

## Fase di raccolta informazioni su un target casuale

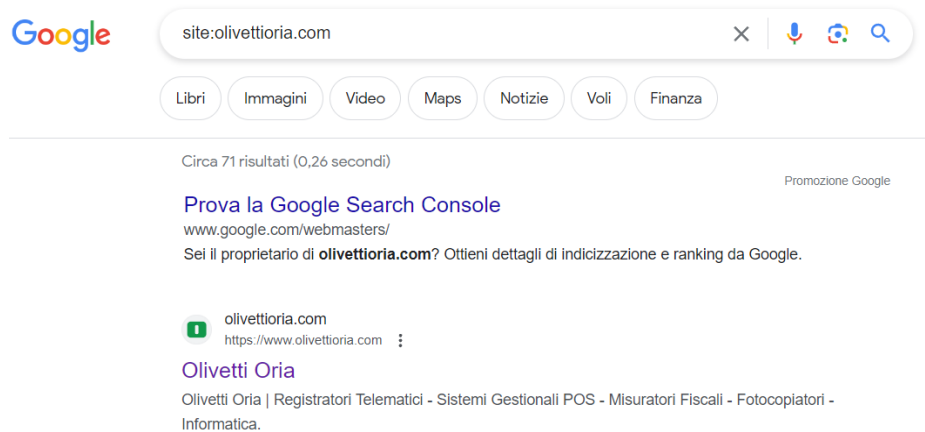
Esercitazione:24/07/2023

Oggi andremo ad utilizzare alcuni comandi di Google Hacking che ci permettono di “filtrare” le informazioni che troviamo normalmente sul WEB.

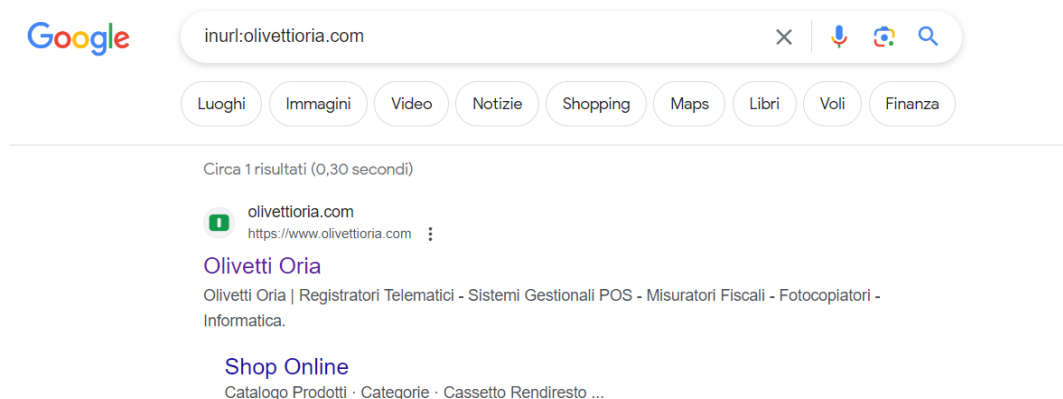
Questi comandi vengono utilizzati prettamente per delle ricerche specifiche riuscendo a ridurre così di molto il tempo passata a ricercare informazioni su una determinata azienda.

Oggi utilizzeremo:

**site:nomedelsito.com** → con questa stringa visualizzeremo tutte le pagine indicizzate di quel determinato sito.

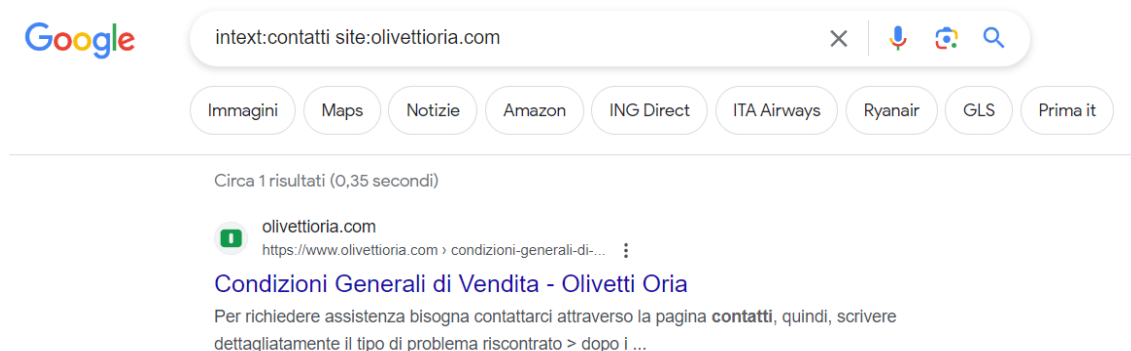


**inurl:nomedelsito.com** → con questa stringa visualizzeremo tutte le pagine contenenti quell'URL contenente il nome del sito.

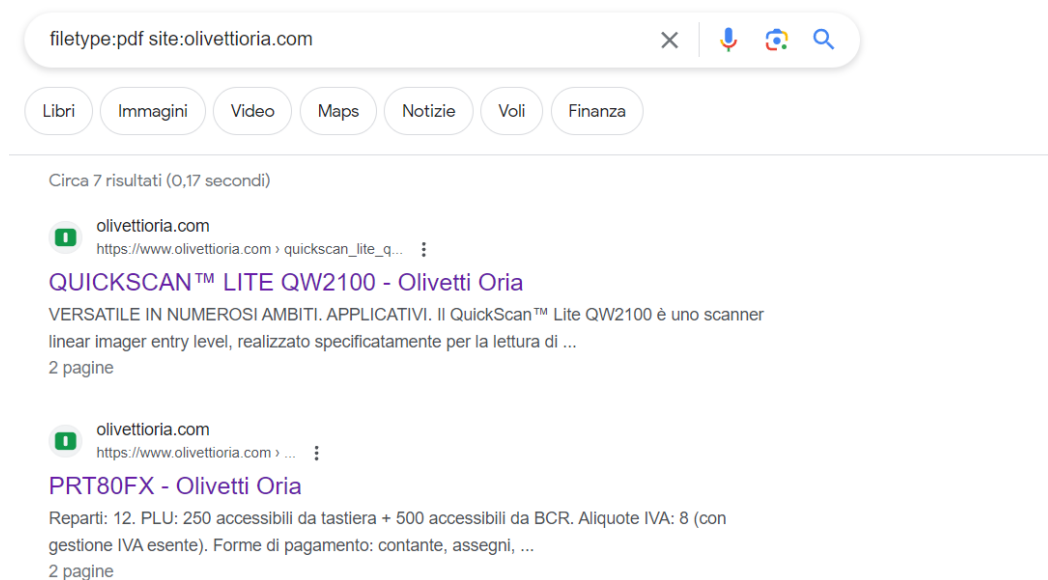


Ovviamente possiamo concatenare anche più stringhe utilizzando gli operatori. (AND,OR,NOT, | ).

**Intext:parolachiave site:nomedelsito.com** → con questa stringa andremo a visualizzare tutte quelle pagine del sito contenente la parola chiave che abbiamo specificato. (In questo caso è contatti)



**Filetype:estensione (pdf,txt,exel) site:nomedelsito.com** → con questa stringa andiamo a visualizzare tutte le estensioni specificate presenti nel sito.



**Ricorda:** si possono concatenare più stringhe assieme. Questo ci permetterà di essere più precisi e veloci nelle ricerche.

Qui Google ci da anche una mano fornendoci un sito con tutte le query utili.

**Google Hacking Database:** <https://www.exploit-db.com/google-hacking-database>