

W10D2

REPORT RACCOLTA DATI

MASSIMILIANO PACE - EPICODE

DESCRIZIONE LAVORO SVOLTO

PER LA REALIZZAZIONE DI QUESTO REPORT SONO STATI UTILIZZATI VARI TOOL E VARIE TECNICHE DI RICERCA PER RECUPERARE PIU' DATI POSSIBILI .

LA PRIMA TECNICA UTILIZZATA SONO I DORKS , DELLE QUERY DI RICERCA AVANZATA CHE UTILIZZANO OPERATORI SPECIALI DI GOOGLE. TENTEREMO DI DI TROVARE INFORMAZIONI SPECIFICHE E EVENTUALI VULNERABILITA' DEL SITO WEB TARGET.

SITO WEB TARGET

WWW.EPICODE.COM

L'OBBIETTIVO PREFISSATO E' IL RIUSCIRE A REPERIRE PIU' INFORMAZIONI POSSIBILI . CERCHEREMO TUTTO CIO' CHE E' COLLEGATO AL SITO PRINCIPALE , QUINDI CI CONCENTREREMO NELLA RICERCA DI SOTTO DOMINI DI FILE SENSIBILI DIRECTORY DI BACKUP NON PROTETTE PAGINE DI LOGIN AMMINISTRATIVE , LISTE UTENTI , O MAGARI PAGINE DI CONFIGURAZIONI ESPOSTE PER ERRORE.

GOOGLE HACKING

Trovare directory e file sensibili

site:epicode.com intitle:"index of"

File di configurazione

site:epicode.com ext:env OR ext:ini OR ext:conf OR ext:log

Backup o vecchi database

site:epicode.com ext:bak OR ext:old OR ext:sql

Pagine di login amministrative

site:epicode.com inurl:admin OR inurl:login

Documenti sensibili

site:epicode.com ext:pdf OR ext:docx OR ext:xlsx confidential

Sottodomini

site:*.epicode.com -www

Errori o messaggi di debug

site:epicode.com "Warning" OR "Error" OR "Fatal error"

Password e credenziali

site:epicode.com intext:"password" OR intext:"credentials"

Risultato ricerca Dorks

Nella ricerca effettuata dei sotto domini ho evidenziato circa 16 pagine web

The screenshot shows a Google search results page with the query 'site:epicode.com -www'. The results include:

- EPCODE | Learning Platform**: https://learn.epicode.com/auth/login/dashboard [EPICODE Learning Management System | Access your courses, track progress, and engage with interactive learning tools for a seamless educational experience.]
- EPICODE Institute of Technology**: https://instituteoftechnology.epicode.com/_L_IQ... [VERSION 5.5 – JULY 2025] (3 lug 2023 — Our working and learning environment promote inclusivity and actively condemn discrimination, ensuring that all students feel welcome in ...)
- Corso AI & Prompt Design**: https://instituteoftechnology.epicode.com/_PDF... [DATA: Silvio Luchetti, 28/11/2023, Introduzione a AI / LLM & GPT / Prompt design per ChatGPT / Le immagini: Midjourney e Dall-E, Automazioni & API]

Below the results, there is a snippet from a document titled 'Corso AI & Prompt Design' by Silvio Luchetti, dated 28/11/2023, which includes the following text:

3 lug 2023 — Our working and learning environment promote inclusivity and actively condemn discrimination, ensuring that all students feel welcome in ...

Indietro 7 8 9 10 11 12 13 14 15 16

I risultati sono personalizzati - Prova senza risultati personalizzati

Italia • Bussolengo, Città metropolitana di Milano - In base ai tuoi luoghi (caso) - Aggiorna posizione

Guida Invia feedback Privacy Termini

Tra i risultati si evidenzia la pubblicazione online di molte certificazioni ottenute dagli iscritti al corso.
benchmark.epicode.com)



The screenshot shows a Google search results page with the query 'site:benchmark.epicode.com'. The results include several entries for 'EPCODE School — Benchmark Management' with various descriptions and links to the site.

Epicode School — Benchmark Management
EPICODE COURSE SPECIFICATIONSCompletion date: 30/08/2023 Awarded to Niccolò Starfella
Description: Introduction to Java Programming, Flow Control, COP in Java, ...

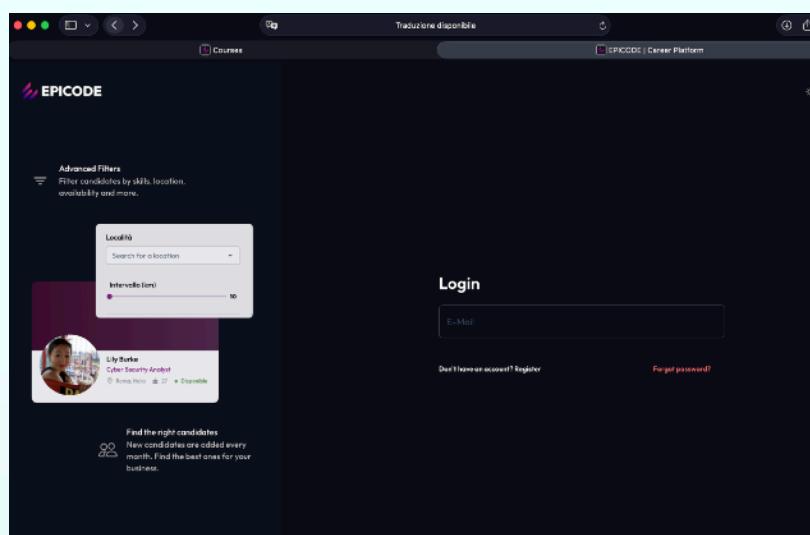
Epicode School — Benchmark Management
EPICODE COURSE SPECIFICATIONSCompletion date: 27/08/2023 Awarded to Jamila Allegria
Description: Introduction to Database Relations: table, query, join, view, ...

Epicode School — Benchmark Management
EPICODE COURSE SPECIFICATIONSCompletion date: 19/11/2023 Awarded to Andrea Burghella
Description: Content Marketing, SMM, SEM, SEO, SEA

Epicode School — Benchmark Management
Write your future, one line of code at a time. EPICODE: where ambitious individuals train to become brilliant developers, launching their careers with ...

Epicode School — Benchmark Management
Write your future, one line of code at a time. EPICODE: where ambitious individuals train to become brilliant developers, launching their careers with ...

Nella ricerca effettuata sono emersi dei sottodomini dedicati alle aziende interessate all'assunzione e ricerca di nuovi talenti. E' stato trovato anche il pdf con le condizioni generali per l'accesso al sito da parte di aziende esterne.



CONDIZIONI GENERALI DI ACCESSO E CONSULTAZIONE DELLA PIATTAFORMA AZIENDE

1. OGGETTO

Le presenti Condizioni Generali regolamentano i termini e le condizioni di accesso e consultazione della Piattaforma Aziende on-line, dedicato alle aziende, (di seguito "Piattaforma Aziende") di proprietà della Epic Education S.r.l. c.f. e p.I. 15878410068, n. iscrizione al registro delle Imprese di Roma 1820967, cap. soc. I.v. € 1417,65, con sede legale in Roma, via dei Magazzini Generali 16, pec. epiceducation@legalmail.it, email info@epicode.school (di seguito "Epic Education"), accessibile dal sito www.epicode.it (di seguito "Sito"). La Piattaforma Aziende costituisce lo strumento mediante il quale Epic Education promuove attivamente l'incontro tra domanda ed offerta di lavoro in relazione alla figura professionale di specialista in area ICT.

1.2. L'accesso alla Piattaforma Aziende è consentito a tutte le persone fisiche o giuridiche – mediante propri incaricati – che, in relazione allo proprio area di attività esercitata, sono interessati a cercare personale specializzato da inserire nel proprio organico, preventivamente registrato sul Sito mediante compilazione dell'apposito modulo di registrazione (di seguito "Azienda") e dei dati caratteristici dell'Azienda (di seguito Profile Azienda).

1.3. La registrazione dell'Azienda e la compilazione del relativo Profilo Azienda sono subordinate all'approvazione da parte della Epic Education. In caso di accettazione, verrà inviata una comunicazione a mezzo e-mail all'indirizzo indicato in sede di registrazione, contenente il link per la verifica di tale indirizzo a completamento dell'avvenuta registrazione.

1.4. Il contrassegno dell'apposita spunta dalla casella "Terms and Condition" posta in calce al formato di iscrizione presente sul Sito equivale a sottoscrizione delle presenti Condizioni Generali. Contrassegnando con l'apposita spunta la casella "Terms and Condition" posta in calce al formato di iscrizione presente sul Sito, l'Azienda dichiara di accettare integralmente le clausole contenute nelle presenti Condizioni Generali, nonché del contenuto delle disposizioni, dei documenti e delle procedure in esse richiamate.

2. ACCESSO E CONSULTAZIONE DELLA PIATTAFORMA AZIENDE

2.1. Completata la registrazione, l'Azienda accede alla Piattaforma Aziende inserendo le proprie credenziali.

2.2. L'accesso e la consultazione della Piattaforma Aziende sono a titolo gratuito, fermo quanto previsto dai

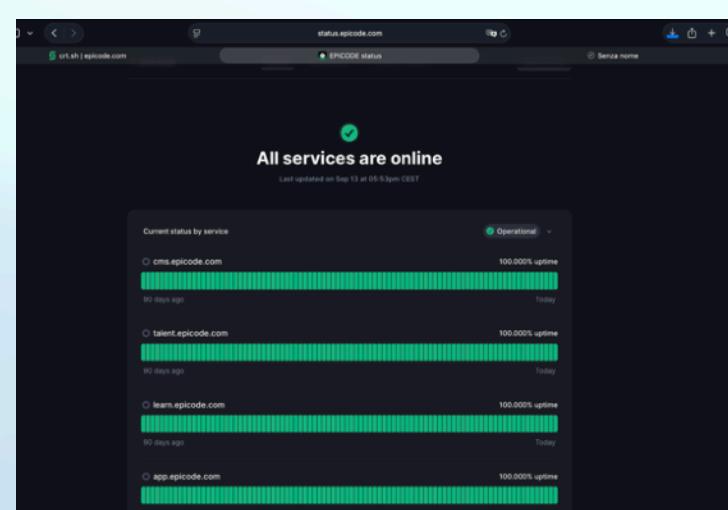
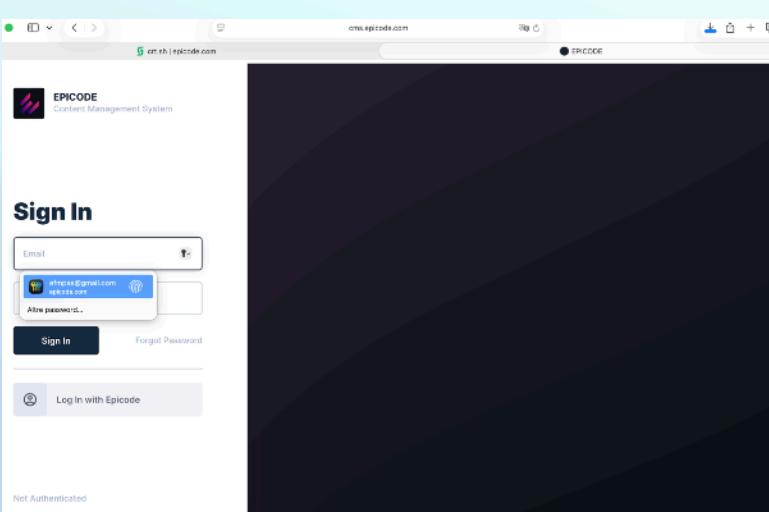
Visti gli scarsi risultati ottenuti con i dorks ho preso la decisione di affidarmi al sito crt.sh.

Crt.sh è un sito davvero utile per chi si occupa di sicurezza informatica o semplicemente vuole monitorare i certificati SSL/TLS. In pratica, è un motore di ricerca di certificati pubblici.

In questo caso i risultati sono stati piu' incoraggianti

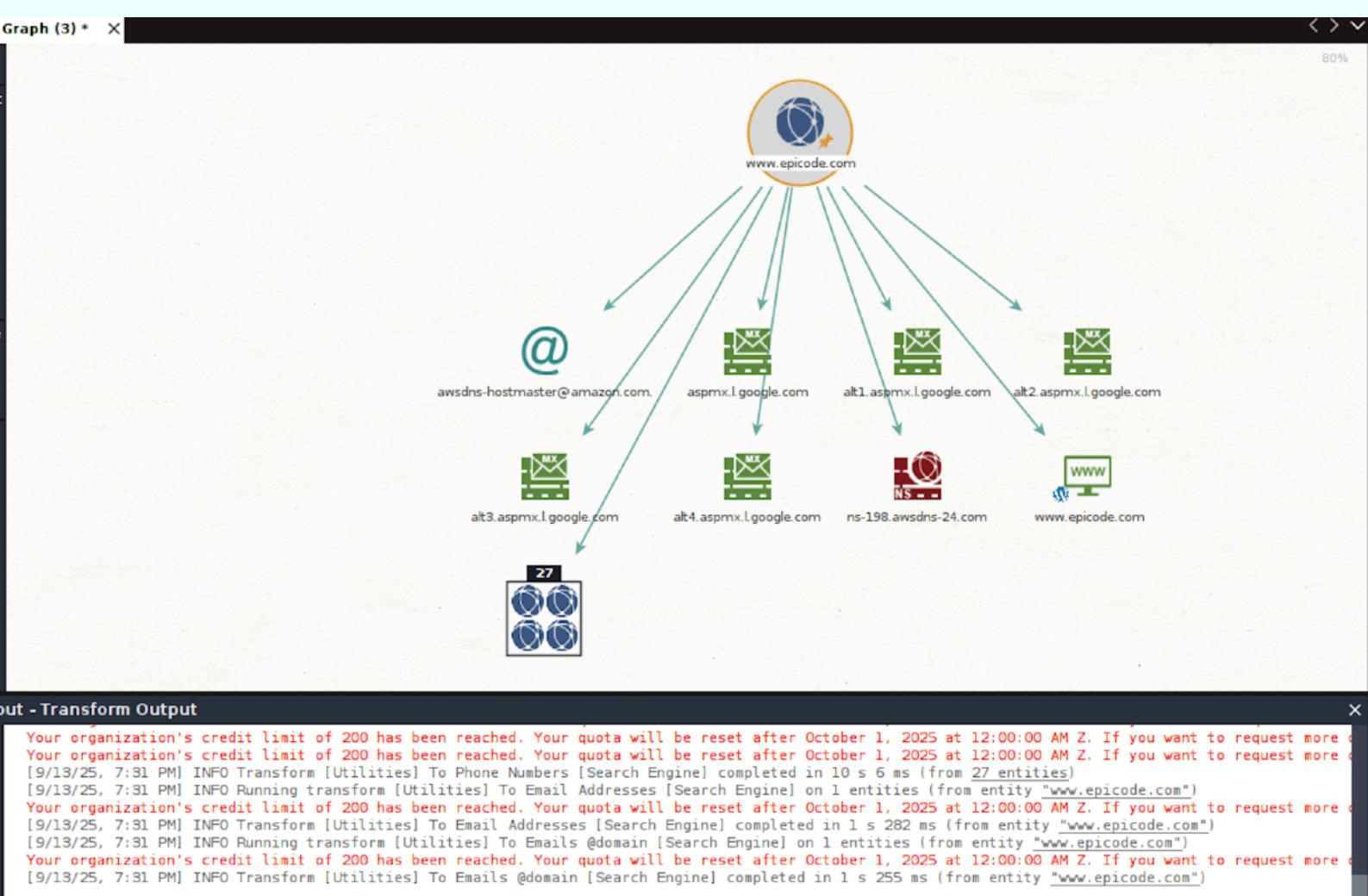
crt.sh			
2081954524	2025-09-06	2025-09-06 2025-12-05	institutetechnology.epicode.com
20819540586	2025-09-06	2025-09-06 2025-12-05	institutetechnology.epicode.com
20810110357	2025-09-05	2025-09-05 2025-12-04	demo.epicode.com
20810078399	2025-09-05	2025-09-05 2025-12-04	demo.epicode.com
20774216300	2025-09-03	2025-09-03 2025-12-02	ouewwtwotgbif.eu-1.tagmanagerserverside.it
20773528379	2025-09-03	2025-09-03 2025-12-02	ouewwtwotgbif.eu-1.tagmanagerserverside.it
20724403736	2025-09-01	2025-09-01 2025-11-30	join.epicode.com
20724403903	2025-09-01	2025-09-01 2025-11-30	join.epicode.com
20723186308	2025-09-01	2025-09-01 2025-11-30	auth.epicode.com
20723178450	2025-09-01	2025-09-01 2025-11-30	auth.epicode.com
20723184233	2025-09-01	2025-09-01 2025-11-30	cool.epicode.com
20723177556	2025-09-01	2025-09-01 2025-11-30	cool.epicode.com
20617968178	2025-08-28	2025-08-26 2025-09-26	parser.epicode.com
20576857441	2025-08-26	2025-08-25 2025-11-23	linkedout.epicode.com
20576856969	2025-08-26	2025-08-25 2025-11-23	linkedout.epicode.com
20576815185	2025-08-26	2025-08-25 2025-11-23	benchmark.epicode.com
20576815499	2025-08-26	2025-08-25 2025-11-23	benchmark.epicode.com
20480056639	2025-08-21	2025-08-21 2025-11-19	status.epicode.com
20479053587	2025-08-21	2025-08-21 2025-11-19	status.epicode.com
20418433630	2025-08-18	2025-08-18 2025-11-16	gol.epicode.com
20418481728	2025-08-18	2025-08-18 2025-11-16	gol.epicode.com
20418417625	2025-08-18	2025-08-18 2025-11-16	gol.epicode.com
20408447206	2025-08-18	2025-08-18 2025-11-16	gol.epicode.com
20317914470	2025-08-14	2024-09-13 2025-10-12	docgen.epicode.com
20317885234	2025-08-14	2025-08-14 2026-09-12	docgen.epicode.com
20296674042	2025-08-13	2025-08-13 2026-09-11	ai.epicode.com
20176200857	2025-08-07	2025-08-07 2025-11-05	local.ml.epicode.com
20176182737	2025-08-07	2025-08-07 2025-11-05	local.ml.epicode.com
20169585045	2025-08-07	2025-08-07 2025-11-05	dev.ml.epicode.com
20169585388	2025-08-07	2025-08-07 2025-11-05	dev.ml.epicode.com
20166109321	2025-08-06	2025-08-06 2025-11-04	ml.epicode.com
20166109683	2025-08-06	2025-08-06 2025-11-04	ml.epicode.com
20087329512	2025-08-03	2025-08-03 2025-11-01	apollo.epicode.com
20087329127	2025-08-03	2025-08-03 2025-11-01	apollo.epicode.com
19958050452	2025-07-28	2025-07-28 2025-10-26	onboarding.epicode.com
19958049842	2025-07-28	2025-07-28 2025-10-26	onboarding.epicode.com
19933249650	2025-07-27	2025-07-27 2025-10-25	dashboard.epicode.com
19933249986	2025-07-27	2025-07-27 2025-10-25	dashboard.epicode.com
19911644806	2025-07-26	2025-07-26 2025-10-24	epicode.com
19911644536	2025-07-26	2025-07-26 2025-10-24	epicode.com
19876550171	2025-07-24	2025-07-24 2025-10-22	bucket.epicode.com
19876551685	2025-07-24	2025-07-24 2025-10-22	bucket.epicode.com
19876551032	2025-07-24	2025-07-24 2025-10-22	console-bucket.epicode.com
19876551020	2025-07-24	2025-07-24 2025-10-22	console-bucket.epicode.com
19771116075	2025-07-19	2025-07-19 2025-10-17	microlearn.epicode.com
19771113530	2025-07-19	2025-07-19 2025-10-17	microlearn.epicode.com
19763962778	2025-07-18	2025-07-18 2025-10-16	fehigcii.eu-1.tagmanagerserverside.it
19763951988	2025-07-18	2025-07-18 2025-10-16	fehigcii.eu-1.tagmanagerserverside.it
19522257823	2025-07-08	2025-07-08 2025-10-06	institutetechnology.epicode.com

Sono stati trovati molti sottodomini con diversi login di sistema e lo status dashboard , che mostra lo stato operativo dei vari servizi e sottodomini.



ESERCIZIO FACOLTATIVO MALTEGO e RECON-NG

L'ESERCIZIO FACOLTATIVO CI CHIEDE DI UTILIZZARE 2 TOOL IN PARTICOLARE . MALTEGO E RECON-NG SONO MOLTO SIMILI NELLA SOSTANZA MA SI DIFFERENZIANO PER UN PARTICOLARE, L'INTERFACCIA GRAFICA. MALTEGO VISIVAMENTE E' PIU INTUITIVO , RECON-NG SI UTILIZZA CON COMANDI DA TERMINALE.



File Actions Edit View Help

```
[*] mtu.epicode.com => No record found.  
[*] music.epicode.com => No record found.  
[*] multimedia.epicode.com => No record found.  
[*] mx.epicode.com => No record found.  
[*] mu.epicode.com => No record found.  
[*] mta.epicode.com => No record found.  
[*] mw.epicode.com => No record found.  
[*] mv.epicode.com => No record found.  
[*] mysql.epicode.com => No record found.  
[*] mysql01.epicode.com => No record found.  
[*] my.epicode.com => No record found.  
[*] mysql0.epicode.com => No record found.  
[*] Country: None  
[*] Host: ml.epicode.com  
[*] Ip_Address: 66.33.60.129  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] n.epicode.com => No record found.  
[*] mysql1.epicode.com => No record found.  
[*] na.epicode.com => No record found.  
[*] mz.epicode.com => No record found.  
[*] nashville.epicode.com => No record found.  
[*] nameserv.epicode.com => No record found.  
[*] nas.epicode.com => No record found.  
[*] names.epicode.com => No record found.  
[*] name.epicode.com => No record found.  
[*] nameserver.epicode.com => No record found.  
[*] nat.epicode.com => No record found.  
[*] nds.epicode.com => No record found.  
[*] nc.epicode.com => No record found.  
[*] nd.epicode.com => No record found.  
[*] ne.epicode.com => No record found.  
[*] neptune.epicode.com => No record found.  
[*] nebraska.epicode.com => No record found.  
[*] netdata.epicode.com => No record found.  
[*] net.epicode.com => No record found.  
[*] netapp.epicode.com => No record found.  
[*] netgear.epicode.com => No record found.  
[*] netscaler.epicode.com => No record found.
```

File Actions Edit View Help

```
[*] Ip_Address: 13.226.175.118  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] certificates.epicode.com => (A) 13.226.175.32  
[*] classroom.epicode.com => No record found.  
[*] clicktrack.epicode.com => No record found.  
[*] classifieds.epicode.com => No record found.  
[*] cleveland.epicode.com => No record found.  
[*] client.epicode.com => No record found.  
[*] classes.epicode.com => No record found.  
[*] clients.epicode.com => No record found.  
[*] Country: None  
[*] Host: certificates.epicode.com  
[*] Ip_Address: 13.226.175.32  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] clientes.epicode.com => No record found.  
[*] club.epicode.com => No record found.  
[*] cm.epicode.com => No record found.  
[*] cmail.epicode.com => No record found.  
[*] clusters.epicode.com => No record found.  
[*] clubs.epicode.com => No record found.  
[*] cms.epicode.com => (A) 18.158.255.147  
[*] code.epicode.com => No record found.  
[*] co.epicode.com => No record found.  
[*] columbus.epicode.com => No record found.  
[*] coldfusion.epicode.com => No record found.  
[*] cocoa.epicode.com => No record found.  
[*] cn.epicode.com => No record found.  
[*] Country: None  
[*] colorado.epicode.com => No record found.  
[*] columbus.epicode.com => No record found.  
[*] cluster.epicode.com => No record found.
```

TABELLA RIEPILOGATIVA

NOME	RISULTATI TROVATI
MALTEGO	DOMINI,SOTTODOMINI,EMAIL,SOA,WHOIS,HOST
RECON-NG	DOMINI,SOTTODOMINI
CRT	DOMINI,SOTTODOMINI,CERTIFICATI SSL-TLS
DORKS	DOMINI,SOTTODOMINI,PDF

RIFLESSIONI E DIFFICOLTA' RISCONTRATE

UTILIZZANDO MALTEGO MI SONO RESO CONTO DEI LIMITI DEL PROGRAMMA. MALTEGO SI BASA SU CREDITI A CONSUMO E QUESTO POTREBBE ESSERE UN PROBLEMA NELLA CREAZIONE CONTINUA DI NUOVE MAIL CON CUI REGISTRARE IL PROGRAMMA OGNI VOLTA.

CON RECON-NG HO AVUTO PROBLEMI DI MODULI NON FUNZIONANTI IN PARTICOLARE COL MODULO WHOIS.

CRT.SH MI HA SORPRESO POSITIVAMENTE PER LA QUANTITA' DI INFORMAZIONI RACCOLTE.

Conclusioni

Dopo avere effettuato vari tipi di ricerca utilizzando diversi Dorks, sono giunto alla conclusione che il sito www.epicode.com ha preso delle misure per rendere piu' difficile o meno efficace l'utilizzo di questa tecnica. Esiste la possibilita' di dire ai motori di ricerca di non indicizzare certe directory o tipi di file, magari implementando header di sicurezza o configurazioni che rendano meno visibili certi contenuti