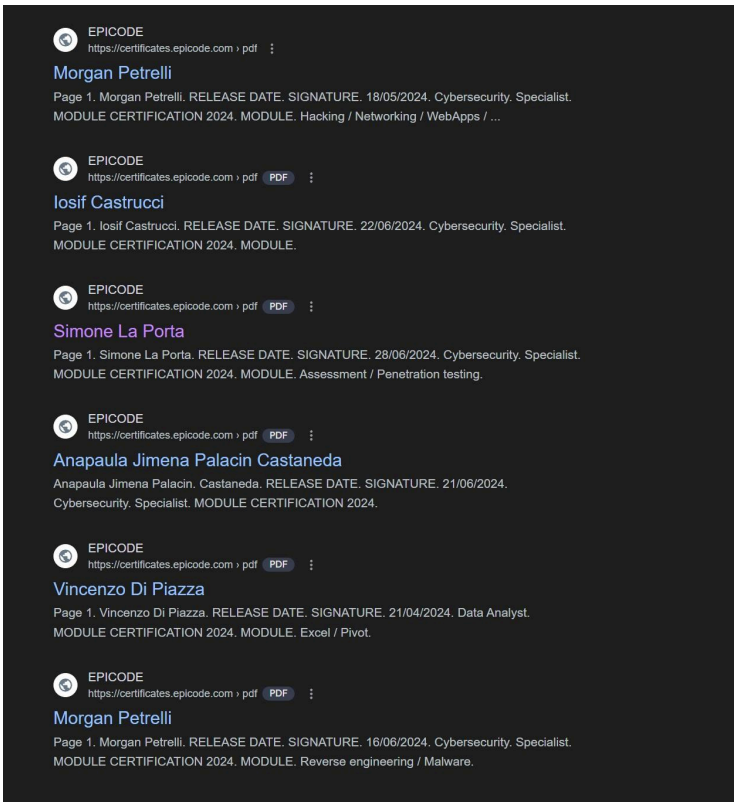
Esercizio S5L1 - Google Hacking e Maltego

L’esercizio di oggi si basava sui primi passi da compiere per la raccolta di informazioni e l’utilizzo del Google Hacking e Maltego con le informazioni OSINT disponibili sul web.

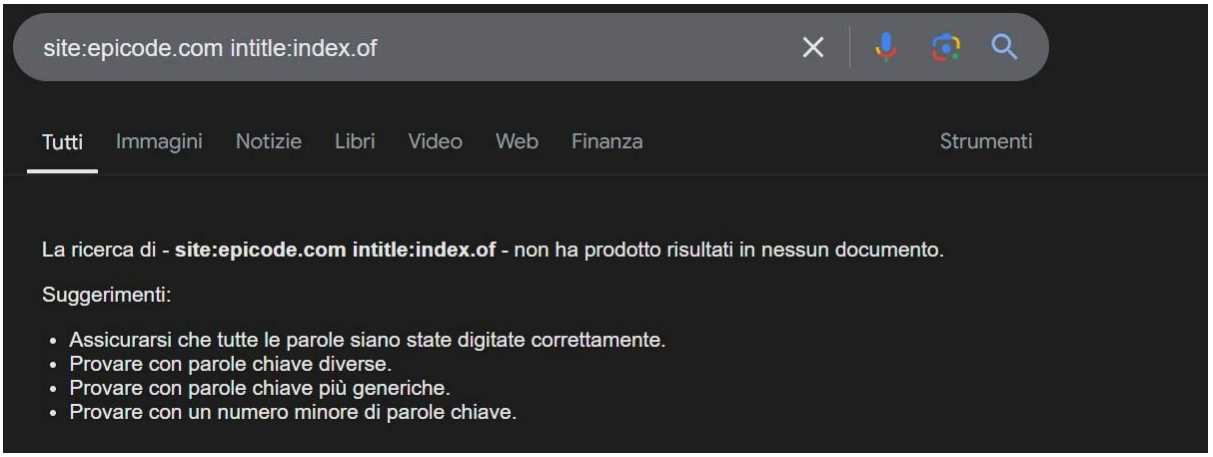
Riguardo al Google Hacking, ho tentato di reperire tutti i file pdf pubblici legati al domani epicode.com: attraverso questo ho ottenuto come risultati numerosi certificati pdf di ex-studenti: nonostante non siano informazioni sensibili, possiamo ottenere tutti i nomi e la data di diploma da qualunque dei certificati nello screenshot qui sotto:



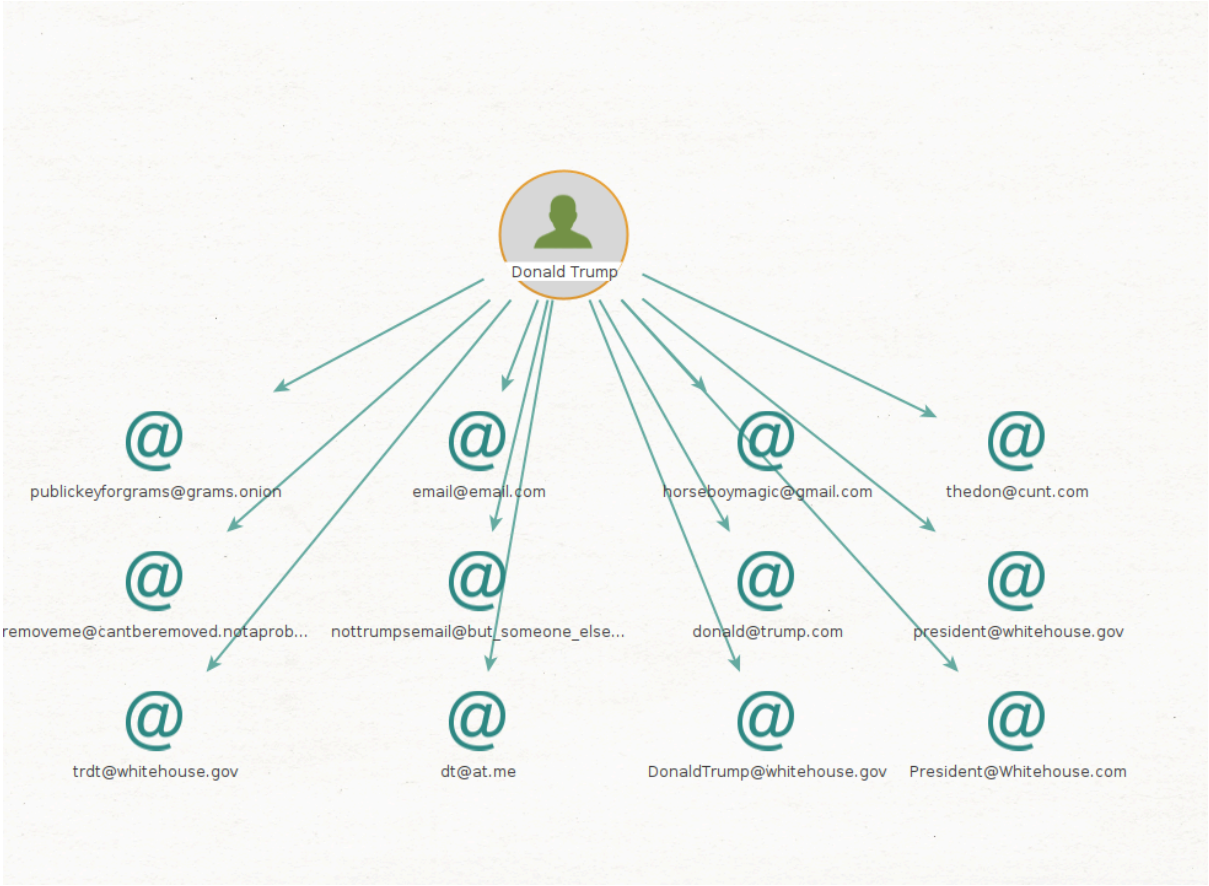
Qui un esempio di certificato:

Ho poi provato a vedere se sono disponibili file xls o doc, quindi modificabili, sullo stesso domain, ma come ci aspettavamo non c'era nulla del genere: da questo punto di vista il domain è sicuro.

Cercando invece di trovare directory o file nascosti utilizzando intitle con una combinazione di altri prompt di ricerca, abbiamo anche assodato che questa parte è più sicura rispetto ai filetype pdf.



Passando invece a Maltego, ho deciso di controllare il nome di Donald Trump:



Da quello che possiamo vedere, il nome di Donald Trump è associato a numerose email come anche il sito giornalistico satirico the Onion, la mail presidenziale, mail finte associate: questi potrebbero essere tutti metodi di raccolta dati utili per un'eventuale assessment su rischi di phishing, e in generale un modo di farsi un'idea generica di luoghi di origine di attacchi informatici o simili.