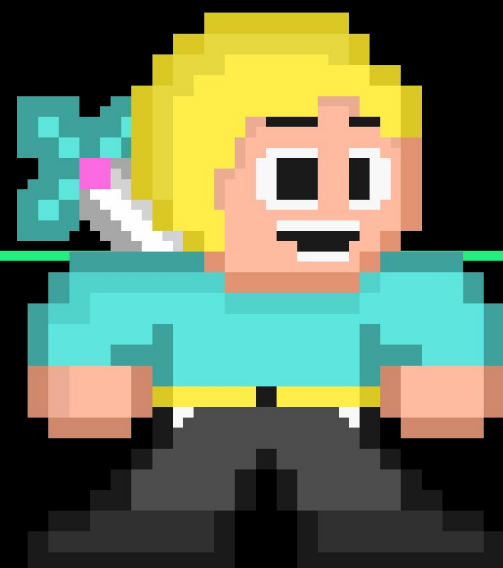


INTRODUCTION RECONNAISSANCE & OSINT TO ANALYZING DATA BREACH

START

Bayu Aji aka Suyab



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

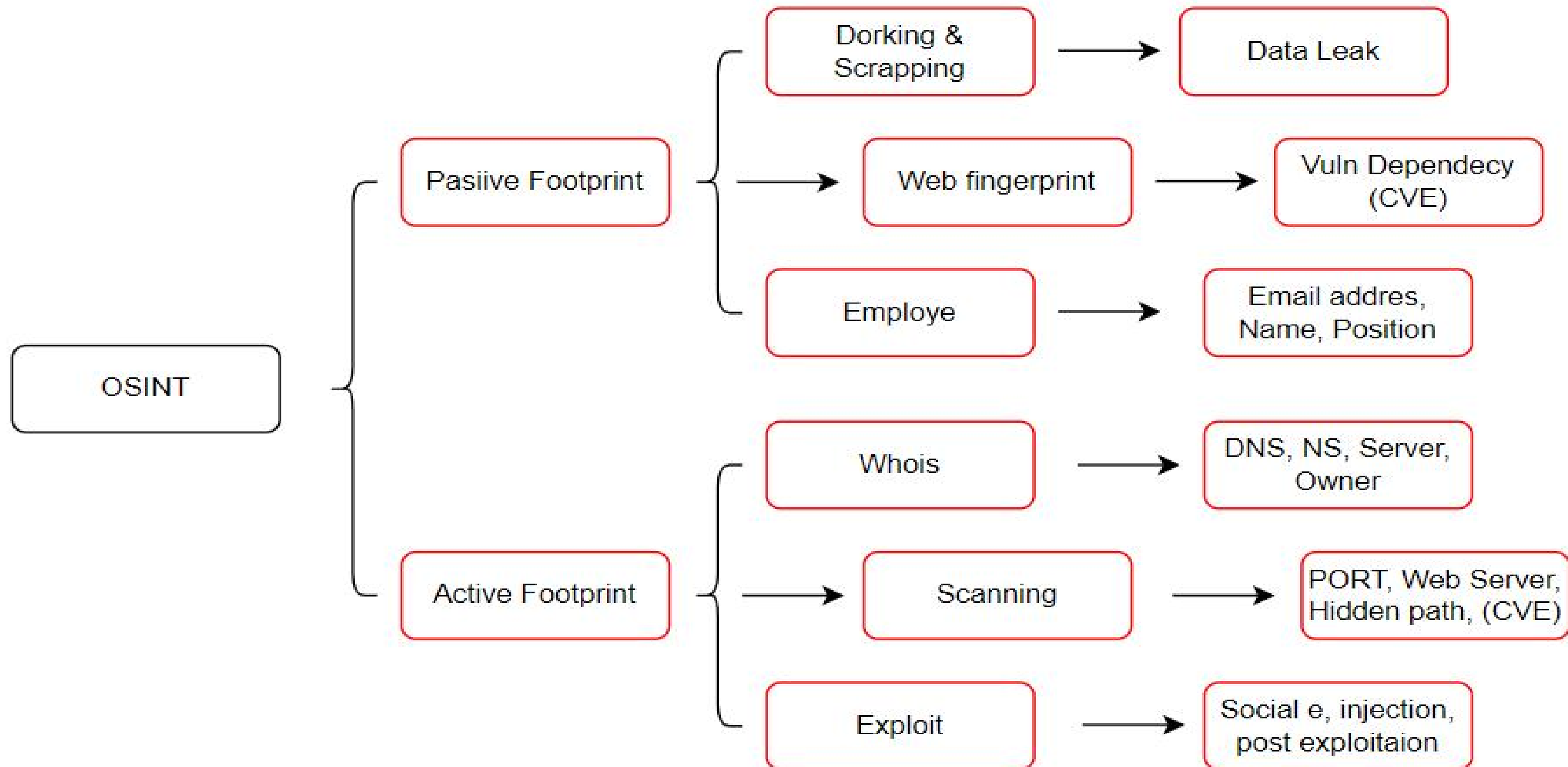
Passive Footprinting

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



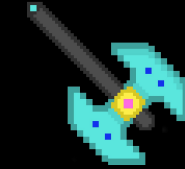
Social e and Spear
Phishing



Malware



Credential Reuse



CVE or Zero Day Exploit

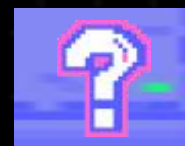
SIGN IN



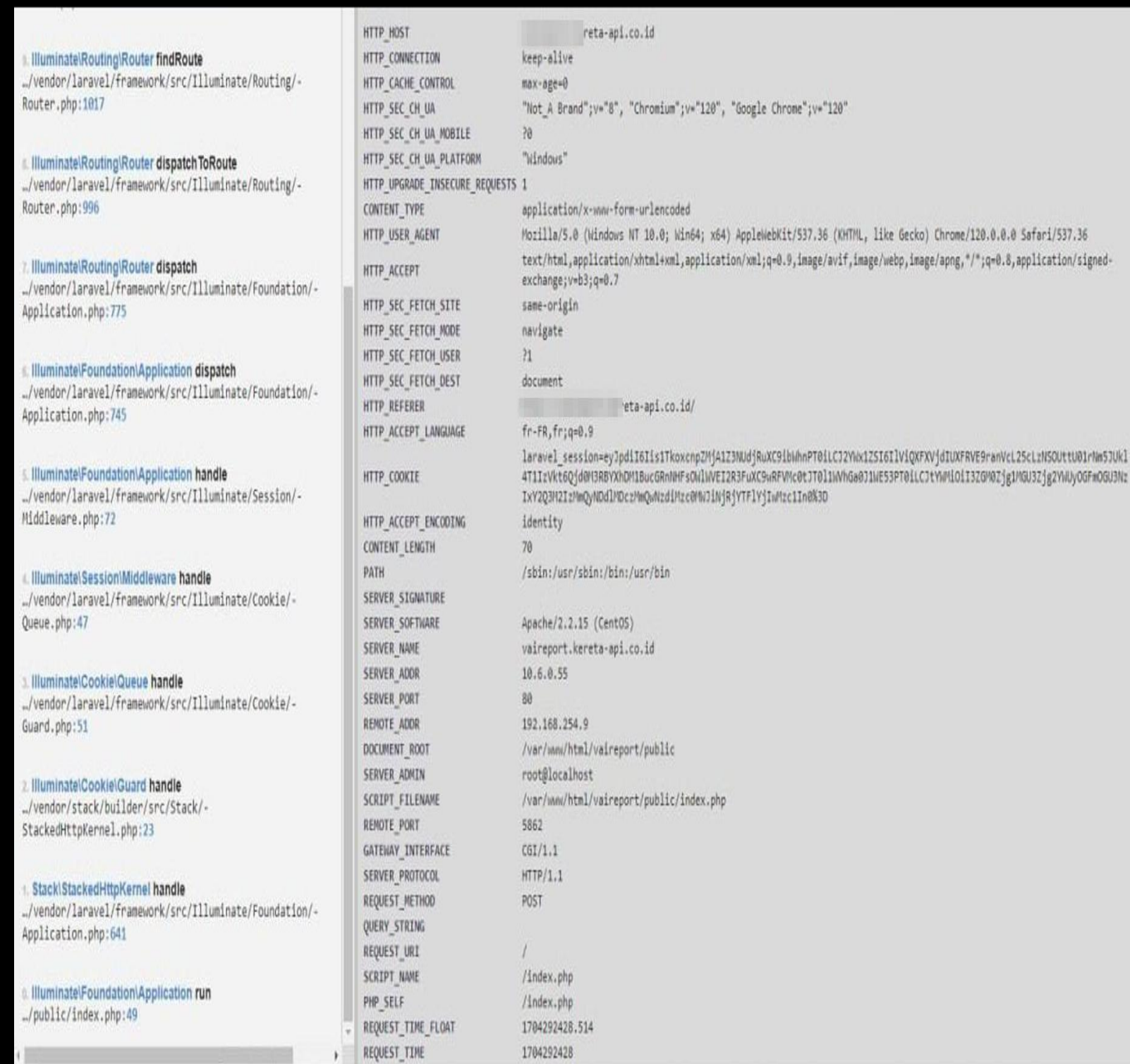
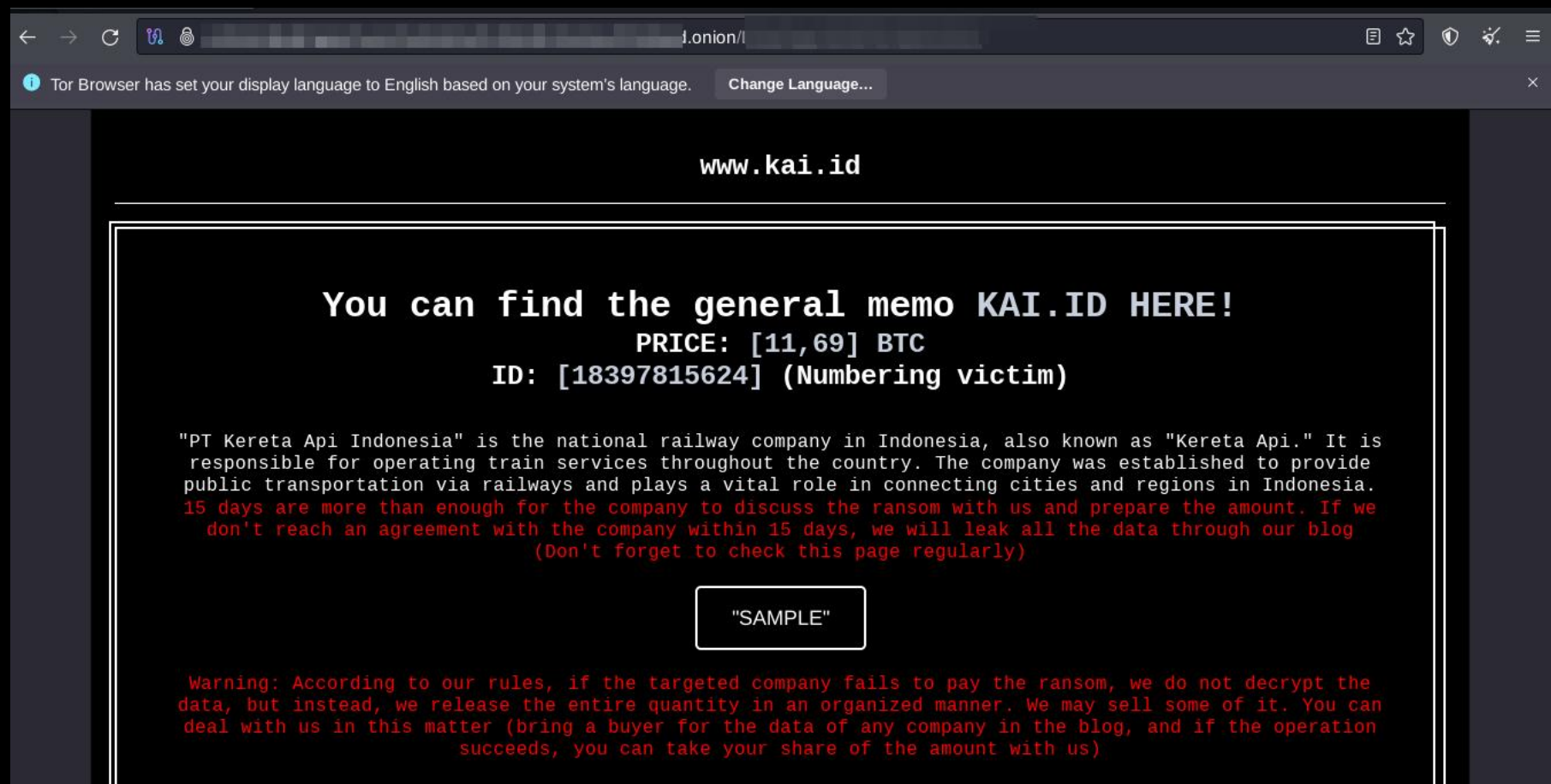
SIGN IN



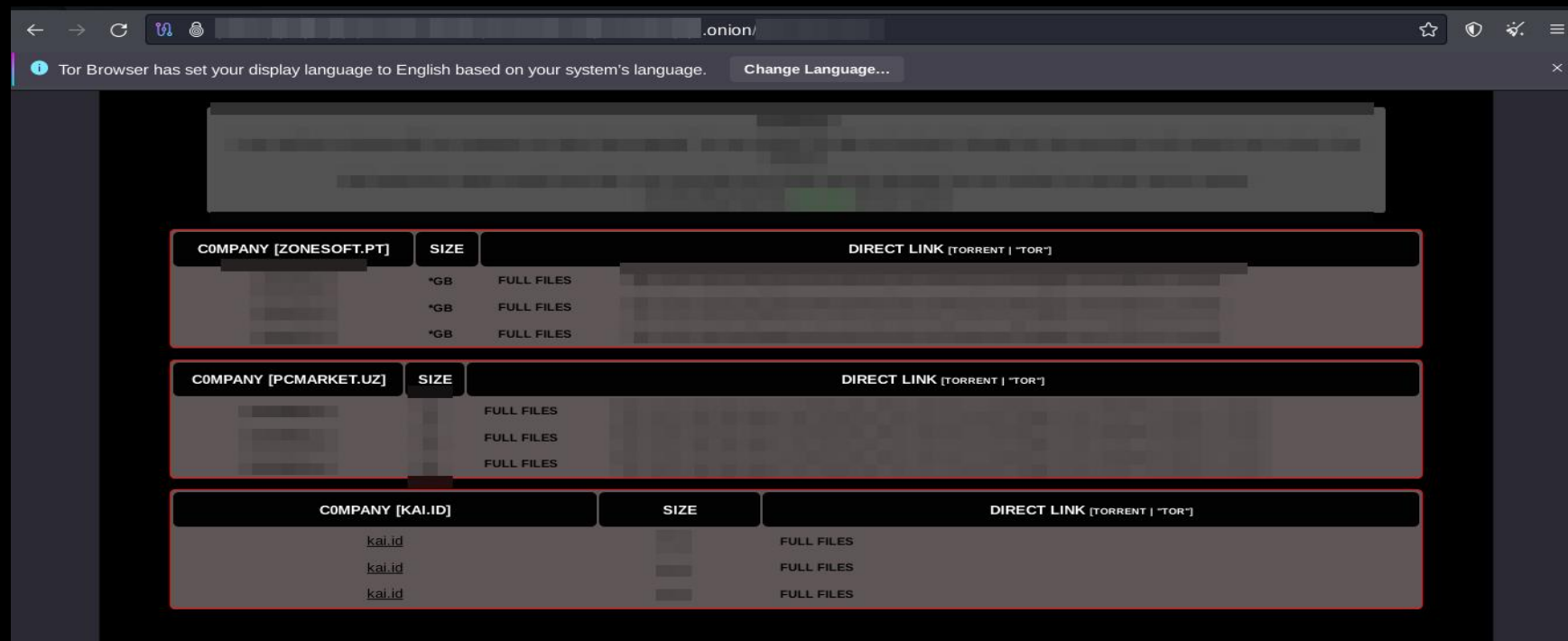
Example Case



KAI Data Breach

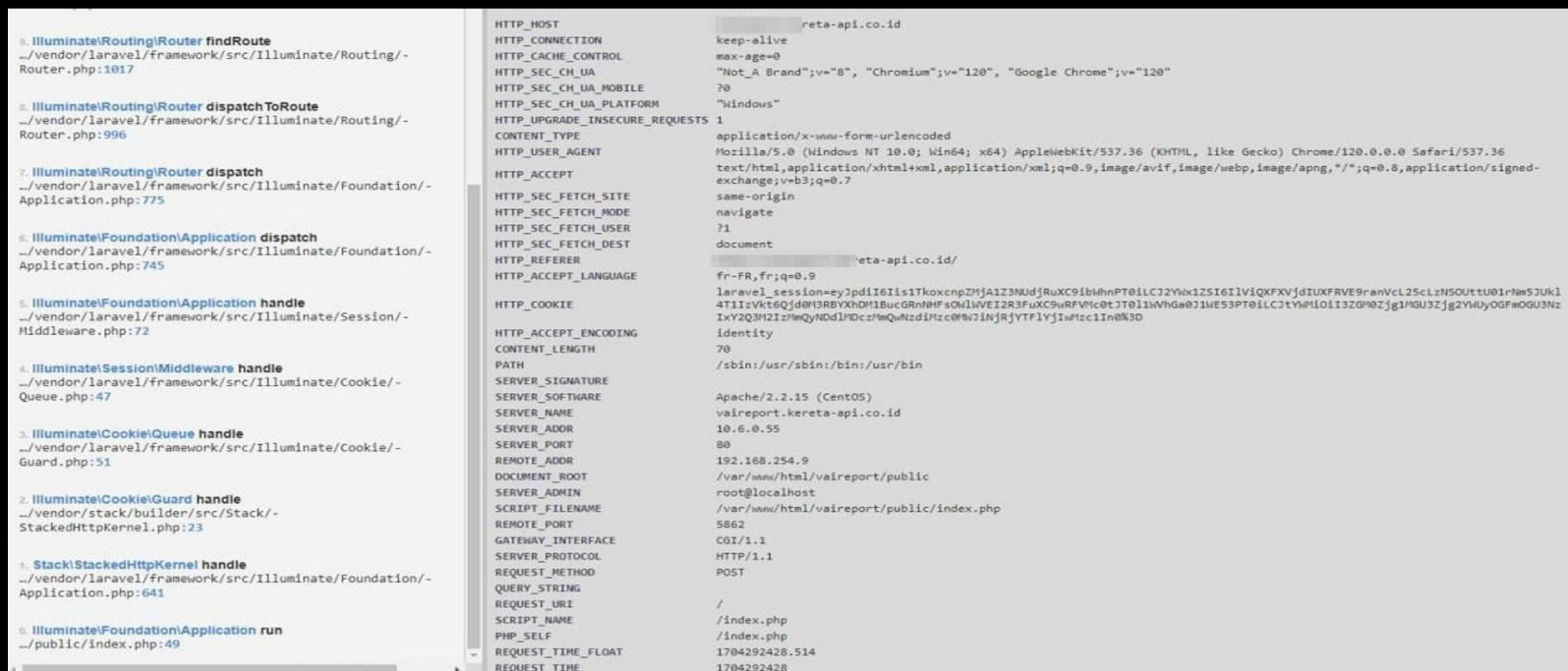


KAI Data Breach



Analysis results


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



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

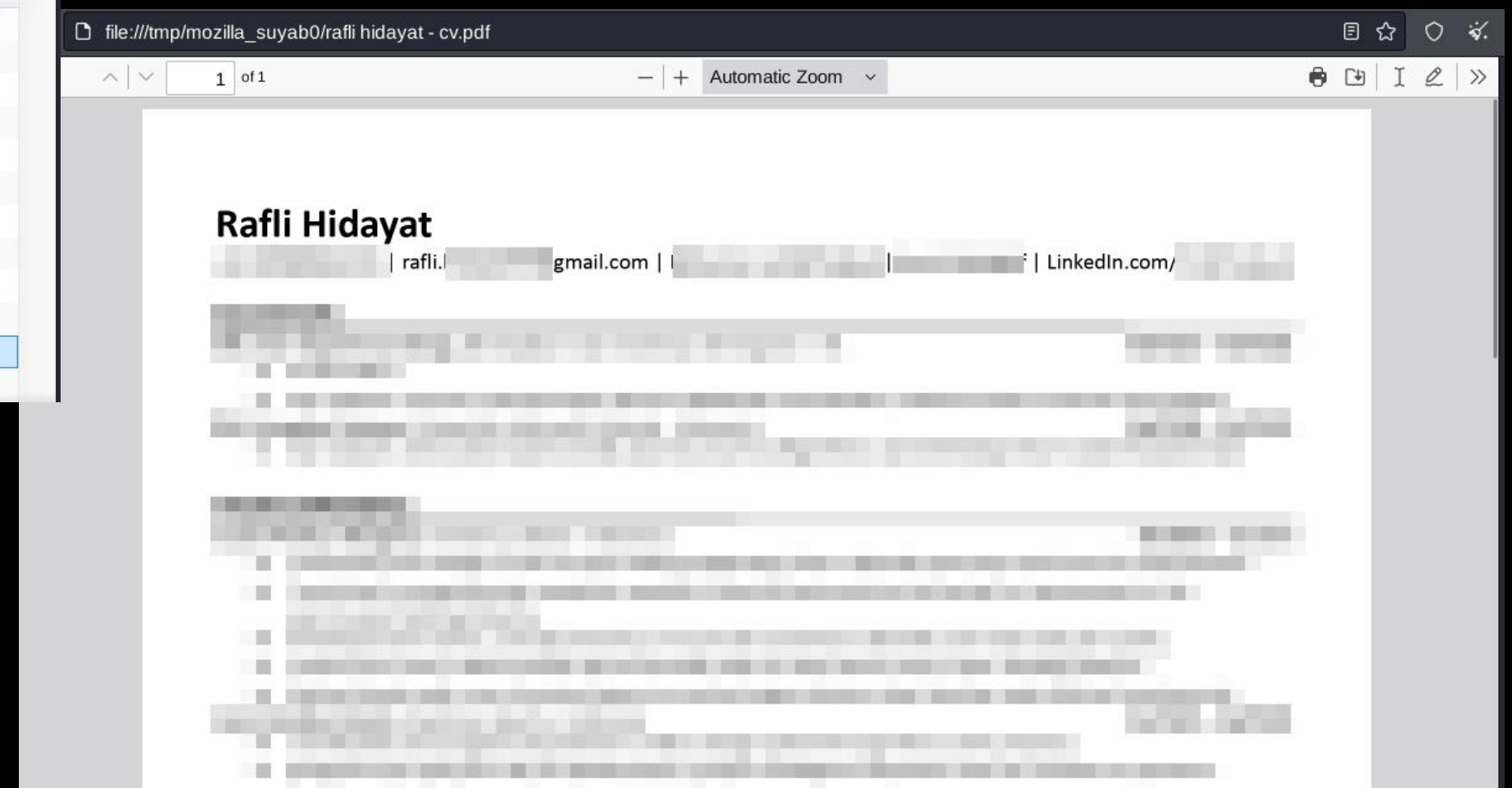
FILES ARE PUBLISHED !

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



Analysis Result

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

<div><div>Company: PDL</div><div>Company Domain:</div><div>Date of Breach: 2019-10-16</div><div>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.</div><div>Total Accounts Effected: 622,161,052</div><div>Data Exposed in Breach: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles</div><div>Copy this Data</div></div>	<div><div>Company: LinkedIn</div><div>Company Domain: linkedin.com</div><div>Date of Breach: 2012-05-05</div><div>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.</div><div>Total Accounts Effected: 164,611,595</div><div>Data Exposed in Breach: Email addresses, Passwords</div><div>Copy this Data</div></div>
<div><div>Company: LinkedInScrape</div><div>Company Domain: linkedin.com</div></div>	<div><div>Company: Tokopedia</div><div>Company Domain: tokopedia.com</div></div>

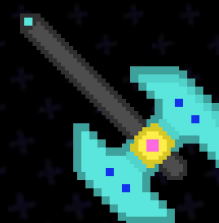
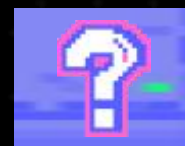
SIGN IN



SIGN IN



Prevention



Edu employee

Audit

WAF, IPS & IDS or SIEM

Backup & Backup

Encrypt document, email
message and sensitive stuff

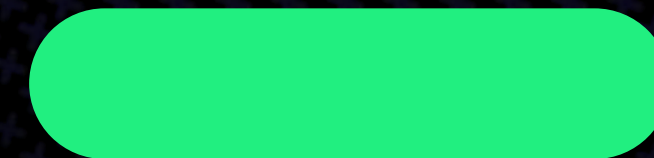
Takedown sensitive
information on internet

Maintance credentials access

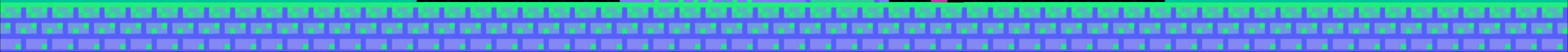
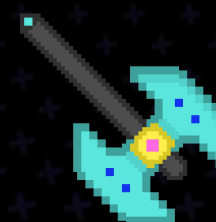
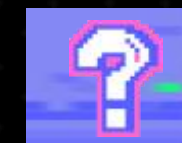
Enable 2FA for credentials

Monitoring data breach

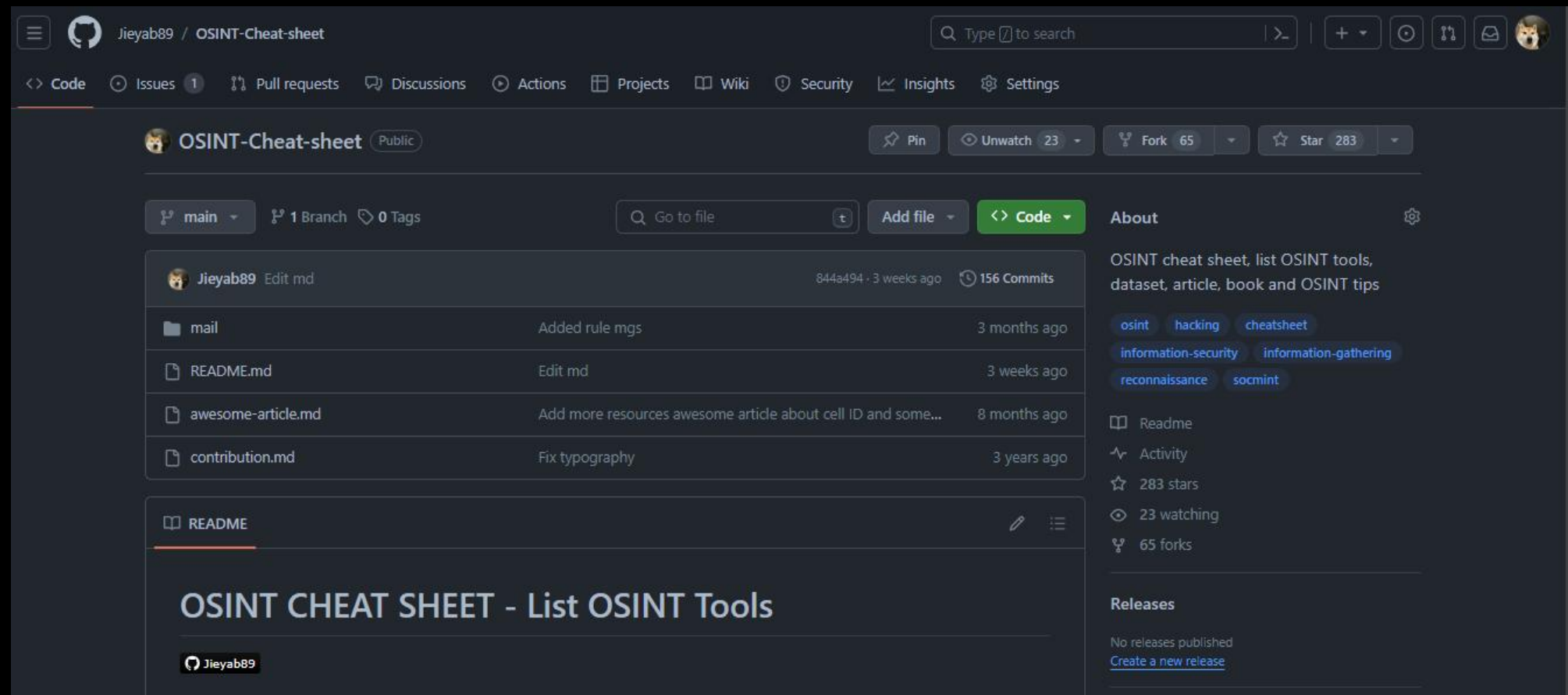
SIGN IN



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

