Browser Metrics

Fingerprinting

Assessing browser defenses against fingerprinting poses a unique challenge due to the technique of ”farbling,” where browsers purposefully supply incorrect values for queries that may be used to generate a unique hash, identifying the user across sites and visits. If browsers were to block access to all such requests, that might be inadvertently aiding the fingerprinting process. Therefore, we analyze the meta-information browsers willingly disclose to ascertain the extent to which they may be susceptible to fingerprinting tactics.

PrivacyTests.org

Media query screen height: Height of the user’s screen in pixels.

Media query screen width: Width of the user’s screen in pixels.

outerHeight: Height of the browser window in pixels, including browser chrome.

screen.height: Height of the user’s screen, in pixels.

screen.width: Width of the user’s screen, in pixels.

screenX: Position, in pixels, of the left edge of the browser window on screen.

screenY: Position, in pixels, of the top edge of the browser window on screen.

Privacy Test Pages

Harmful APIs: Tests if web APIs that are considered harmful are available in browsers.

Browser Leaks

TCP/IP Fingerpinting: Tests data fields in a TCP/IP packet to identify various configuration attributes of a networked device.

TLS Fingerprint: Generates a TLS fingerprint in JA3 format.

Unicode Glyphs: Simulates a unicode glyphs measurement technique.

WebGL Extensions: Pulls supported WebGL Extensions.

WebGL Fingerprint: Generates WebGL Report and Image Hash.

WebRTC IP Address Detection: Tests if there is WebRTC leak.

WebRTC Media Devices: Checks for API support and requests audio and video permissions.

WebRTC Support Detection: Tests for feature-detection of RTCPeerConnection and RTCDataChannel.

Screen Object: Information about user’s screen.

Date/Time: System date and time information.

Internationalization API: Tests language-sensitive string comparison, number formatting, and date and time formatting.

Navigator Object: Information about the state and the identity of the user agent.

Navigator.userAgentData: Tests a set of HTTP Headers and JavaScript API that allow web browsers to send detailed information about the device and browser to a web server.

Navigator.plugins:	The information about the web browser extensions that can mitigate potential threats from JavaScript.
Batery Status API:	Battery status information.
Network Information API:	Information about the system's connection.
Canvas Fingerprinting:	Generates Canvas fingerprint and checks uniqueness.
Web Browser:	Attempts to identify browser via HTTP User-Agent.
CSS Features Detection:	Tests if CSS features are enabled.
Font Enumeration:	Simulates font enumeration attack by comparing the rendered element's size with default values from a dictionary of known typefaces.
HTML5 Features Detection:	Tests if HTML5 features are enabled.
HTTP/2 Fingerprint:	Tests if the web server can identify which client is sending the request to them and can identify the browser type and version.
Image File Details:	Tests if a browser can provide image file details that can be used for fingerprinting.

Targeted Advertising

Tracking query parameter **-** *Test if browsers remove known URL tracking parameters.*

PrivacyTests.org

hsfp:	HubSpot tracking parameter.
hssc:	HubSpot tracking parameter.
hstc:	HubSpot tracking parameter.
s:	email address tracking parameter.
hsenc:	HubSpot tracking parameter.
openstat:	Yandex tracking parameter.
dclid:	DoubleClick Click ID.
fbclid:	Facebook Click Identifier.
gclid):	Google Click Identifier.
hsCtaTracking:	HubSpot tracking parameter.
igshid:	Unknown high-entropy tracking parameter.
mc eid:	Mailchimp Email ID (email recipient's address).
mkt tok:	Adobe Marketo tracking parameter.
ml subscriber:	MailerLite email tracking.
ml subscriber hash:	MailerLite email tracking.
msclkid:	Microsoft Click ID.
oly anon id:	'anonymous' customer id.
oly enc id:	'known' customer id.
rb clickid:	Unknown high-entropy tracking parameter.
s cid:	Adobe Site Catalyst tracking parameter.
vero conc:	Vero tracking parameter.

wickedid:	e-commerce tracking.
yclid:	Yandex Click ID.

Privacy Test Pages

Query Parameters:	Tests URLs with Tracking Parameters.

Tracker content blocking - Test if browsers block known tracking scripts from https://whotracks.me/. We provide the tracker address for reference.

PrivacyTests.org

Adobe:	https://munchkin.marketo.net/munchkin.js
Adobe Audience Manager:	https://dpm.demdex.net/ibs
Amazon adsystem:	https://s.amazon-adsystem.com/dcm
AppNexus:	https://ib.adnxs.com/px?id=178248&t=1
Bing Ads:	https://bat.bing.com/bat.js
Criteo:	https://dis.criteo.com/dis/rtb/appnexus/cookiematch.aspx
DoubleClick (Google):	https://securepubads.g.doubleclick.net/static/glade.js
Facebook tracking:	https://connect.facebook.net/en US/fbevents.js
Google (third-party ad pixel):	https://www.google.com/pagead/1p-user-list/
Index Exchange:	https://dsum-sec.casalemedia.com/crum?cm dsp id=10&external user id=629685505537&C=1
Quantcast:	https://pixel.quantserve.com/pixel
Taboola:	https://trc.taboola.com/futureplc-tomsguide/trc/3/json
Twitter pixel:	https://t.co/i/adsct
Yandex Ads:	https://yandex.ru/ads/system/header-bidding.js

Privacy Test Pages

Facebook ClickToLoad:	Embeds the Facebook SDK and tests if it is possible to create social elements using the SDK and in iFrames.
YouTube ClickToLoad:	Tests if requests to YouTube are blocked.

Reporting/Analytics

Analytics tracker content blocking - PrivacyTests.org
Test if browsers block known tracking scripts from https://whotracks.me/ used for analytics and reporting. We provide the tracker address for reference.

Chartbeat:	https://static.chartbeat.com/js/chartbeat.js
Google Analytics:	https://google-analytics.com/urchin.js
Google Tag Manager:	https://www.googletagmanager.com/gtag.js?id=GTM-NX4SMZL
New Relic:	https://js-agent.newrelic.com/nr-1212.min.js
Scorecard Research Beacon:	https://sb.scorecardresearch.com/internal-c2/default/cs.js

Behavioral Profiling

PrivacyTests.org

cookie (HTTP): Checks the usage and storage of HTTP cookies for tracking and maintaining stateful information.

cookie (JS): Checks the usage and storage of JS cookies for tracking and maintaining stateful information.

fetch cache: Attempts to abuse the Fetch API for caching.

indexedDB: Ensures the transactional database accessible via the indexedDB API is partitioned to mitigate the risk of cross-site tracking.

localStorage: Ensures the key-value database exposed by the localStorage API is partitioned to mitigate the risk of cross-site tracking.

ServiceWorker: Ensures the ServiceWorker API can not be used to track users across sites.

document.referrer: Checks the referrer request header is trimmed to minimize the information available for cross-site tracking.

sessionStorage: Similar to the localStorage API but does not persist across tabs or browser sessions, it is susceptible to the same abuse.

window.name: Ensures the data stored via the window.name API is partitioned so it will not persist across sites.

Privacy Test Pages

Geolocation: Tests that websites cannot access the API without the user's explicit permission, and if it is allowed, display all retrievable data.

Local Storage: Tests local and cookies storage and validates the effectiveness of data clearing.

Client Hints: Tests all client hints possible via headers and via JS.

Leak Extentions ID's via CSP: Tests if the browser is able to block injected scripts and leak them to the server via CSP reports.

Request Blocking: Tests if different types of requests are getting blocked.

Storage Partitioning: Tests whether storage APIs are partitioned or blocked across origins.

Browser Leaks

Geolocation API: Tests that websites cannot access the API without the user's explicit permission.

Permissions API: Tests if the Geolocation API works in the browser.

DNS Leak: Tests which DNS servers the browser is using to resolve domain names.

IPv6 Leak: Tests internet connectivity for IPv6 activity.

Feature Detection: Tests if the browser has features that may impact online identity.