CS-6387-50 - Topics in Software Engineering - Cybersecurity

Benjamin Ray

Final project – Legit DNS Browser Extension

Installation

Open the Extension Management page by navigating to chrome://extensions.

* Alternatively, open this page by clicking on the Extensions menu button and selecting Manage Extensions at the bottom of the menu.
* Alternatively, open this page by clicking on the Chrome menu, hovering over More Tools then selecting Extensions

Enable Developer Mode by clicking the toggle switch next to Developer mode.

Click the Load unpacked button and select the extension directory.

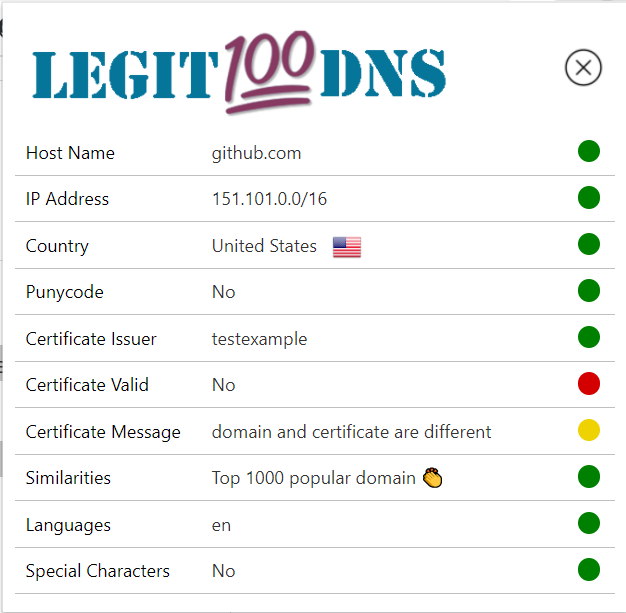
Extension Architecture

Google Chrome extensions are only allowed to use front end technology for coding. Therefore, LegitDNS is written in HTML, JavaScript, and CSS. No JavaScript frameworks were used. Google Chrome offers a robust API which can allow control over the application lifecycle, when the extension starts, when the domain is open, etc.

Aside from these front-end technologies, two APIs were used to retrieve DNS information such as certificate information and domain location. The APIs are mentioned below.

Color Codes

LegitDNS evaluates properties of a domain and provide an assessment of how safe a particular metric is. A green circle indicates that the metric is most likely safe. A yellow circle is a warning to users to use caution and evaluate on their own whether a certain metric on a domain is dangerous. A red circle indicates that a domain is potentially dangerous and that the user should take extreme caution when viewing the site.



Domain Name

The domain name is retrieved by the extension by taking the url of the current request, removing damin prefixes and paths. It displays the domain suffix though.

For Example, <https://developer.chrome.com/docs/extensions/> will get reduced to chrome.com

Network Address

Retrieved from the location API from ipfind.io, network path provides the user information about the IP and network on which it’s hosted.

Unicode Characters

The Unicode characters functionality will detect non-ascii characters in the domain name string. If it finds that there are non-ascii characters and it is converted to Punycode, the extension will decode the Punycode to show the converted string with the Unicode characters. Beside the domain, it ill list the special characters from the domain in brackets.

There are cases where Unicode variables are valid because they are used in international web domains.

The extension will display a red alert to show user that there are non-ascii characters in the domain name. The user can decide whether or not the domain is legitimate by analyzing the

apple.com

аpplе.com

A malicious example could be using the Cyrillic letters Ye (е) and A (а) in the domain Apple.com.

аpplе.com (Unicode and ascii) looks identical to apple.com (ascii).

The extension will show: аpplе.com (а,е) and display the red alert.

Country

Country of which the domain is hosted in is displayed as well as the country’s flag. The country is retrieved from an API from IPFind.io.

Knowing which country, a domain is hosted in could help a user indicate whether a domain is hosted where they think it is.

API

There are two external APIs used in the extension.

One API used by the extension is from IPfind.io, an API featured on Rapid API. It is used to retrieve location and language information for the requested domain.

find-any-ip-address-or-domain-location-world-wide.p.rapidapi.com

The other API is from Check SSL, an offered by Rapid API detects certificate information from a specified domain name. The API returns the certificate issuer, whether the certificate is valid and customized message based on information about the certificate. The certificate is considered self-signed if the issuer and subject are the same

check-ssl.p.rapidapi.com

Certificate Issuer

From the rapid Api used in the extension, the certificate issuer is retrieved. It is up to the user to determine whether the issuer is from a legitimate domain provider such as GoDaddy or VeriSign.

Certificate Validity

The certificate is determined legitimate by the Check SSL. A valid certificate will match the domain and isn’t self-signed. A Yes or No will be displayed based on whether the certificate is deemed valid.

Certificate Message

A message will return from the API to indicate anything unusual about the certificate. For example, the domain and certificate may be different or may come from an unreputable domain issuer.

Languages

The domain location API sued will detect the country in which the site is hosted. It will also indicate which languages the website supports.

This could potentially help decipher is Punycode is a character in a language that the site supports.

Similarities

The similarities section compares the viewed domain string is suspiciously similar to popular websites. Hackers will sometimes host domains similar to those of popular legitimate sites in order confuse users into believing they are using the spoofed site.

Using the Levenstein distance, a script is used to one by one compare the domain to the top popular website. A json string containing the current top 1000 most popular sites is fetched in JavaScript.

For this extension, a domain is considered close to a popular website if the Levenstein distance is between 1 and 3. This system works especially well with longer domains.

An example of this in action is a user typing in nytimesr.com when they meant to input nytimes.com. The Levenstein distance is one, so the extension displays a yellow circle indicating a warning to check if that is the site they meant to access.

Punycode

The extension detects Punycode simply by checking for “xn—” in the domain name. This is the standard prefix specified by the IDNA (Internationalized Domain Names in Applications). Most modern browser will detect non-ascii characters in the domain and redirect to the ASCII version of the domain name.

This feature is used in conjunction with the Unicode Characters section in the extension. If a domain contains Punycode, the Unicode characters section will display the original Unicode/ASCII version of the domain and display which characters are Unicode in a comma separated list in Brackets.