Exposed By Default

"Exposed By Default": La Radiografía de tu Navegador que Demuestra el Peligro del *Fingerprinting*

La página web **Exposed By Default** (Expuesto Por Defecto), alojada en GitHub Pages, es una herramienta de demostración crítica que pone al descubierto una realidad a menudo invisible para el usuario promedio: **la gran cantidad de información única que tu navegador web revela automáticamente a cada sitio que visitas, incluso sin tu permiso explícito.**

Su función principal es actuar como un espejo digital, mostrando de forma exhaustiva y detallada todos los "rasgos de identidad" que tu dispositivo y software entregan por defecto, haciendo posible el rastreo avanzado conocido como **"fingerprinting"** (huella digital del navegador).

¿Qué Hace la Web: El Inventario de la Huella Digital

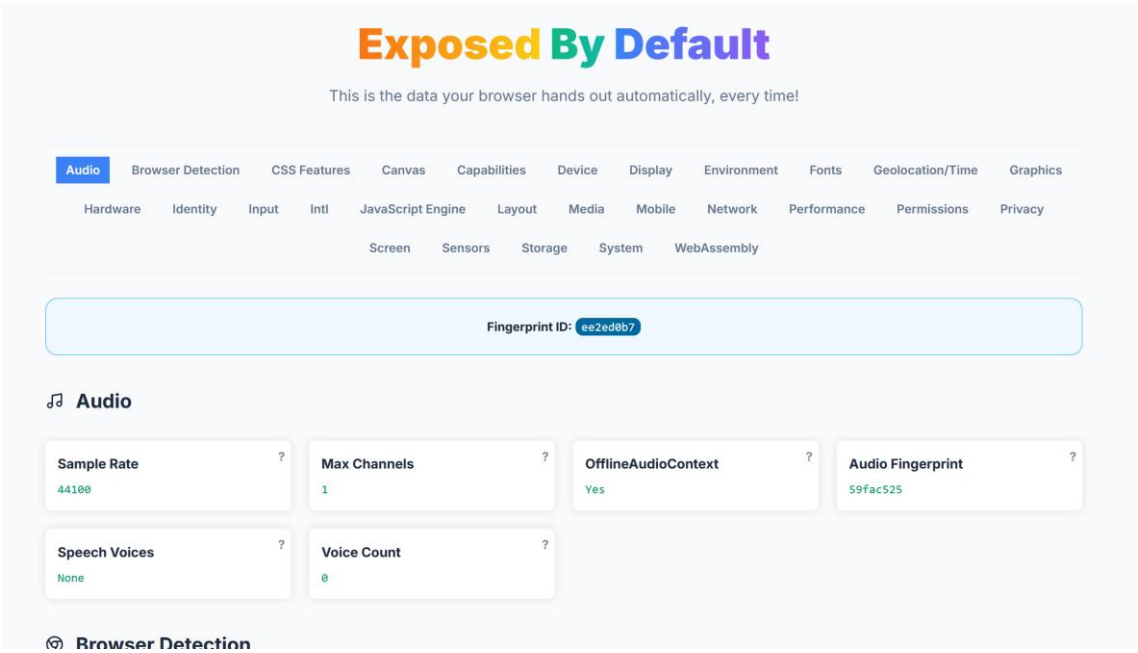
Exposed By Default realiza una inspección exhaustiva utilizando tecnologías web estándar (como JavaScript y APIs del navegador) para extraer docenas de métricas sutiles. El sitio organiza esta información en categorías detalladas, demostrando cómo se combinan para crear un perfil de dispositivo altamente único.

Entre los datos más sensibles que revela la web se encuentran:

1. **Huellas Digitales de Hardware (Fingerprints):**
    - **Canvas Fingerprint:** Un código único generado al renderizar gráficos y texto ocultos. Varía según tu GPU, *drivers*, sistema operativo y motor de renderizado.
    - **Audio Fingerprint:** Un identificador generado al procesar una señal de audio corta. Varía según la configuración de tu hardware de audio.

2. **Identificadores de Sistema y Navegador:**
    - **User Agent:** La cadena de texto que identifica tu navegador, versión, sistema operativo y arquitectura.
    - **Lista de Fuentes Instaladas:** Una lista de las tipografías que tienes en tu sistema.
    - **Configuración del Idioma (*Intl*):** Tu zona horaria local, formato de fecha, reglas de redondeo y otros ajustes de localización.
    - **Núcleos de CPU y Memoria RAM:** Una estimación de los recursos de hardware disponibles.
3. **Métricas de Pantalla y Red:**
    - **Resolución y Profundidad de Color:** El tamaño físico de tu pantalla y la cantidad de colores que puede mostrar.
    - **Capacidades Gráficas (WebGL/WebGPU):** El nombre exacto de tu tarjeta gráfica y proveedor de *drivers*.
    - **Preferencias de Visualización:** Si tienes activado el Modo Oscuro (prefers-color-scheme) o la reducción de movimiento (prefers-reduced-motion).

En resumen, la web te muestra el **"código de barras" digital** que llevas puesto, un código único generado por la suma de todos estos pequeños detalles.



¿Por Qué es Importante: La Amenaza del Browser Fingerprinting

La importancia de Exposed By Default radica en que ilustra de manera práctica la amenaza del **Browser Fingerprinting**, un método de rastreo mucho más difícil de eludir que las *cookies* tradicionales.

1. Rastreabilidad Persistente sin Cookies

Las *cookies* se pueden borrar fácilmente o bloquear por configuración. Sin embargo, el *fingerprinting* no necesita almacenar nada en tu dispositivo. Simplemente combina las decenas de métricas de *hardware* y *software* (como la huella de Canvas + la huella de Audio + la lista de fuentes + el idioma) para crear un **identificador estadísticamente único**. Una vez que este perfil está asociado a un usuario, puede ser rastreado a través de diferentes sitios web, incluso si:

- Borraste tus *cookies*.
- Estás usando el modo incógnito/privado (aunque algunos navegadores avanzados lo mitigan).
- Utilizas una VPN (solo cambia tu dirección IP, pero el navegador sigue filtrando tus rasgos internos).

¿Qué es Canvas Fingerprinting?

- Los navegadores web recopilan diferentes tipos de información mientras realizan sus funciones. Cuando parte de esta información se recopila para identificar a un usuario de un sitio web, se llama huella digital del navegador.
- La huella digital del navegador incluye la siguiente información del navegador: modelo del dispositivo, tipo y versión del navegador, sistema operativo (OS), resolución de pantalla, zona horaria, identificador de formato de archivo p0p, marca de tiempo, cadena del agente de usuario (UA), configuración de idioma, complementos y extensiones.
- **Canvas fingerprinting es una de estas tecnologías de huellas digitales del navegador. Se basa en el elemento Canvas del código HTML5 de la Web.**

2. Detección de Modos de Navegación

Al analizar elementos como las claves del objeto window o los tiempos de ejecución de JavaScript, los sitios web pueden incluso intentar detectar si estás usando un navegador con fuertes protecciones de privacidad (como Tor o Brave), o incluso si has habilitado bloqueadores de rastreadores (Tracker Blocking).

3. El Principio de Entropía

La importancia es que cada dato recopilado es un punto de **"entropía"** (aleatoriedad o singularidad). Cuantos más puntos de entropía se combinen, más único y, por lo tanto, más fácil de identificar es tu perfil. Exposed By Default demuestra que esta entropía es alarmantemente alta para la mayoría de los usuarios.

Las lámparas de lava se usan para crear un **Muro de Entropía** en la empresa Cloudflare que genera códigos de seguridad impredecibles para proteger el tráfico de internet. Los movimientos aleatorios de las burbujas son capturados por cámaras, y esta información se transforma en un código criptográfico seguro que es casi imposible de hackear, ya que la aleatoriedad impide predecir el código

Conclusión y Soluciones

Exposed By Default es una poderosa herramienta educativa que convierte un concepto abstracto de privacidad en una realidad tangible. Su mensaje final es claro: **la privacidad en línea no**

es solo cuestión de qué permisos otorgas, sino de qué datos filtra tu propio *software*.

Para combatir esta exposición por defecto, la página sugiere:

1. **Usar Navegadores con Protecciones Anti-Fingerprinting:** Algunos navegadores (como Brave, Tor Browser o Firefox con la configuración *resistFingerprinting* activada) están diseñados específicamente para reducir o "disminuir" la entropía de tu perfil, haciendo que luzcas idéntico a otros miles de usuarios.
2. **Deshabilitar APIs Innecesarias:** Limitar el acceso a APIs de navegador que son altamente identificables (como la API de Canvas o la API de WebGL).
3. **Reducir la Variación:** Cuanto más "estándar" sea tu configuración de software, menos único serás.

La herramienta ofrece esta demostración de forma segura, ya que su código está diseñado para ejecutarse **100% del lado del cliente**, lo que significa que **ninguno de tus datos de *fingerprinting* es transmitido o almacenado** por los creadores del sitio. Es puramente una demo de concienciación.

La afirmación de que la resolución y la configuración de pantalla pueden identificar a un usuario de manera "casi inequívoca" es correcta, no por un único dato, sino por el **poder de la combinación** de varios parámetros de alta **entropía**.

El Concepto Clave: Entropía y el Conjunto de Anonimato

La identificación no se basa en un solo valor, sino en la **singularidad estadística** que se genera al combinar decenas de variables. Cada variable, por sí sola, tiene baja capacidad de identificación (baja entropía), pero al sumarlas, la entropía se dispara.

Métricas de Pantalla que Filtran Información:

1. Device Pixel Ratio (Relación de Píxeles del Dispositivo)

- **Qué es:** La relación entre los píxeles físicos de la pantalla y los píxeles que usa el navegador para el diseño

(CSS pixels). Se obtiene a través de window.devicePixelRatio.

- **Por qué es crucial:** Aunque muchos dispositivos tienen relaciones estándar (1, 1.5, 2, 3), algunas *laptops* o monitores específicos tienen valores atípicos, como **1.25, 2.625 o 1.75**. Un devicePixelRatio de 2.625, por ejemplo, es altamente específico y sugiere inmediatamente un modelo de *hardware* concreto (por ejemplo, ciertos teléfonos o tabletas). Este es uno de los identificadores más fuertes.

2. Screen Resolution (Resolución Física)

- **Qué es:** El número total de píxeles físicos (screen.width x screen.height).
- **Por qué es crucial:** Si bien resoluciones como 1920x1080 son comunes, al combinarse con otros factores se vuelven únicas. Por ejemplo, un usuario con un monitor ultra-ancho de 3440x1440 se distingue inmediatamente del 90% de la población.

3. Available Screen Size (Tamaño de Pantalla Disponible)

- **Qué es:** La resolución total de la pantalla *menos* el espacio ocupado por barras de herramientas permanentes del sistema operativo (como la barra de tareas de Windows o el Dock de macOS). Se obtiene a través de screen.availWidth y screen.availHeight.
- **Por qué es crucial:** Si dos usuarios tienen la misma resolución de 1920x1080, pero uno tiene su barra de tareas arriba y el otro abajo (o una barra más gruesa), el tamaño disponible (availHeight) será diferente. Esta diferencia revela la **configuración personal del usuario dentro de su sistema operativo**.

4. Color Depth (Profundidad de Color)

- **Qué es:** El número de bits utilizados para representar el color de un píxel (típicamente 24 bits o 32 bits).
- **Por qué es crucial:** Si bien no es muy único, suma un punto de entropía. Un usuario que tenga configurada una profundidad de color inusual añade un rasgo más a su perfil.

El Caso de Tails OS y el "Conjunto de Anonimato"

La recomendación de **Tails OS** (y el **Tor Browser**) de no cambiar la resolución de la pantalla se basa en un concepto llamado **Conjunto de Anonimato (Anonymity Set).**

1. **Estrategia Estándar (Tor Browser/Tails):** Para combatir el *fingerprinting*, estos navegadores adoptan una estrategia llamada **"letterboxing"** o **"standardization".** En lugar de mostrar la resolución real, fuerzan el tamaño de la ventana del navegador a un valor redondo y muy común (por ejemplo, 1000x1000 píxeles, 1280x1024, etc.). Esto hace que miles de usuarios de Tor Browser se vean **exactamente iguales** para un sitio web rastreador.
2. **El Peligro de Cambiar la Resolución:** Si el usuario, por comodidad, cambia la resolución de su pantalla o de su ventana, **rompe esa uniformidad.** Introduce una métrica de pantalla y ventana personalizada que lo separa inmediatamente del gran grupo de usuarios anónimos.
3. **Identificación Inequívoca:** Al cambiar la resolución, el usuario se vuelve un "copo de nieve" en lugar de ser una "gota de lluvia". El rastreador puede entonces tomar esta resolución única, sumarle su **huella de Canvas** (que también depende de la resolución y el motor de renderizado), su **huella de Audio** y otros 50 puntos de datos, creando un perfil que solo coincide con una persona: **tú.**

En conclusión, la configuración de la pantalla es un pilar fundamental en la huella digital porque ofrece una combinación de métricas **altamente estables** y **específicas del hardware/configuración de OS**, lo que permite distinguir un dispositivo de otro con gran precisión.

https://neberej.github.io/exposedbydefault/