OWASP
Open Web Application
Security Project

Tor

isn't as "anonymous" as you thought!

FingerprintJS says it has identified a more dubious fingerprinting technique capable of generating a consistent identifier across different desktop browsers, including Tor browser.

What's the deal :

Using Safari, Firefox, or Chrome for some websites, and use the Tor browser to anonymously view others, there is a chance of someone being able to link your browser histories across all those sessions using a unique identifier, thus deanonymize and track you.

Who said so:

Konstantin Darutkin,

Software Engineer at FingerprintJS.

FingerprintJS is a browser fingerprinting library that queries browser attributes and computes a hashed visitor identifier from them.

The buzzword is “scheme flooding”

The scheme flooding vulnerability allows an attacker to determine which applications you have installed. In order to generate a 32-bit cross-browser device identifier, a website can test a list of 32 popular applications and check if each is installed or not.

What not?

The issue has been reported to the Chromium team which is currently looking at ways to address the problem.

In Firefox and Safari, scheme flooding works because the browser loads different internal pages depending upon whether the requested app is present or absent, which is all the information needed for that bit in the 32-bit app-count identifier.

The situation is similar for the Tor browser, which is based on Firefox code but requires the use of iframe elements to check app presence and time. It can take minutes to fingerprint a user.