

OSINT : Open Source Intelligence

Mickael Rigonnaux

Twitter : @tzkuat

mickael.rigonnaux@rm-it.fr

<https://net-security.fr>

Plan

- Introduction & Définitions
- Méthodologie
- Exemples & explications techniques
- Conclusion & Questions
- Démo / Pratique ?

Définition “Intelligence”

- HUMINT – Human Intelligence
- SIGINT – Signal Intelligence
- GEOINT – Imagery Intelligence
- OSINT – Open Source Intelligence

Intelligence = Renseignement

“Ensemble des activités coordonnées de collecte, de traitement et de diffusion de l’information utile à un acteur, en vue de son exploitation.”

Open Source Intelligence (OSINT)

La source a-t-elle délivré l'information de son plein gré ?

- Oui → Info. ouverte
- Non → Info. fermée

OSINT = collecte de source ouverte

Pourquoi l'OSINT ?

- Mettre en place une veille (pro/perso)
- Cartographier son environnement
- Préparation d'un audit/red-team
- Rechercher des informations ciblées

L'OSINT ne concerne pas seulement le WEB

Rappel – Loi

- Loi Godfrain

“Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.”

- Code pénal – Art 226-4

“L'introduction dans le domicile d'autrui à l'aide de manoeuvres, menaces, voies de fait ou contrainte, hors les cas où la loi le permet, est puni d'un an d'emprisonnement et de 15 000 euros d'amende.”

OSINT : Open Source Intelligence

Méthodologie

Le marché et l'entreprise

- Analyse du marché
- Capital
- Historique
- Recherche document
- Société.com



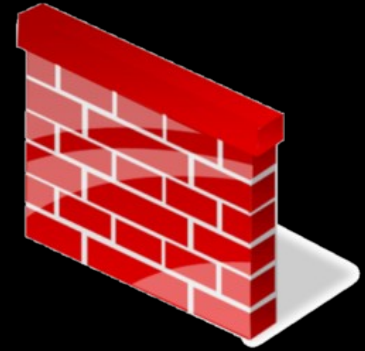
Emplacement Physique

- Localisation géographique
 - Trouver la localisation géographique d'une personne ou d'une entreprise
 - Google Maps, Yahoo, Qwant Maps, etc



Information sur l'infrastructure

- Block de réseau
- Email
- Technologies utilisées
- Accès distant
- Applications
- Moyens de défenses



Employés - Réseaux sociaux

- Recherche LinkedIn
 - Liste des employés
- Vérification des publications
 - Informations sur l'entreprise
- Fréquence des publications



Recherche sur les employés

- Email
- Pseudo personnel
- Nom de domaine perso?
- IP publique

Plus concrètement

Exemples & outils

Recherches

- Google, Qwant, Yandex, etc.
- Societe.com
- WayBackMachine
- LinkedIn
- Dorks



Google Dorks

- `inurl:password`
- `intext:confidentiel`
- `site:ynov.com`
- `ext:pdf`
- `filetype:xls`



<https://www.exploit-db.com/google-hacking-database>

<https://korben.info/google-dorks-2019-liste.html>

Google Dorks

inurl:payline ext:pdf restraint

Tous Actualités Images Vidéos Shopping Plus Paramètres Outils

2 résultats (0,23 secondes)

[PDF] Annexe juridique Données à caractère personnel - Payline
https://www.payline.com/sites/default/.../annexe_juridique_clients_v1e_juin_2019.pdf ▼
6 juin 2019 - C2 –restraint. Page : 1/10. « Page 1 / 10 ». Ce document est la propriété exclusive de MONEXT. Toute reproduction intégrale ou partielle, toute ...

inurl:payline ext:pdf réseau

Tous Actualités Images Shopping Vidéos Plus Paramètres Outils

4 résultats (0,28 secondes)

PAYLINE-GUIDE-Descriptif des appels webservices-FR-v2.Y - Citelis
www.citelis.fr/wp.../PAYLINE-GUIDE-Descriptif-des-appels-webservices-FR-v2.Y.pdf ▼
order. deliveryMode. Mode de livraison : 1 : retrait de la marchandise chez le marchand. 2 : Utilisation d'un réseau de points-retrait tiers (type kiala, alveol, etc.).

inurl:monext ext:pdf audit

Tous Actualités Images Maps Vidéos Plus Paramètres Outils

Environ 4 résultats (0,34 secondes)

[PDF] Certificate of Compliance MONEXT - PAYLINE
https://www.monext.fr/.../monext_pcidss_payline_certificate-of-co... ▼ Traduire cette page
30 nov. 2017 - The Report on Compliance (RoC) and Attestation of Compliance (AoC) were completed by the QSA accordingly to the PCI DSS Security. Audit ...

La plate-forme d'acquisition internationale de Monext certifiée PCI DSS
www.kable-cf.com/data/file/monext/CP_Monext_acquisition_internationale.pdf
21 nov. 2011 - L'audit a été réalisé par XMCO, cabinet de conseil en sécurité des Systèmes d'Information. Monext devient ainsi le premier et unique acteur ...

[PDF] MONEXT Acheives Continous PCI Compliance with Tufin
<https://web.tufin.com/.../continuous-pci-dss-compliance-Monext-ca...> ▼ Traduire cette page

inurl:monext ext:pdf rapport

Tous Actualités Images Maps Vidéos Plus Paramètres Outils

4 résultats (0,24 secondes)

[PDF] Bilan Monext en 2017
https://www.monext.fr/sites/default/files/.../180213_-_monext_-_bilan_2017_fin.pdf ▼
13 févr. 2018 - Avec une progression de 25% par rapport à l'année précédente du nombre de transactions traitées, Monext se positionne comme un acteur ...

Google Dorks



Google

intitle:"Index of" secret

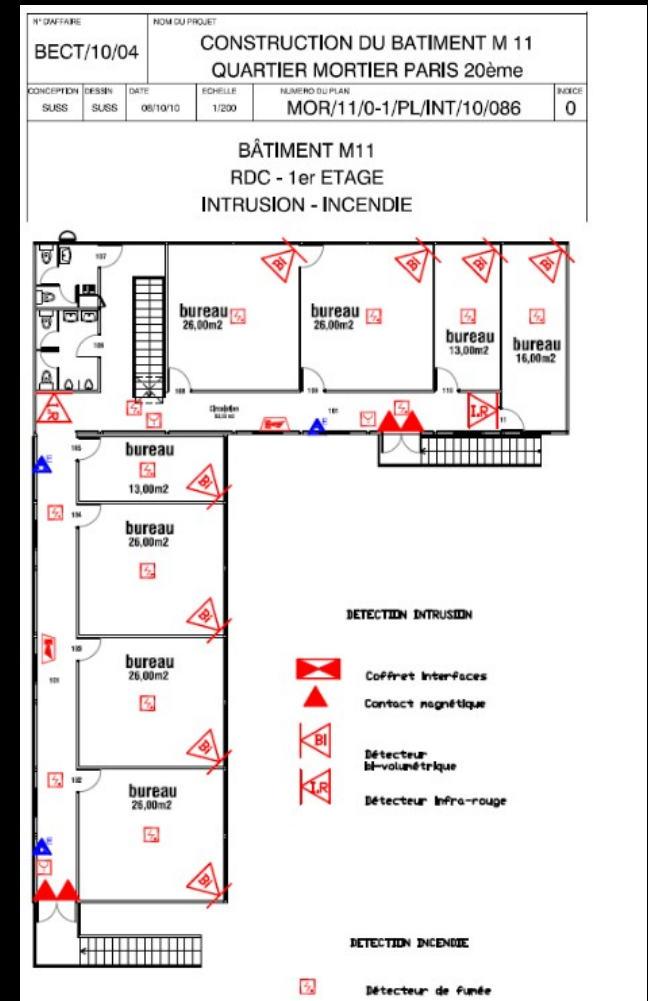
Tous Images Vidéos Actualités Shopping Plus Paramètres Outils

Environ 1 040 000 résultats (0,51 secondes)

Conseil : Recherchez des résultats uniquement en français. Vous pouvez indiquer votre langue de recherche sur la page Préférences.

Index of /secret
cicerone-tandem.fr > secret ▼
Index of /secret. Icon Name Last modified Size Description. [PARENTDIR] Parent Directory - [TXT] htaccess.txt 2013-02-13 15:05 13 [TXT] passlist.txt 2013-02-13 ...

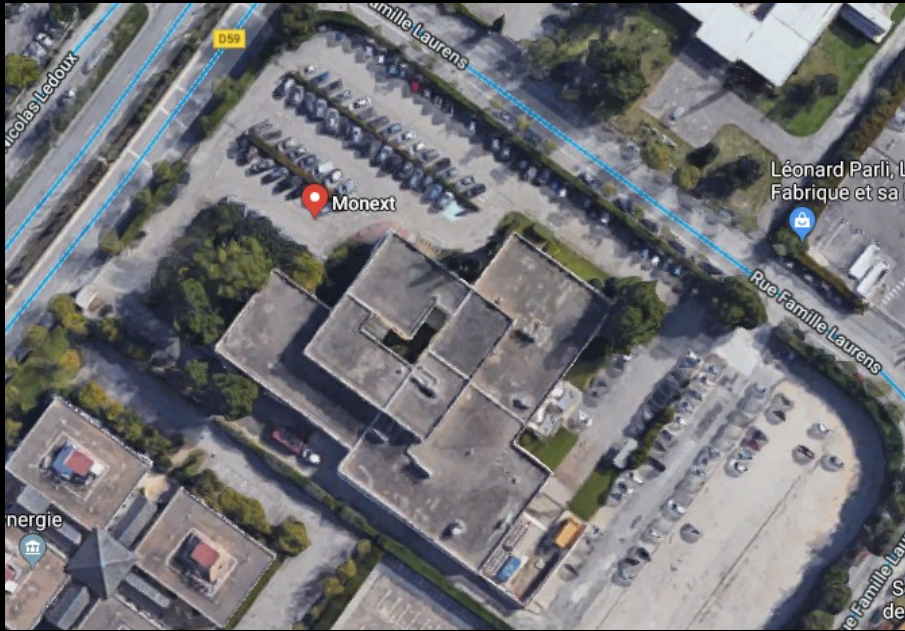
Index of /secret - Pentester Academy Lab
pentesteracademylab.appspot.com > secret ▼ Traduire cette page
Index of /secret. Parent Directory; credit-card.txt. Credit Card.txt Contents. 4738 8334 2323 9898 <-- Vivek's Credit Card Number :)



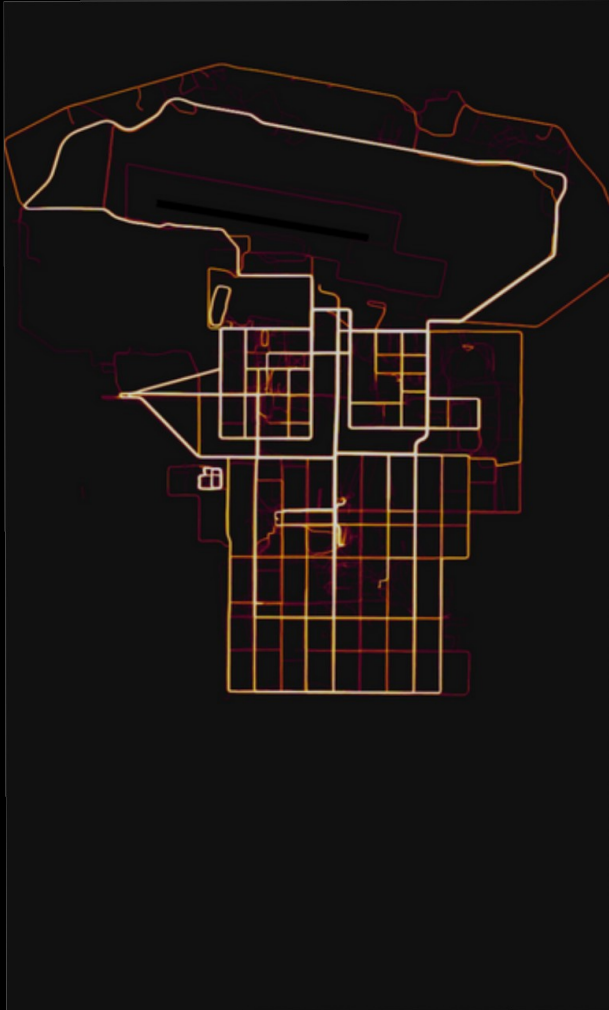
Maps : Monext



Maps : Monext



Strava : Armée américaine



Recherche technique











- Les domaines ?
- Les sous domaines ?
- Plages IP ?
- Technologies utilisées ?
- Les mails ?
- Les moyens de défenses ?
- Les accès distants ?

Recherche technique

RIPE

<input checked="" type="checkbox"/>	Highlight RIPE NCC managed values
inetnum:	193.27.68.0 - 193.27.69.255
netname:	SQLI
country:	FR
org:	ORG-SS149-RIPE
admin-c:	MP17442-RIPE
admin-c:	SC10224-RIPE
tech-c:	MP17442-RIPE
tech-c:	SC10224-RIPE
status:	ASSIGNED PI
mnt-by:	RIPE-NCC-END-MNT
mnt-by:	NEO-MNT
mnt-routes:	NEO-MNT
mnt-domains:	NEO-MNT
created:	2010-03-23T13:43:55Z
last-modified:	2016-04-14T10:30:38Z
source:	RIPE
sponsoring-org:	ORG-NTG3-RIPE

Spyse

Subdomains	sqli.com
Filters	Results — 147
CIDR — 6	
193.27.68.0/24 (24)	 ishare.airbus.sqli.com
193.27.69.0/24 (7)	IP 41.137.123.150   Morocco
194.230.101.0/24 (3)	 proxyrabat.sqli.com
41.137.123.0/24 (2)	IP 41.137.123.150   Morocco
193.105.238.0/24 (1)	 reverseproxy-oujda.sqli.com - 401 U
81.192.97.0/24 (1)	IP 81.192.97.231   Morocco
 hide	

Recherche technique

- <https://dnsdumpster.com/>
- Certificate Transparency
- Sublister

Rechercher des certificats par nom d'hôte

sqli.com



☐ Inclure les certificats arrivés à échéance

☒ Inclure les sous-domaines

État actuel :

Autorité de certification	Nombre de certificats émis	
C=FR, O=Gandi, L=Paris, ST=Paris, CN=Gandi Standard SSL CA 2	33	Filtrer
C=US, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, L=Scottsdale, ST=Arizona, CN=Go Daddy Secure Certificate Authority - G2	1	Filtrer
C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	220	Filtrer
C=US, O=CloudFlare, Inc., L=San Francisco, ST=CA, CN=CloudFlare Inc RSA CA-1	1	Filtrer
C=US, O=CloudFlare, Inc., L=San Francisco, ST=CA, CN=CloudFlare Inc ECC CA-2	1	Filtrer
C=US, O=Amazon, OU=Server CA 1B, CN=Amazon	1	Filtrer

SUBLISTER

Coded By Ahmed Aboul-Ela - @aboul31a

```
[*] Enumerating subdomains now for sqli.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
[*] Total Unique Subdomains Found: 196
www.sqli.com
ae1-suisse.sqli.com
www.ae1-suisse.sqli.com
gitlab.agency.sqli.com
project.agency.sqli.com
agency-recette.sqli.com
agendas-lyon.sqli.com
agora-pocbigdata-cloudera-toulouse.sqli.com
agora-pocbigdata-hue-toulouse.sqli.com
ishare.airbus.sqli.com
amundi-gsm-pb.sqli.com
amundi-gsm-sg.sqli.com
apache-ly.sqli.com
app.sqli.com
app2.sqli.com
app4.sqli.com
appsan.sqli.com
blog.atlantique.sqli.com
autodiscover.sqli.com
bd.sqli.com
bmci.sqli.com
booster.sqli.com
bordeaux.sqli.com
```

Recherche technique

- Firewall

Fortinet, ForcePoint/StoneSoft, PaloAlto Switch, Cisco, Arista, Passerelles SSL, F5 APM, Pulse Secure

- Proxy

TrendMicro, Squid, SS5, Routeurs, Juniper, Passerelles messagerie, Cisco ESA IronPort

- ReverseProxy

DenyAll, LoadBalancer, A10 Networks, F5, DNS, Bind

Environnement technique : PaloAlto, Checkpoint, ReverseProxy F5, CISCO, VPN, MPLS, Load Balancing A10, X25.

Alternance – Assistant(e) Cyber Sécurité F/H - Offres d'emploi | Monext


<https://www.monext.net/fr/offres/alternance-assistante-cyber-securite-fh> ▼


Réaliser une étude cyber-sécurité,; Traiter les demandes des certificats et clés de sécurité,; Maintenir et faire évoluer les outils Wazhu et Suricata. Au quotidien ...

- Contrôle de la conformité par rapport au standard sécurité Monext Système d'exploitation (Windows),
- Contrôle de la conformité par rapport au standard sécurité Monext Bases de Données (PostgreSQL),
- Contrôle de la conformité par rapport au standard sécurité Web (Apache, Tomcat, PHP et Drupal).

Vous serez amené(e) à travailler avec des équipes variées système, réseau, bases de données, exploitation, développement.

Shodan + Dorks

 SHODAN




[Home](#) [Explore](#) [Downloads](#) [Reports](#) [Pricing](#) [Enterprise Access](#) [My Account](#)

[Exploits](#) [Maps](#) [Share Search](#) [Download Results](#) [Create Report](#)

TOTAL RESULTS

71

TOP COUNTRIES



France 71

TOP SERVICES

HTTPS	30
HTTP	30
HTTP (8080)	2
DNS	2
SMTP	2


New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

301 Moved Permanently

193.27.68.31

SQLI SA

Added on 2019-11-27 09:08:37 GMT

 France, Villeneuve-la-garenne

HTTP/1.1 301 Moved Permanently

Date: Wed, 27 Nov 2019 09:08:31 GMT

Server: Apache/2.4.10 (Debian)

X-Frame-Options: SAMEORIGIN

Location: http://www.sqli-carrieres.com:808

Content-Length: 320

Connection: close


Content-Type: text/html; charset=iso-8859-1

302 Found

193.27.68.31

SQLI SA

Added on 2019-11-27 20:44:22 GMT

 France, Villeneuve-la-garenne


HTTP/1.1 302 Found

Date: Wed, 27 Nov 2019 20:44:22 GMT

Server: Apache/2.4.10 (Debian)

X-Frame-Options: SAMEORIGIN

Location: https://www.sqli-carrieres.com/

 193.27.68.169 [View Raw Data](#)

City	Villeneuve-la-garenne
Country	France
Organization	SQLI SA
ISP	SQLI SA
Operating System	Linux 3.x
Last Update	2019-11-28T01:25:17.293904
ASN	AS50778

Ports

80

443

Services

80

tcp

http

Apache httpd Version: 2.2.22

HTTP/1.1 200 OK

Date: Thu, 28 Nov 2019 01:25:30 GMT

Server: Apache/2.2.22 (Debian)

Last-Modified: Wed, 10 Dec 2014 17:18:00 GMT

ETag: "c12a8-b1-509dfd779d34e"

Accept-Ranges: bytes

Content-Length: 177

Content-Type: text/html

443

tcp

https


Apache httpd Version: 2.4.29


HTTP/1.1 200 OK


Date: Thu, 21 Nov 2019 02:28:58 GMT

Server: Apache/2.4.29 (Ubuntu)

Last-Modified: Mon, 19 Aug 2019 14:45:55 GMT

 Web Technologies

 jQuery

 Vulnerabilities

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

CVE-2017-7679

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

CVE-2018-1312

In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Shodan + Dorks

90 millions d'enregistrements de données personnelles divulgués sur Internet par la Chine

Via un serveur Elasticsearch non sécurisé

Le 9 juillet 2019 à 22:25, par [Bill Fassinou](#) | [0 commentaire](#)



139 PARTAGES

TrueDialog, spécialiste du SMS, au cœur d'une fuite de données massive

Par [Mathieu Chartier](#) ([@chartier_mat](#)) | Publié le 03/12/19 à 17h16

Partager :



COMMENTER

CHINE : UNE BASE DE DONNÉES EN FUITE LISTE LES FEMMES PRÊTES À PROCRÉER

Bastien L 12 mars 2019 Sécurité [Ecrire un commentaire](#)

Shodan + Dorks

SHODAN

Exploits Maps **Share Search** Download Results Create Report

TOTAL RESULTS
403

TOP COUNTRIES

South Africa 403

TOP CITIES
Johannesburg 403

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

156.255.149.202
icidc Network
Added on 2019-11-28 10:05:59 GMT
South Africa, Johannesburg

database

Database Name	Size
mulu2019	3.6 GB
config	132.0 kB
local	64.0 kB

3.6 GB **4 Databases**

MongoDB Server Information

```
{
  "metrics": {
    "commands": {
      "updateUser": {
        "failed": 0,
        "total": 0
      },
      "killAllSessions": {
        "failed": 0,
        "total": 0
      },
      "dropRole": ...
    }
  }
}
```

SHODAN

Exploits Maps Images **Share Search** Download Results Create Report

TOTAL RESULTS
732

TOP COUNTRIES

China 388
Germany 163
United States 72

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

104.199.66.247
247.66.199.104.bc.googleusercontent.com
Google Cloud
Added on 2019-11-28 13:18:35 GMT
United States, Mountain View

cloud database

Cluster Name	gamerprices
Status	green
Number of Indices	5

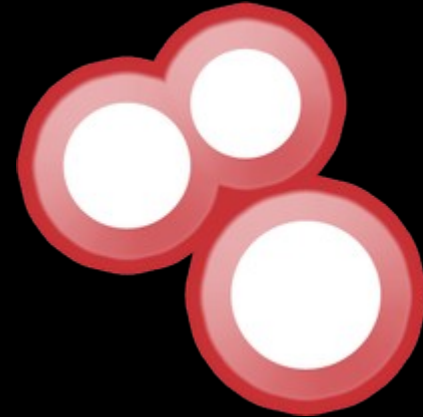
4.0 GB **3 Nodes**

HTTP/1.1 200 OK
content-type: application/json; charset=UTF-
content-length: 500

Elastic Indices:
es_product
search
gamemaster
game
product_search

Shodan Dorking

- net:192.178.2.0/24
- port:8080
- country:FR
- http.title:"SCADA"
- os:"Windows 10"



<https://github.com/jakejarvis/awesome-shodan-queries>

Recherche mail

<https://hunter.io>

sqli.com

Find email addresses

Most common pattern: {f}{last}@sqli.com

143 email addresses

c lien@sqli.com ✓

g andjean@sqli.com ✓

c lko@sqli.com ✓

i o@sqli.com ✓

k dford@sqli.com ✓

138 more results for "sqli.com"



sqli



Accueil



Réseau



Emplois



Messagerie

Noti

Personnes

Emplois

Contenu

Plus ▼

Filtres de personnes

Relations ▼

Lieux ▼

Entreprises ac

10 585 résultats affichés



Baptiste Largent • 1er

Talent Acquisition Recruter chez Groupe SII
France

Entreprise actuelle: HR Recruter chez SQLI

Benjamin LEVI, Jérôme Masson et 78 autres relations en commun

Message



Kévin T. • 2e

SQLI chez SQLI
Région de Lyon, France

Entreprise précédente: Développeur Java/Java EE en alternance chez SQLI

Teaserpub Com, Laurent Le Moing et 5 autres relations en commun

Se connecter



Aurélie JUIGNE • 2e

Responsable RH chez SQLI
Région de Bordeaux, France

Entreprise actuelle: Chargée de recrutement chez SQLI

Ramy El Hani, Omar SALIHINE et 5 autres relations en commun

Se connecter

Recherche mail

```
tzkuat@pop-os:~/Documents/CrossLinked$ python3 crosslinked.py -f '{f}{last}@sqli.com' SQLI
[*] Searching google for valid employee names at SQLI
[*] 0 : https://www.google.com/search?q=site:linkedin.com/in+"SQLI"&num=100&start=0
[*] 98 : https://www.google.com/search?q=site:linkedin.com/in+"SQLI"&num=100&start=167
[*] 194 : https://www.google.com/search?q=site:linkedin.com/in+"SQLI"&num=100&start=316
[*] Searching bing for valid employee names at SQLI
[*] 0 : https://www.bing.com/search?q=site:linkedin.com/in+"SQLI"&first=0
[*] 10 : https://www.bing.com/search?q=site:linkedin.com/in+"SQLI"&first=45
```

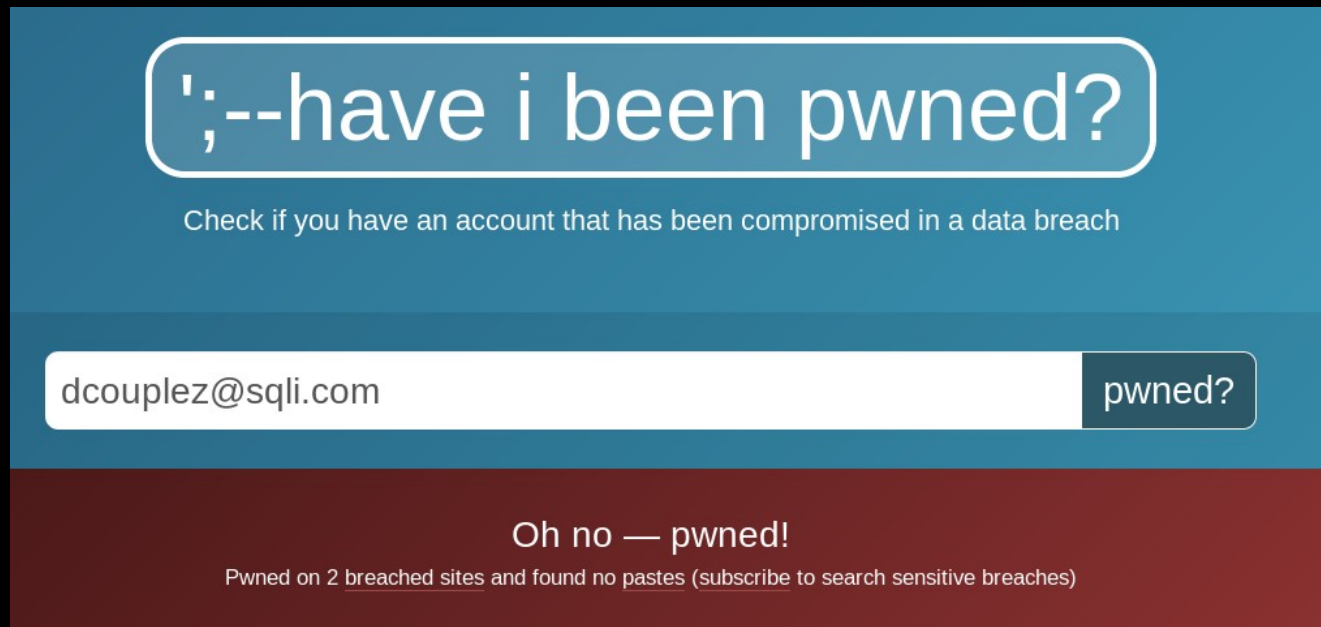
```
tzkuat@pop-os:~/Documents/CrossLinked$ cat names.txt
```

```
olarribe@sqli.com
tcainne@sqli.com
abendimered@sqli.com
jyeremian@sqli.com
ewaterlot@sqli.com
vgontard@sqli.com
fmillet@sqli.com
tdevaux@sqli.com
nmatti@sqli.com
mcondé@sqli.com
lchevallier@sqli.com
cmichel@sqli.com
lbourret@sqli.com
pmichel@sqli.com
snasri@sqli.com
spialat@sqli.com
echanal@sqli.com
fouhaichi@sqli.com
prebel@sqli.com
sverstraeten@sqli.com
```

```
pcamicas@sqli.com
rrezig@sqli.com
gdubois@sqli.com
saragon@sqli.com
achaufournier@sqli.com
shamelin@sqli.com
fnarboux@sqli.com
lcornu@sqli.com
mchardon@sqli.com
ahamon@sqli.com
apavon@sqli.com
mlauga@sqli.com
dbreton@sqli.com
snantes@sqli.com
lpeyronnet@sqli.com
chenaff@sqli.com
mbonnet@sqli.com
bsadkaoui@sqli.com
```

Pour aller plus loin

- Chercher dans les différents Leaks
 - <https://hashes.org/leaks.php>



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

dcouplez@sqli.com pwned?

Oh no — pwned!

Pwned on 2 [breached sites](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

Réseaux Sociaux

- Suivi des RH/Com
- Récupération d'informations sur les locaux/matériels

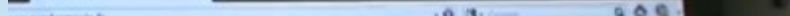
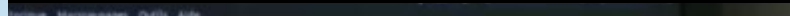
Outils

- Twitter Advanced Search
- Instagram/Facebook
- LinkedIn Premium
- Youtube
- Etc.



Réseaux Sociaux





Si on devait aller + loin

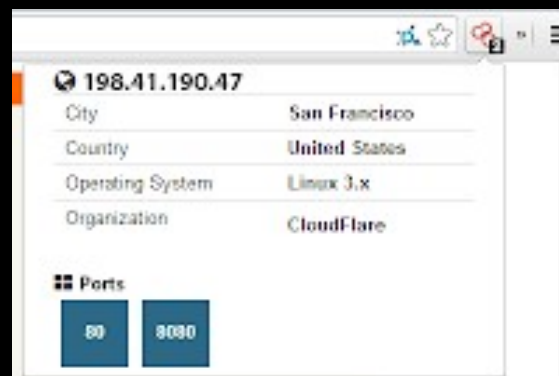
- Recherche poussée sur les RS
 - RH, RSSI, CTO, etc.
- Recherche Leaks nom/prénom ou pseudo
- Recherche sur les prestataires & filiales
- Se rendre physiquement sur site

OSINT Tips

- Wappalyzer

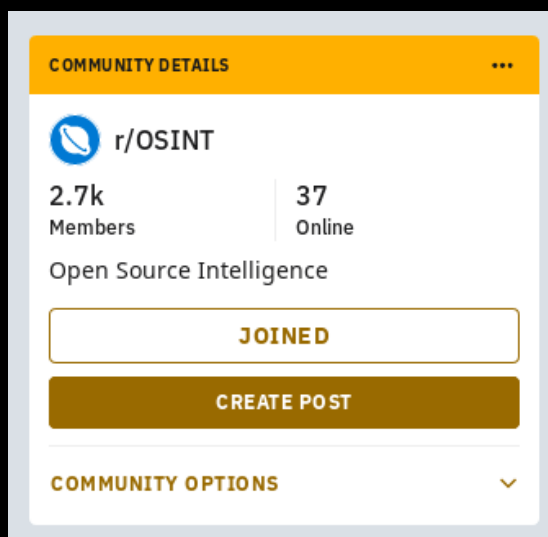


- Shodan Extension



Et si ça vous intéresse

<https://www.reddit.com/r/OSINT/>



- Communauté OSINT-FR
- Twitter : <https://twitter.com/frosint>
- Discord : <https://discordapp.com/invite/E2XDKNc>

Ressources & autres

- Stop Child Abuse
 - <https://www.europol.europa.eu/stopchildabuse>
- Bellingcat
 - <https://www.bellingcat.com/>
- Spying Challenge
 - <https://spyingchallenge.com/>
- OSINT Ressources
 - <https://github.com/tzkuat/Ressources/>



bellingcat



Bellingcat

<https://docs.google.com/document/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA>

OSINT Landscape v.1 February 2018

Open Source Intelligence (/OSINV – Open Source Investigation)



This landscape shows data sources (mostly platforms, tools or apps) that provide publicly available data which may be of use in OSINT. Some tools may charge for data access. It is intended to be extensive, but not exhaustive, and may be updated periodically.

Authors:
H I Sutton, (@CovertShores) Covert Shores and Jane's contributor,
Aliaume Leroy, (@Yach) Bellingcat & BBC,
Tony Roper, (@Topol_MSS27), planesandstuff, Jane's contributor

Merci à tous !
Des questions ? Une démo ?

Mickael Rigonnaux
Twitter : @tzkuat
mickael.rigonnaux@rm-it.fr
<https://net-security.fr>