OSINT : Everything Counts

By : Lakshit Verma
Founder We Are Plymouths (WAP)

Who Am I ?

- Myself Lakshit Verma aka Acelakshit
- Independent Security Researcher
- Founder We Are Plymouths (WAP)

“If You're Online You're Vulnerable.”

What Is Osint ?

- **O**pen **S**ource **Int**elligence (OSINT) — gathering information from publicly available sources and its analysis to produce an actionable intelligence.

- Example : Usernames , Location Etc.

Steps In OSINT ?

- Start with what you know (email, username, etc.)
- Define requirements (what you want to get)
- Gather the data
- Analyze collected data
- Pivot as-needed using new gathered data
- Validate assumptions
- Generate report

How OSINT Can Help Us ?

- Locating Digital footprints
- Performing digital investigations
- Gathering information for competitive intelligence or penetration testing.

OSINT : What To Look For ?

- Social Media
- IP Addresses
- Geolocation
- Reverse Image Search
- Phone Numbers
- Leaked Documents
- Vulnerable Web Servers , Devices Etc.

Who Is Interested In OSINT ?

- Govt.
- International Organisation
- National Security Agencies (CBI , FBI , CIA)
- Law Enforcement Agencies
- Private Investigators
- Criminals/Terrorists
- Red Teamers (Pentesters , Researchers)

Terminologies :

- Metadata & Use Of Metadata In Osint ?
- Metadata : data Supporting the main data , Information Gathering & Forensics
- SOCMINT is a subset of OSINT that concentrates on data gathering and monitoring on social media platforms.

ReadMyBoP - Read My Boarding Pass

www.bighugesystems.com Travel & Local

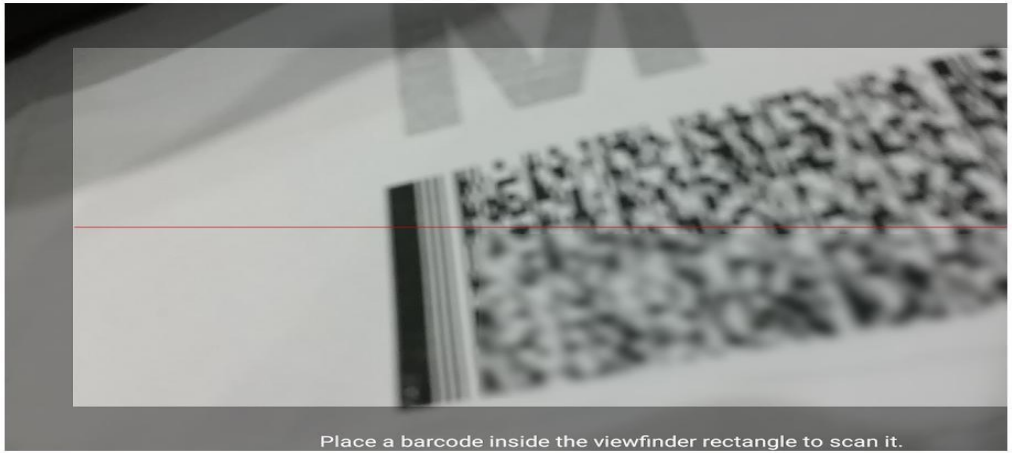
★★★½☆ 33

3+

This app is compatible with all of your devices.

Add to Wishlist

Install




Email Boarding Pass (Web Check in)
GoIndiGo.In
Don't be late, your flight won't wait
Name
From Delhi
To Jaipur
Flight No. 6E 5098
Date 30 Nov 19
Boarding Time 05:35 AM
Departure Time 06:20 AM
Sequence No. 1
Class R
Gate No.
Seat No. 15E
Boarding gate closes 25 minutes prior to the departure time. Boarding gate numbers are subject to changeplease check the flight information screen for latest updates. Checking of photo id and hand baggage is a mandatory procedurePassengers are requested to cooperate with IndiGo and the relevant authorities. Have a pleasant flight. Call 0 99 10 38 38 38 / 0124 661 3838
SPECIAL SERVICES
NIL
Name : MS SS TEST
PNR : QJRD8N
Flt No. : 6E 5098
Seat No. : 15E
Seq No. : 1
MS Anshika Mittal
From Delhi
To Jaipur
Flight No. 6E 5098
Date 15 May 19
Boarding Time 05:35 AM
Departure Time 06:20 AM
Seq No. 1 Class R
Gate No Seat No 15E

Boarding Pass Can Help Can Get You ?

- Gender
- Which passenger number in the ticket
- Passenger Last name
- Passenger First name
- Ticket Type (Online/Physical)
- PNR
- Source
- Destination
- Flight Carrier
- Flight Number

Boarding Pass Can Help Can Get You ?

- Passenger Seat Class
- Seat Number
- Flight Sequence Number
- Passenger Clearance Status
- Passenger Checked IN/Not
- What document type this is
- Where this document was printed ar airport or somewhere else R. Printed
- Flight Date
- TDocument issuing Flight company
- Document is authorised or not

Dorks & Dorking

- Google hacking, also named Google dorking, is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code.

Example : inurl:/8080/admin.html

Advance Operators

Examples:

1. site:cia.gov “top secret” (search within a specific website)
2. filetype:pdf "cannabis licence" site:gov.bc.ca (search a specific file type from a website)
3. Inurl:resume “john smith”

(search within the URL of websites)

4. Intext:resume “john smith”

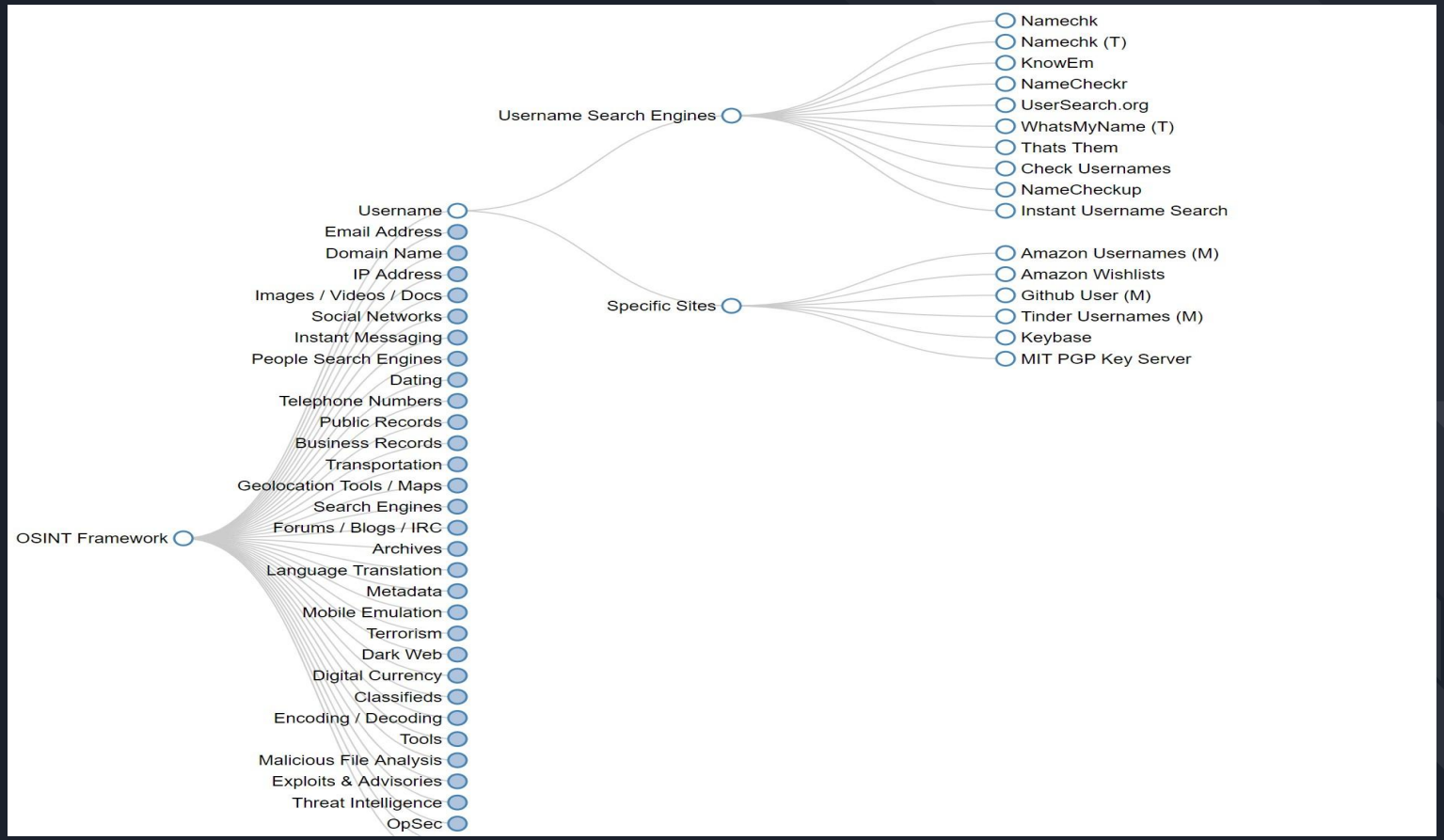
(search within the text websites)

Lets Make Our Hands Dirty !

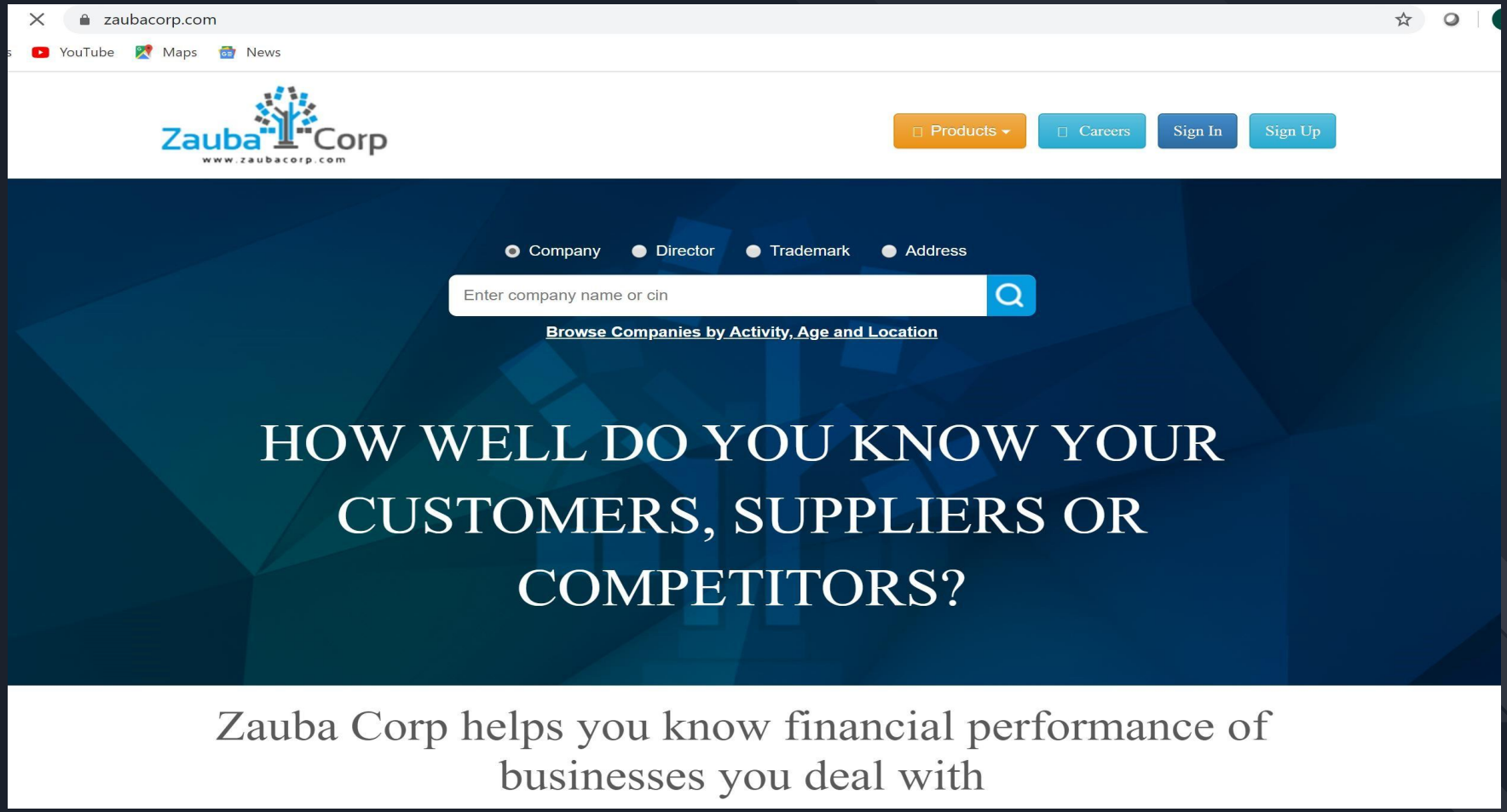
Tools Used In OSINT ?

- Maltego
- Google Hacking Database (GHDB)
- Metagoofill
- Shodan
- TheHarvester
- Osint Framework

Osintframework.com



Zaubacorp.com



Careers In OSINT ?

- **Financial Research**
- **National Security Agencies (CBI , FBI , CIA)**
- **Law Enforcement Agencies (LEA)**

Any questions?

You can find me at:

Twitter : @acelakshitverma

acelakshitverma@gmail.com