Passive Reconnaissance with Digital Certificates

@mmar

AIM

- We are trying to find subdomains of a website that may be using the same digital certificate

Digital certificates are primarily used to ensure the security and authenticity of websites. They help to establish a secure connection between a user's browser and the website they are trying to access, by verifying that the website is legitimate and encrypting the data that is exchanged between the two parties.

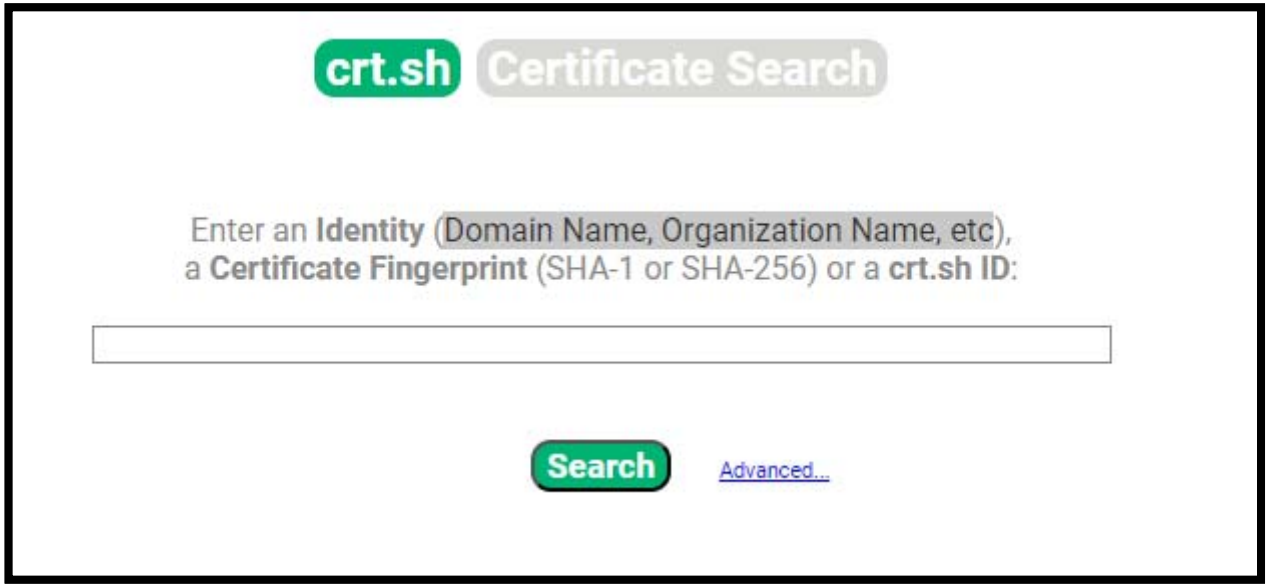
Digital certificates can also be used to discover subdomains of a website. When a certificate is issued for a specific domain, it is typically issued for that domain and any of its subdomains. Therefore, by searching for certificates issued to a particular domain, it is possible to discover subdomains that are associated with that domain.

Digital Certs search engines

Crt.sh

- Allows searching with Domain Name, Organization Name, etc

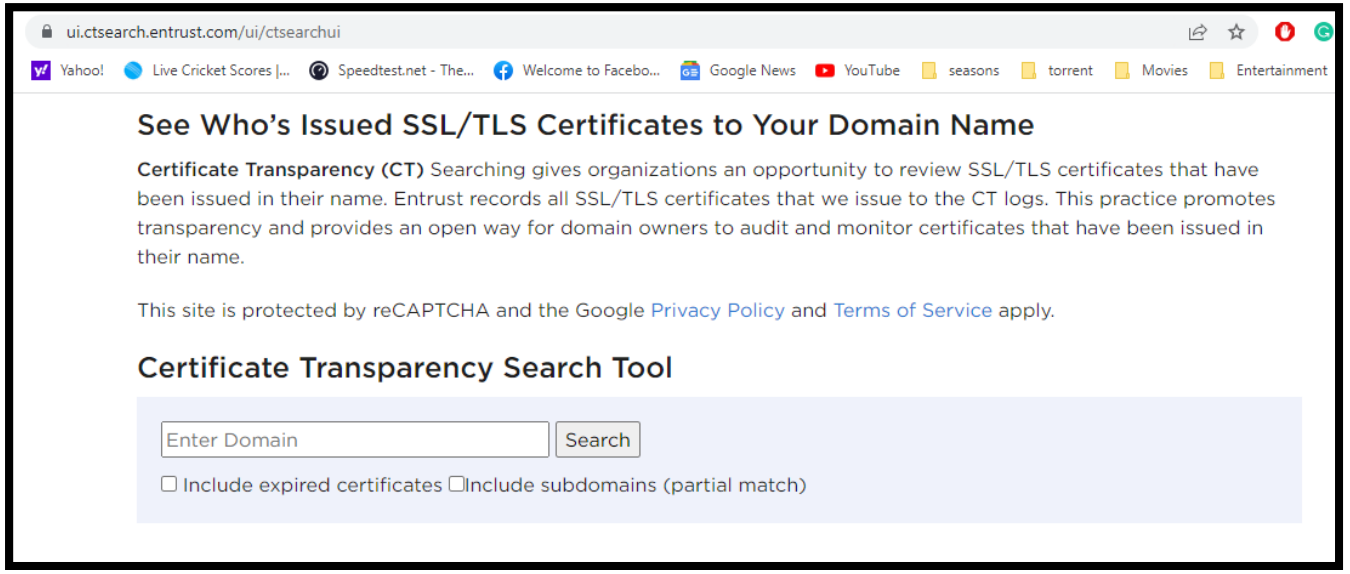
https://crt.sh/



Entrust cert search

- Allows searching for partial as well as expired certificates

https://ui.ctsearch.entrust.com/ui/ctsearchui



Censys

- Censys is a search engine for all internet connected devices and has a separate functionality to search digital certificates

https://search.censys.io/

DEMO