato , sobre a rede , informações técnicas e administrativas

Censys -

Temos informações como por exemplo

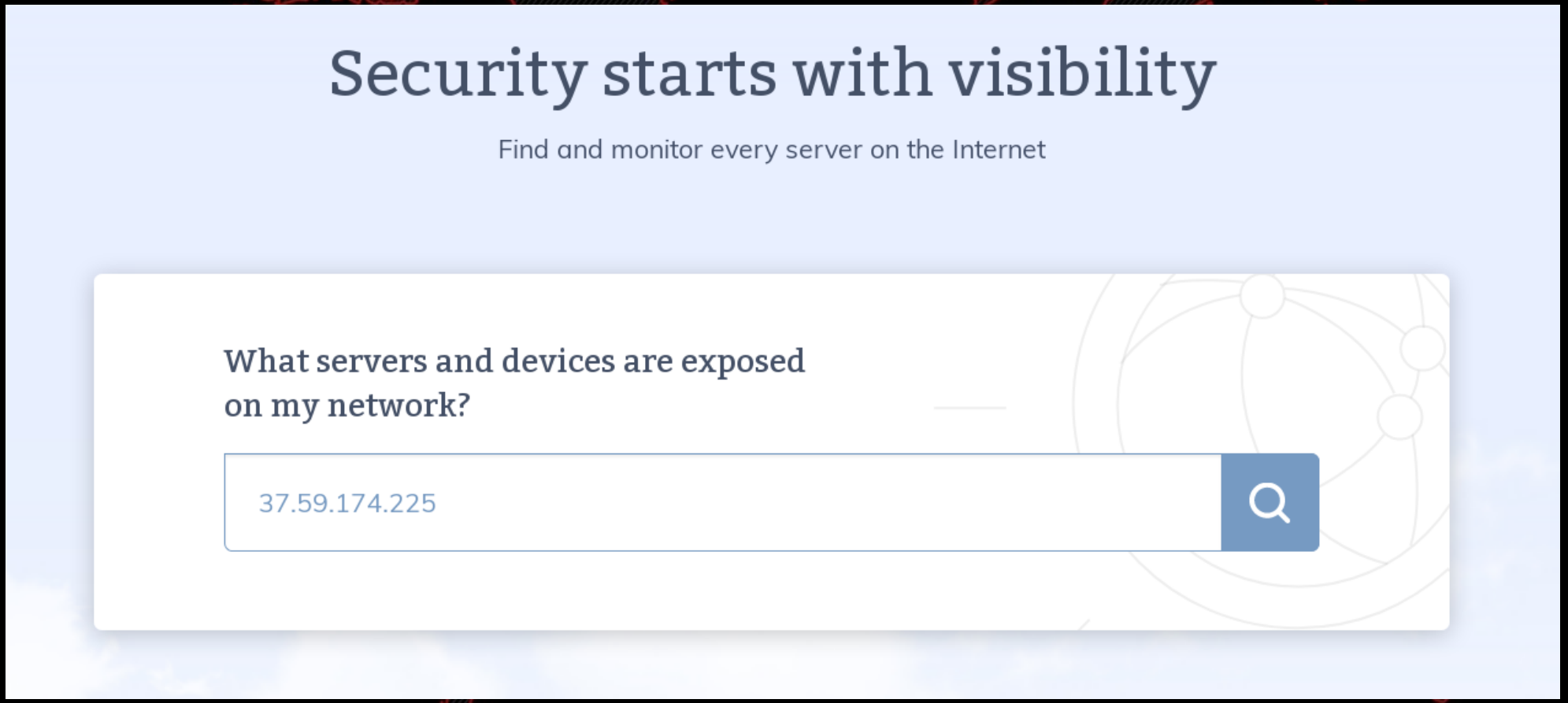
- Alexa rank , Protocolos disponível
- Informações sobre as portas que estão abertas
- Qual o servidor usado , Titilo do site
- Informações sobre certificados do HTTPS ,
- Banner do serviço e configurações de DNS

Censys -

O que podemos fazer com essas informações ?

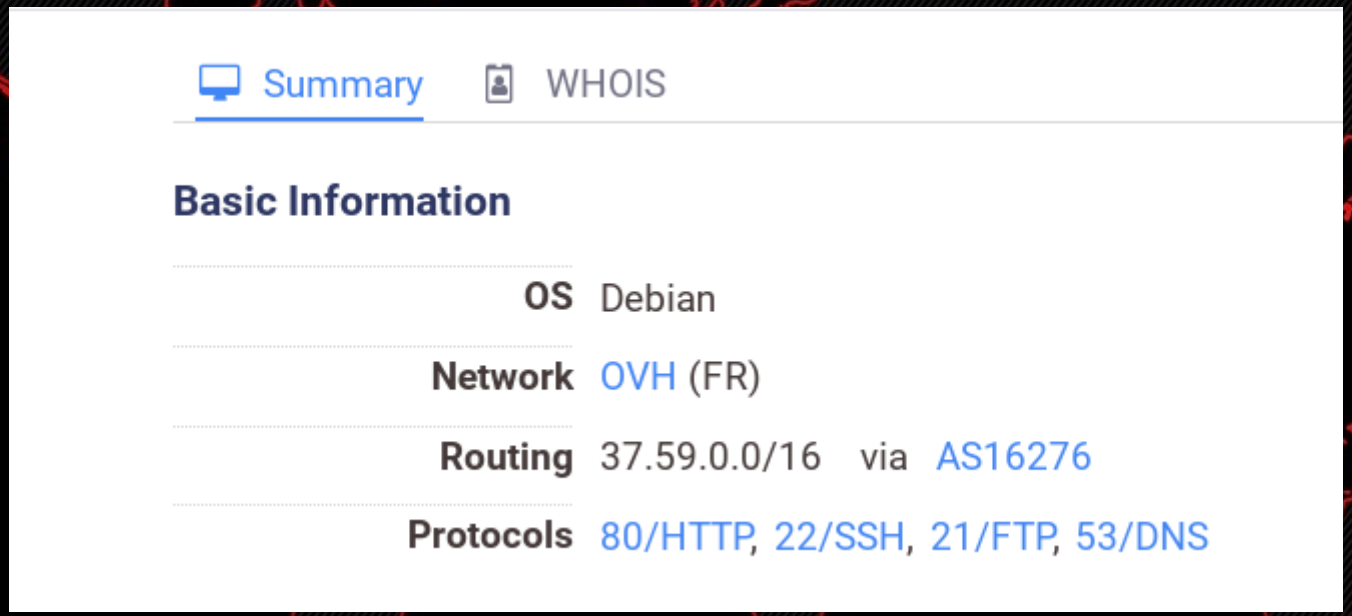
- Obter emails
- Range de rede
- Descobrir outros servidores
- CIDR
- Encontrar servidores na mesma rede

Censys -



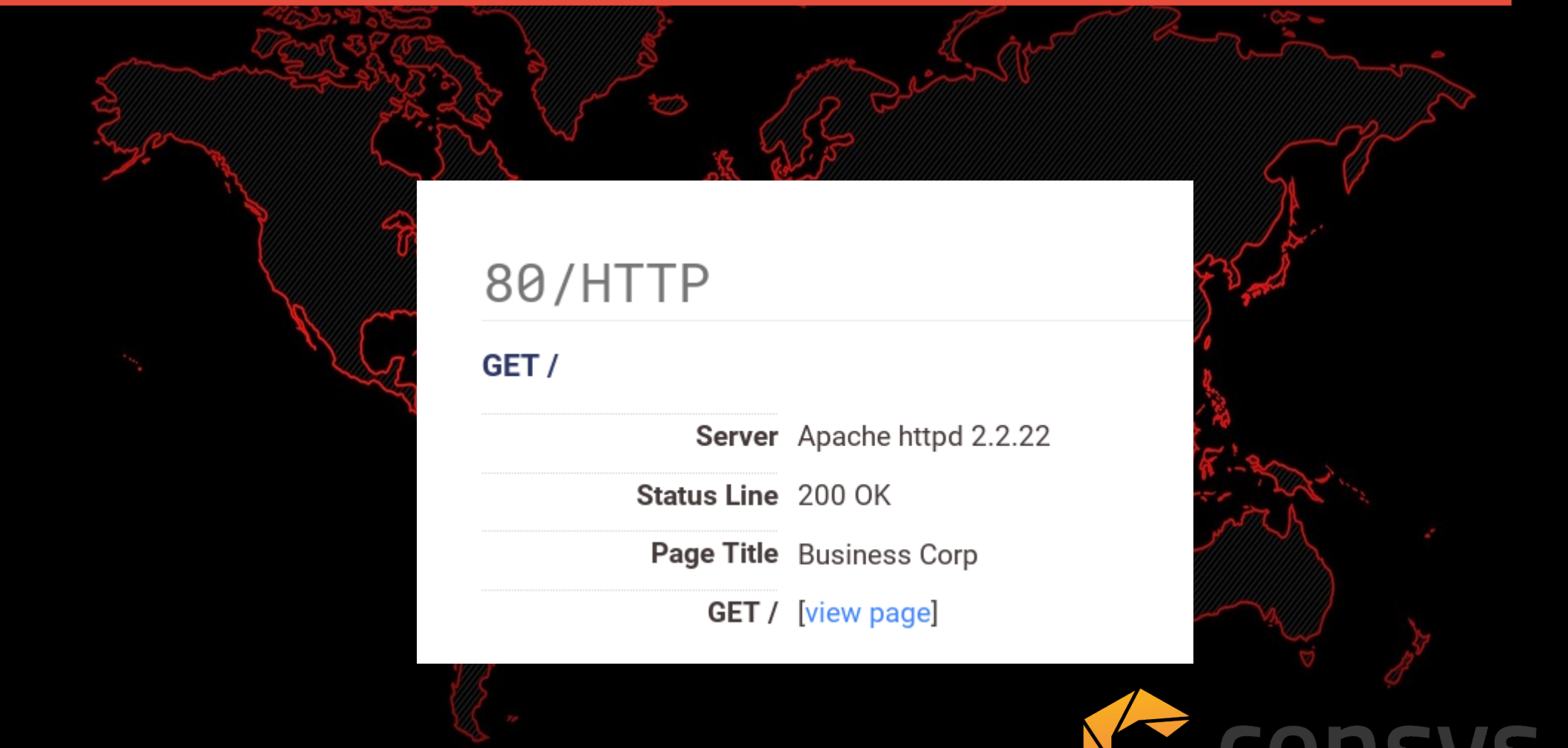
censys

Censys -

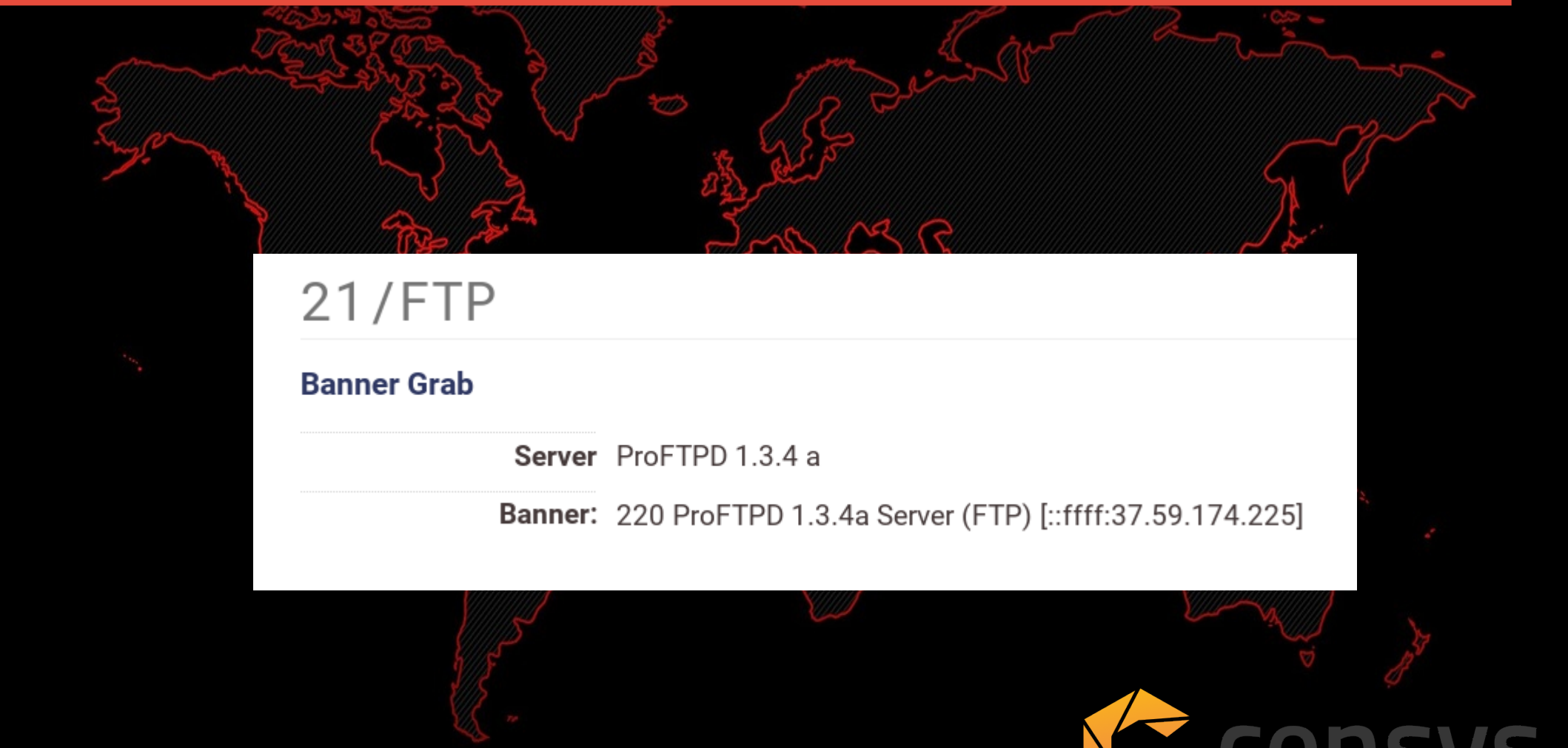


censys

Censys -


80/HTTP
GET /
Server Apache httpd 2.2.22
Status Line 200 OK
Page Title Business Corp
GET / [view page]
censys

Censys -



censys

Censys -

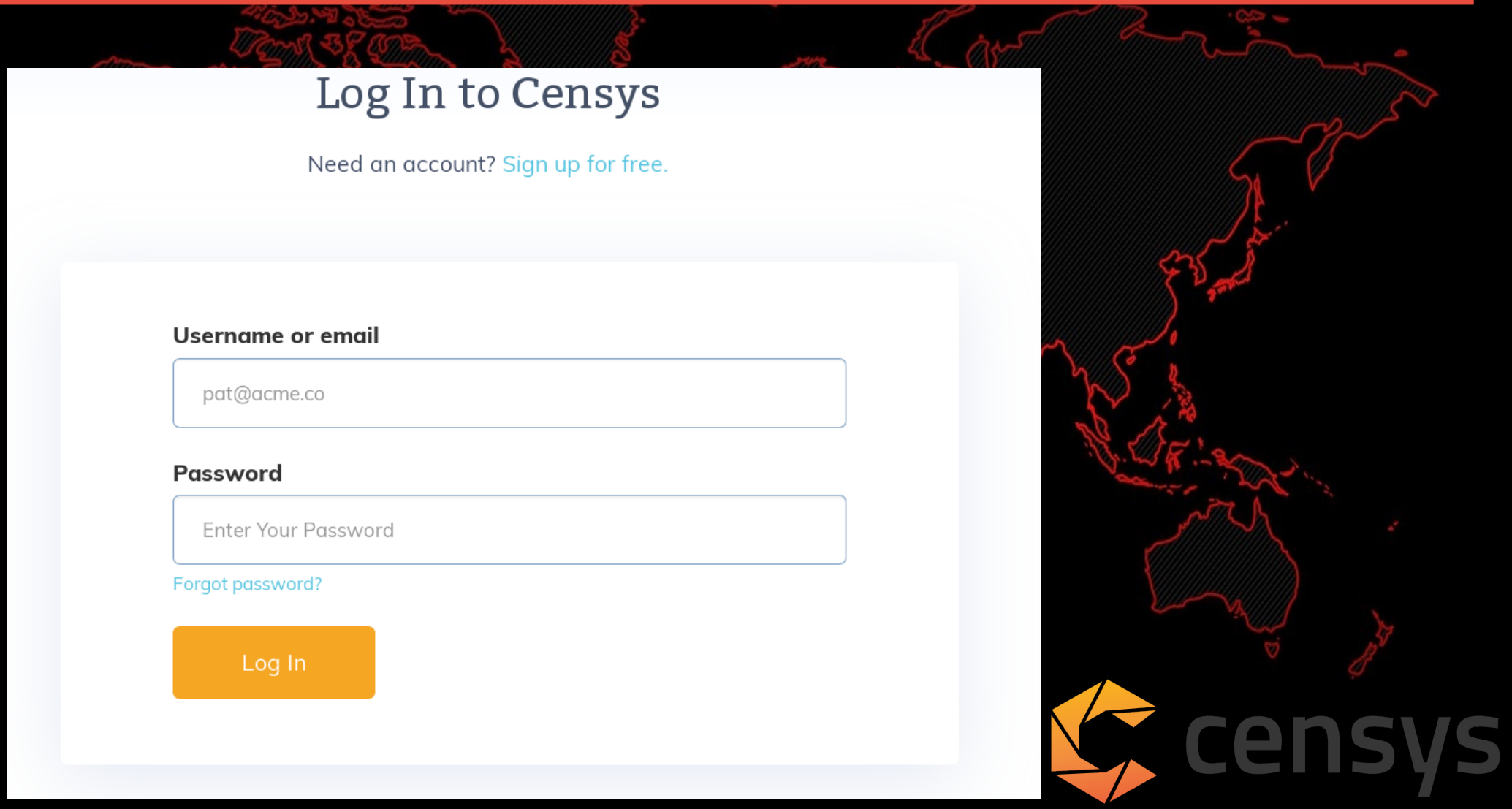
censys

Censys -

Geographic Location

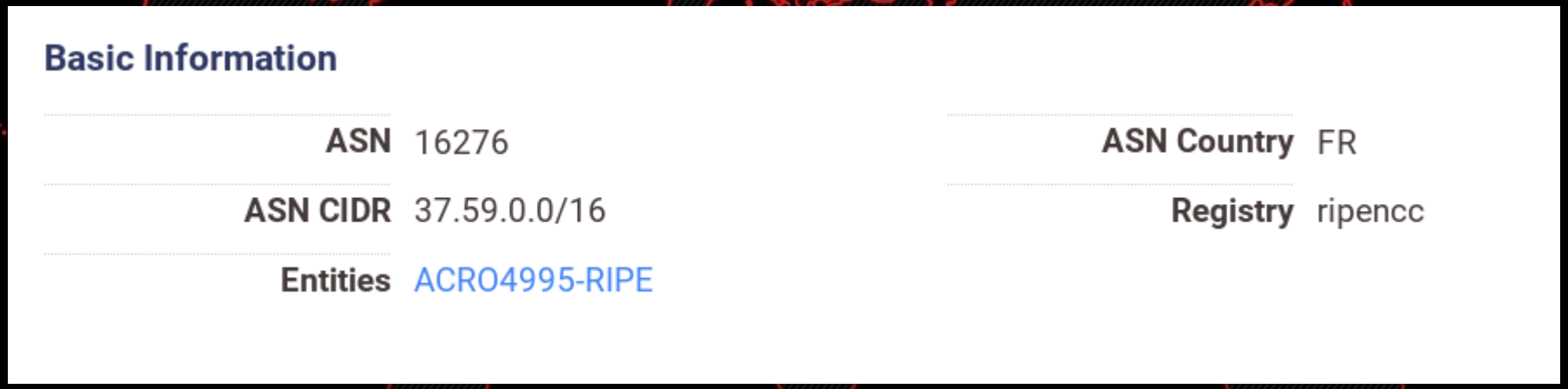
Country	France (FR)
Lat/Long	48.8582, 2.3387
Timezone	Europe/Paris

Censys -


Log In to Censys
Need an account? Sign up for free.
Username or email
pat@acme.co
Password
Enter Your Password
Forgot password?
Log In
censys

Censys -

Buscando informações sobre Whois



Censys -

ACRO4995-RIPE (abuse)

Contact Information

Name	Abuse contact role object (group)
Email	contato@desec.com.br
Address	---

Other Information

Entities	OVH-MNT

censys

Censys -


Network
Name OVH_134187362
Type ASSIGNED PA
Handle 37.59.174.224 - 37.59.174.239
Parent FR-OVH-20120116
CIDR 37.59.174.224/28 (v4)
censys

Censys -

Coletando informações com Python + API

```
 % python script-censys.py
{   u'21': {   u'ftp': {   u'banner': {   u'banner': u'220 ProFTPD 1.3.4a Server (FTP) [::ffff:37.59
                                          u'metadata': {   u'description': u'ProFTPD 1.3.4 a',
                                                           u'product': u'ProFTPD',
                                                           u'revision': u'a',
                                                           u'version': u'1.3.4'}}}},
    u'22': {   u'ssh': {   u'v2': {   u'banner': {   u'comment': u'Debian-4+deb7u2',
                                                     u'raw': u'SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u2
                                                     u'software': u'OpenSSH_6.0p1',
                                                     u'version': u'2.0'},
```

censys

Censys -

Coletando informações com Python + API

```
u'ip': u'37.59.174.225',
u'location': {   u'continent': u'Europe',
                 u'country': u'France',
                 u'country_code': u'FR',
                 u'latitude': 48.8582,
                 u'longitude': 2.3387,
                 u'registered_country': u'France',
                 u'registered_country_code': u'FR',
                 u'timezone': u'Europe/Paris'},
u'metadata': {   u'os': u'Debian', u'os_description': u'Debian'},
u'ports': [80, 21, 22, 53],
u'protocols': [u'80/http', u'22/ssh', u'21/ftp', u'53/dns'],
u'tags': [u'ftp', u'http', u'ssh', u'dns'],
u'updated at': u'2019-05-24T14:07:42+00:00'}
```

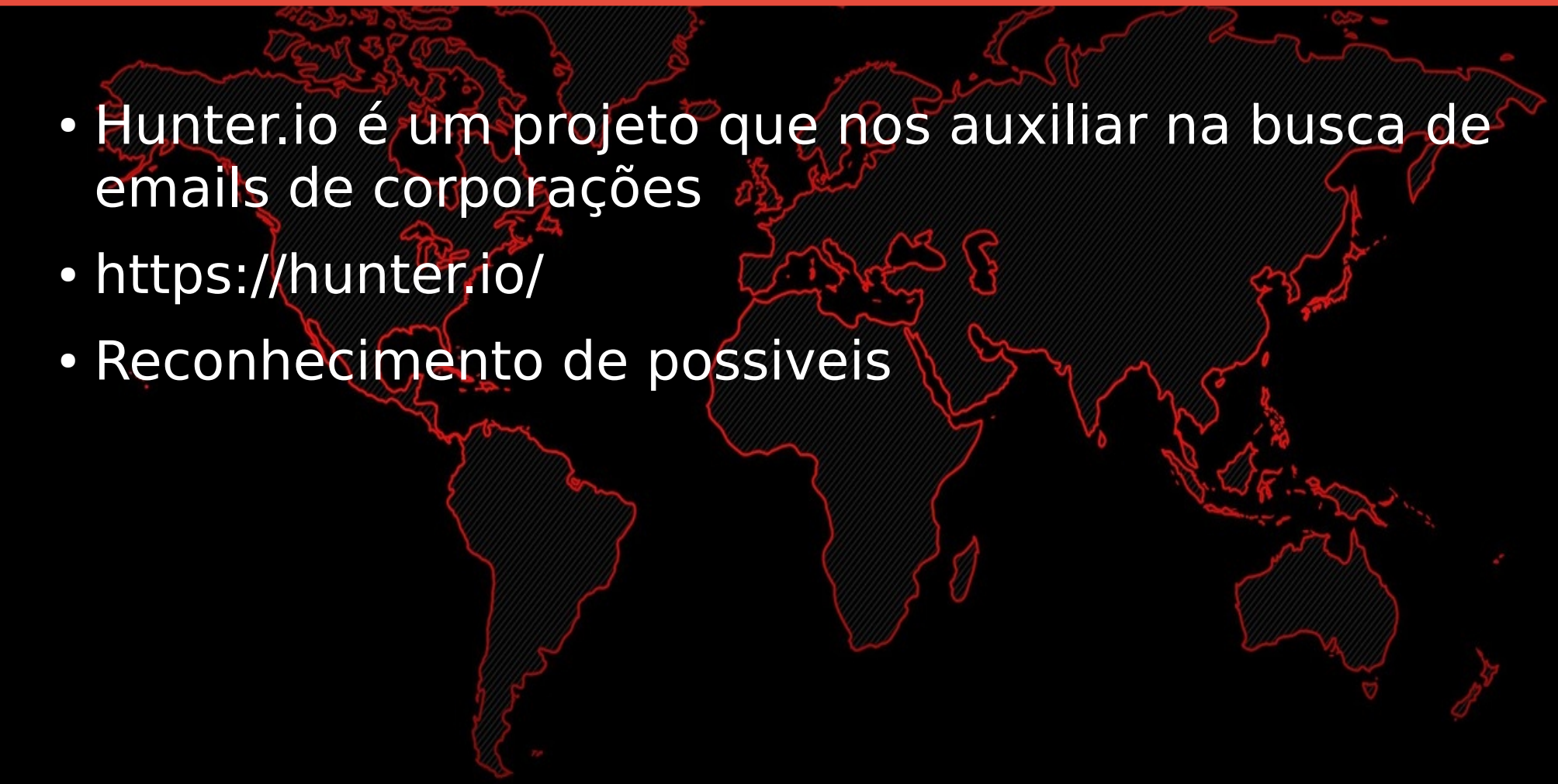
censys

OSINT – Buscando informações públicas

Informações sobre pessoas

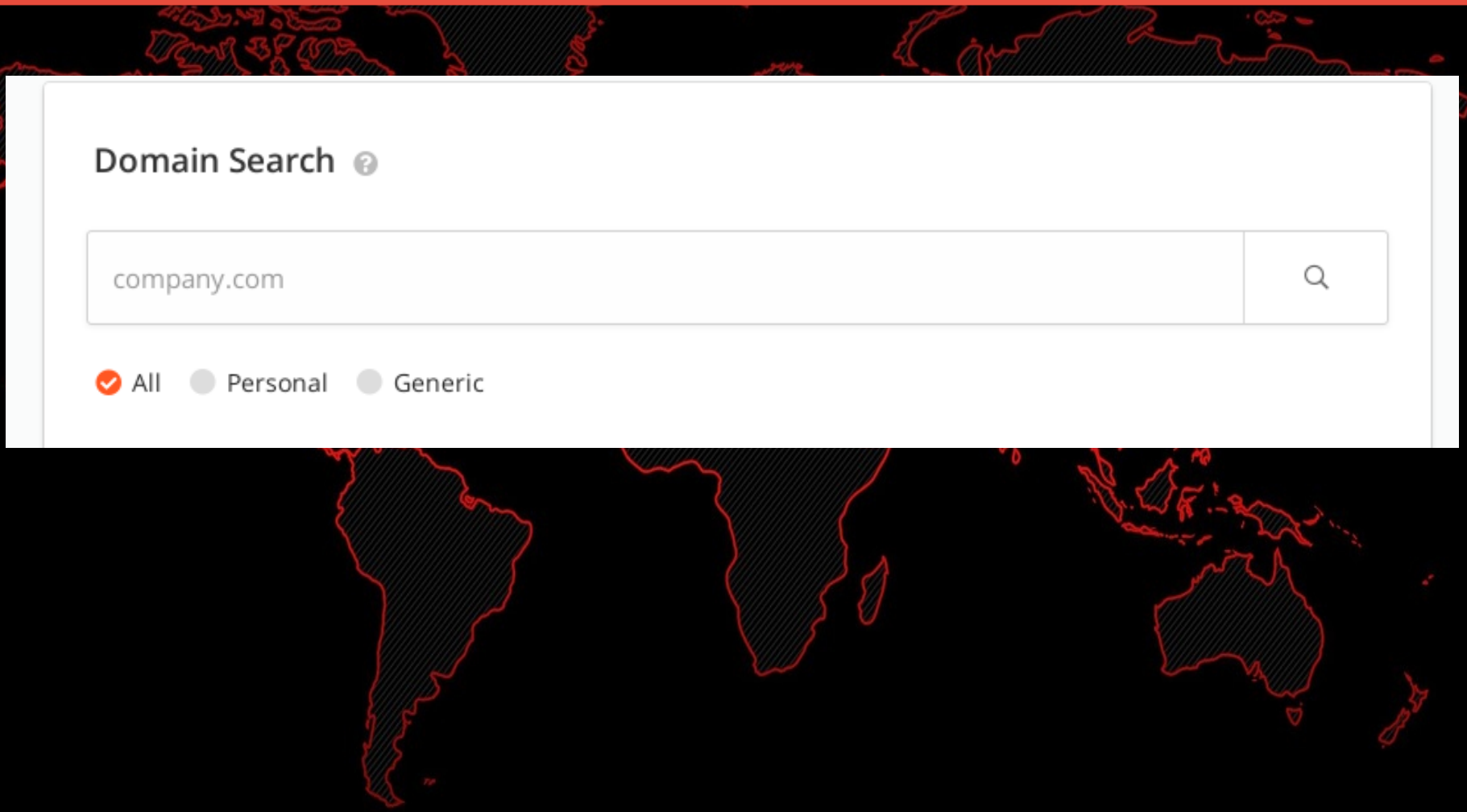
- PwnedOrNot , Sherlock , TheHarvester , Photon , Twitter-intelligence e Hunter.io

Hunter.io

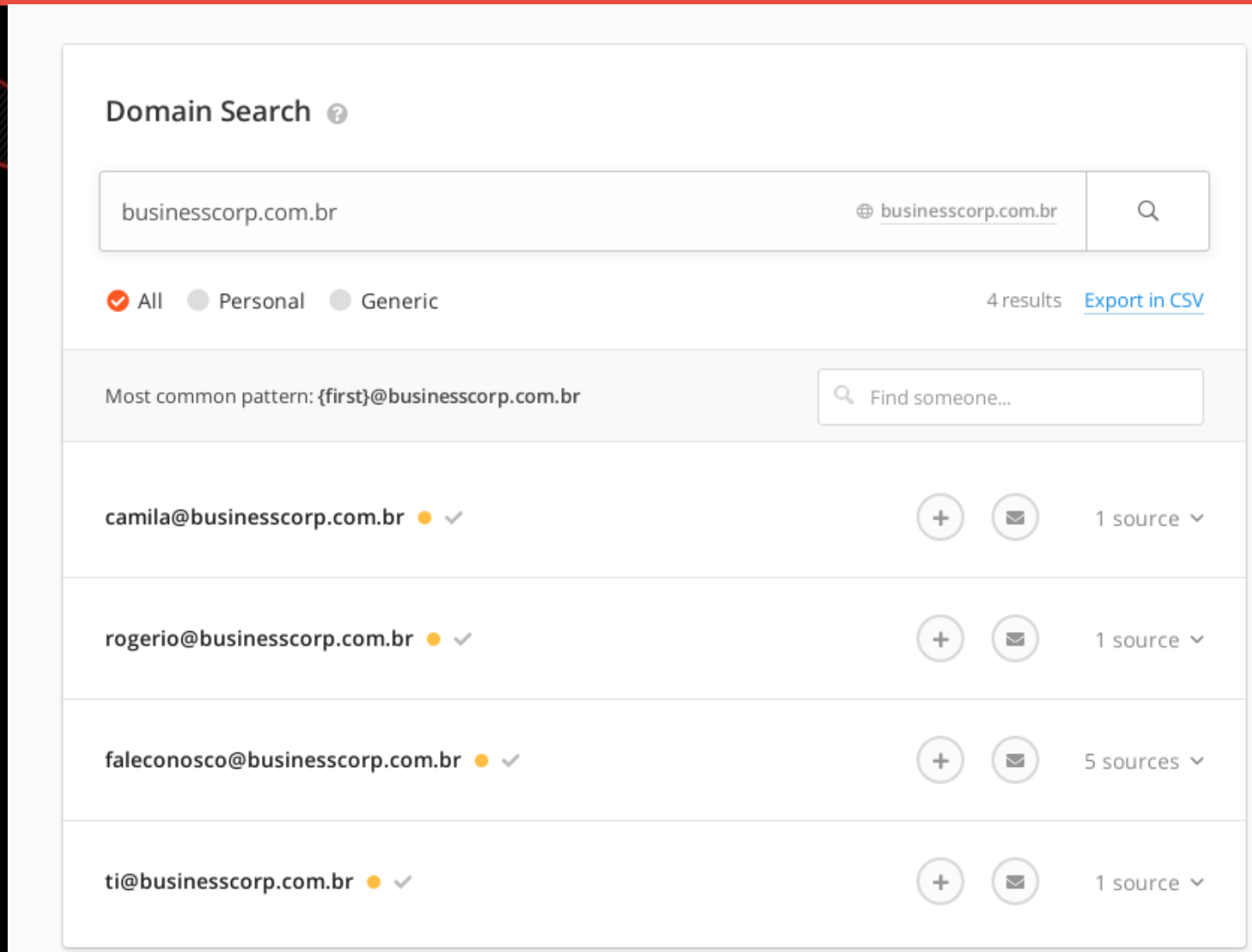


- Hunter.io é um projeto que nos auxiliar na busca de emails de corporações
- https://hunter.io/
- Reconhecimento de possiveis

Hunter.io



Hunter.io


Domain Search
businesscorp.com.br
businesscorp.com.br
All
Personal
Generic
4 results
Export in CSV
Most common pattern: {first}@businesscorp.com.br
Find someone...
camila@businesscorp.com.br
1 source
rogerio@businesscorp.com.br
1 source
faleconosco@businesscorp.com.br
5 sources
ti@businesscorp.com.br
1 source

Hunter.io

Coletando informações com Python + API

```
 % python3 script-hunter.py
{   'disposable': False,
    'domain': 'businesscorp.com.br',
    'emails': [   {   'confidence': 44,
                      url':  'http://bus
'twitter': None,
'type': 'personal',
'value': 'camila@businesscorp.com.br'},
'confidence': 44.
                      url':  'http://atcom.com.br
    'twitter': None,
    'type': 'personal',
    'value': 'faleconosco@businesscorp.com.br'},
{   'confidence': 35,
    'department': None,
    'first name': None,
                                    'type': 'personal',
                                    'value': 'rogerio@businesscorp.com.br'},
                                {   'confidence': 38,
```

Hunter.io

Coletando informações com Python + API

```
 % python3 script-hunter.py
{   'disposable': False,
    'domain': 'instagram.com',
    'emails': [   {   'confidence': 94,
                      'department': None,
                      'first_name': 'Darren',
                      'last_name': 'Romanelli',
                      'linkedin': None,
                      'phone_number': None,
                      'position': None,
                      'seniority': None,
                      'sources': [   {   'domain': 'nowre.com',
                                         'extracted_on': '2019-02
                                         'last_seen_on': '2019-04
                                         'still_on_page': True,
                                         'uri': 'http://nowre.com
                      'twitter': None,
                      'type': 'personal',
                      'value': 'romanelli@instagram.com'},
                  {   'confidence': 94,
```

Hunter.io

Coletando informações com Python + API

```
        'type': 'personal',
        'value': 'romanelli@instagram.com'},
{       'confidence': 94,
        'department': None,
        'first_name': 'Jimmy',
        'last_name': 'Barnes',
        'linkedin': None,
        'phone_number': None,
        'position': None,
        'seniority': None,
        'sources': [    {   'domain': 'eventbrite.com.au',
                            'extracted_on': '2018-10-26',
                            'last_seen_on': '2019-05-03',
                            'still_on_page': True,
                            'uri': 'http://eventbrite.com.au/e/s
        'twitter': None,
        'type': 'personal',
        'value': 'jimmybarnes@instagram.com'},
```

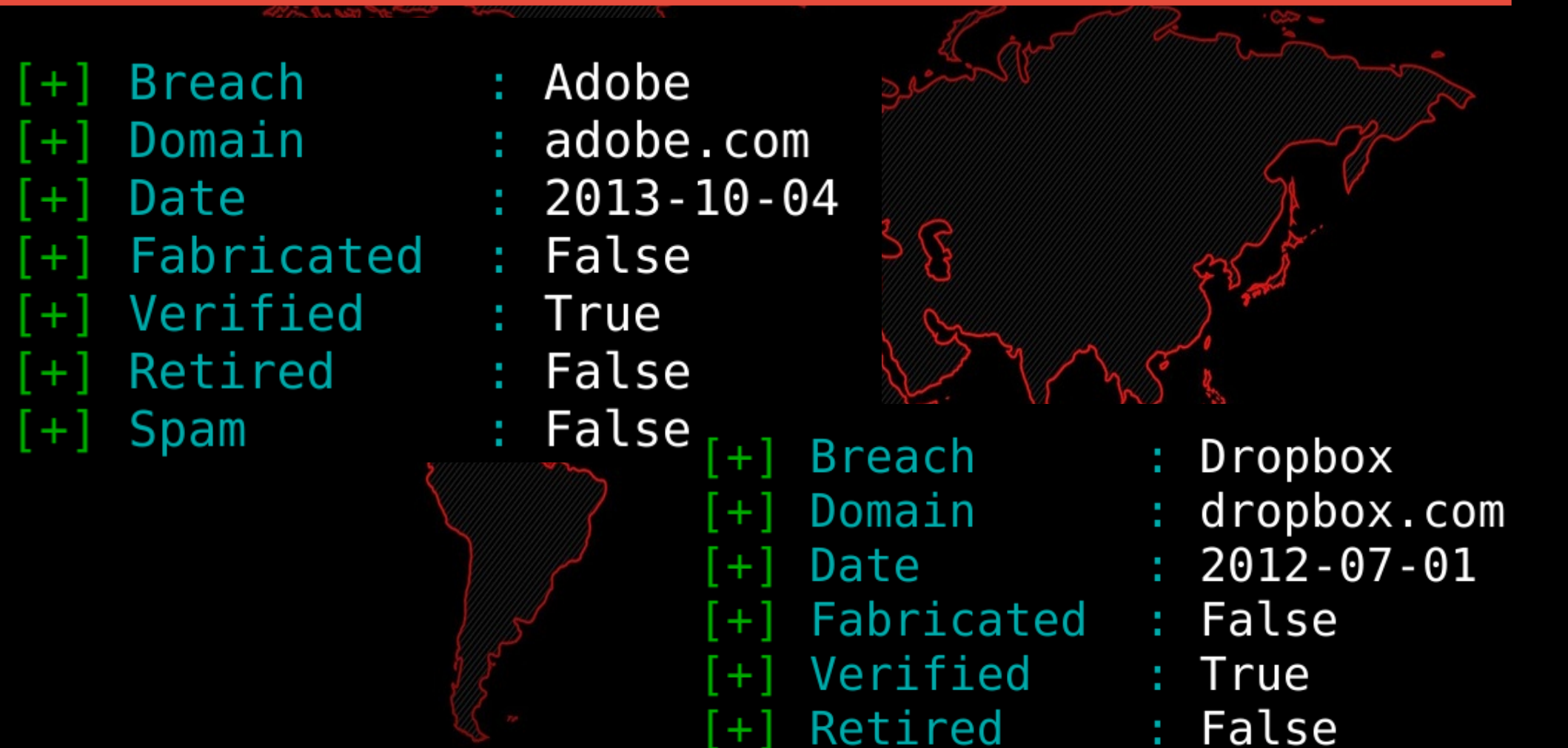
PwnedOrNot

- O pwnedOrNot usa informações OSINT
- Nos ajuda a encontrar senha
- Encontrar endereços de email comprometidos

PwnedOrNot

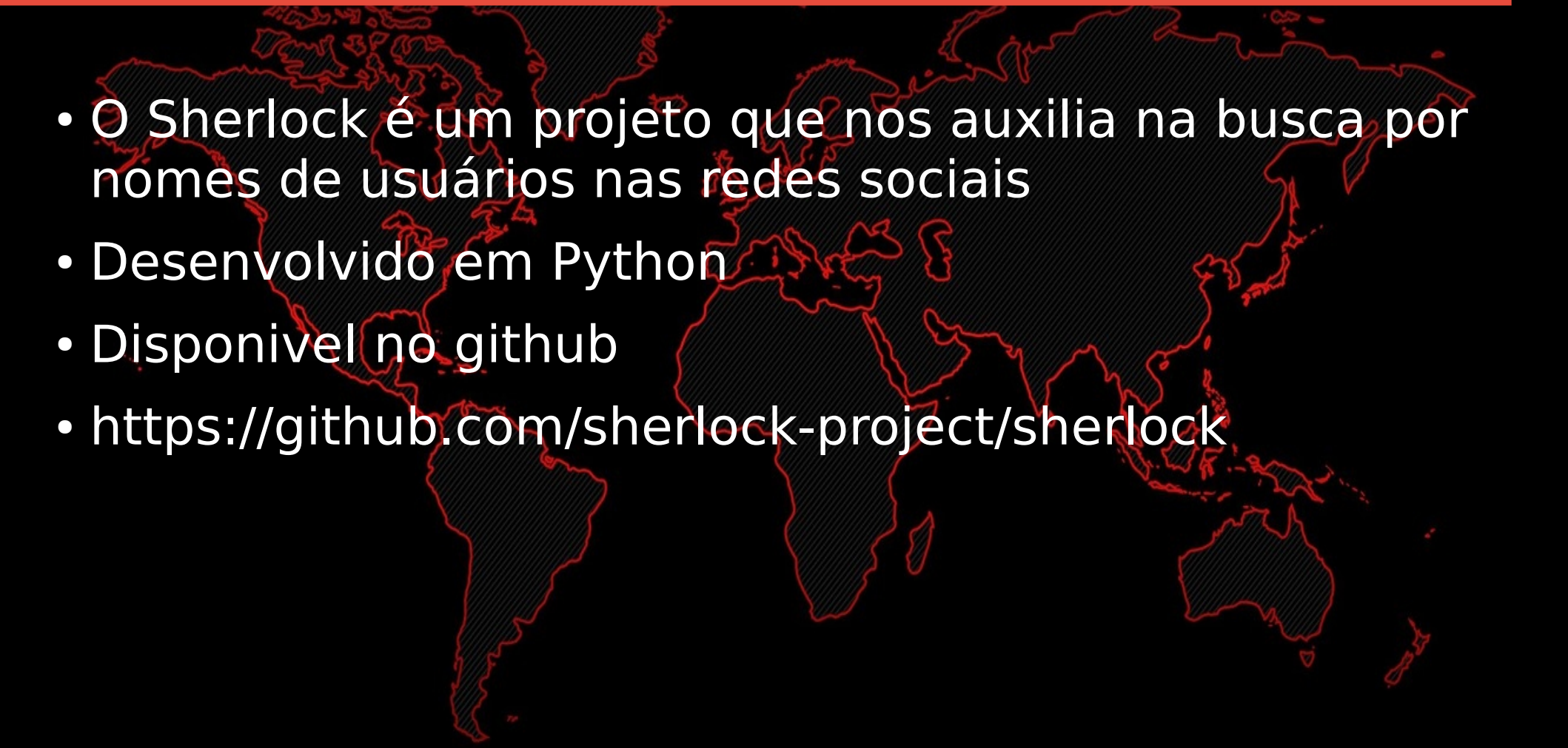
```
[+] Checking Breach status for nadine.blaser@vale.com [ pwned ]
```

PwnedOrNot



```
[+] Breach      : Adobe
[+] Domain      : adobe.com
[+] Date        : 2013-10-04
[+] Fabricated  : False
[+] Verified    : True
[+] Retired     : False
[+] Spam        : False
[+] Breach      : Dropbox
[+] Domain      : dropbox.com
[+] Date        : 2012-07-01
[+] Fabricated  : False
[+] Verified    : True
[+] Retired     : False
[+] Spam        : False
```

Sherlock



- O Sherlock é um projeto que nos auxilia na busca por nomes de usuários nas redes sociais
- Desenvolvido em Python
- Disponivel no github
- https://github.com/sherlock-project/sherlock

Sherlock


```
# clone the repo
$ git clone https://github.com/sherlock-project/sherlock.git

# change the working directory to sherlock
$ cd sherlock

# install python3 and python3-pip if not exist

# install the requirements
$ pip3 install -r requirements.txt
```

sherlock-project / **sherlock**

<> Code | Issues 25 | Pull requests 5 | Projects 1 | Wiki

🔎 Find usernames across social networks http://sherlock-project.github.io

Sherlock

```
[+] Twitch: https://m.twitch.tv/greenmind
[+] Twitter: https://www.twitter.com/greenmind
[+] Unsplash: https://unsplash.com/@greenmind
[+] VK: https://vk.com/greenmind
[+] VSCO: https://vsco.co/greenmind
[-] Venmo: Not Found!
[+] Vimeo: https://vimeo.com/greenmind
[+] VirusTotal: https://www.virustotal.com/ui/users/greenmind/tr
[+] Wattpad: https://www.wattpad.com/user/greenmind
[+] We Heart It: https://weheartit.com/greenmind
[-] WebNode: Not Found!
[+] Wikia: https://wikia.com/wiki/User:greenmind
[+] Wikipedia: https://www.wikipedia.org/wiki/User:greenmind
[-] Wix: Not Found!
[+] WordPress: https://greenmind.wordpress.com/
[-] YouNow: Not Found!
[-] YouPic: Not Found!
[-] YouTube: Not Found!
[+] Zhihu: https://www.zhihu.com/people/greenmind
[-] devRant: Not Found!
[-] iMGSRC.RU: Not Found!
[+] last.fm: https://last.fm/user/greenmind
```

Twitter-intelligence

- O projeto twitter-intelligence nos ajuda no rastreamento e analise do Twitter
- Desenvolvido em Python e disponivel no github
- https://github.com/batuhaniskr/twitter-intelligence

Twitter-intelligence

```
python3 tracking.py --username "greenmind_br"

@greenmind_br: A parte mais legal da necessidade é que ela t
es.

@greenmind_br: Init Gamehttps://twitter.com/sagazeando/statu

@greenmind_br: Init Bot ..

@greenmind_br: @shodanhq site is instability? Error 502 serv
 project :Dpic.twitter.com/0XhANBA3hw

@greenmind_br: Hello :D.


[+] 15 tweet received...
```

Twitter-intelligence

```
python3 tracking.py --query "leak password"

python3 tracking.py --query "leak passwords"
```

```
python3 tracking.py --query "leak pass"
```

Twitter-intelligence

```
python3 tracking.py --query "leak senha" 2019-05-20 2019-05-22

@MesninoOwna: #hacked #DB_leak #C00n3tTeam #OPbr #Vazamento_de_dados_lula_website URL DE USERS
: https://lula.com.br/wp-json/wp/v2/users/ … … URL USERS ADMINISTRADOR : https://lula.com.br/wp
-json/oembed/1.0/embed?url=https://lula.com.br/&format=json … … URL LOGIN : https://lula.com.br
/wp-login.php?redirect_to=https%3A%2F%2Flula.com.br%2Fwp-admin%2F&reauth=1 … … -----We Are C00n
3t Team ! ------ #OpAssange @LabDefCon @g1tecnologia

@PC00n3t: #hacked #DB_leak #C00n3tTeam #OPbr #Vazamento_de_dados_lula_website URL DE USERS : ht
tps://lula.com.br/wp-json/wp/v2/users/ … URL USERS ADMINISTRADOR : https://lula.com.br/wp-json/
oembed/1.0/embed?url=https://lula.com.br/&format=json … URL LOGIN : https://lula.com.br/wp-logi
n.php?redirect_to=https%3A%2F%2Flula.com.br%2Fwp-admin%2F&reauth=1 … -----We Are C00n3t Team !
#OpAssange @LabDefCon @g1tecnologiapic.twitter.com/uzcfRcBokB

 @PC00n3t: #hacked #leaks #Vazamento @LabDefCon @g1tecnologia #OpLulaLindo Camera Aurora [SC] LI
 NK : https://pastebin.com/c0tXeyxb by : Pep1no && Web Kiddie ------We Are C00n3t------- #FreeAs
 sange #OpAssange #OpBr @Tec_Mundopic.twitter.com/NDv66nx6zn

 @PC00n3t: #Vazamento #leaks #C00n3tTeam #OpLulaLindo @LabDefCon Se não me der uma namorada, vou
  continuar vazando, rsrs. Vazamento DETRAN Link : https://pastebin.com/erRjtcES by : Pep1no &&
 Web Kiddie ----We Are C00n3t Team----- #OpAssange #FreeAssange @g1tecnologiapic.twitter.com/Llz
 sqekCmH
```

Conclusão

- OSINT pode nos ajudar durante o reconhecimento
- Podemos buscar informações sobre vazamentos
- Podemos buscar informações sobre uma empresa
- Ajuda na espionagem e contra espionagem
- Auxilia na inteligencia comercial e competitiva

Obrigado

- https://github.com/abase-br/osint ← Material
- https://github.com/abase-br/ ← Outros materiais
- Greenmind.sec@gmail.com ← Meu contato

“A solução dos seus problemas não é dinheiro, politicos ou o governo. . . É conhecimento compartilhado!” - Ton Gadioli