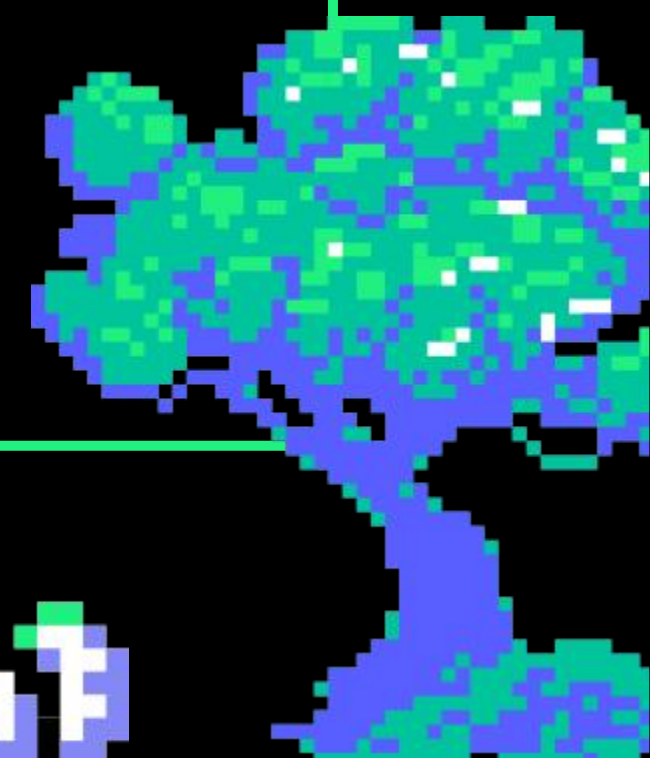


Introduction Reconnaissance & OSINT to Analyzing Data Breach

START



Topic

- ☐ Introduction About Reconnaissance
- ☐ Introduction About OSINT
- ☐ Attack Scenario
- ☐ Type Attack
- ☐ Study Case
- ☐ Prevention
- ☐ Bonus Resources

What is Reconnaissance?



Type of OSINT?

- ❑ SOCMINT (Social Media Int)
- ❑ HUMINT (Humant Int)
- ❑ SIGINT (Signal Int)
- ❑ GEOINT (Geospatial Int)
- ❑ DARKINT (Darkweb Int)

Other Technique

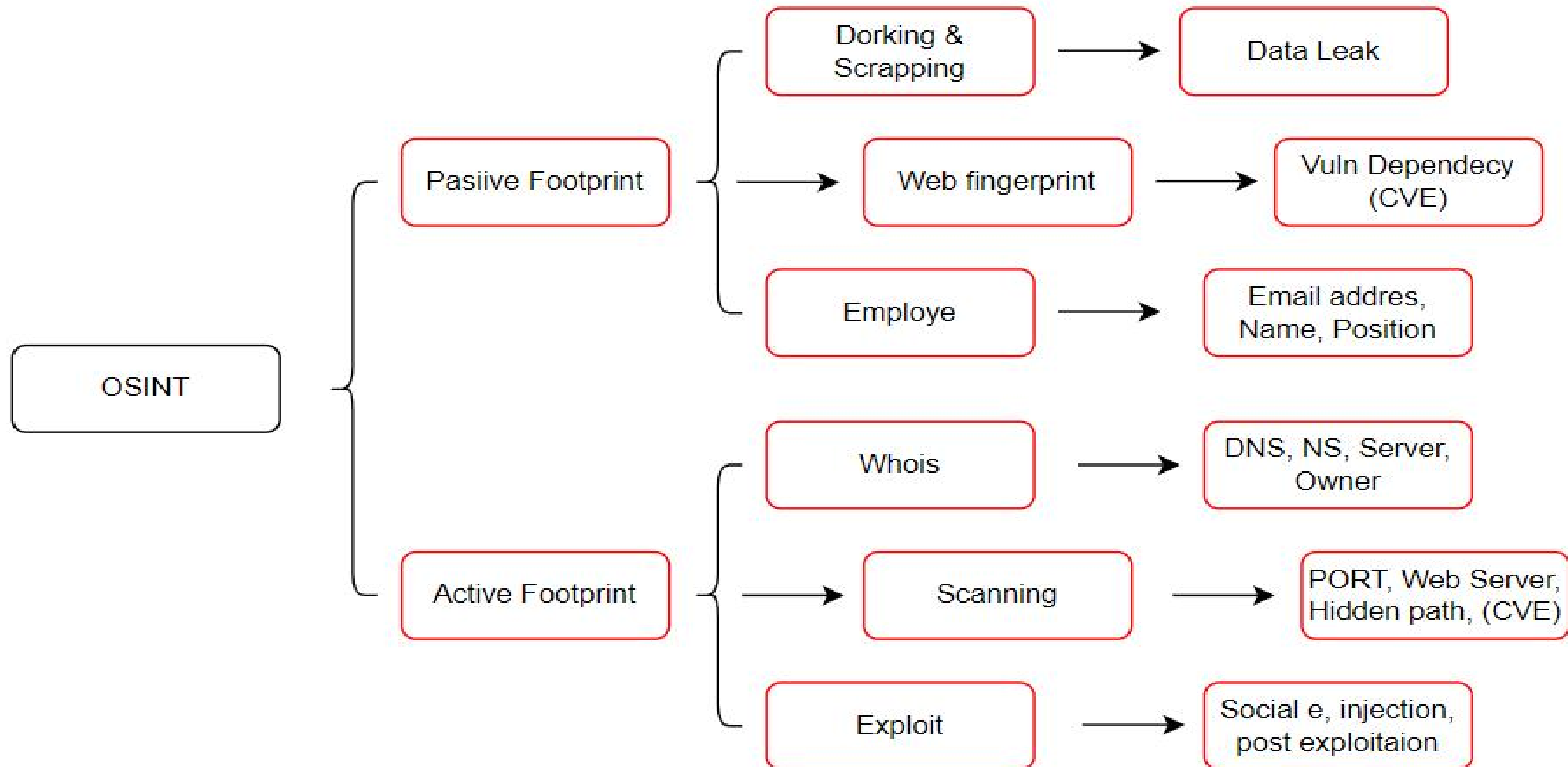
Passive Footprinting

Search information on internet, e.g dorking, scrapping, web fingerprint, document, relation, employee, email & phone number

Active Footprinting

Using tools, techniques and interaction to target, e.g whois, social e, scanning, injection, exploit and post exploitation

Example Scenario



Types Attack



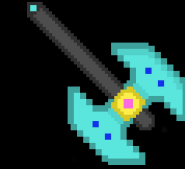
Social e and Spear
Phishing



Malware

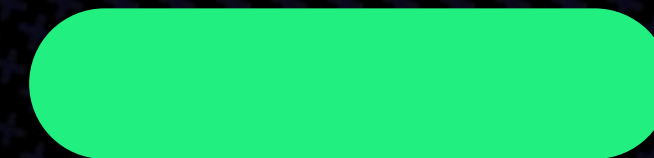


Credential Reuse

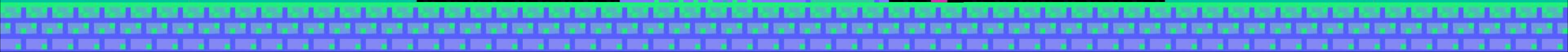
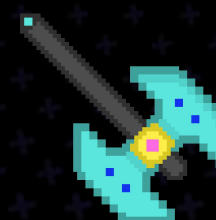
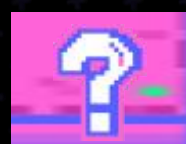
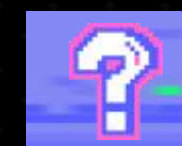


CVE or Zero Day Exploit

SIGN IN



Example Case



KAI Data Breach

Tor Browser has set your display language to English based on your system's language.

Change Language...

www.kai.id

You can find the general memo KAI.ID HERE!

PRICE: [11,69] BTC

ID: [18397815624] (Numbering victim)

"PT Kereta Api Indonesia" is the national railway company in Indonesia, also known as "Kereta Api." It is responsible for operating train services throughout the country. The company was established to provide public transportation via railways and plays a vital role in connecting cities and regions in Indonesia. 15 days are more than enough for the company to discuss the ransom with us and prepare the amount. If we don't reach an agreement with the company within 15 days, we will leak all the data through our blog (Don't forget to check this page regularly)

SAMPLE

Warning: According to our rules, if the targeted company fails to pay the ransom, we do not decrypt the data, but instead, we release the entire quantity in an organized manner. We may sell some of it. You can deal with us in this matter (bring a buyer for the data of any company in the blog, and if the operation succeeds, you can take your share of the amount with us)



www.kai.id "FF"

"PT Kereta Api Indonesia" is the national railway company in Indonesia, also known as "Kereta Api." It is responsible for operating train services throughout the country. The company was established to provide public transportation via railways and plays a vital role in connecting cities and regions in Indonesia.

More information ...

ID: 18397815624

1TB

VPN access

Illuminate\Routing\Router findRoute
../vendor/laravel/framework/src/Illuminate/Routing/-Router.php:1017

Illuminate\Routing\Router dispatchToRoute
../vendor/laravel/framework/src/Illuminate/Routing/-Router.php:996

Illuminate\Routing\Router dispatch
../vendor/laravel/framework/src/Illuminate/Foundation/-Application.php:775

Illuminate\Foundation\Application dispatch
../vendor/laravel/framework/src/Illuminate/Foundation/-Application.php:745

Illuminate\Foundation\Application handle
../vendor/laravel/framework/src/Illuminate/Session/-Middleware.php:72

Illuminate\Session\Middleware handle
../vendor/laravel/framework/src/Illuminate/Cookie/-Queue.php:47

Illuminate/Cookie/Queue handle
../vendor/laravel/framework/src/Illuminate/Cookie/-Guard.php:51

Illuminate/Cookie/Guard handle
../vendor/stack/builder/src/Stack/-StackedHttpKernel.php:23

Stack\StackedHttpKernel handle
../vendor/laravel/framework/src/Illuminate/Foundation/-Application.php:641

Illuminate\Foundation\Application run
../public/index.php:49

HTTP_HOST
reta-api.co.id

HTTP_CONNECTION
keep-alive

HTTP_CACHE_CONTROL
max-age=0

HTTP_SEC_CH-UA
"Not_A Brand";v="8", "Chromium";v="120", "Google Chrome";v="120"

HTTP_SEC_CH-UA-MOBILE
?0

HTTP_SEC_CH-UA-PLATFORM
"Windows"

HTTP_UPGRADE_INSECURE_REQUESTS
1

CONTENT_TYPE
application/x-www-form-urlencoded

HTTP_USER_AGENT
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

HTTP_ACCEPT
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

HTTP_SEC_FETCH_SITE
same-origin

HTTP_SEC_FETCH_MODE
navigate

HTTP_SEC_FETCH_USER
?1

HTTP_SEC_FETCH_DEST
document

HTTP_REFERER
eta-api.co.id/

HTTP_ACCEPT_LANGUAGE
fr-FR,fr;q=0.9

HTTP_COOKIE
laravel_session=eyJpdjI6IjE1s1TKoxcnpZMjA1Z3NmZjRwXC9lbWlnPT0iLCJ2YXkiLCJ1ZSI6IjVlQXVYdXJlXFRVVE9ranVcl25cLzNSOulttU01rNm5JUkI4T1IzVkt6QjdhI3RBYXh0M1BucGRnIHFsOUI1MVEI2R3FuXC9uRFVlc0tJT0I1IiwGa0I1MVE5PT0iLCJ1Ym91IiI3ZG90Zjg1MGU3Zjg2YVlyOGFmOGU3MzIxY2Q3M2IzImQyNDd1YDczMmQyMzdlMzcxMzI1NjRjYTF1YjIwMzcxIn0K3D

HTTP_ACCEPT_ENCODING
identity

CONTENT_LENGTH
70

PATH
/sbin:/usr/sbin:/bin:/usr/bin

SERVER_SIGNATURE
Apache/2.2.15 (CentOS)

SERVER_SOFTWARE
vaireport.kereta-api.co.id

SERVER_NAME
10.6.0.55

SERVER_PORT
80

REMOTE_ADDR
192.168.254.9

DOCUMENT_ROOT
/var/www/html/vaireport/public

SERVER_ADMIN
root@localhost

SCRIPT_FILENAME
/var/www/html/vaireport/public/index.php

REMOTE_PORT
5862

GATEWAY_INTERFACE
CGI/1.1

SERVER_PROTOCOL
HTTP/1.1

REQUEST_METHOD
POST

QUERY_STRING
/

REQUEST_URI
/index.php

SCRIPT_NAME
/index.php

PHP_SELF
/index.php

REQUEST_TIME_FLOAT
1704292428.514

REQUEST_TIME
1704292428

KAI

KAI Data Breach

Tor Browser has set your display language to English based on your system's language. [Change Language...](#)

COMPANY [ZONESOFT.PT]	SIZE	DIRECT LINK [TORRENT .TOR]
	*GB	FULL FILES
	*GB	FULL FILES
	*GB	FULL FILES

COMPANY [PCMARKET.UZ]	SIZE	DIRECT LINK [TORRENT .TOR]
	FULL FILES	
	FULL FILES	
	FULL FILES	

COMPANY [KAI.ID]	SIZE	DIRECT LINK [TORRENT .TOR]
kai.id	FULL FILES	
kai.id	FULL FILES	
kai.id	FULL FILES	

Analysis results


- Data leak sensitive information exposure (Laravel debug true)
- Data breach employee
- Credential reuse
- Malware or backdoor C2C

Illuminate\Routing/Router findRoute	retax-api.co.id
./vendor/laravel/framework/src/Illuminate/Routing/Router.php:1017	keep-alive
	HTTP_CACHING_CONTROL max-age=0
	"Not-A Brand";v="B", "Chromium";v="120", "Google Chrome";v="120"
	HTTP_SEC_CH_UA MOBILE 70
	HTTP_SEC_CH_UA_PLATFORM "Windows"
	HTTP_UPGRADE_INSECURE_REQUESTS 1
	CONTENT_TYPE application/x-www-form-urlencoded
	HTTP_USER_AGENT Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
	test/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
	HTTP_ACCEPT same-origin
	HTTP_SEC_FETCH_SITE navigate
	HTTP_SEC_FETCH_MODE 71
	HTTP_SEC_FETCH_DEST document
	HTTP_REFERER retax-api.co.id/
	HTTP_ACCEPT_LANGUAGE fr-FR;q=0.9
	laravel_sessioneyJpdi1lIistKoxcnpZjYJAIzNudXRUxCR9ibWlnPmT0LCj2Ykx1ZS161VlVQXFVjdUFXUEF9anVm25cl2NS0tU0B1bm53Uk14TT1icVt6QndwQ3RBVXNDM1BucGRnNHFSOWUyI2R3fXFCXFRVC0BjT01hWda081WE53PT0LLCjTmFlOL1ZGZWZjIGU3RjZjg2YmYwOGNmOUB3ZnIiwzODI1bmQybDd1MDczMQwmdzFzc0Rlc7LWJrJGVJVTFVJmFlZnc1In03SD
	HTTP_COOKIE Identity
	CONTENT_LENGTH 70
	PATH /sbin:/usr/sbin:/bin:/usr/bin
	SERVER_SIGNATURE Apache/2.2.15 (CentOS)
	SERVER_SOFTWARE vaireport-kereta-api.co.id
	SERVER_NAME 10.6.0.95
	SERVER_ADDR 80
	SERVER_PORT 192.168.254.9
	REMOTE_ADDR /var/www/html/vaireport/public
	DOCUMENT_ROOT root@localhost
	SCRIPT_FILENAME /var/www/html/vaireport/public/index.php
	REMOTE_PORT 5862
	GATEWAY_INTERFACE CGI/1.1
	HTTP_PROTOCOL CG/1.1
	REQUEST_METHOD POST
	QUERY_STRING /
	REQUEST_URI /index.php
	SCRIPT_NAME /index.php
	PHP_SELF 1704292428.514
	REQUEST_TIME_FLOAT 1704292428
	REQUEST_TIME 1704292428

Warning to PT KAI Indonesia Company

Tox ID support :

Mandiri Data Breach















Mandiri Sekuritas merupakan mitra investasi tepercaya yang menyediakan solusi pasar modal komprehensif dengan beragam produk dan layanan unggulan

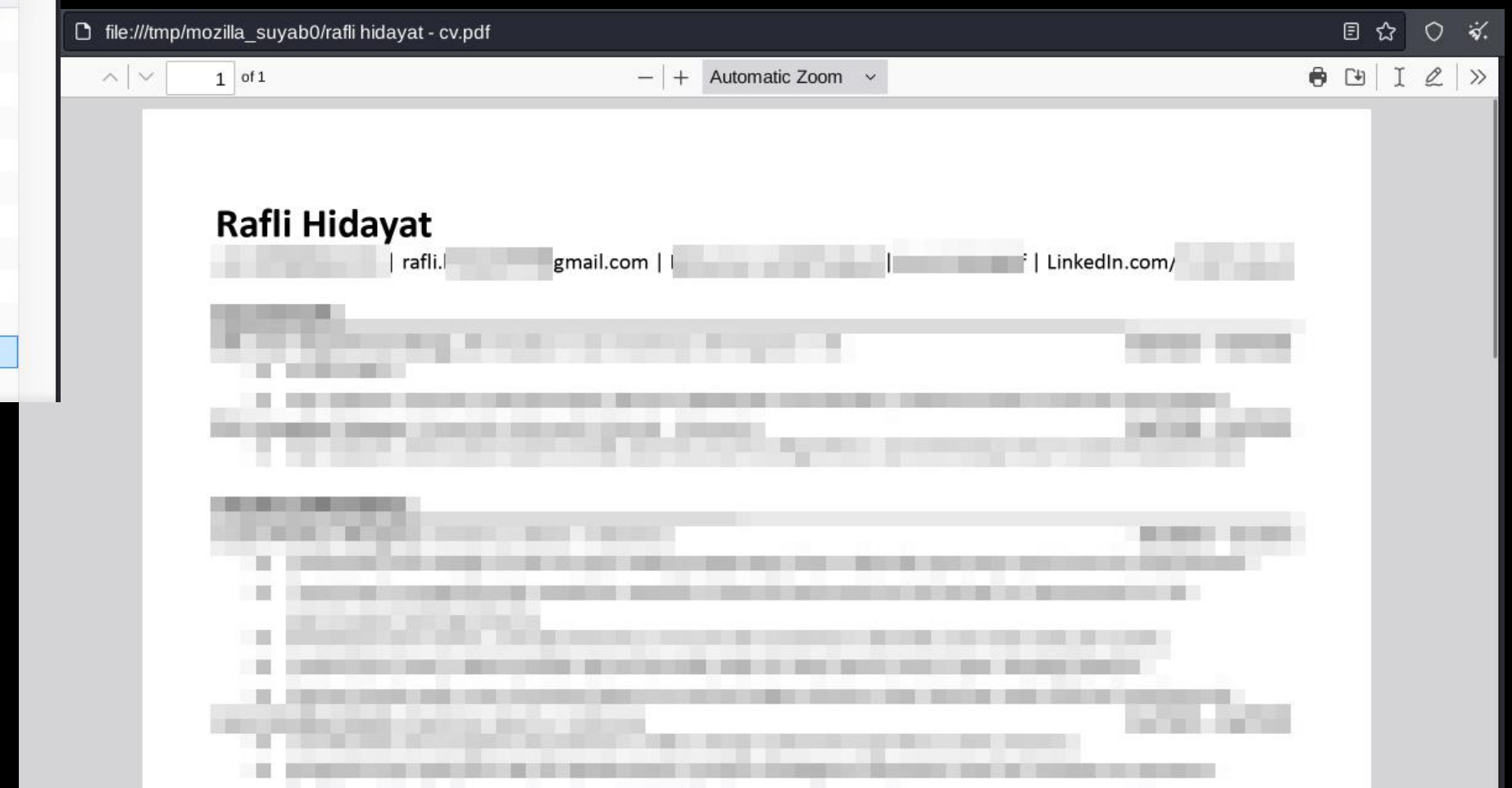
FILES ARE PUBLISHED !

UPLOADED: 16 MAR, 2023 09:05 UTC UPDATED: 01 DEC, 2023 11:44 UTC

FILE LISTING

[RETURN BACK](#)
WIN-ADK8840J08F / D / data / mandirisekuritas.co.id / recruitment

NAME	DATE	SIZE
 ifist	12 Mar, 2023	4.00kB
 job posting	17 Jun, 2023	4.00kB
 rejection email.docx	15 Jun, 2023	10.74kB
 email	12 Mar, 2023	4.00kB
 application form - employment shannon shi suparsono.pdf	12 Mar, 2023	1.20MB
 research	12 Mar, 2023	4.00kB
 ib	12 Mar, 2023	4.00kB
 open - project manager it	15 Jun, 2023	4.00kB
 recruitment day - feui - icmss feb 2017.pptx	12 Mar, 2023	11.52MB
 closed	29 Mar, 2023	4.00kB
 rafli hidayat - cv.pdf	12 Mar, 2023	92.47kB
 social media officer	12 Mar, 2023	4.00kB



Mandiri

Mandiri Data Breach

```
▼ 17 {2}
  key : SMTP_PORT
  value : 25
▼ 18 {2}
  key : SMTP_SENDERMAIL
  value : ████████████████████
▼ 19 {2}
  key : SMTP_PASSWORD
  value : ████████████████████
▼ 20 {2}
  key : EMAIL_SUBJECT_DISABLED_USER
  value : [ePRO] Akun Dinonaktifkan
▼ 21 {2}
  key : SMTP_HOST
  value : ████████████████████.mandiri.co.id
▼ 22 {2}
  key : SMTP_TLS_ENABLE
  value : true
▼ 23 {2}
  key : SMTP_SSL_ENABLE
  value : true
▼ 24 {2}
  key : SMTP_USER
  value : supporting\\ipa.wavemaker
▼ 25 {2}
  key : EMAIL_BODY_CERTIFICATE_WILL_EXPIRE
```

harry.sutanto@bankmandiri.co.id [peopledatalabs]	harry.sutanto@bankmandiri.co.id
ignace.widiatmoko@bankmandiri.co.id [Unknown]	ignace.widiatmoko@bankmandiri.co.id
jenny@bankmandiri.co.id [antipublic-combo]	jenny@bankmandiri.co.id
jenny@bankmandiri.co.id [verifications.io]	jenny@bankmandiri.co.id
riyani.t.bondan@bankmandiri.co.id [antipublic-combo]	riyani.t.bondan@bankmandiri.co.id
riyani.t.bondan@bankmandiri.co.id [linkedin.com]	riyani.t.bondan@bankmandiri.co.id
riyani.t.bondan@bankmandiri.co.id [peopledatalabs]	riyani.t.bondan@bankmandiri.co.id
riyani.t.bondan@bankmandiri.co.id [tokopedia.com]	riyani.t.bondan@bankmandiri.co.id

Amfs Lissan	amfs.lissan@bankmandiri.co.id
Dewi Kusumawardani	dewi.kusumawardani@bankmandiri.co.id
Dewi Mulyanti Kusumawardani	dewi.mulyanti.kusumawardani@bankmandiri.co.id
Dyah Anggraini	dyah.anggraini@bankmandiri.co.id
Frits Soejodi	frits.soejodi@bankmandiri.co.id
Hanung Herutomo	hanung.herutomo@bankmandiri.co.id
Harry Sutanto	harry.sutanto@bankmandiri.co.id
Ignace Widiatmoko	ignace.widiatmoko@bankmandiri.co.id

Mandiri Data Breach

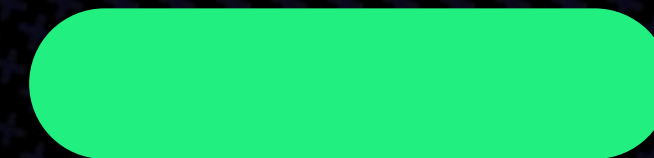


Analysis Result

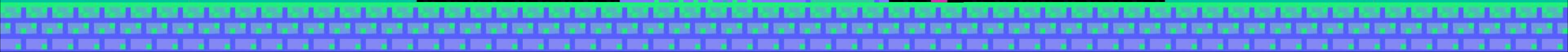
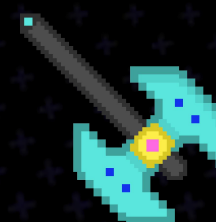
- Data leak email
- Data breach employe and platform third party
- From data breach to social engineering (init access)

Company: PDL	Company: LinkedIn
Company Domain:	Company Domain: linkedin.com
Date of Breach: 2019-10-16	Date of Breach: 2012-05-05
Breach Description: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data . The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.	Breach Description: In May 2016, LinkedIn had 164 million email addresses and passwords exposed . Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.
Total Accounts Effected: 622,161,052	Total Accounts Effected: 164,611,595
Data Exposed in Breach: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles	Data Exposed in Breach: Email addresses, Passwords
Copy this Data	Copy this Data
Company: LinkedInScape	Company: Tokopedia
Company Domain: linkedin.com	Company Domain: tokopedia.com

SIGN IN



Prevention



Edu employee

Audit

WAF, IPS & IDS or SIEM

Backup & Backup

Encrypt document, email
message and sensitive stuff

Takedown sensitive
information on internet

Maintance credentials access

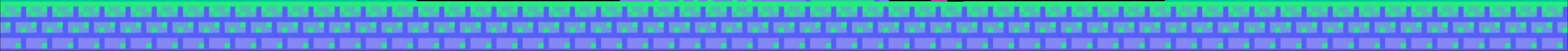
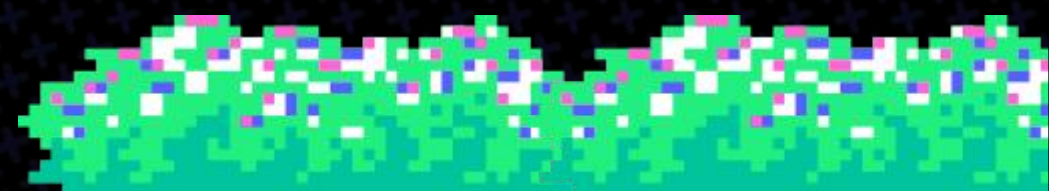
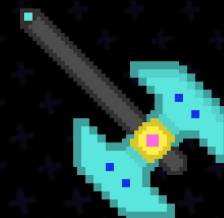
Enable 2FA for credentials

Monitoring data breach

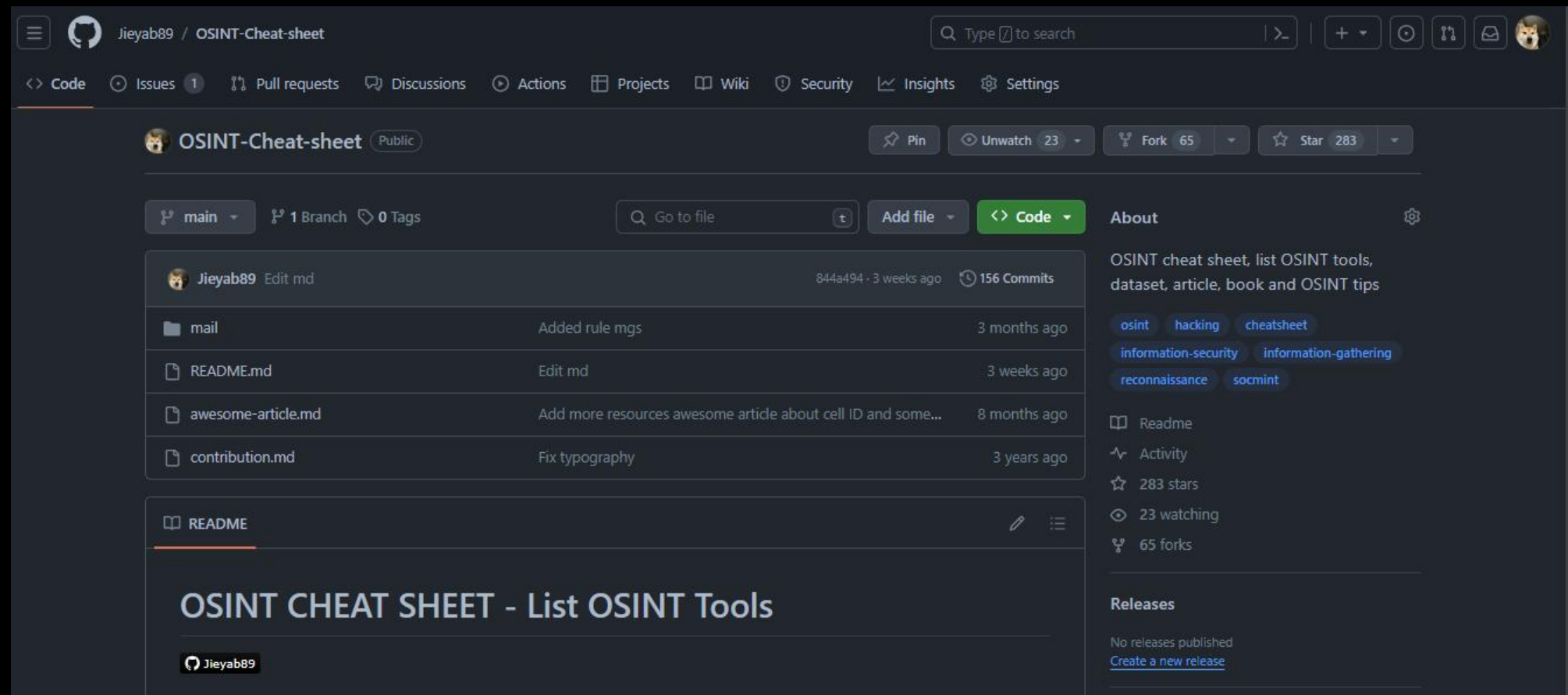
SIGN IN



Bonus Section



Free Resources & Book



OSINT CHEAT SHEET

Table of Content

- Web Intel
- SOCMINT
- SIGINT
- Collection Dataset
- GEOINT
- Darkweb Intel
- CTI
- Cryptocurrency Intel



Free Resources & Book



OSINT Handbook

Table of Content

- Intro about cyber threats intelligence
- Technique cyber threats intelligence
- Platform cyber threats intelligence
- Sample files and case study
- Prevent OSINT technique
- Real case and live target
- Prevent cyber threats
- Social engineering
- Intro about OSINT
- OSINT technique
- Spiderfoot tool
- Maltego tool
- Bonus
- Quiz



LOGOUT



LOGOUT



THANK YOU

