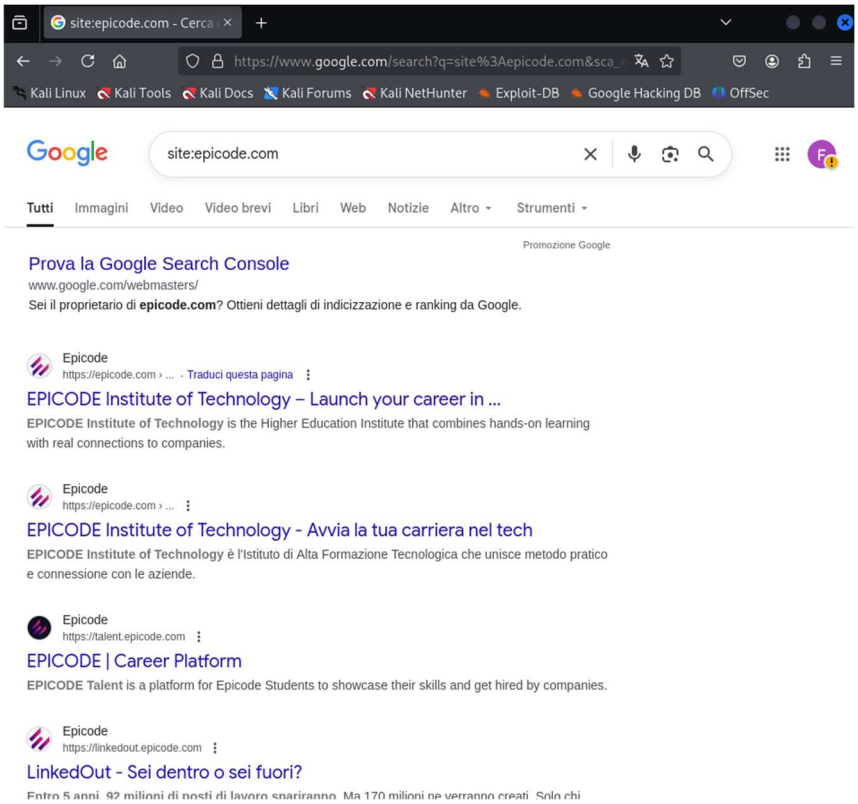
CONSEGNA W10D2

La traccia ci chiede di utilizzare i comandi di Goggle Hacking per raccogliere informazioni su un sito web.

Ovviamente abbiamo deciso di utilizzarli sul sito della nostra piattaforma “epicode.com” i vari comandi come mostrato nelle figure successive dove abbiamo utilizzato:

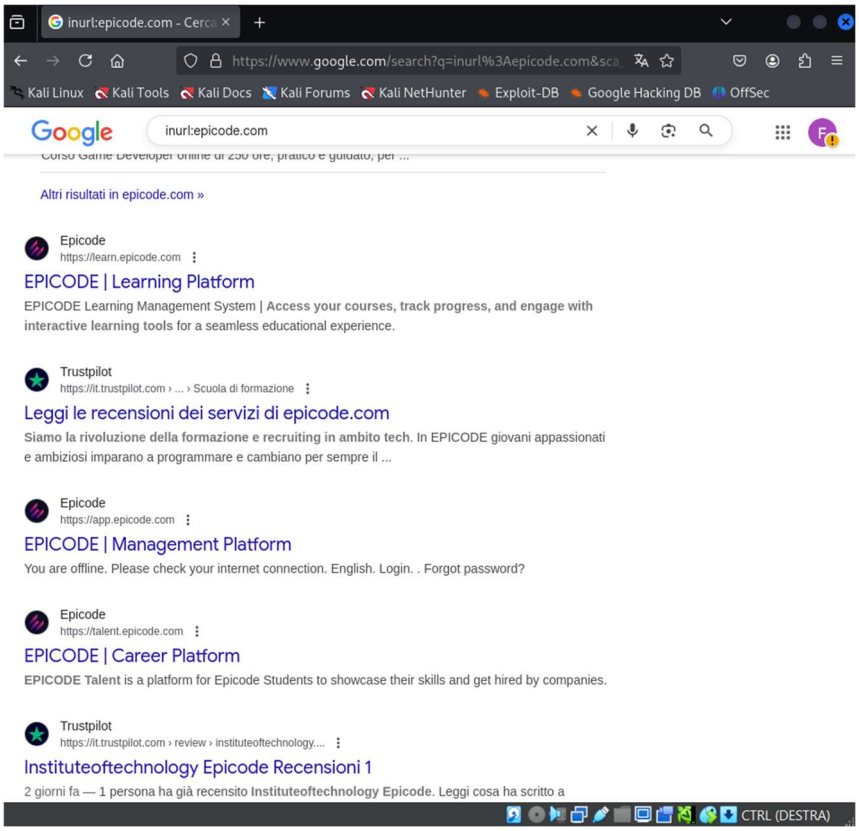
- Site:epicode.com

Il cui scopo è mostrare tutte le pagine indicizzate da Google appartenenti al dominio “epicode.com”. Quindi serve a farci capire la struttura del sito al fine ad esempio di scoprire le varie sottopagine come nel caso nostro corsi, contatti ecc.



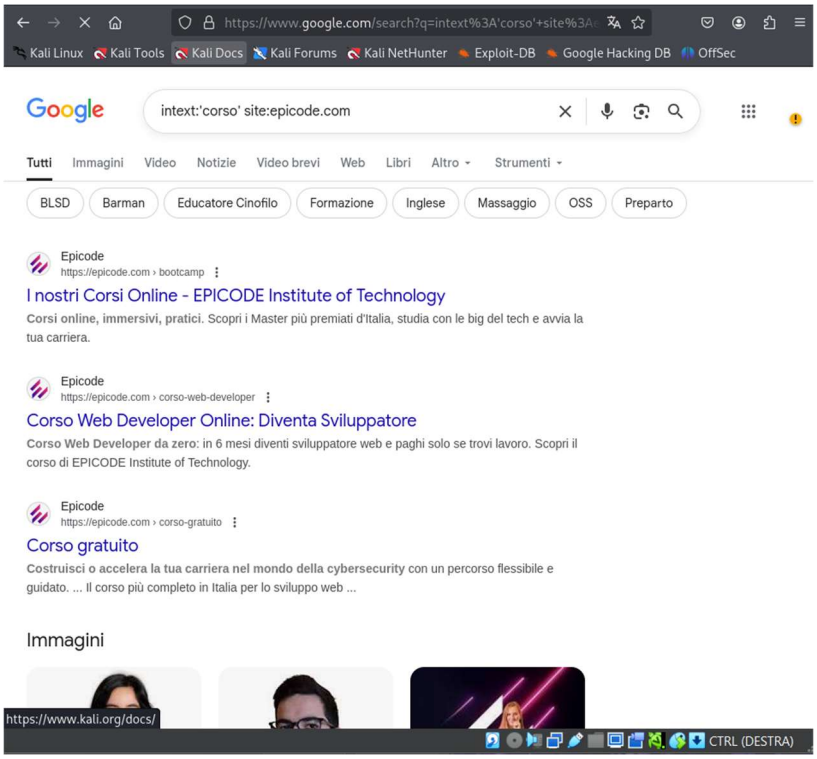
- Inurl:epicode.com

Lo scopo di questo comando è quello di cercare URL che contengono il nome del sito scelto, anche se non sono direttamente indicizzati. Questo comando è utile per individuare eventuali sottodomini o directory nascoste, ma soprattutto trovare URL con parametri specifici (come admin e login)



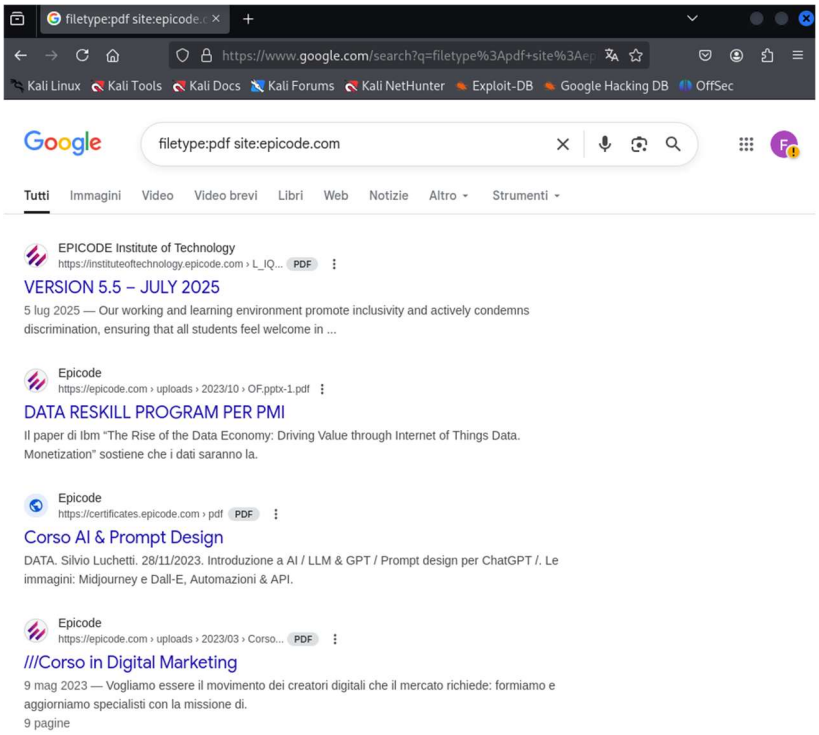
- Intext:”corso” site:”epicode.com”

Questo comando cerca sul sito indicato le pagine che contengono la parola “corso” nel testo. Serve a trovare contenuti specifici e fare ricerche mirate su temi scelti



- Filetype:pdf site:epicode.com

Con questo comando andiamo a cercare il tipo di file all'interno del sito. Nel nostro caso serve a trovare tutti i file in formato pdf.



Per il terzo punto della richiesta proviamo invece a:

- Analisi di file esposti

  Usiamo l'ultimo comando visto con lo scopo di cercare documenti contenenti dati sensibili riguardanti personale o studenti

- Cercare pagine di login o admin

  Qui proviamo tramite il comando "inurl" seguito da termini come ad esempio "login" al fine di cercare pagine di accesso non protette perché un pannello di amministrazione esposto può essere un punto di accesso.

- Directory indicizzate

  Tramite il comando "intitle" andiamo a cercare pagine contenenti liste di file e cartelle accessibile direttamente dal browser questo perché directory pubbliche possono contenere backup o configurazioni.

- Contenuti testuali sensibili

  Andiamo a cercare pagine che contengono parole come "password", "admin", "accesso" perché da questa ricerca è possibile scovare ad esempio qualche password che ovviamente può compromettere la sicurezza del sito.

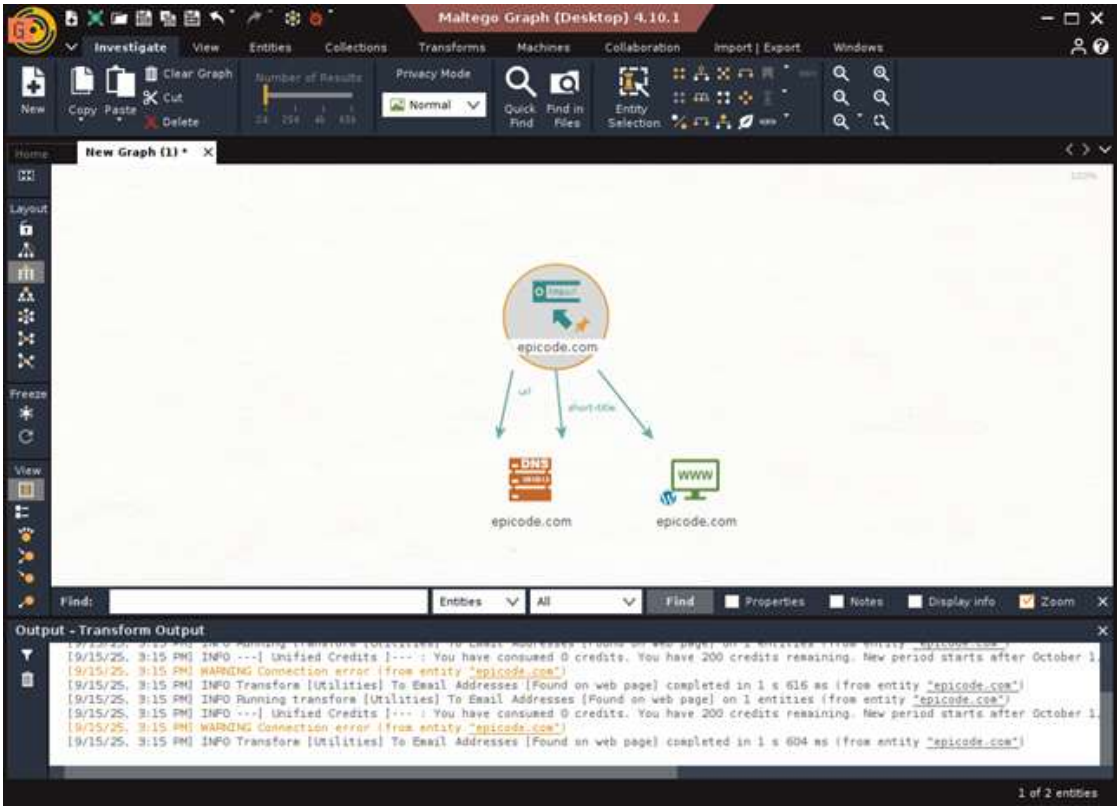
CONCLUSIONE

Il sito epicode.com risulta essere ben configurato dal punto di vista della sicurezza (basato ovviamente solo per le tecniche di Google Hacking) in quanto i vari comandi dati non risultano trovati file sensibili, directory esposte, nessuna info testuale critica rilevata e nessuna pagina di login/admin visibile. Segue una piccola tabella riassuntiva dei risultati.

AREA	STATO	NOTE
File sensibili	Sicuro	Nessun file riservato visibile
Directory esposte	Sicuro	Nessuna directory accessibile
Pagine di login/admin	Sicuro	Nessuna pagina rilevata via Google
Dati testuali sensibili	Sicuro	Nessuna parola chiave critica trovata

FACOLTATIVO

Usando maltego per fare un'analisi del dominio "epicode.com" questo è il risultato

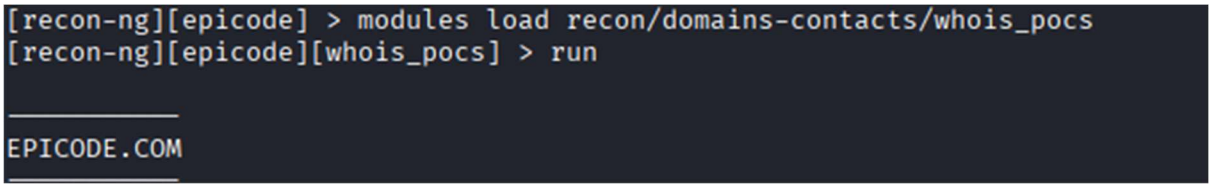


Da questo scan risulta che il dominio è attivo, al quale sono legate entità URL, Website e DNS. È emersa almeno una email pubblica associate a questo dominio come si vede dalla riga "INFO Running trasform to Email address" .

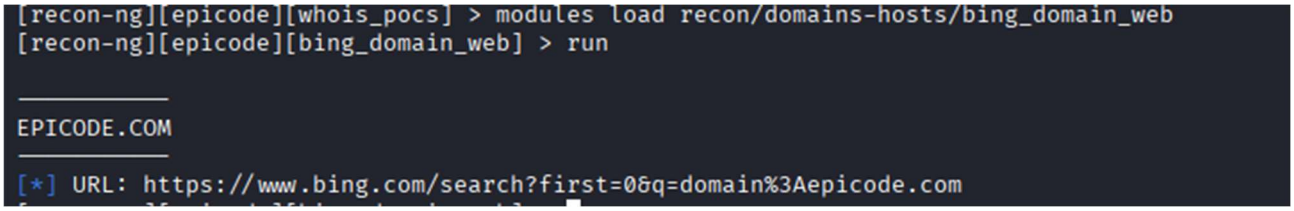
TRASFORMAZIONE	RISULTATO OTTENUTO	NOTE
DNS Name to IP ADDRESS	IP rilevato dal DNS	Conferma della risoluzione DNS
CONTENT FROM NET	Contenuto trovato sul sito	Potenziale fingerprinting del server
TO EMAIL ADDRESSES	Email pubbliche rilevate	Utili per analisi di contatto
TO WEBSITE / TO URL	Identificazione del sito WEB	Mappatura visiva delle entità

Allo stesso modo abbiamo fatto uno scan con recon-ng con lo stesso obiettivo.

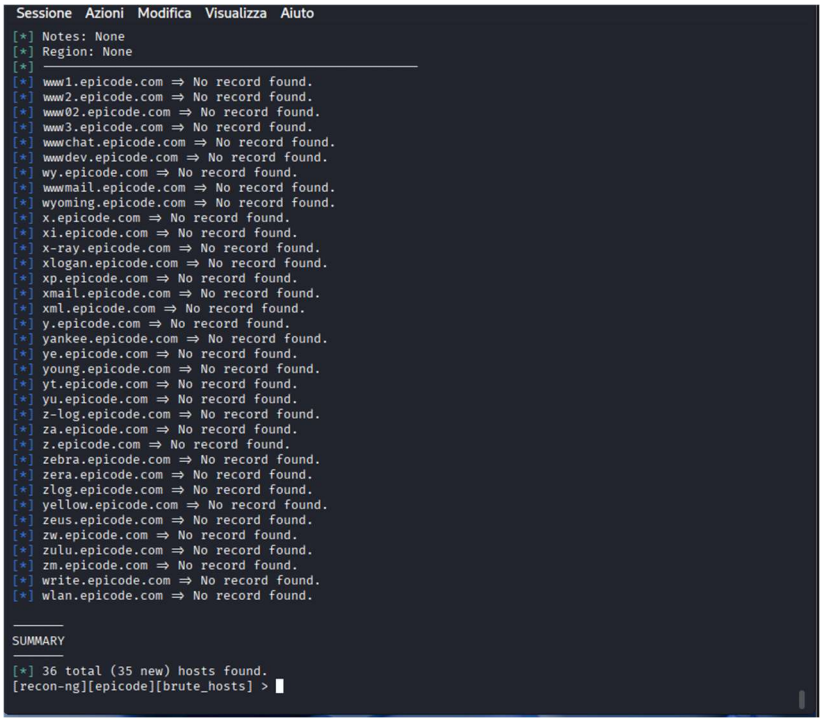
Utilizziamo “whois_pocs” identifichiamo chi va a registrare il dominio.



Dopo andiamo ad utilizzare il comando “bing_domain_web” con lo scopo di scoprire sottodomini.



Successivamente usiamo “brute-hosts” per vedere se e quali sottodomini nascosti o non indicizzati sono presenti nel dominio target non visibili tramite motori di ricerca.



L’attività ha evidenziato come Maltego sia ideale per una prima analisi visiva e relazionale, mentre Recon-ng offre una raccolta tecnica più profonda. In questo caso, il modulo brute_hosts ha permesso di scoprire numerosi sottodomini attivi, rivelando la complessità e distribuzione dell’infrastruttura di epicode.com.