

# Whoami - Quem sou eu ?

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

Fatec  
Bauru

EZ.devs

# OSINT - O que é

Esse termo é usado para descrever a inteligencia, no sentido da informação, no sentido da inteligencia, obtida atraves de dados publicos disponíveis e alguns exemplos são:

- Jornais
- Revistas
- Televisão

# Historia - Onde se iniciou

- Tudo começou no Foreign Broadcast Information Service (FBIS)
- Pioneiro no uso de Open Source Intelligence (OSINT)
- Deram início ao projeto na década de 1930 na Universidade de Princeton
- Sua função era analisar os noticiários por rádio e monitorar publicações oficiais da União das repúblicas Socialistas Soviéticas



# Historia - 11 de Setembro e o FBI

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)

Tinha como objetivo de:

- Coletar
- Reunir
- 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
- Adulterar
- Destruir
- Graças às técnicas de buscas usando OSINT podemos começar a procura de informações válidas e falhas em possíveis clientes.

# Motivação

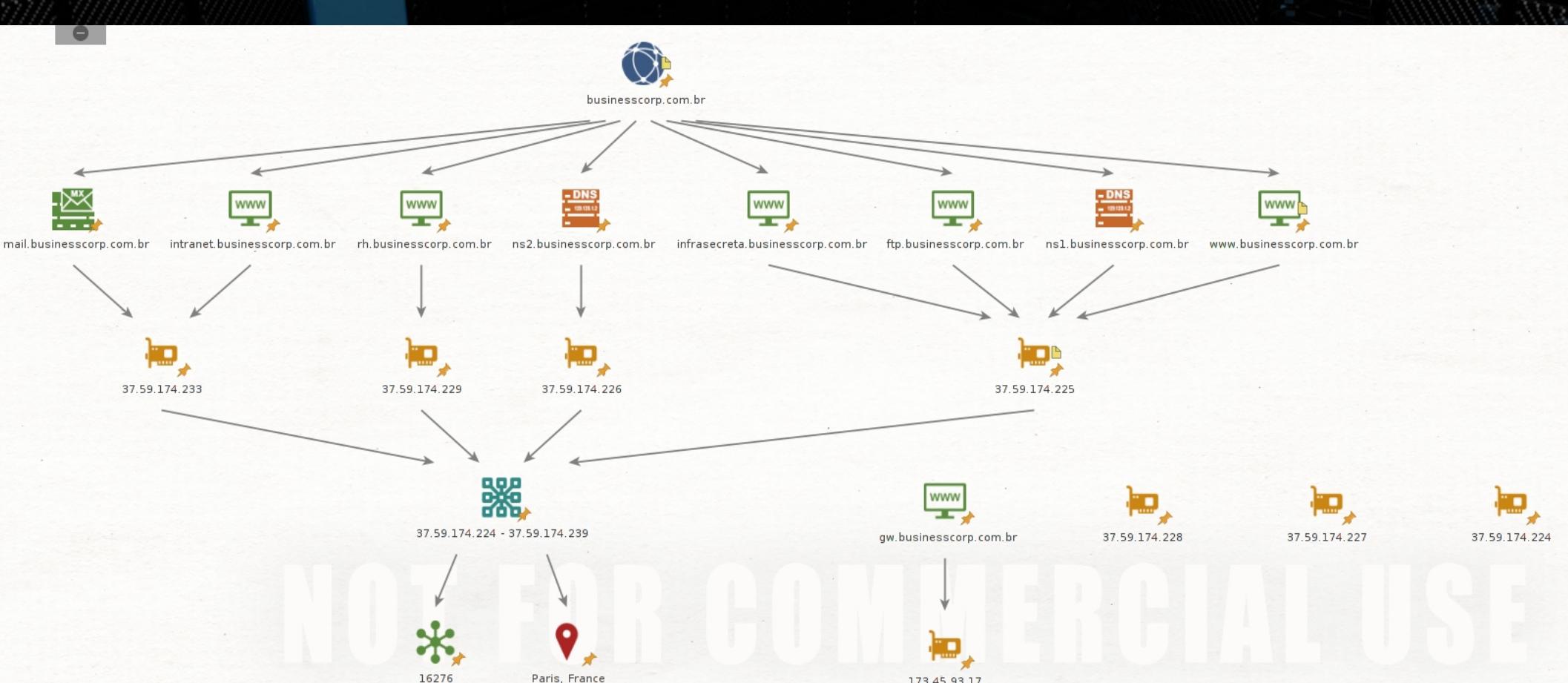
- Problemas com leis
- Problemas com permissão das empresas
- Problemas com logs
- Buscar por determinada vulnerabilidade
- Buscar por arquivos importantes
- Buscar por informações sensíveis
- Monitorar vazamentos



## OSINT - Buscando informações públicas

- Informações sobre infraestruturas

# Um pouco da meta ....



# Whois - Quem é?

## Realizando consulta com Python3 + API

```
% python3 whois-ip.py
```

```
200
```

```
inetnum: 186.192.80.0/20
aut-num: AS28604
abuse-c: CSGL0
owner: Globo Comunicação e Participações SA
ownerid: 27.865.757/0024-90
responsible: Regina Sampaio
country: BR
c: RES59
:: CTG6
w: 186.192.80.0/20
ir: ns01.oghost.com.br
:: 20190524 AA
aa: 20190524
ir: ns04.oghost.com.br
:: 20190524 AA
aa: 20190524
ir: ns03.oghost.com.br
:: 20190524 AA

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

nic-hdl-br: CSGL0
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
```

# 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
```

ENTERING THE IP

# Sharingmyip - Sites que usam mesmo IP

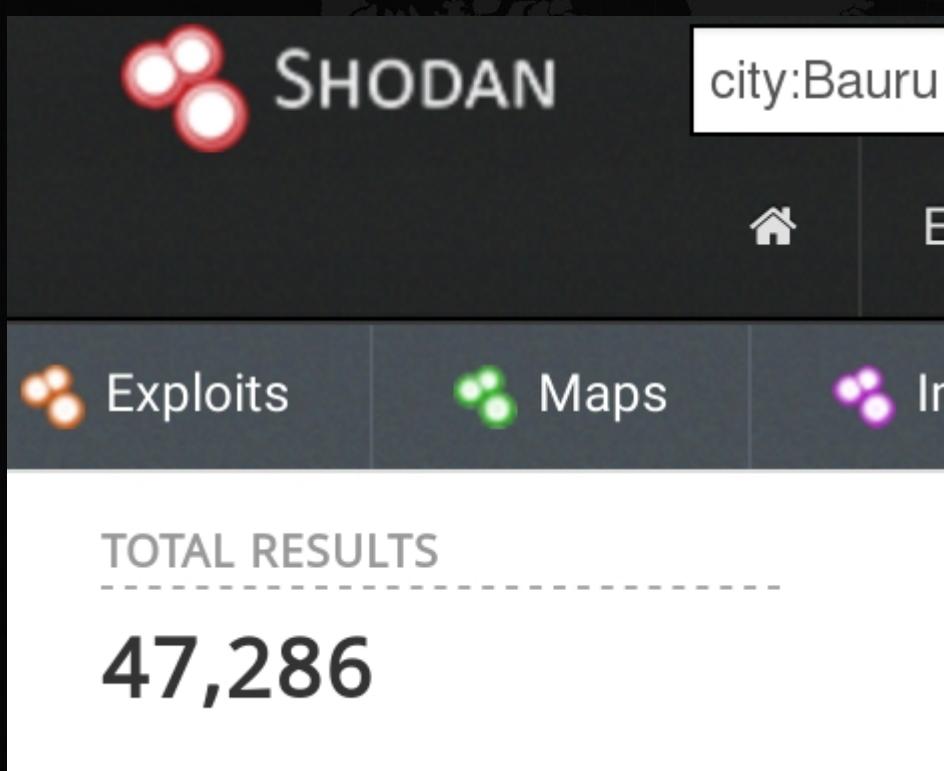
## Coleta de dados com Python3

```
% 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
```

# Shodan - Operadores



SHODAN

city:Bauru

Exploits Maps

TOTAL RESULTS  
47,286

This image shows the Shodan search interface. The search query is "city:Bauru". The results section displays a total of 47,286. Navigation links for "Exploits", "Maps", and "Info" are visible.



SHODAN

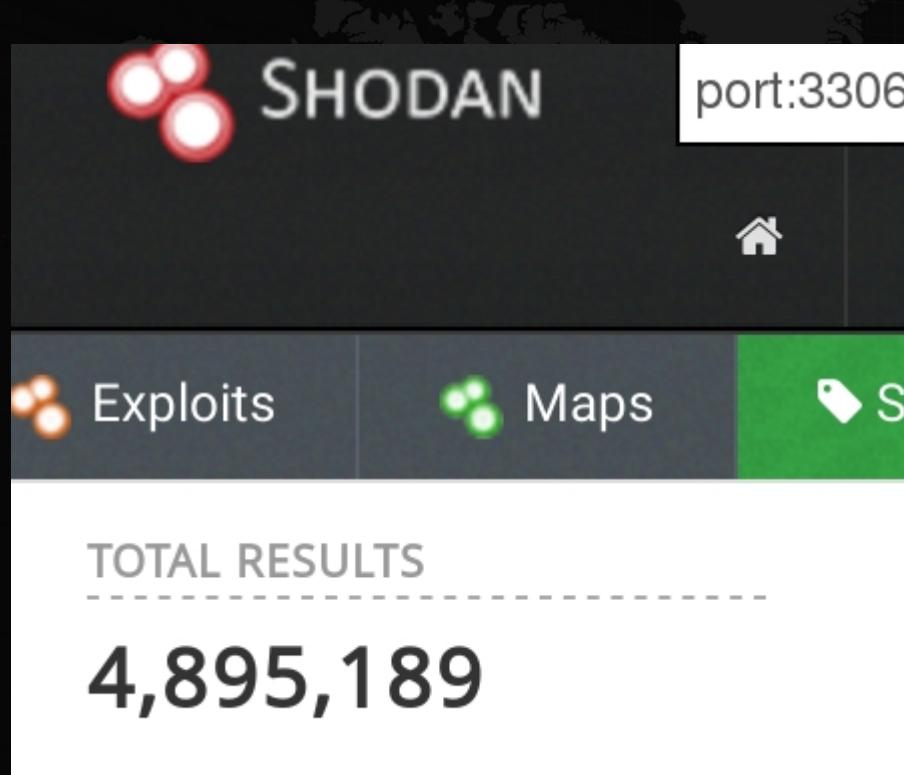
country:br

Exploits Maps

TOTAL RESULTS  
10,204,527

This image shows the Shodan search interface. The search query is "country:br". The results section displays a total of 10,204,527. Navigation links for "Exploits", "Maps", and "Info" are visible.

# Shodan - Operadores



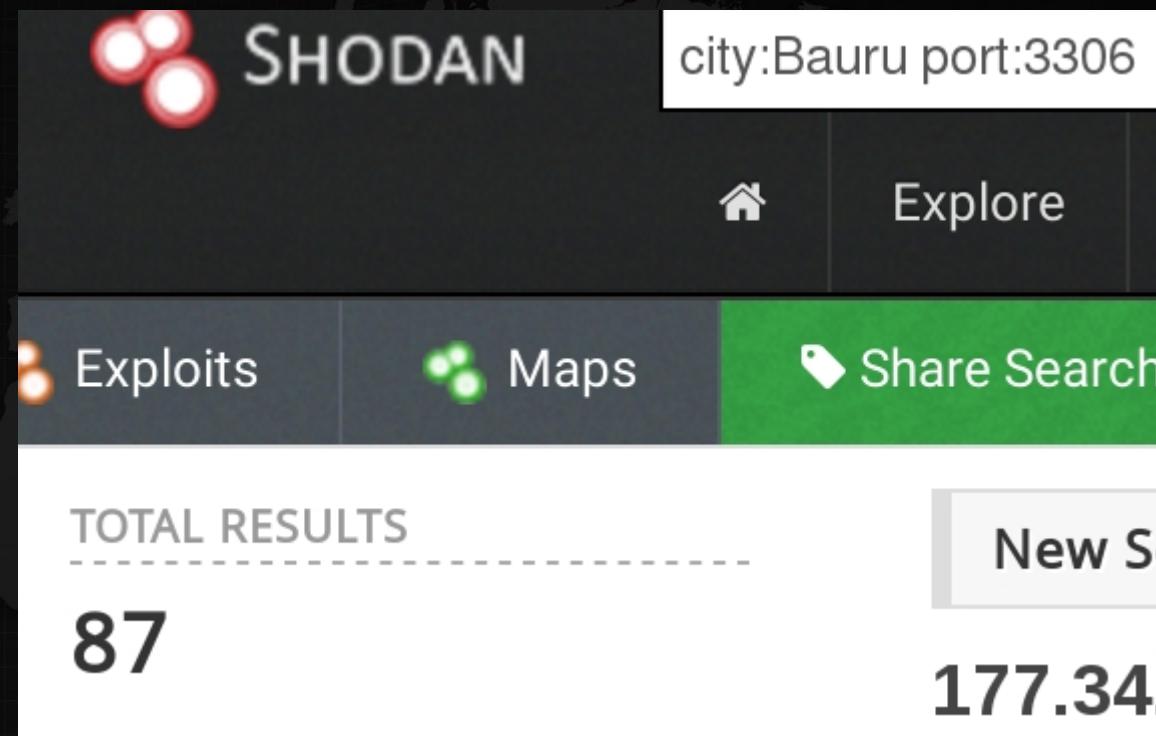
SHODAN

port:3306

Exploits Maps Share Search

TOTAL RESULTS  
4,895,189

This screenshot shows the Shodan search interface. The search bar at the top contains the query "port:3306". Below the search bar, there are navigation links for "Exploits", "Maps", and "Share Search". The main results area is titled "TOTAL RESULTS" and displays the number "4,895,189". The background features a world map with a grid pattern.



SHODAN

city:Bauru port:3306

Explore

Exploits Maps Share Search

TOTAL RESULTS  
87

New S  
177.34

This screenshot shows the Shodan search interface with a more specific query: "city:Bauru port:3306". The search results are displayed in a table with columns for "Exploits", "Maps", and "Share Search". The "TOTAL RESULTS" section shows the number "87". A "New S" button is visible on the right. The background features a world map with a grid pattern.

# Shodan - Operadores

## Ports

21

22

53

80

## ⚡ Web Technologies



jQuery



jQuery Migrate



Modernizr

# 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 - 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-2013-5704	CVE-2017-3169	CVE-2018-100098
-0231	CVE-2017-7679	CVE-2013-2249	CVE-2016-4975	CVE-2017-3167	CVE-2017-3169	CVE-2018-100098
-7668	CVE-2013-6438	CVE-2012-2687	CVE-2017-3167	CVE-2017-3169	CVE-2017-3169	CVE-2018-100098
-0098	CVE-2013-1862	CVE-2016-8612				

```
Ports:
```

```
21/tcp ProFTPD (1.3.4a)
```

```
22/tcp OpenSSH (6.0p1 Debian 4+deb7u2)
```

```
53/udp
```

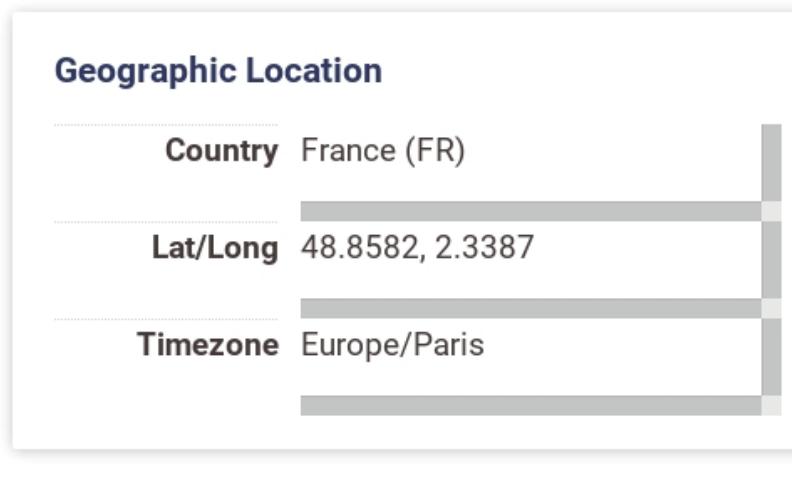
```
80/tcp Apache httpd (2.2.22)
```

# 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 -



# Hunter.io

## Domain Search

businesscorp.com.br  

All  Personal  Generic 4 results [Export in CSV](#)

Most common pattern: {first}@businesscorp.com.br 

camila@businesscorp.com.br  	  1 source 
rogerio@businesscorp.com.br  	  1 source 
faleconosco@businesscorp.com.br  	  5 sources 
ti@businesscorp.com.br  	  1 source 

# 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



# 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 #0Pbr #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](https://lula.com.br/wp-login.php?redirect_to=https%3A%2F%2Flula.com.br%2Fwp-admin%2F&reauth=1) ... -----We Are C00n3t Team ! ----- #0pAssange @LabDefCon @g1tecnologia

@PC00n3t: #hacked #DB\_leak #C00n3tTeam #0Pbr #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](https://lula.com.br/wp-login.php?redirect_to=https%3A%2F%2Flula.com.br%2Fwp-admin%2F&reauth=1) ... -----We Are C00n3t Team ! #0pAssange @LabDefCon @g1tecnologiapic.twitter.com/uzcfRcBokB

@PC00n3t: #hacked #leaks #Vazamento @LabDefCon @g1tecnologia #0pLulaLindo Camera Aurora [SC] LINK : <https://pastebin.com/c0tXeyxb> by : Pep1no && Web Kiddie -----We Are C00n3t----- #FreeAssange #0pAssange #0pBr @Tec\_Mundopic.twitter.com/NDv66nx6zn

@PC00n3t: #Vazamento #leaks #C00n3tTeam #0pLulaLindo @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---- #0pAssange #FreeAssange @g1tecnologiapic.twitter.com/LlzsqekCmH

# LGPD e o futuro

- A Lei Geral de Proteção de Dados Pessoais
- É a legislação brasileira que regula as atividades de tratamento de dados pessoais
- Altera os artigos 7º e 16 do Marco Civil da Internet

# O uso de informações publicas

- Podemos usar toda informação publica
- Não quebramos nenhum sistema de segurança
- Temos diversas fontes de informações

# 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](mailto:Greenmind.sec@gmail.com) ← Meu contato

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