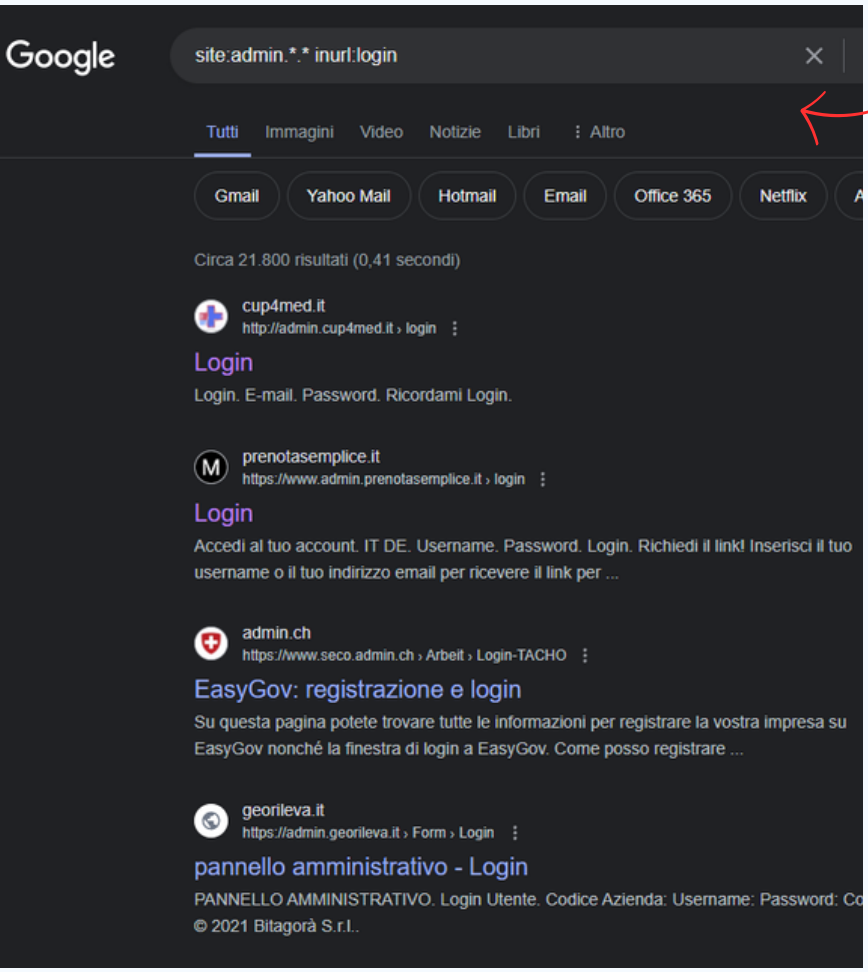
VAN ZWAM
ARJEN
#ByteRebels

REPORT

RACCOLTA INFORMAZIONI

TARGET:
PrenotaSemplice.it

SCELTA DEL TARGET

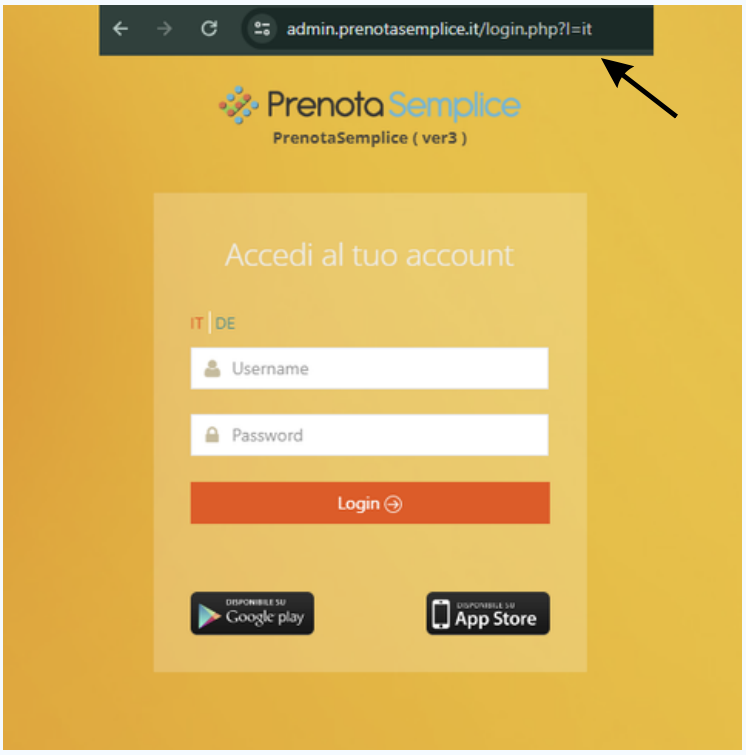


Google Dork

Tramite **Google Hacking** ho voluto scegliere un target che combaciava con un Dork recuperato dall'**Exploit Database**

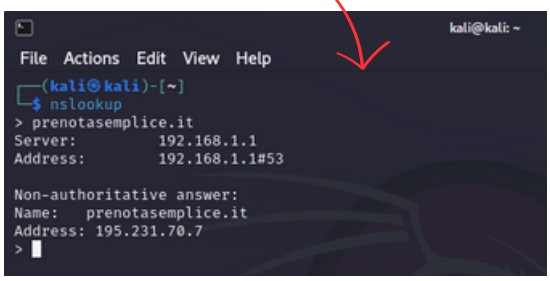
Controllo del link

Il link trovato tramite il **Google Dork** ha evidenziato un form d'accesso per un pannello di controllo **admin**

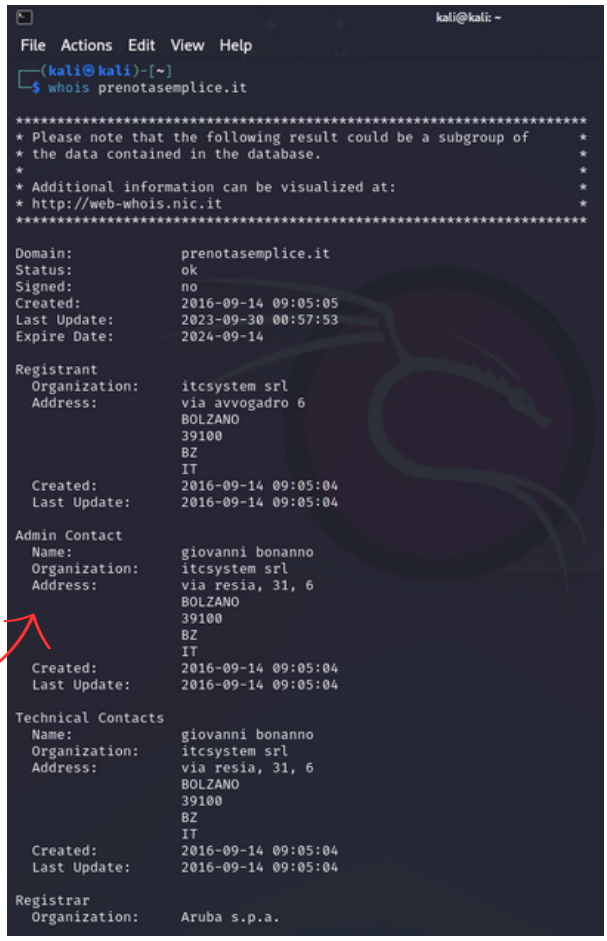


INFO SUL TARGET

Il target scelto totalmente a **random** è una startup di un'applicazione iOS/Android, l'ho ispezionata con vari Tool e come prima cosa ho scoperto l'**IP** con **nslookup**



Al termine ho anche controllato **informazioni** base, come il *nome* dell'organizzazione, l'*hosting provider*, *l'indirizzo* della sede, la *data di creazione* e l'*ultimo Update* del sito in questione.



TECNOLOGIE WEB

Tramite la ricerca sul mitico Shodan.io si evidenziano le tecnologie utilizzate:
Prototype
RequireJS

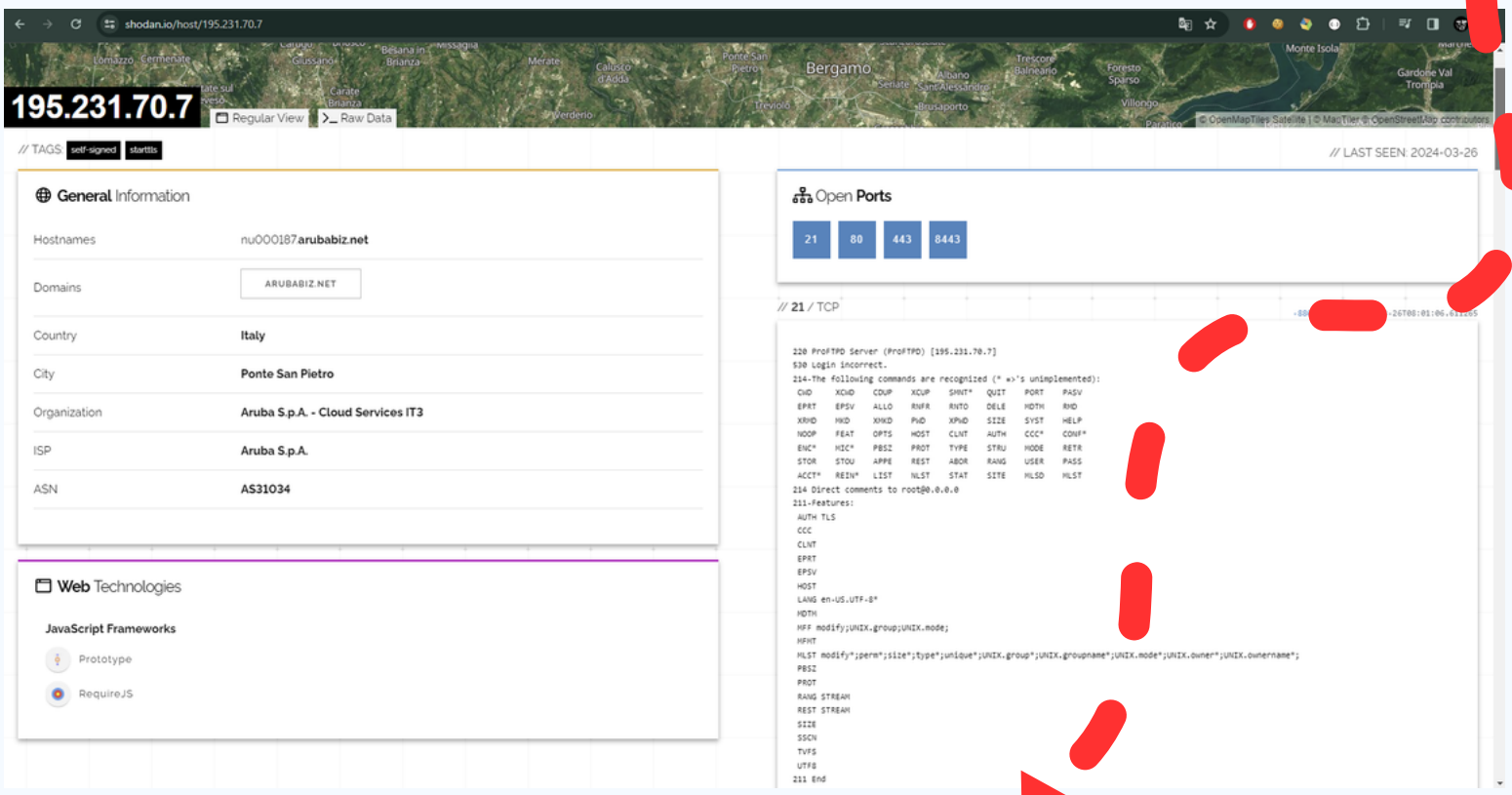
PORTE

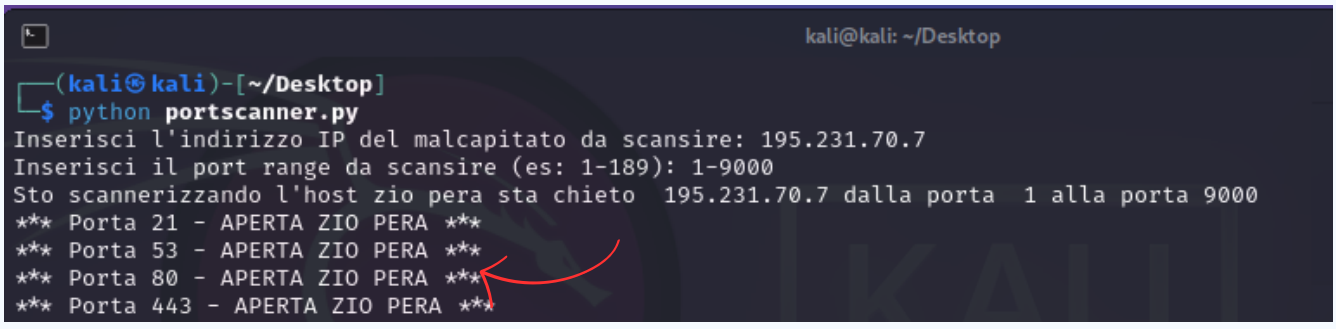
Lo **scan** delle porte aperte è già stato effettuato, ma volendo si può fare con lo script in python.
Le porte aperte sono:
21 - 80 - 443 - 8443

Per un lavoro più meticoloso ho provato col mio script e ho trovato altre porte aperte

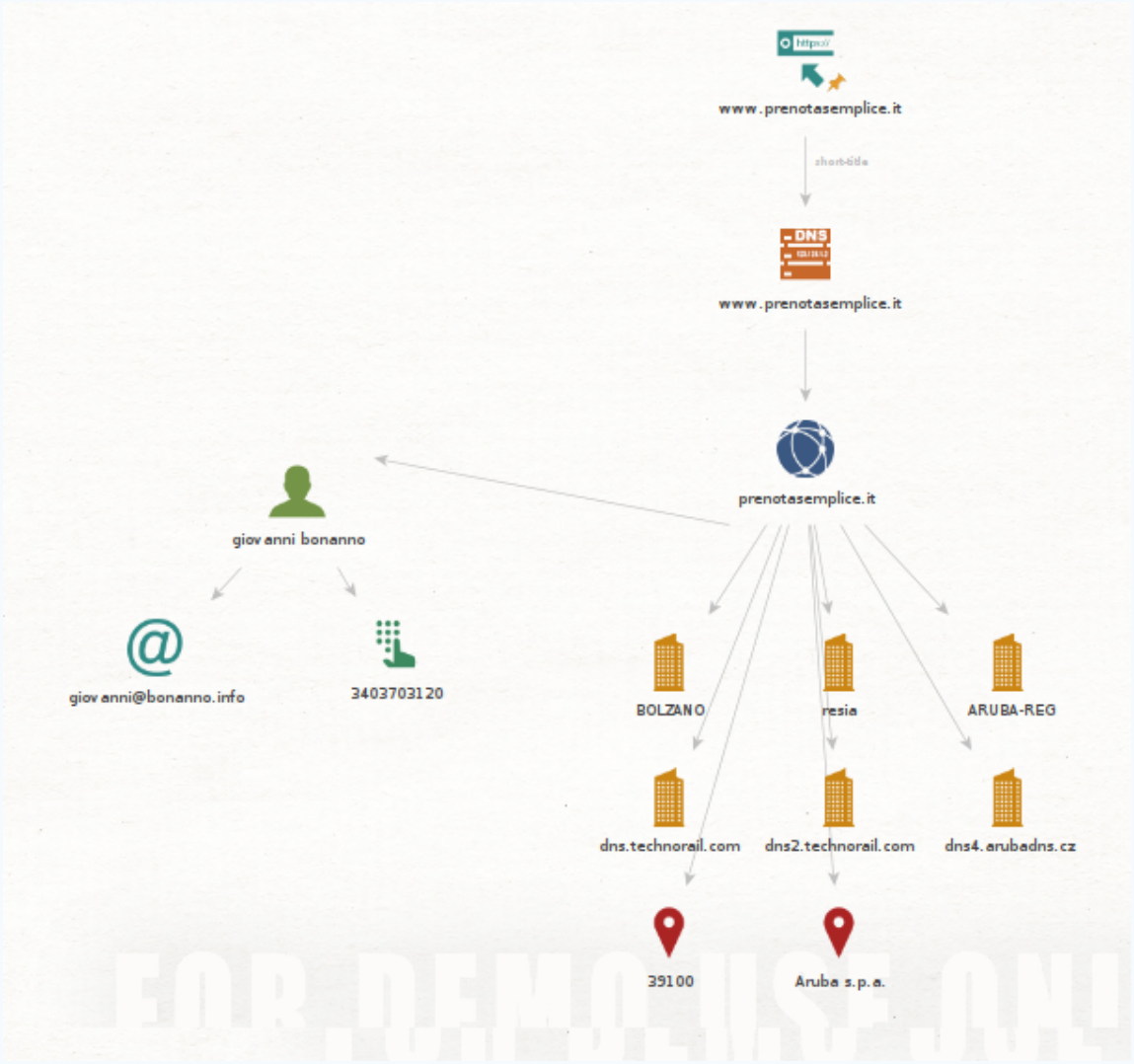
VULNERABILITA'

Tramite Shodan il sito **NON** presenta **vulnerabilità** note



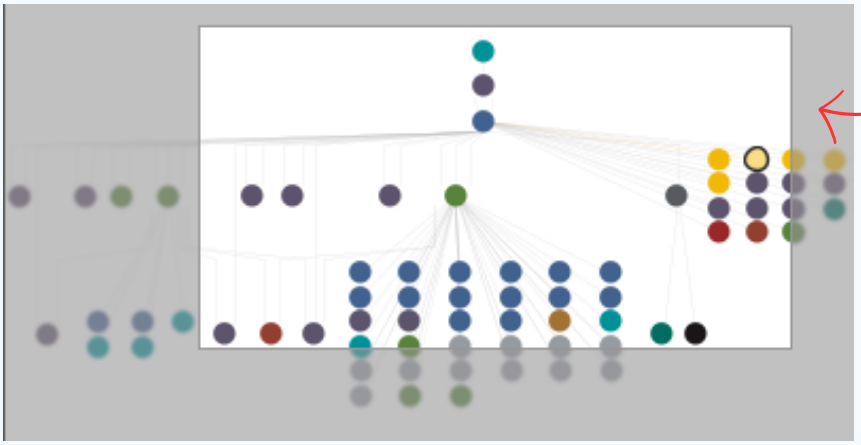


MALTEGO



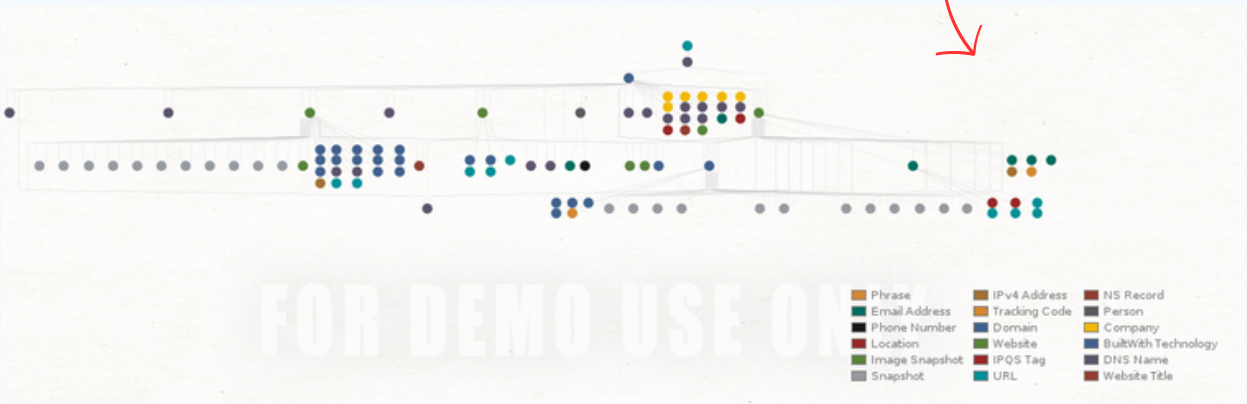
Tramite il tool **Maltego**, ho iniziato a ricostruire il sito con le informazioni inerenti ad esso estrapolando ciò che mi faceva comodo.
Ad esempio, come si vede dall'immagine, sono partito dall' **URL** (target), ho controllato il DNS con "**To DNSNames**".
A sua volta "**To Domains**", che estrae tutti i domini da un nome DNS.
A questo punto ho utilizzato le API di **IBM Watson**, "**To Entities from WHOIS**" e ho trovato info utili come il proprietario del dominio, dove a sua volta ho estrapolato l'email ed il numero di cellulare con "**To email addresses**" e anche il phone number con le API's di Bing "**To phone number [BING]**"

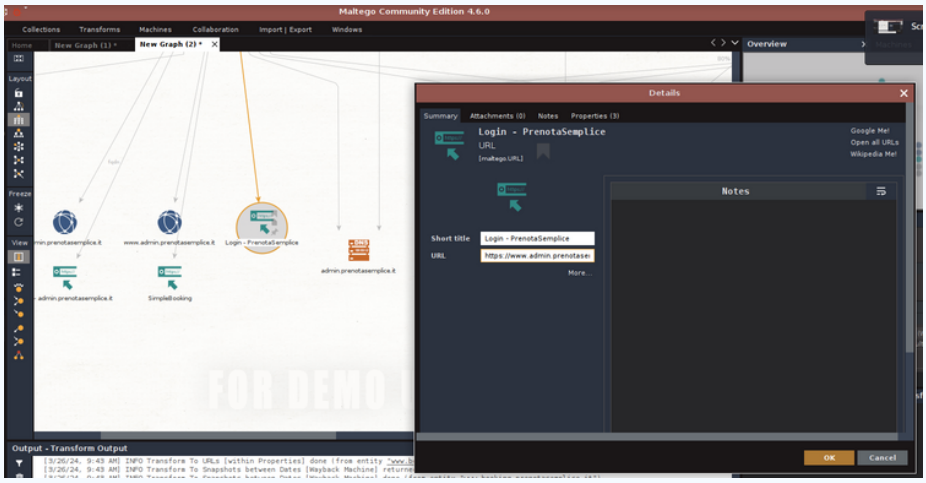
MALTEGO



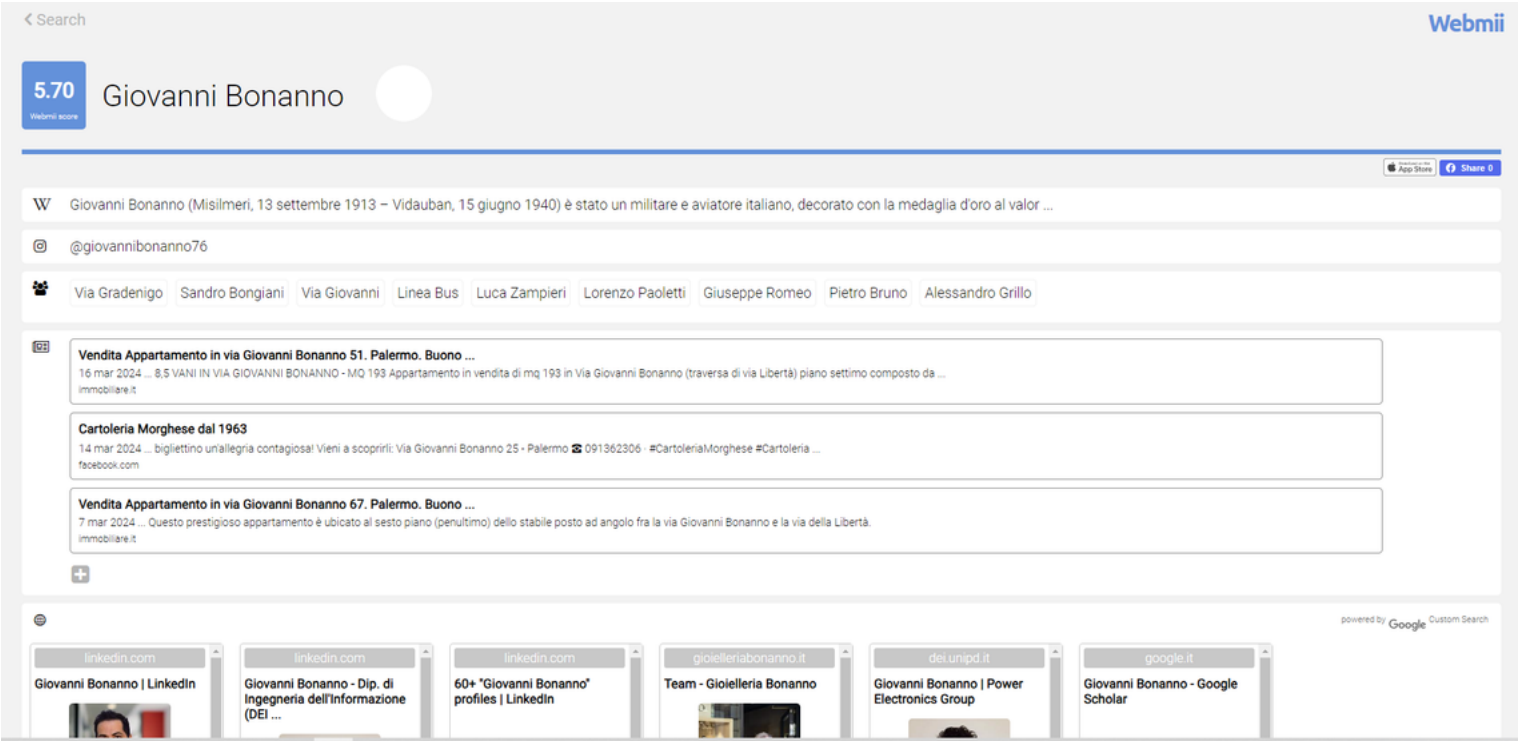
Overview

Una piccola estrapolazione grafica di ciò che sono riuscito ad ottenere con **pochi** e semplici tool



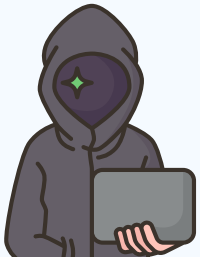


Infine ho notato che tra tutte le pagine del sito in questione appariva un altro form d'accesso **molto, molto buggato.**
Dove provando alcune credenziali l'accesso è possibile.



WEBMII

Questa volta **Webmii** non ha prodotto risultati utili anche se come score ha ottenuto **5.70**
Dovuto dal fatto che non conosco tale persona non sono riuscito a proseguire oltre.



Arjen