

INVESTIGANDO LA WEB



Campus Tecnológico-Deportivo para
Jóvenes

Universidad de Oviedo



JOSÉ MANUEL REDONDO LÓPEZ PROYECTO "S-64 'NARVAL'" v1.0



Fuente: Microsoft Copilot



Organiza:
 Escuela de
Ingeniería
Informática
Universidad de Oviedo

Colaboran:

 CITIPA
Colegio Oficial de Graduados
en Ingeniería Informática e
Ingenieros Técnicos en Informática
Principado de Asturias

 COITPA
Colegio Oficial de
Ingenieros en Informática
Principado de Asturias

 Cátedra Capgemini
PARA LA TRANSFORMACIÓN
DIGITAL SOSTENIBLE

¡BIENVENIDOS!

- En este curso hablaremos de una serie de herramientas para averiguar muchas más cosas acerca de una web

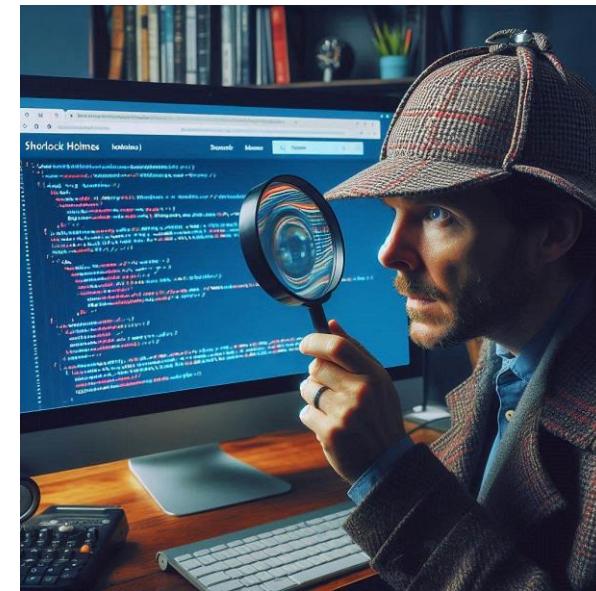
- No requieren instalar nada en un PC, solo un navegador
- Información que excede ampliamente lo que se puede ver a simple vista
 - O lo que puede saber un usuario que no sepa buscar, ¡subirás de nivel! 
- No se requerirá prácticamente ningún conocimiento técnico para usarlas

- El objetivo es responder a la siguiente pregunta

 **¿me fío de esta web?** 

- Es un complemento a los otros cursos, que te dará capacidades de investigación avanzadas

- De los sitios por los que navegues, quieras comprar algo, etc.
- Aunque mejor, de los que vayas a navegar, pero “tus ojos de elfo” te digan que hay algo sospechoso en ellos: ¡evitarás disgustos!



Elemental, querido Webson



La iniciativa
“Cobra Kali” por
José Manuel
Redondo López



Investigar Redes Sociales

Técnicas de investigación para RRSS

F-31 “Descubierta”



Virtualización Básica

Creación y uso de máquinas virtuales

R-11 “Príncipe de Asturias”

Rango 1
(Marinero)



Investigación de Webs

Detección de webs problemáticas

S-64 “Narval”



Entendiendo la Mente del Crimen

Mentes criminales y engaño

M-31 “Segura”



Ataques contra Personas

Ciberacoso

P-74 “Atalaya”

Rango 2
(Marinero de Primera)



Ciberseguridad General

Ciberseguridad general para el día a día

F-74 “Asturias”



Crime-spotting

Ejemplos de fraudes reales para concienciación

“Nautilus”



Vigilancia de Redes

Entendiendo cómo funcionan las redes modernas

F-83 “Numancia”

Rango 3
(Cabo)



Y si el cuerpo te pide marcha... ☺



La iniciativa
"Cobra Kali" por
José Manuel Redondo
López



Introducción a la Ciberdefensa Personal

Técnicas generales contra ciberataques (Niveles A1, A2)
Cursos G-9, PDI, Pr. UNIDIGITAL. "BPM P-51 'Asturias'"



Ciberdefensa Personal Avanzada

Técnicas avanzadas contra ciberataques (Niveles B1, B2)
Cursos G-9, PDI, Pr. UNIDIGITAL. "BPM P-51 'Asturias'"



Liderazgo en Ciberdefensa para Equipos

Herramientas y estrategias de protección (Nivel C1)
Proyecto UNIDIGITAL. "BPM P-51 'Asturias'"



Innovación e Investigación en Ciberdefensa

Avances e innovación en ciberdefensa (Nivel C2)
Proyecto UNIDIGITAL. "BPM P-51 'Asturias'"



Investigación con Fuentes Abiertas (OSINT)

Técnicas de investigación con fuentes abiertas
OCW (parcialmente). "A-21 Poseidón"



Administración Segura de SO

Infrastructure as Code
MUINGWEB, OCW. L-62 "Princesa de Asturias"



Identificación y Análisis de Vulnerabilidades en Web

Seguridad ofensiva:
Reconocimiento y Explotación
MUINGWEB, Microcreenciales.
TK-210 "красный октябрь"
(Octubre Rojo)

Protección de Servidores Web

Seguridad de infraestructuras para startups
Guías INCIBE, F-103 "Blas de Lezo"



Defensa contra el Cibercrimen

Identificación y lucha contra el cibercrimen
Divulgación pública, cursos. P-45 Audaz"



Rango 1
(Sargento)



Rango 2
(Suboficial Mayor)



Rango 3
(Capitán de Fragata)



Desarrollo Seguro de Software

Platform engineering seguro
Guías INCIBE. F-113 "Menéndez de Avilés"



Protección de Servidores y Aplicaciones Web

CISOs de perfil técnico
MUINGWEB, Guías INCIBE,
Microcreenciales. D-73 y C-
33 "Blas de Lezo"

Rango 4
(Almirante)





José Manuel
Redondo López

¿Y TODO EL RESTO DE MATERIAL?

- Durante este curso se hará mención de otros cursos complementarios que te regalo y que forman parte de la misma iniciativa
- Puedes encontrarlos todos aquí:
 - [https://github.com/jose-r-lopez/Formacion_-Seguridad_Joven/wiki/Contenidos-de-la-Iniciativa-%22Cobra-Kali%22-\(Capacitaci%C3%B3n-B%C3%A1sica\)](https://github.com/jose-r-lopez/Formacion_-Seguridad_Joven/wiki/Contenidos-de-la-Iniciativa-%22Cobra-Kali%22-(Capacitaci%C3%B3n-B%C3%A1sica))
- También tengo pensado en el futuro subir videos explicando cada curso en mi canal de YouTube
 - <https://www.youtube.com/@JoseRedondo-dj7xk>

ÍNDICE

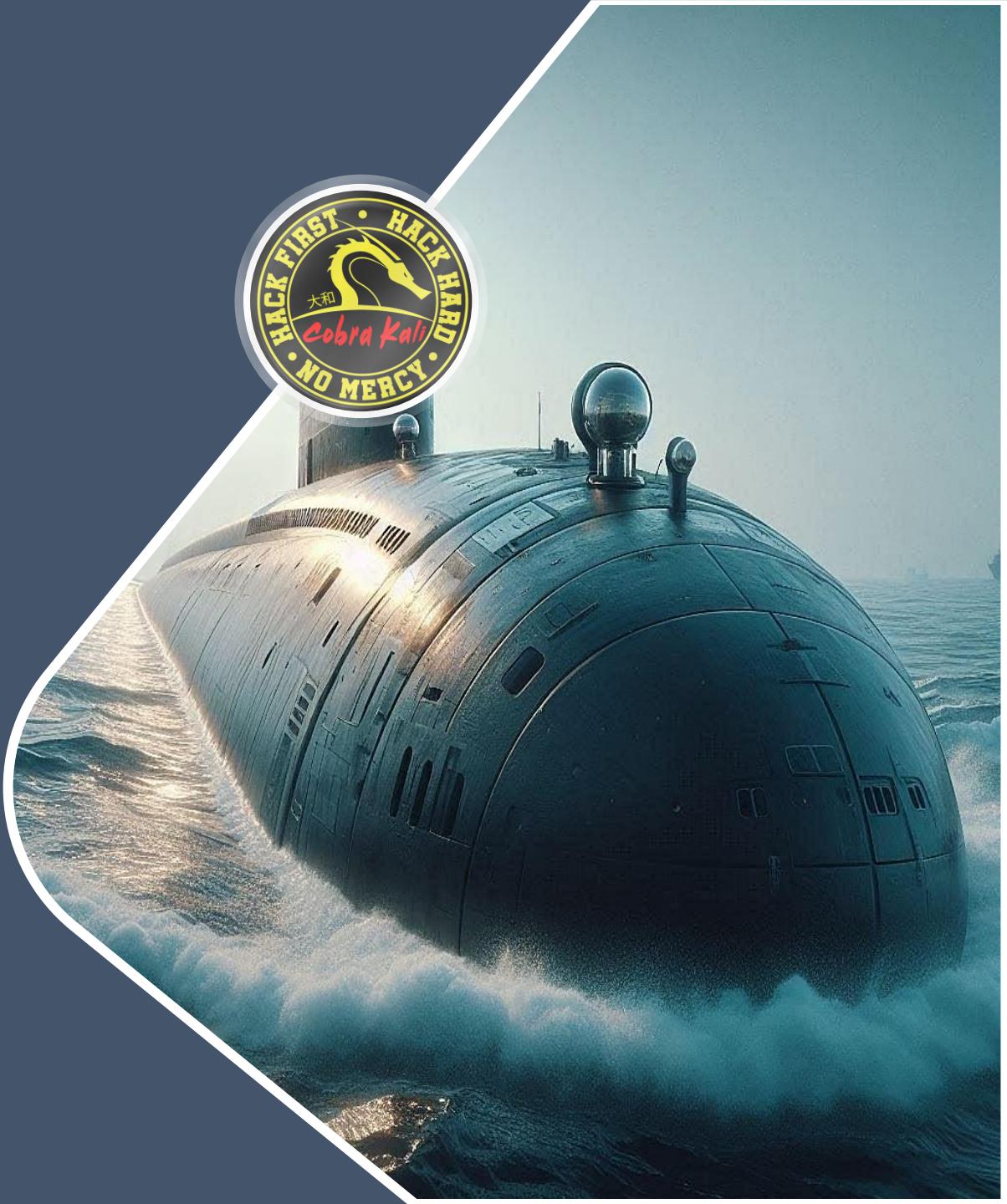


- [He contratado Internet ¿Qué me han instalado?](#)
- [El navegador es la puerta de salida a Internet](#)
 - [¿Qué navegador uso y cómo?](#)
 - [¿Cómo hago el navegador más seguro?](#)
- [Investigando las páginas web](#)
 - [Lo que se ve](#)
 - [Lo que no se ve](#)
 - [¿Se toma en serio su seguridad una web?](#)
 - [Lo que se vio](#)
- [Investigando lo que hay detrás de una web](#)
 - [Las empresas](#)
 - [Las personas](#)
 - [Las máquinas](#)



HE CONTRATADO INTERNET ¿QUÉ ME HAN INSTALADO?

Un breve recorrido sobre lo que es tu conexión a Internet



¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

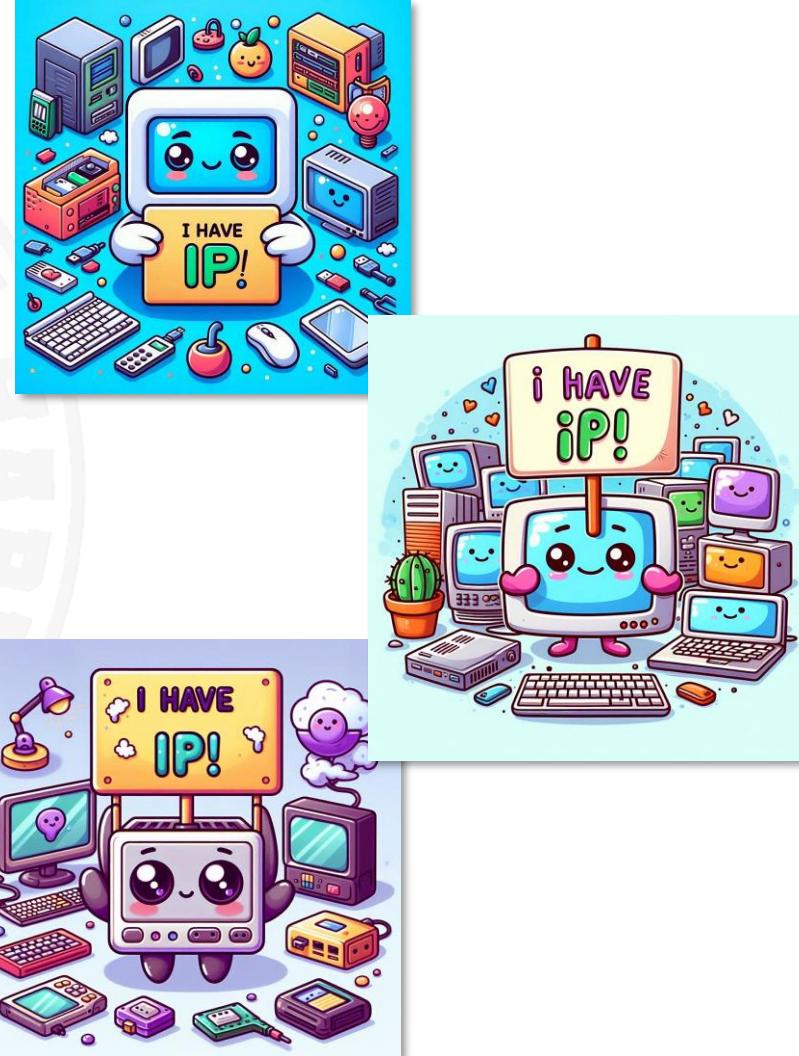


- *¿Alguna vez te has preguntado cómo funciona el internet que tienes contratado en casa?*
 - Yo te lo voy a explicar en esta sección
- **Descubrirás que hay muchas cosas que se ponen de acuerdo para que tú puedas navegar**
 - Y que la mayor parte de las veces son cosas automáticas
- **Así, si algo deja de funcionar, sabrás que realmente es algo bastante complejo y no tan fácil de diagnosticar**
 - Y la razón puede ser cualquiera de los muchos sistemas que se ponen de acuerdo para que tú tengas ese servicio

DIRECCIONES IP Y DNS: Lo QUE HACE FUNCIONAR INTERNET

- Para entender esta presentación hay que tener claras una serie de cosas

- Las páginas web que visitas **están en una máquina** en alguna parte del mundo 
- A la que llegas gracias a Internet, **si te sabes su dirección** (es decir, dónde está) 
- Toda máquina conectada a una red (como Internet) tiene su **"DNI único"**, que es su dirección 
 - Se llama dirección IP y tradicionalmente es un conjunto de nºs separados por “.”
 - Cuatro nºs entre 0 y 255 (Ej.: 192.168.34.1) (llamada **IPv4**)
 - Se está introduciendo una versión más larga, **IPv6**, pero eso lo hablamos en la **F-83 “Numancia”**



DIRECCIONES IP Y DNS: Lo QUE HACE FUNCIONAR INTERNET

• *¿Os imagináis tener que recordar las IPs de todas las máquinas a las que visitáis?*

- ¡Sería inviable! Por eso se usa en su lugar **un nombre simbólico**, llamado **nombre de dominio**
 - Ej.: www.ingenieriainformatica.uniovi.es
- Y, como las IPs siguen siendo necesarias, **hay un traductor automático entre nombres <-> sus IPs**
- Un servicio llamado **DNS** se encarga automáticamente de que, cada vez que tú pones un nombre de una web, se obtenga la IP correspondiente y se vaya al sitio correcto
 - Navegar por Internet hace estas traducciones IP <-> nombre automáticamente **sin que nos enteremos**
 - ¡Todo el tiempo!
- *¿Te gusta esto? ¡En la F-83 “Numancia” te explico mucho más!*



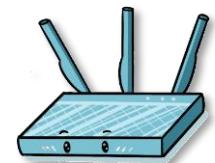
INTERNET EN CASA: COMO SE SUELE INSTALAR

• *¿Todas las máquinas que pueden navegar por Internet están conectadas así?*

• **¡NO!** En casas y en muchas empresas se usa un esquema diferente

- Te dan un dispositivo (router) y **una sola IP** que es capaz de “salir a Internet”
- *¿Cómo que una sola?* ¡Pero si todo el mundo tiene muchos aparatos conectados!
 - PC, teléfonos, tablets, TVs, Playstation, XBox, Switch...
- El **router** lo sabe y lo tiene todo controlado ☺
 - El **router** le da automáticamente a cada aparato conectado a él una **IP privada**
 - Solo vale para comunicarse entre los equipos de tu casa (Ej.: ver una peli de tu **Chromecast** en el teléfono)
 - Cuando uno de esos aparatos quiere navegar a Internet, el **router traduce su IP privada a la que has contratado para salir a Internet**
 - Quizá tu proveedor haga más traducciones intermedias...pero tú no lo sabes ☺
 - *¿Y cuando la máquina de Internet responde?* El **router** traduce de nuevo automáticamente, **pero al revés**
- Todo este proceso es automático, no te enteras y se llama **NAT** (Network Address Translation)

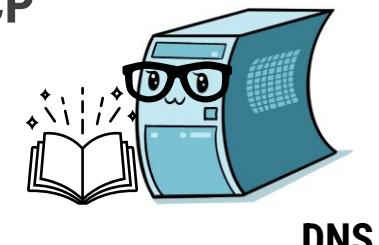
Parezco insignificante,
pero ¡sin mi olvídate de
navegar!



INTERNET EN CASA: COMO SE SUELLE INSTALAR

• *¿Qué quiere decir todo esto?*

- Tú contratas una IP y **puedes conectar N dispositivos a Internet** usando solo esa misma IP
 - Que obtienen automáticamente una IP privada con algo que tiene el router llamado **DHCP**
 - No hace falta que lo entiendas, pero si te interesa, mírate la **F-83 “Numancia”**
 - ¡Así los proveedores de Internet ahorran!
- Para “el exterior”, **todos tus equipos tienen la misma IP**
 - Pero el router sabe a quién mandar las respuestas que le llegan a cada uno por separado
 - (Tranqui, el PC de tus padres no va a recibir por accidente lo que estás navegando tu ni viceversa ☺)



DNS

• *¿Y dónde está el servicio DNS en todo esto?*

- El router sabe dónde está porque **tu proveedor a Internet se lo dice**
- Aunque siempre puedes usar uno propio
 - Lo que sueles hacer si quieras más seguridad (lo vemos luego)

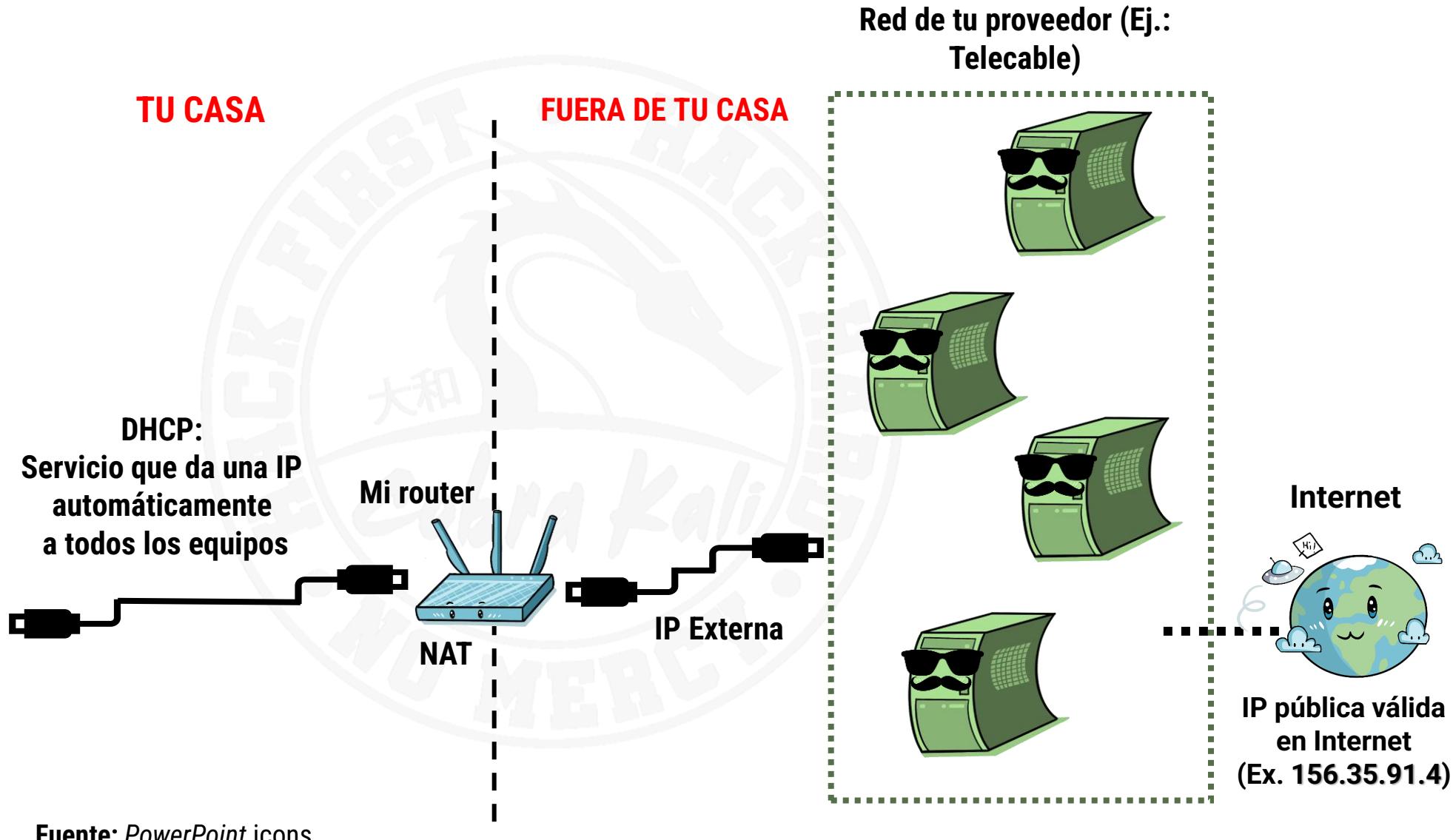
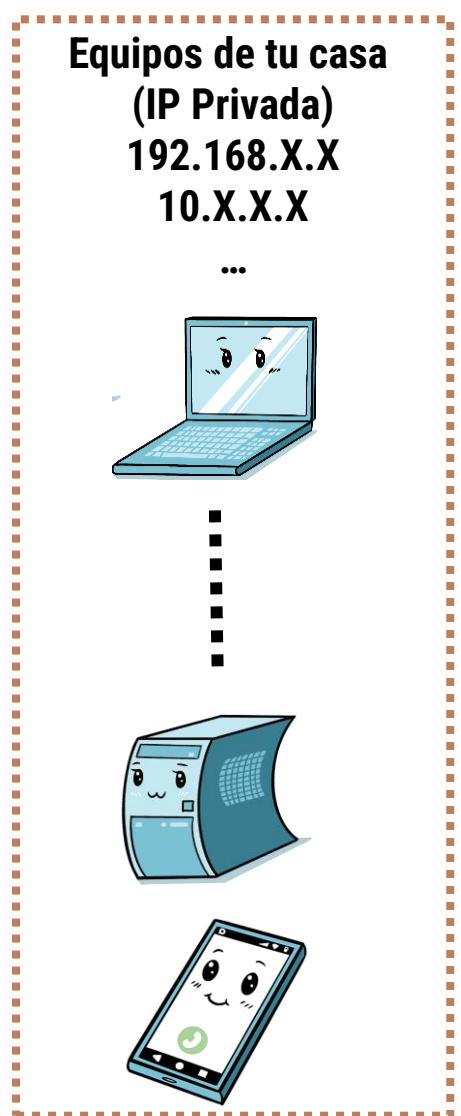


• *Perdona, pero ¿no hay mucha “magia automática” en todo esto?*

- Efectivamente ☺, y menos mal, *¿te imaginas tener que hacer todo esto a mano?*

Internet en realidad son
millones de máquinas
conectadas así...a kind of
magic ☺

INTERNET EN CASA: COMO SE SUELE INSTALAR



¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

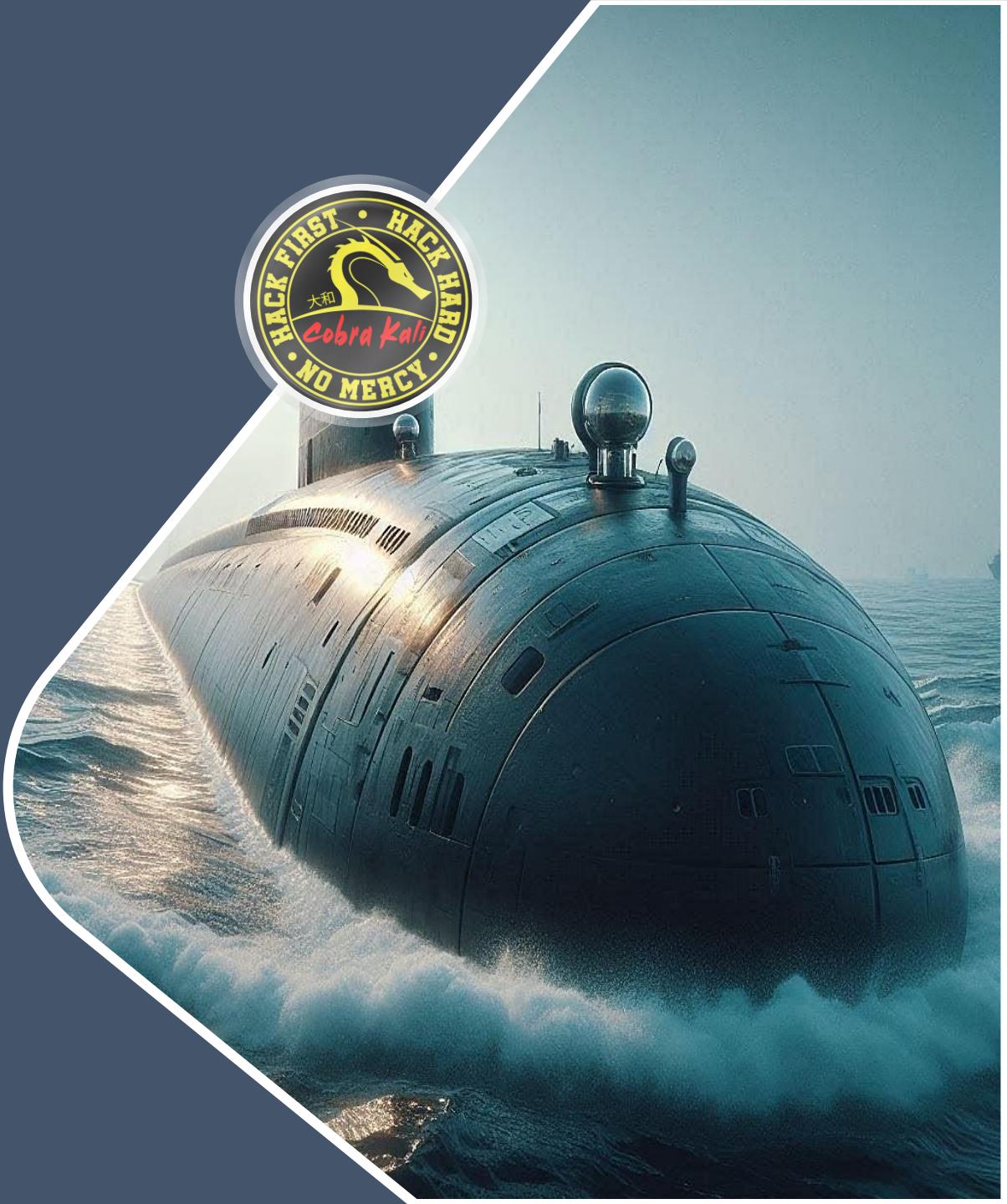


- ¿Entiendes qué es una dirección IP y cómo es parecido a un DNI, pero para máquinas?
- ¿Comprendes ahora la enorme importancia que tiene el router que tienes en casa para conectarte a internet, y cómo básicamente es un “Gran Hermano” que lo controla todo?
- ¿Entiendes también cómo la empresa la que has contratado internet ahorra dinero dándote una sola IP, y luego creando un esquema para que todos tus dispositivos usen la misma?
- ¿Entiendes ahora que hay un servicio de traducción que te permite usar nombres “normales” para acceder a páginas web, y que gracias a eso usar internet dos no auténtico infierno?
- En definitiva, ¿Puedes explicarle a alguien cómo es más o menos el montaje que tenemos todos en casa para Internet?



EL NAVEGADOR ES LA PUERTA DE SALIDA A INTERNET

Antes de investigar ninguna web hay que afinar la herramienta de investigación: tu navegador



¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

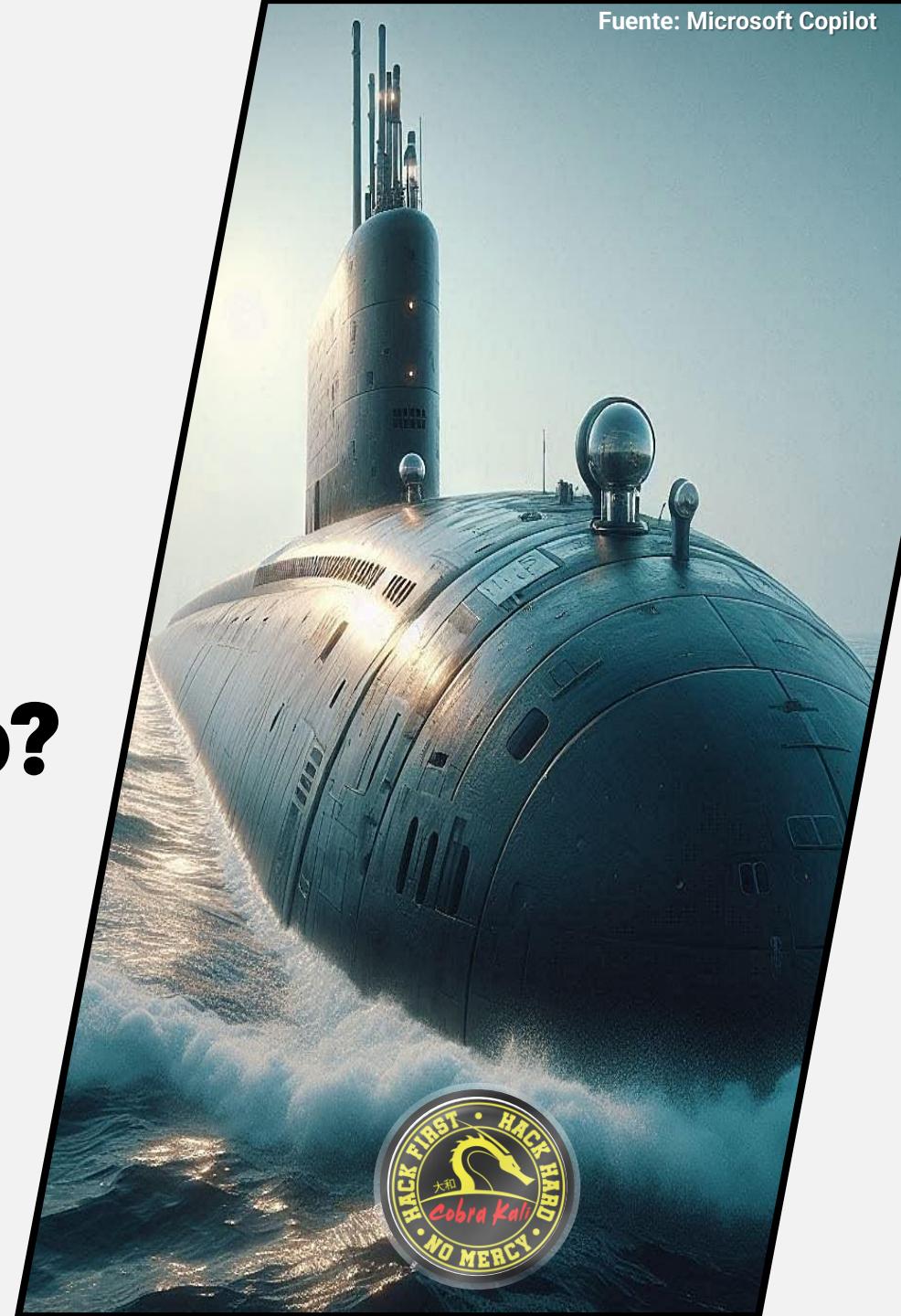


- *¿Te preocupa navegar por Internet porque sabes que hay muchos peligros?*
 - Te voy a enseñar a poner tu navegador “a tono” para que sea menos peligroso
- **Defendiéndote automáticamente de muchas cosas que te puedan ocurrir simplemente por visitar páginas web**
- **Y, aunque no te voy a poder defender de todos los problemas, sí que puedo enseñarte a dejar tu navegador “fino”**
 - Para que tengas muchos menos que los que puedes tener ahora



¿Qué navegador uso y cómo?

Es la primera decisión que tomar, y no es trivial



¿QUÉ NAVEGADOR USAR?



José Manuel
Redondo López

- Todos los navegadores son más o menos equivalentes en prestaciones
 - La decisión de usar uno u otro se basa en sus características
 - Por ejemplo, como preservan tu **privacidad** 
 - Es decir, si venden o no tus datos a empresas de publicidad
 - Es la **forma más común de financiarse**  de muchos proyectos
 - En este estudio vemos que Brave gana
 - <https://brave.com/>
 - Aunque puedes usar otros con los plugins que veremos luego
 - <https://privacytests.org/>

¿QUÉ NAVEGADOR USAR?

- Otro criterio son las **características integradas de seguridad**

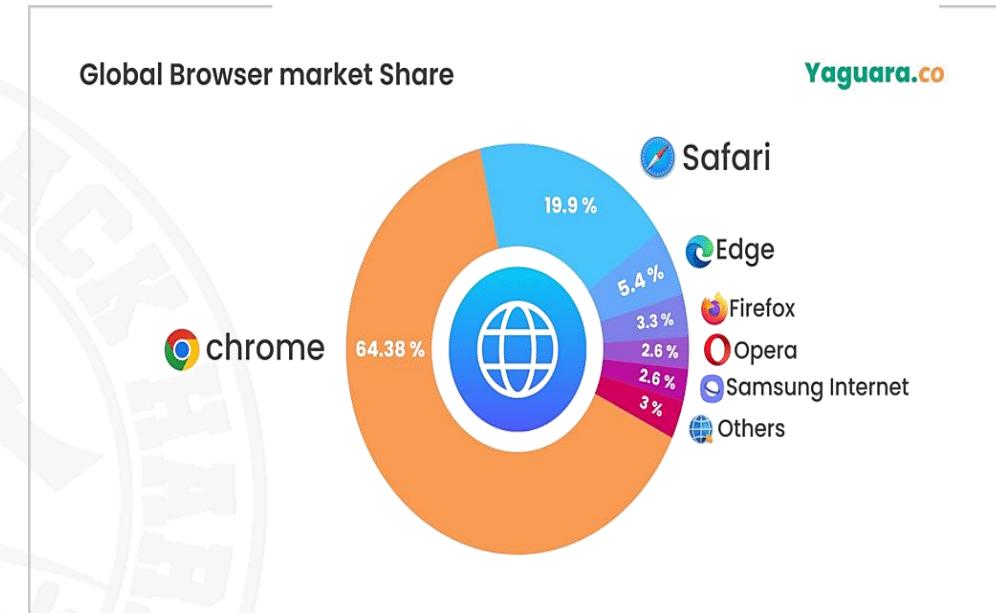
- Muchos vienen ya con ciertas medidas de seguridad integradas que podemos activar

- Podemos también aplicar el criterio de **mayor cuota de uso en el mercado**

- Indicativo de mayor soporte, pero también mayor nº de posibles vulnerabilidades descubiertas
- **Chrome gana** en ese aspecto por goleada

- También podemos elegirlo por su **tecnología**

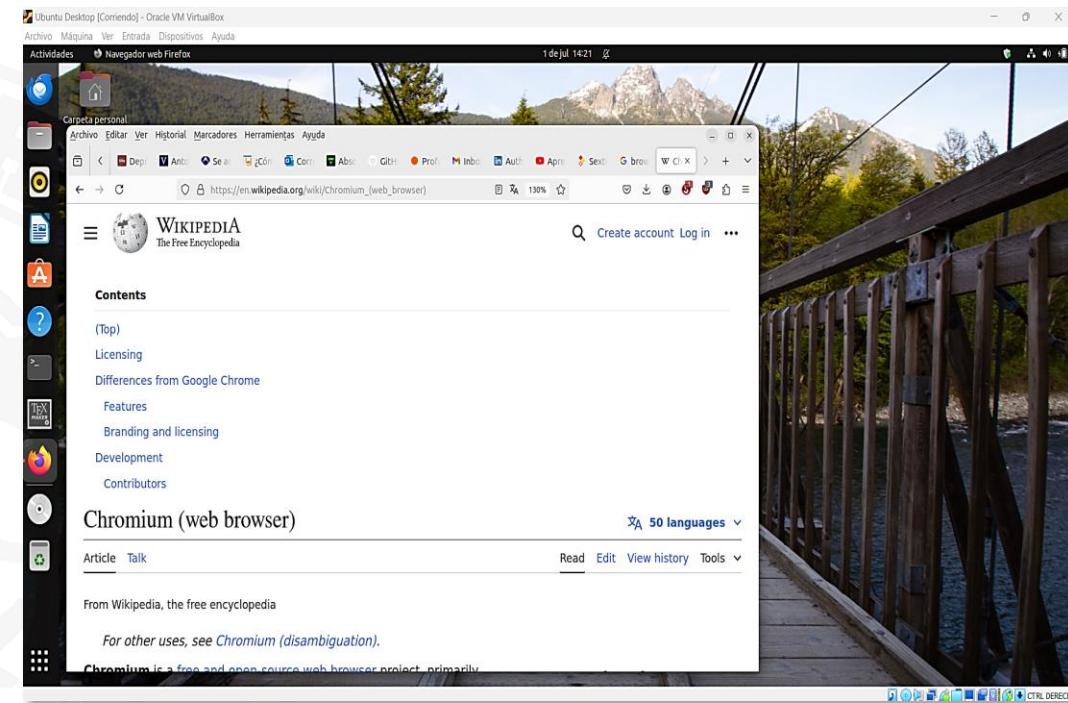
- Los navegadores típicos modernos, salvo Safari y Firefox, están basados en el **proyecto Chromium**
 - Chrome (y muchos más) están basados en él
 - <https://www.chromium.org/chromium-projects/>
- Es un navegador de código abierto de **Google** que adaptan otros fabricantes



En realidad, los navegadores actuales son “Los basados en Chromium (**Chrome a la cabeza**) y el resto...”. Fuente: <https://www.yaguara.co/browser-market-share/>

¿CÓMO LO USO?

- Finalmente, otro criterio es si tiene complementos de seguridad
 - Más o menos todos tienen bloqueadores de publicidad, de scripts y de mejora de la privacidad
- Con todos estos criterios en marcha, recomendamos usar Firefox o Brave
- Elijas el que elijas, intenta navegar siempre dentro de una máquina virtual (MV)
 - Mira el R-11 “Príncipe de Asturias”
 - ¿Metes la pata? ¡No pasa nada! ¡Todo queda dentro de la máquina virtual!
 - Y, puestos a elegir, mejor una MV Linux, como Ubuntu
 - Menos probabilidad de ser víctima de malware que con Windows



Firefox dentro de una máquina virtual Ubuntu con VirtualBox, corriendo en un Windows. ¿Navegas de esta forma? Las opciones de que puedan atacarte con éxito bajan bastante ☺

¿CÓMO LO USO?

- Algo que la gente hace y que puedes probar es tener “navegadores temáticos”

- Uno para “el bisnes” , es decir, para trabajar en cosas del colegio, tu curro, etc.
 - Office vía web, el webmail de las cosas importantes, etc.
 - O, como dice un amigo mío, para “lo serio”
 - Con este **solo navegas a un conjunto muy limitado de páginas conocidas y fiables**
- Otro para ocio  : Navegar “por ahí” a donde quieras
 - Noticias, foros, redes sociales, páginas de críticas, hobbies, etc.
 - Con todas las medidas de seguridad que vamos a ver
 - Y en una máquina virtual, como recomendamos

- Además de por seguridad, asociar un navegador a trabajo y otro a ocio **ayuda a la “desconexión digital”** 

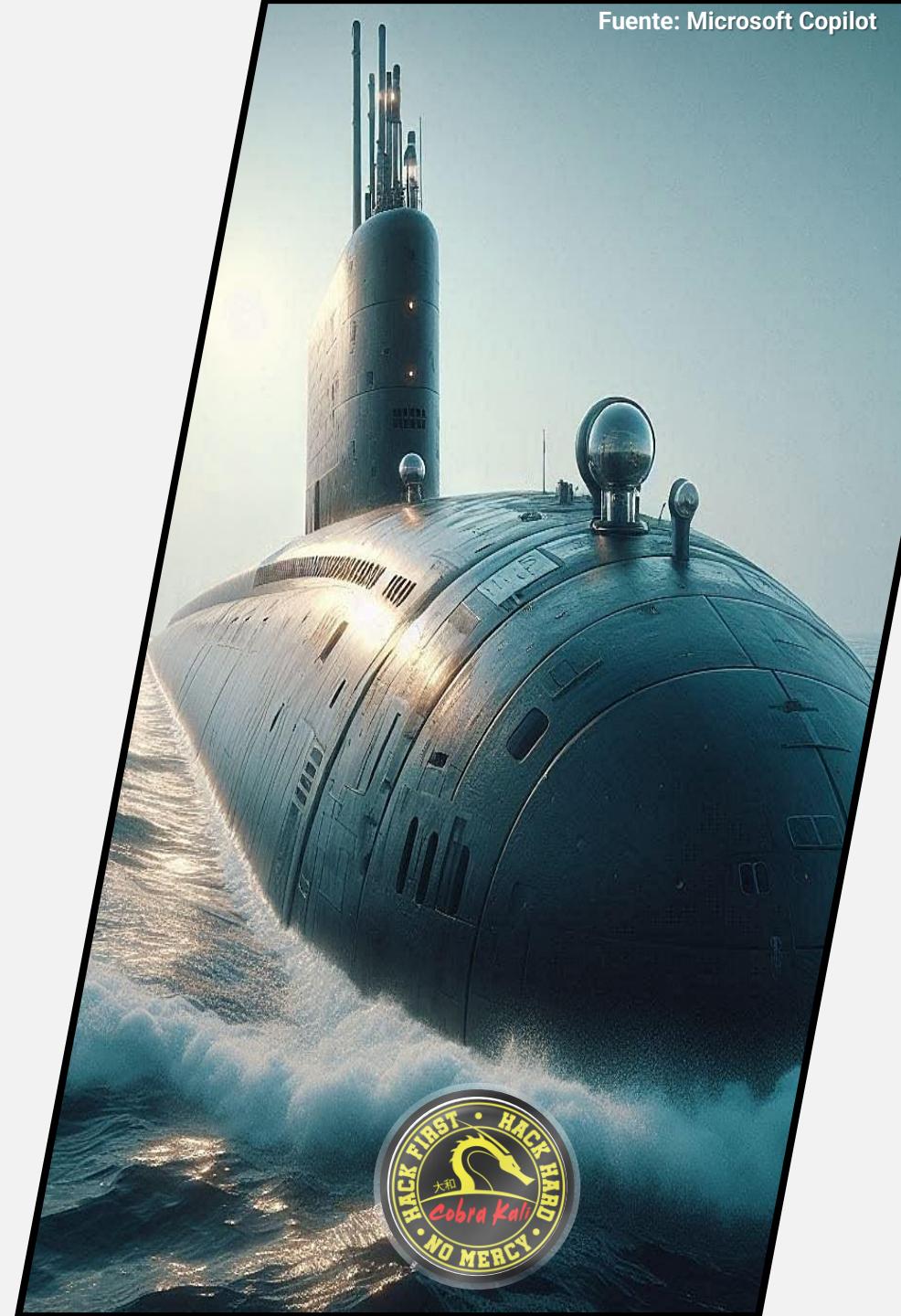


No te engañes, en ambos casos hay riesgo. Pero si una medida de seguridad de las que veremos interfiere con temas serios, no tienes que desactivarla cuando es más necesaria



¿Cómo hago el navegador más seguro?

Uno no va y simplemente se pone a navegar...



NAVEGADORES SEGUROS

- Para navegar por Internet de forma segura hay que hacer tres cosas

- Instalar extensiones del navegador que mejoren la seguridad de este
- Mantener el navegador actualizado
- Activar determinadas configuraciones de seguridad integradas en el navegador

- En esta sección vamos a hablar de estas tres cosas

- Pondremos de ejemplo ciertos navegadores, pero prácticamente todos tienen las mismas opciones de protección
- Incluso las mismas extensiones del mismo autor

- Una vez termines de aplicarlas, estarás en una posición mucho más ventajosa para investigar webs

- Y para navegar en tu día a día



Navegar por Internet es una actividad de riesgo para la que debemos prepararnos

EXTENSIONES DE NAVEGADORES

- Añadidos que mejoran aspectos de la navegación

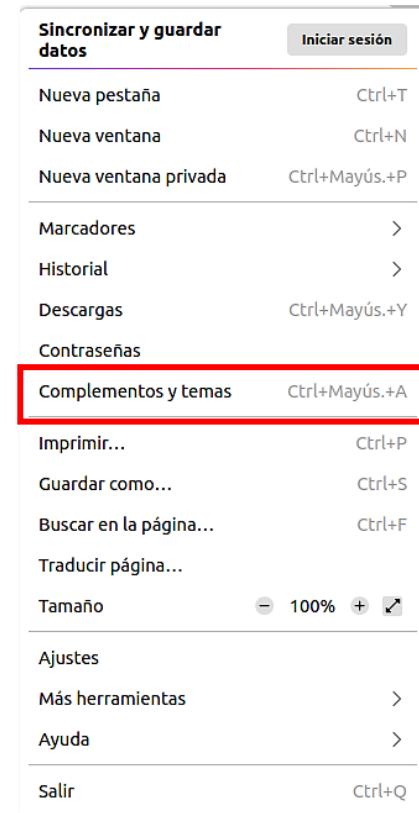
- Hay miles de ellas, y algunas mejoran **aspectos relativos a la seguridad**

- Todos los navegadores tienen extensiones

- ¡Pero no es bueno instalar cualquiera! ¡Algunas **pueden tener/ser malware!**!

- Lo mejor es instalar aquellas que

- Estén **recomendadas/verificadas** por el fabricante
- Tengan **muchos** (millones) de **usuarios**
- Tengan muchas y muy buenas **valoraciones**
- No pidan **demasiados permisos** (como con las aplicaciones del móvil)



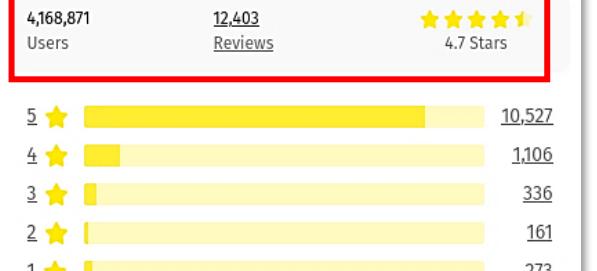
uBlock Origin
by Raymond Hill

Finally, an efficient wide-spectrum content blocker. Easy on CPU and memory.

 Recommended

Verificada por el
fabricante

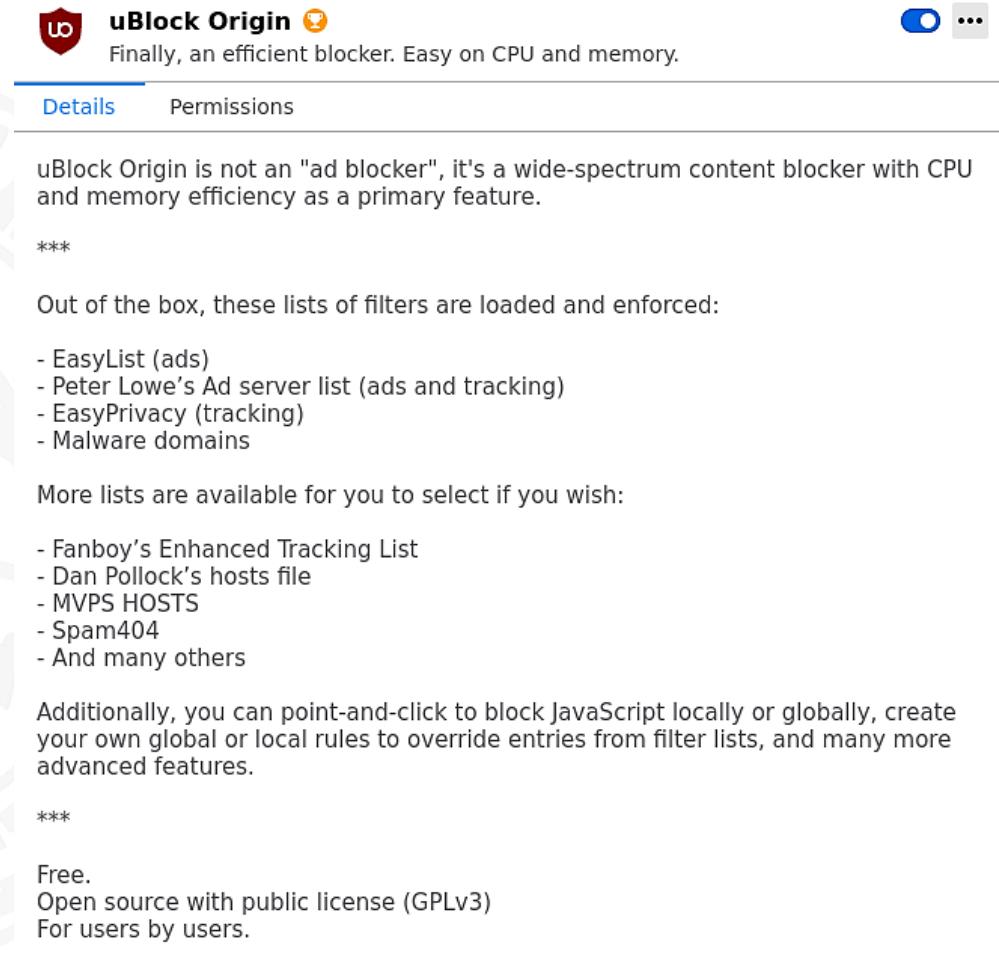
+ Add to Firefox



Millones de usuarios,
buenas valoraciones.
Es un sí ☺

¿CÓMO PUEDO NAVEGAR CON MENOS RIESGO? BLOQUEAR ANUNCIOS

- La mayoría de web se financian con anuncios
- Esto no sería malo si no fuese porque...
 - Algunos son realmente **molestos**
 - Otros hacen que navegar sea **mucho más lento**
 - A veces, **incluso son maliciosos** (debido a cómo funciona el mercado de la publicidad web)
- Hay extensiones para bloquearlos
 - Uno de los más usados es uBlock Origin
 - Para Firefox y Chrome (Chrome Web Store)
- No es el único que hace este trabajo, pero este funciona muy bien
 - Lo hay para Firefox móvil también



The screenshot shows the "Details" tab of the uBlock Origin extension page. At the top, there's a logo with a shield containing a 'u' and the text "uBlock Origin". Below it, a subtext reads "Finally, an efficient blocker. Easy on CPU and memory." To the right is a blue toggle switch and three dots for more options. The "Details" tab is underlined. Below the tabs are two sections: "Description" and "Reviews". The "Description" section contains text about the extension's purpose as a content blocker, its efficiency, and a list of pre-loaded filter lists like EasyList, Peter Lowe's Ad server list, EasyPrivacy, and Malware domains. It also mentions Fanboy's Enhanced Tracking List, Dan Pollock's hosts file, MVPS HOSTS, and Spam404. The "Reviews" section shows a 5-star rating with 1,000 reviews and an average rating of 5.0. At the bottom, there's a "Free" note, a link to the open source license (GPLv3), and a "For users by users" badge.

uBlock Origin en Firefox. Ojo, ¡no instales imitaciones!
(mira autor, valoración, nº de descargas...)

EFFECTOS DE LOS BLOQUEADORES DE PUBLICIDAD

● Un buen bloqueador de publicidad...

- Bloquea **sin que te enteres ni tengas que hacer nada**: Los anuncios simplemente no están
- No impide que las webs a las que navegues funcionen
 - Algunas como YouTube los intentan detectar y “se enfadan” si los usas
 - **Instándote a que lo desinstales o desactives**: ¡No lo hagas! Tienes mucho que perder
 - Actualízalo (las nuevas versiones suelen esconderse mejor de los métodos de detección)

Sin bloqueador: publicidad en 33% de la pantalla

La crisis del coronavirus

Datos actualizados Casos en España y resto del mundo Situación global Expansión del virus en cada país App de rastreo Descárgate Radar-Covid Nueva Normalidad Buscador Avance del virus Evolución por provincias

Última hora · Podcast · Ver especial

Torra destituye a tres consejeros para satisfacer al ala dura del independentismo

PERE RÍOS | Barcelona 13 Los consejeros que ya han salido del Govern son los de Interior, Miquel Buch; la de Cultura, Mariàngela Vilallonga, y la de Empresa, Àngels Chacón



EL PAÍS

Con bloqueador: no hay publicidad, todo es contenido

La crisis del coronavirus

Datos actualizados Casos en España y resto del mundo Situación global Expansión del virus en cada país App de rastreo Descárgate Radar-Covid Nueva Normalidad Buscador Avance del virus Evolución por provincias

Última hora · Podcast · Ver especial

Torra destituye a tres consejeros para satisfacer al ala dura del independentismo

PERE RÍOS | Barcelona 13 Los consejeros que ya han salido del Govern son los de Interior, Miquel Buch; la de Cultura, Mariàngela Vilallonga, y la de Empresa, Àngels Chacón

Tres nuevos consejeros a medida de Puigdemont

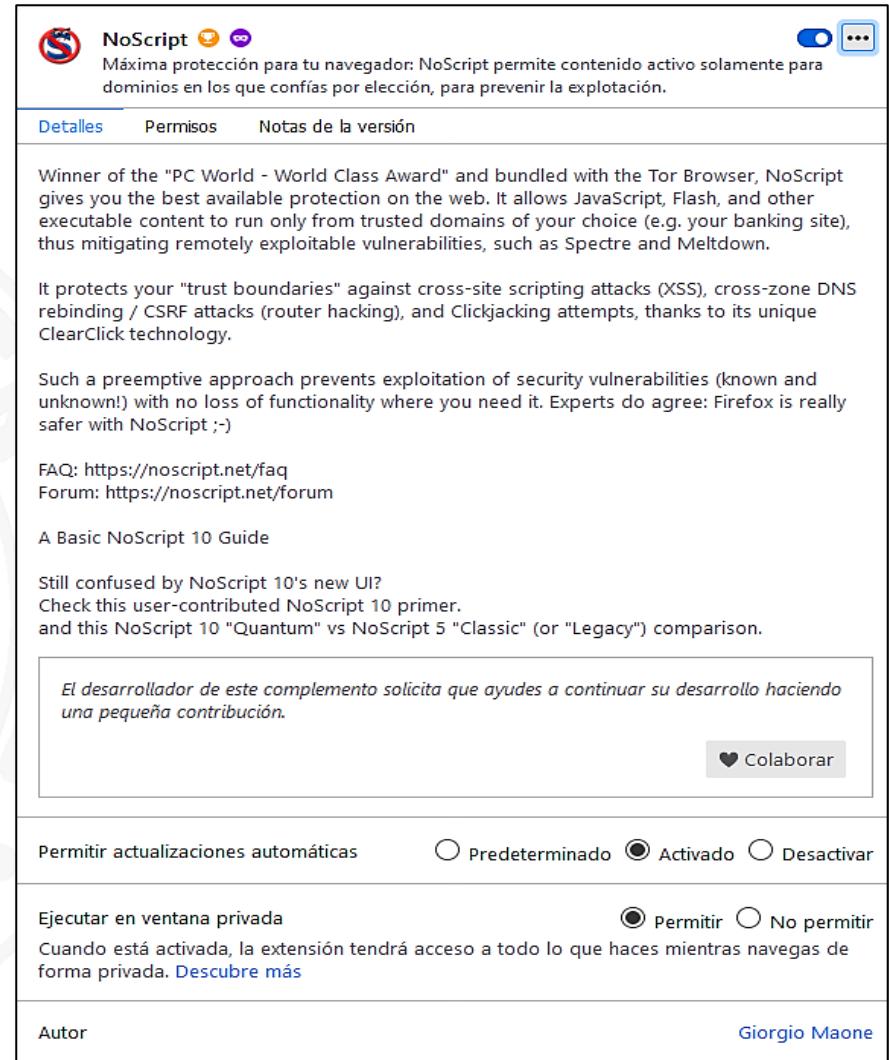


Personal sanitario hace el seguimiento de enfermo por coronavirus en Barcelona. A.G. (EFE)

Un estudio de 64.000 enfermos de covid en España

¿CÓMO PUEDO NAVEGAR CON MENOS RIESGO?

- Navegar es un problema no solo por los anuncios, también por los contenidos
- Muchas webs usan un lenguaje de programación llamado **JavaScript** para mostrar elementos
 - Tiene usos 100% legítimos
 - Pero también puede usarse para saber qué webs visitas, engañarte, mostrar anuncios, contenidos falsos o maliciosos...
 - Puede hacer que navegar sea más lento
- Una extensión que bloquea esto es **NoScript**
 - Para Firefox y para Chrome
 - Bloquea también otros ataques



The screenshot shows the configuration page for the NoScript extension. At the top, there's a summary section with a red 'S' icon, the text 'NoScript' with a gear icon, and a 'Máxima protección para tu navegador' message. Below this are tabs for 'Detalles', 'Permisos', and 'Notas de la versión'. The 'Notas de la versión' tab is active, displaying text about the extension's history and security features like ClearClick technology. Further down, there's a 'FAQ' link, a forum link, and a 'A Basic NoScript 10 Guide'. A note about the new UI is also present. At the bottom, there are sections for 'Permitir actualizaciones automáticas' (radio buttons for 'Predeterminado', 'Activado', and 'Desactivar'), 'Ejecutar en ventana privada' (radio buttons for 'Permitir' and 'No permitir'), and an 'Autor' field containing 'Giorgio Maone'.

Hacerte a **NoScript** te puede llevar un poco de tiempo, pero una vez lo domines estarás mucho más seguro



¿CÓMO PUEDO NAVEGAR CON MENOS RIESGO?

● Para usarlo bien hay que “entrenarlo”

- Al ir a una página, **se cargan muchas otras secundarias mediante scripts**
 - Incluidas las que te hacen **seguimiento (tracking)**
- Esta extensión lista todas y **bloquea la mayoría**
- Como consecuencia, seguramente la página **se vea mal o falten trozos**
- Así que miramos la lista haciendo clic en su ícono
 - Y empezamos a desbloquear las que suenan menos “sospechosas”
 - Hasta que la web “se pueda leer” 😊
- La extensión **recuerda** esta selección para siempre
 - ¡Solo hay que hacerlo 1 vez por página!

● Debido a ello, se recomienda solo en el navegador que uses para “ocio” 😊

X	C	Q	
✗	✓	✗	...youtube.com
✗	✓	✗	...gstatic.com
✗	✓	✗	...ytimg.com
✗	✗	✗	...adszone.net
✗	✗	✗	...ad-delivery.net
✗	✗	✗	...addthis.com
✗	✗	✗	...addthisedge.com
✗	✗	✗	...btserve.com
✗	✗	✗	...cdnjquery.com
✗	✗	✗	...consensu.org
✗	✗	✗	...disqus.com
✗	✗	✗	...disquscdn.com
✗	✗	✗	...disqusservice.com
✗	✗	✗	...doubleclick.net
✗	✗	✗	...facebook.com
✗	✗	✗	...facebook.net
✗	✗	✗	...google-analytics.com
✗	✗	✓	...google.com
✗	✗	✓	...google.es
✗	✗	✓	...googletagmanager.com
✗	✗	✓	...googletagservices.com
✗	✗	✓	...gstatic.com
✗	✗	✓	...marfeel.com
✗	✗	✓	...marfeelcache.com
✗	✗	✓	...moatads.com
✗	✗	✓	...moonmail.io
✗	✗	✓	...onesignal.com
✗	✗	✓	...reznyc.com

Usando esto uno se da cuenta de la cantidad de cosas que cargan las webs que no son de la web en sí...

PRIVACY BADGER



- Esta extensión se usa para bloquear páginas que guardan porque sitios navegas (tracking)
 - Se usa para personalizar anuncios...¡o con fines maliciosos!
- Indica a las páginas que no quieres que recojan tus datos de navegación
 - Aunque es algo que pueden simplemente ignorar...
 - Esta extensión identifica estas páginas y las bloquea
- También elimina intentos de tracking de Facebook, Google, Twitter...
- E implementa también otras medidas que protegen la privacidad de sus usuarios
 - El tracking se usa muchísimo (y se abusa de él), y esto es una respuesta que puedes darle

 Privacy Badger 
Privacy Badger aprende automáticamente a bloquear rastreadores invisibles.

[Details](#) [Permissions](#)

Privacy Badger automatically learns to block invisible trackers. Instead of keeping lists of what to block, Privacy Badger learns by watching which domains appear to be tracking you as you browse the Web.

Privacy Badger sends the Do Not Track signal with your browsing. If trackers ignore your wishes, your Badger will learn to block them. Privacy Badger starts blocking once it sees the same tracker on three different websites.

Besides automatic tracker blocking, Privacy Badger removes outgoing link click tracking on Facebook, Google and Twitter, with more privacy protections on the way.

To learn more, see the FAQ on Privacy Badger's homepage.

Privacy Badger is a project of the Electronic Frontier Foundation.

Allow automatic updates Default On Off

Run in Private Windows Allow Don't Allow
When allowed, the extension will have access to your online activities while private browsing. [Learn more](#)

Author [EFF Technologists](#)

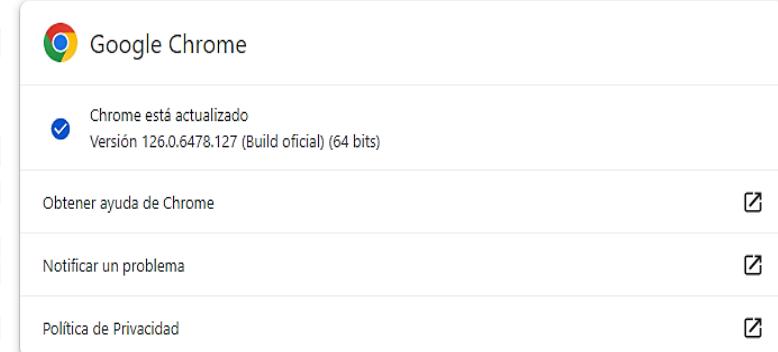
Version 2020.2.19

Idealmente, esto mejora tu privacidad sin que te enteres, lo que lo hace muy interesante 😊

ACTUALIZAR UN NAVEGADOR

- Todos los programas tienen fallos de seguridad
 - Y la mayoría se arregla con actualizaciones
- En Linux se suele actualizar de la que se actualiza el SO (R-11 “Príncipe de Asturias”)
- En Windows lo hacen automáticamente por lo general
 - Pero puede迫使se en Ayuda – Acerca de / Información
 - Hazlo por si acaso, **no te conviene navegar con un navegador desactualizado**
 - Es buena idea por ejemplo acostumbrarse a usar la opción de actualizar un día fijo de la semana por si acaso

Información de Chrome



Google Chrome

Chrome está actualizado
Versión 126.0.6478.127 (Build oficial) (64 bits)

Obtener ayuda de Chrome

Notificar un problema

Política de Privacidad

Tus navegadores son lo más expuesto a peligros que tienes en tu PC, por lo que actualizarlos ¡es más que una necesidad!

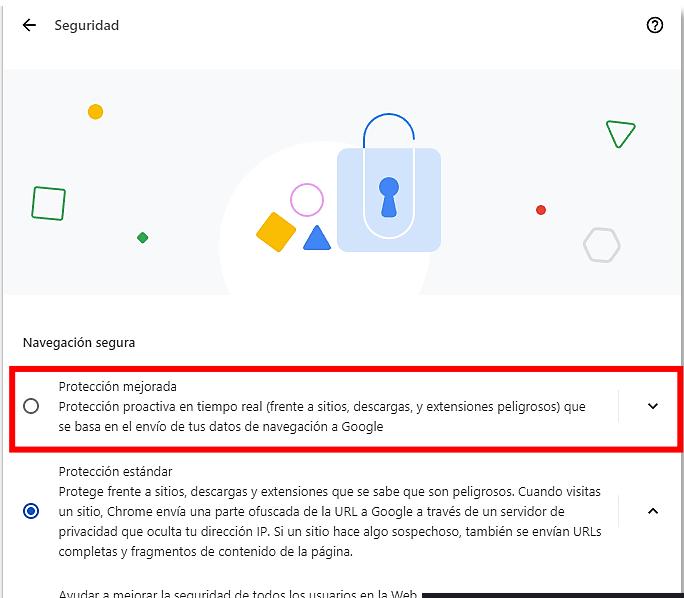
NAVEGAR EN MODO ESTRICTO

- Todos los navegadores modernos tienen un modo estricto  de navegar

- Bloquean más elementos potencialmente perjudiciales
- Pero puede “romper” páginas legítimas
- Es por tanto algo a usar en el navegador de ocio

- Se activa en una opción del navegador, por ejemplo

- **Chrome:** Privacidad y Seguridad – Privacidad
- **Firefox:** Ajustes – Privacidad y Seguridad
- **Edge:** Privacidad, búsqueda y servicios
 - Elegir “Estricta”



Navegación segura

- Protección mejorada
- Protección proactiva en tiempo real (frente a sitios, descargas, y extensiones peligrosos) que se basa en el envío de tus datos de navegación a Google

Protección estándar

Protege frente a sitios, descargas y extensiones que se sabe que son peligrosos. Cuando visitas un sitio, Chrome envía una parte ofuscada de la URL a Google a través de un servidor de privacidad que oculta tu dirección IP. Si un sitio hace algo sospechoso, también se envían URLs completas y fragmentos de contenido de la página.

Ayudar a mejorar la seguridad de todos los usuarios en la Web

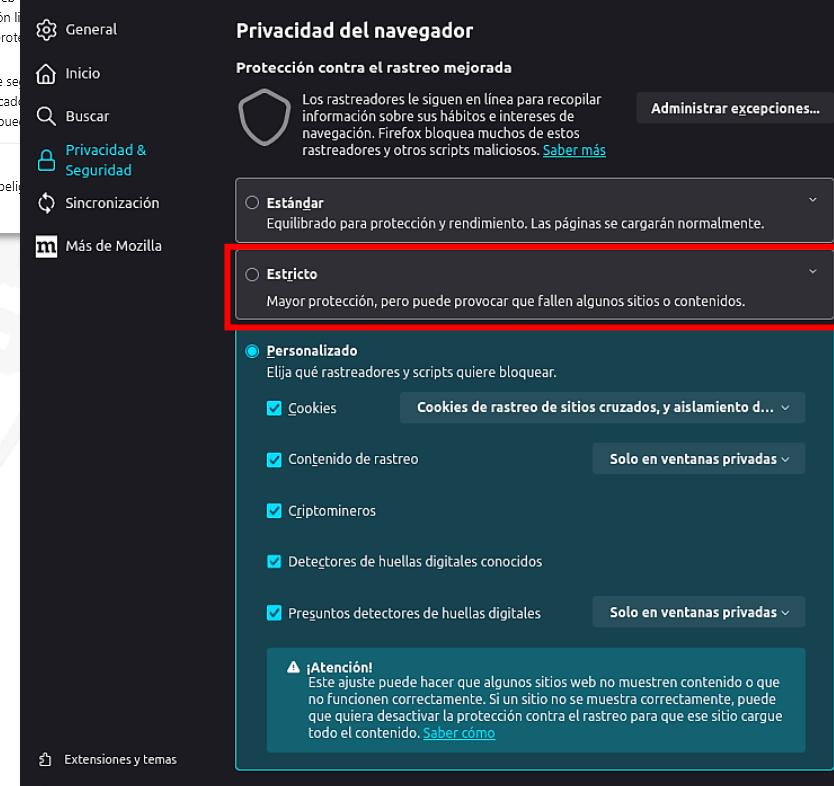
Envía a Google las URL de las páginas que visita, información de las páginas para ayudar a descubrir nuevas amenazas y proteger a los demás.

Avisarte si se ha vulnerado una contraseña en una brecha de seguridad

Cuando usas una contraseña, Chrome te avisa si se ha publicado en línea. Las contraseñas y nombres de usuario se cifran para que nadie pueda leerlas.

Sin protección (no recomendado)

No te protege frente a descargas, extensiones ni sitios web peligrosos. La navegación es más rápida, pero no es tan segura en otros productos de Google no se verá afectada.



Privacidad del navegador

Protección contra el rastreo mejorada

Estandar

Los rastreadores te siguen en línea para recopilar información sobre tus hábitos e intereses de navegación. Firefox bloquea muchos de estos rastreadores y otros scripts maliciosos. [Saber más](#)

Estricto

Mayor protección, pero puede provocar que fallen algunos sitios o contenidos.

Personalizado

Elige qué rastreadores y scripts quiere bloquear.

Cookies

Contenido de rastreo

Criptomineros

Detectores de huellas digitales conocidos

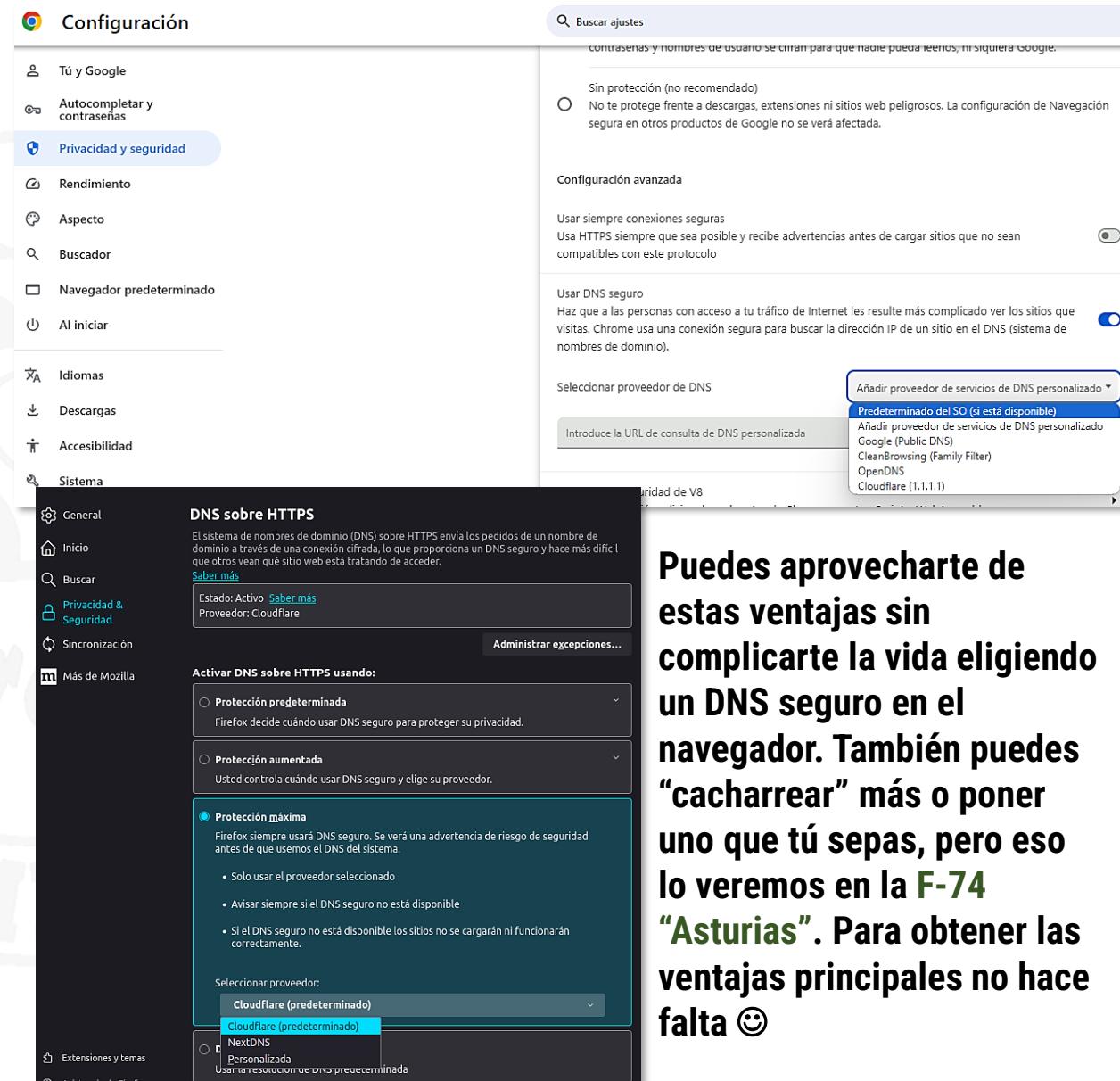
Presuntos detectores de huellas digitales

Atención! Este ajuste puede hacer que algunos sitios web no muestren contenido o que no funcionen correctamente. Si un sitio no se muestra correctamente, puede que quiera desactivar la protección contra el rastreo para que ese sitio cargue todo el contenido. [Saber como](#)

Firefox también lo tiene. En realidad, todos los navegadores deberían tener ya algo similar

No IR A WEBS QUE SE SABE QUE SON PERJUDICIALES

- Antes vimos que el DNS es el “traductor” que actúa siempre que navegamos
- ¿Qué pasaría si el DNS supiera que vamos a ir a una web que sabe que es perjudicial por algún motivo?
 - Tiene virus, sirve contenidos inadecuados...
- No te lo preguntes, ¡puedes hacerlo!
 - Activando un DNS seguro sin complicaciones en el navegador
 - **Chrome:** Privacidad y seguridad – Seguridad – Seleccionar “CloudFlare”
 - **Firefox:** Ajustes – Privacidad y Seguridad – Seleccionar “NextDNS”
 - Otros navegadores también los tienen



The screenshot shows two browser settings panels side-by-side.

Google Chrome Settings (Left):

- Panel title: Configuración
- Left sidebar categories: Tú y Google, Autocompletar y contraseñas, **Privacidad y seguridad** (selected), Rendimiento, Aspecto, Buscador, Navegador predeterminado, Al iniciar, Idiomas, Descargas, Accesibilidad, Sistema.
- Main content area: **DNS sobre HTTPS** section. It explains that DNS over HTTPS (DoT) encrypts domain name requests, making them harder for others to intercept. It shows "Estado: Activo" and "Proveedor: Cloudflare". Buttons for "Saber más" and "Administrar excepciones..." are present.
- Bottom navigation: Extensiones y temas, Asistencia de Firefox.

Mozilla Firefox Settings (Right):

- Panel title: Buscar ajustes
- Left sidebar categories: Sin protección (no recomendado), Usar siempre conexiones seguras, Usar DNS seguro, Seleccionar proveedor de DNS.
- Right sidebar categories: Contraseñas y nombres de usuario, Configuración avanzada, Usar siempre conexiones seguras, Usar HTTPS siempre que sea posible y recibir advertencias antes de cargar sitios que no sean compatibles con este protocolo, Usar DNS seguro, Seleccionar proveedor de DNS.
- Bottom right: A dropdown menu titled "Añadir proveedor de servicios de DNS personalizado" lists several options: Predeterminado del SO (si está disponible), Añadir proveedor de servicios de DNS personalizado, Google (Public DNS), CleanBrowsing (Family Filter), OpenDNS, Cloudflare (1.1.1.1).

Text on the right:

Puedes aprovecharte de estas ventajas sin complicarte la vida eligiendo un DNS seguro en el navegador. También puedes “cacharrear” más o poner uno que tú sepas, pero eso lo veremos en la F-74 “Asturias”. Para obtener las ventajas principales no hace falta ☺

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

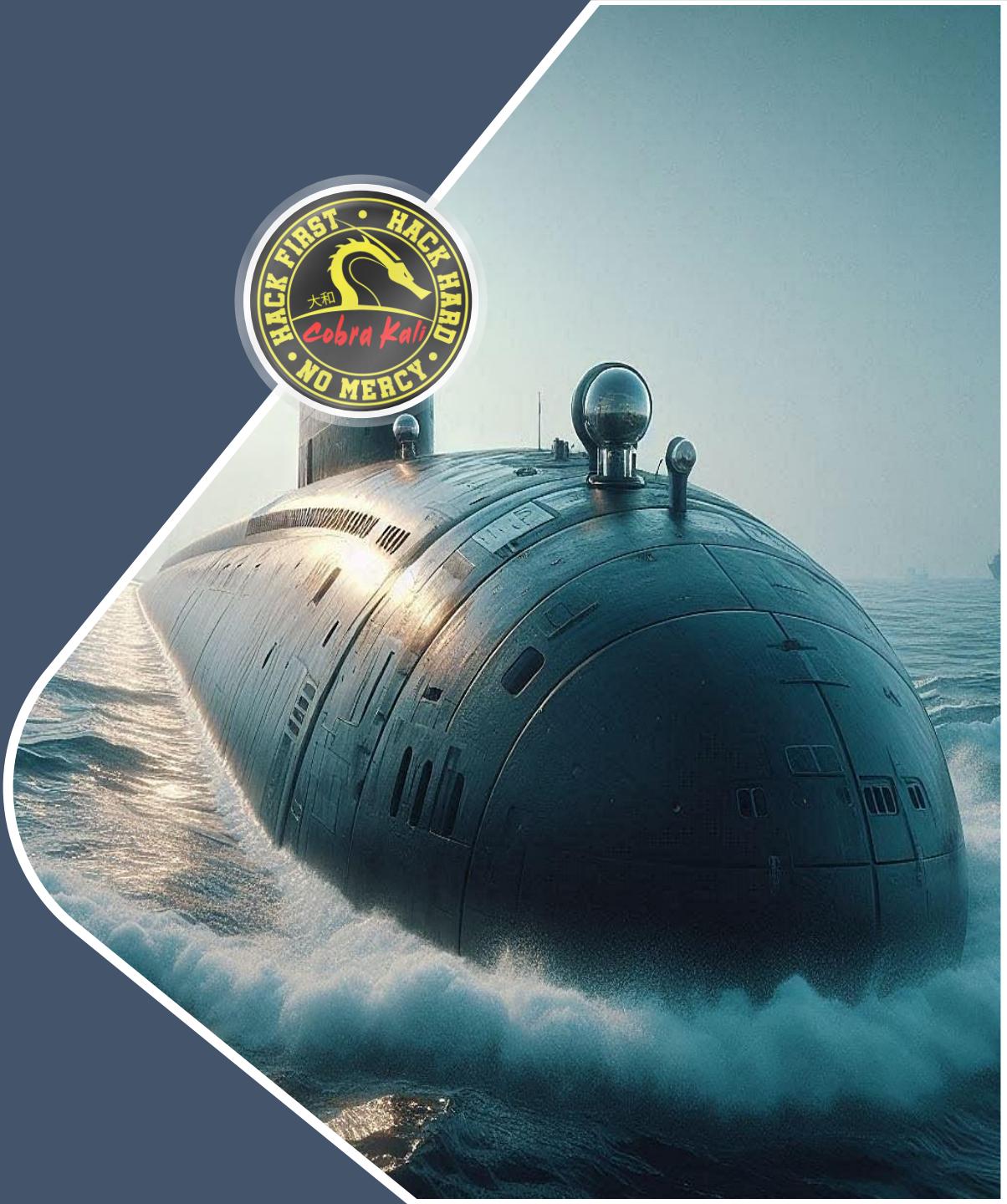


- *¿Comprendes que usar un navegador u otro es una decisión que depende de varios factores, y que no todos los navegadores son exactamente iguales, aunque todos valgan para navegar?*
- *¿Has entendido lo importante que es usar máquinas virtuales para navegar más seguro, porque en el caso de que ocurra alguna desgracia todo va a quedar dentro de ella?*
- *¿Entiendes la utilidad de tener un navegador para ocio y otro para el trabajo?*
- *¿Te ha quedado claro que, como mínimo, debes aspirar a tener un navegador actualizado y con bloqueador de publicidad para estar más seguro?*
- *¿Comprendes para qué puede servir un bloqueador selectivo de scripts como el que te recomiendo?*
- *¿Te ha quedado claro que el tema de la privacidad es más importante de lo que parece, y que puedes hacer algo para tener un mínimo de ella?*
- *¿Has entendido también que, aunque no entiendas muy bien lo que hay por debajo, hay cosas sencillas que puedes hacer para que tu navegación sea mucho más segura?*



INVESTIGANDO LA WEB

Una web es mucho más que lo que ven nuestros ojos...



¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?



- En esta sección voy a darte la capacidad de ver con “ojos de hacker”
 - Dicho de otra forma, voy a enseñarte a “mirar en profundidad” esa página web que tienes ahora mismo delante tuyo abierta en un navegador de tu PC o móvil ☺
- Te voy a enseñar a sacar más datos de lo que ves, a descubrir cosas que no se ven a simple vista y que ocurren en “las tripas” de la web, e incluso a ver cómo era esa web en el pasado
 - Se trata de una serie de pruebas para que sepas si una web “huele bien” o “huele mal” ☺
- ¿Te comerías algo que huele mal? Pues tampoco vayas a webs que “huelen mal”
 - Lo que pasa es que hay que entrenar tu “olfato hacker” para saber cómo huele una web ☺



00 Lo que se ve

Sacando información de lo que recibe nuestro navegador para ver si una web “huele mal”



¿ME FÍO DE UNA WEB?

- Una vez podemos navegar con más seguridad, vamos a responder a una pregunta
¿Puedo fiamse de una web realmente con lo que veo en ella?
- El objetivo es ver si tiene sentido dar mis datos o comprar algo en una web con un mínimo de seguridad o
 - Es cutre 💔
 - “Huele” a timo 🐾
- Estas técnicas no solo habría que aplicarlas a la web “principal” sino a otras secundarias que dependen de ella
 - Nos permiten “ver” mucho más que lo que se ve a simple vista
 - Si vemos cosas mal hechas, alguien no se ha tomado la molestia de mejorar su seguridad básica
 - Y, por tanto, es mejor **huir de esa web** por si acaso...e irse a la competencia
 - *¿Comerías en un restaurante que huele fatal al entrar? ¿Te alojarías en un hotel que tiene marchas de moho a simple vista? ¿Comprarías un coche que ves que pierde líquido están parado?*
 - **Esto es lo mismo, pero en web**

CÓDIGO Y COMENTARIOS

● A veces en los propios comentarios de una web hay demasiada información

- No es algo común, pero tampoco es broma...
- Productos y versiones usadas (luego veremos qué se hace con eso)
- Referencias a páginas no enlazadas
 - Potencialmente no terminadas o “secretas”
- ¡Usuarios y claves! :O

● ¿Te encuentras algo así?



Menú de tu navegador - Desarrollador web o herramientas de desarrollador - ver código fuente...

Todo texto en verde entre <!-- ... --> es un comentario

```
<html>
  > <head>... </head>
  > <body>
    > <nav role="navigation" class="navbar navbar-default">... </nav>
    > <div class="container">
      >   ::before
      >   <div class="row">... </div>
      >   <div class="row">
        >     ::before
        >     ...
        >     <p>...</p>
        >     <!--
        >       Error: user.admin is not equal to true.
        >       {
        >         "_id": "570a28f7935cal060099e0be",
        >         "username": "ciao",
        >         "password": "$2a$10$BZt.bwSE09hRaDgmAlluXONT0YlOPvWF7V06awwxzFkE.e8Zn3iKi",
        >         "uid": "rfisvzxf856wm8npdpuyt9v41"
        >       }
        >     -->
        >     ::after
        >   </div>
        >   ::after
        > </div>
```

UUUUUUUUFFFFFFFFFFFFFFFFFFFFFFF ☺

Da igual que no entiendas lo que pone, si ves algo que parecen usuarios, contraseñas o páginas web que dependen de la principal de esta forma, esa web “huele mal”

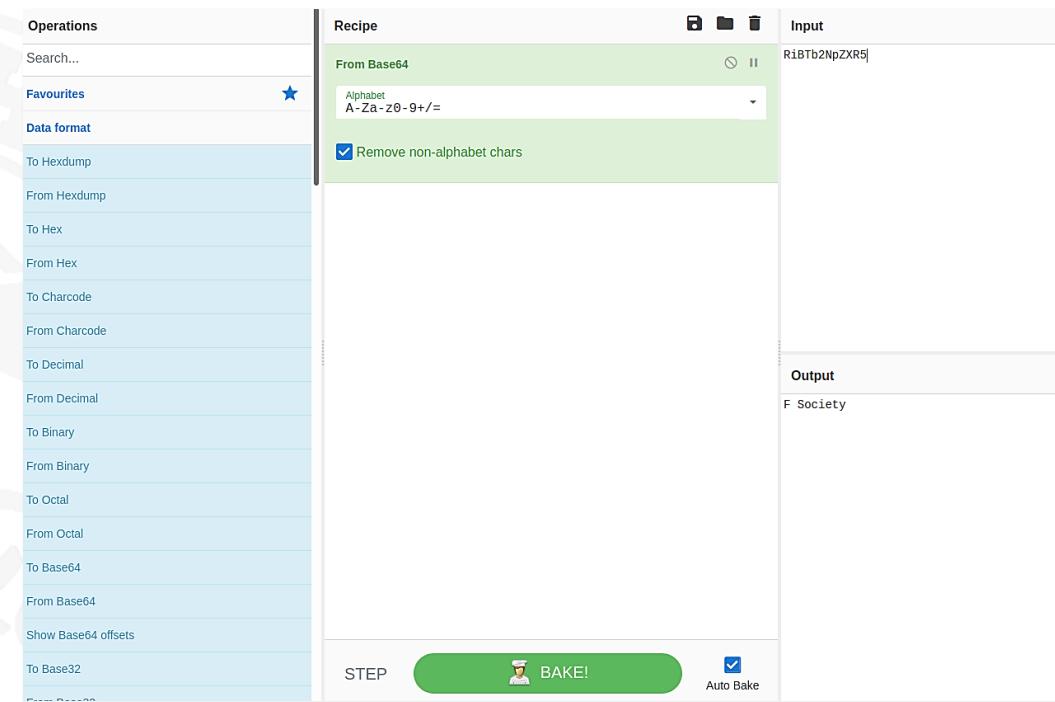
¿COSAS OFUSCADAS? (ESCRITAS EN “RARUÑOL” ☺). No PROBLEM

● A veces en la web aparecen textos ofuscados o en formatos que no entendemos

- Típicos casos de valores hexadecimales o en un formato de codificación llamado Base64
 - Ej.: Información sin sentido que acaba en “==”
- <https://es.wikipedia.org/wiki/Base64>

● ¿No lo entiendes? No hay problema

- The Cyberchef (<https://gchq.github.io/CyberChef/>) te permite **descifrar información**
 - Que se encuentre en muchos formatos diferentes
- Con ello puedes **entender mejor lo que está pasando** en una web
- **Arrastra y suelta una “receta” para transformar datos y ¡mira que pasa!**



¡Vale para muchísimas cosas! Hasta lo puedes usar para enviar mensajes cifrados a otras personas (que saben la clave que usas). ¡Puedes “jugar” con él de muchas maneras!

¿Y SI LO QUE NO ENTIENDO ES EL CÓDIGO?

• ¿Tienes algo de experiencia en programación? Igual te interesa leer el código

- Pero el código no solo puede ser ininteligible porque no entiendas el lenguaje, sino por que esté ofuscado a propósito para que **no entiendas qué hace la página**
- El código JavaScript **suele ofuscarse** para, entre otras cosas, que **no sepas que hay enlaces a web que no puedes ver navegando** y no las explores

• Por suerte hay herramientas que lo “enguapecen”

- Ej.: <https://beautifier.io/>



```
eval(function(p,a,c,k,e,r){e=function(c){return c.toString(a)};if(!''.replace(/\^/,String)){while(c--)r[e(c)]=k[c]||e(c);k=[function(e){return r[e]}];e=function(){return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('4 0(){5 2=6.7.8.9(a,1,3);b2}c.d(0,e,f,g,h,i,j)',20,20,'getGrades||args||function|var|Array|prototype|slice|call|arguments|return|console|log|90|100|75|40|89|95'.split('|'),0,{})
```

¡Vaya glow up!

```
function getGrades() {
  var args = Array.prototype.slice.call(arguments, 1, 3);
  return args
}
console.log(getGrades(90, 100, 75, 40, 89, 95));
```

Si no entiendes de programación, puedes saltarse este paso. También te digo que algunas webs creen que esto es una forma de seguridad. Y, obviamente, NO

INFORMACIÓN DE LAS WEBS Y CVEs

● Cuando navegamos a una web, nos llegan cabeceras

- Información de la web que no vemos en el sitio habitual
- Se ven con las **herramientas de desarrollador** del navegador
- *¿Y yo para que quiero saber eso?*, jaja saludos ☺
- Porque a veces **dicen los productos (y su versión)** con los que se hizo la web
 - Si, las webs se fabrican con herramientas, no se pica código desde cero ☺
- Esta información se usa para **buscar en un repositorio de vulnerabilidades**
 - **Y saber qué vulnerabilidades tienen** todos los productos encontrados
- Estas vulnerabilidades tienen un **código internacional único** (como el DNI)
 - **Se llama CVE**, y lo puedes usar para buscar información de ellas

● Es decir, para poner en Google “<producto> <versión> CVEs”

- Ej.: “Apache 2.4.38 CVEs”
- Entrar en una web que liste sus vulnerabilidades (Ej.: <https://www.cvedetails.com/>)
- **Y llorar...o no ☺**



¿Que Internet funcione en el estado en el que está es el milagro que demuestra que existe un ser divino? No lo descartaría...

INFORMACIÓN DE LAS WEBS Y CVEs



José Manuel
Redondo López

- **¿No me crees? Mira estos ejemplos “delatores”**
- **Un producto llamado Liferay, incluida su versión**
 - Aquí tienes sus vulnerabilidades:
https://www.cvedetails.com/vulnerability-list/vendor_id-2114/product_id-12592/version_id-109268/Liferay-Portal-5.2.3.html
- **Otro llamado Apache, versión 2.4.38**
 - Y de nuevo sus vulnerabilidades:
https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-613554/Apache-Http-Server-2.4.38.html
- **Ahora puedes probar con cualquier web que conozcas, igual te sorprendes (o no)**
 - Hacer esto es legal, no te preocupes
 - Otra cosa es divulgar públicamente que una web tiene estos problemas: **NO LO HAGAS**
 - Es información para que tú decidas si una web es o no fiable

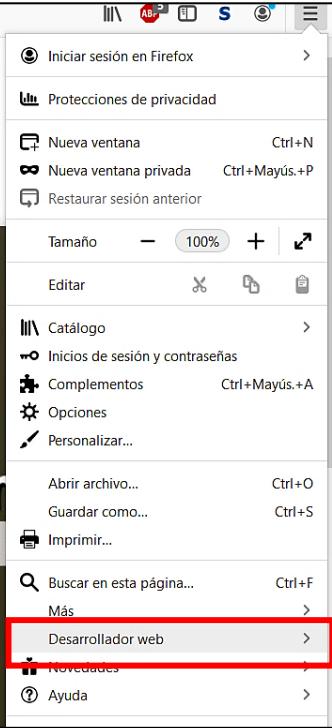
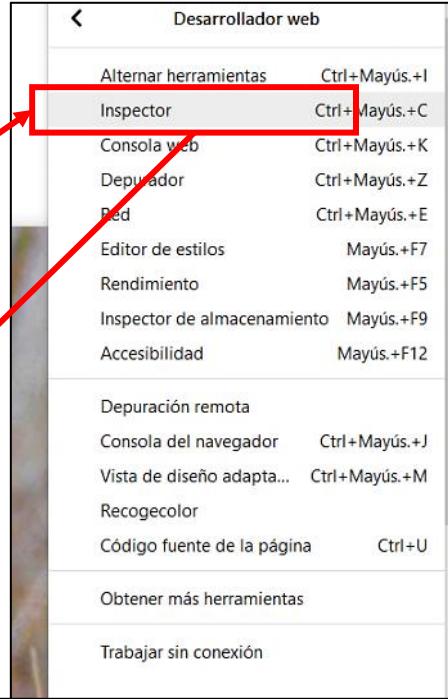
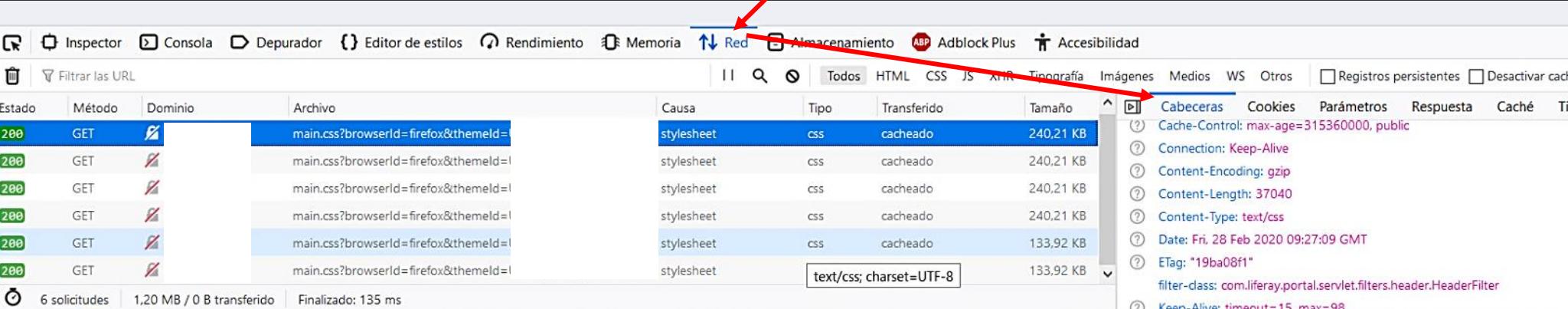
The screenshot shows a browser's developer tools Network tab. A request to 'Liferay-Portal' is selected, revealing its details:

- General**: Shows a large blue redacted area for the response body.
- Response Headers**:
 - Connection: Keep-Alive
 - Content-Encoding: gzip
 - Content-Length: 6856
 - Content-Type: text/html; charset=UTF-8
 - Date: Thu, 22 Sep 2016 11:52:11 GMT
 - Keep-Alive: timeout=15, max=100
 - Liferay-Portal: Liferay Portal Standard Edition 5.2.3 (Augustine / Build 5203 / May 20, 2009)
- Request Headers**:
 - Accept: text/html,application/xhtml+xml,application/xml,application/json
- Protocol**:
 - 443
 - tcp
 - https
- Apache httpd**: Version: 2.4.38
 - HTTP/1.1 200 OK
 - Date: Wed, 22 Dec 2020 16:57:49 GMT
 - Server: Apache/2.4.38 (Debian)
 - Set-Cookie: MoodleSession=...; path=/; secure
 - Expires:
 - Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
 - Pragma: no-cache
 - Content-Language: es
 - Content-Script-Type: text/javascript
 - Content-Style-Type: text/css
 - X-UA-Compatible: IE=edge
 - Accept-Ranges: none
 - X-Frame-Options: sameorigin
 - Vary: Accept-Encoding
 - Transfer-Encoding: chunked
 - Content-Type: text/html; charset=utf-8

¿CÓMO VEO ESTA INFORMACIÓN?

- Una web que exponga esto tendrá problemas de seguridad gordos
- Si te lo encuentras, la web “huele (muy) mal”

Exponer qué productos y versiones usas es completamente innecesario para el funcionamiento de cualquier web: se hace por descuido o ignorancia

Estado	Método	Dominio	Archivo	Causa	Tipo	Transferido	Tamaño	Cabeceras	Cookies	Parámetros	Respuesta	Caché	Tie
200	GET		main.css?browserId=firefox&themeld=1	stylesheet	css	cacheado	240.21 KB	Cache-Control: max-age=315360000, public					
200	GET		main.css?browserId=firefox&themeld=1	stylesheet	css	cacheado	240.21 KB	Connection: Keep-Alive					
200	GET		main.css?browserId=firefox&themeld=1	stylesheet	css	cacheado	240.21 KB	Content-Encoding: gzip					
200	GET		main.css?browserId=firefox&themeld=1	stylesheet	css	cacheado	240.21 KB	Content-Length: 37040					
200	GET		main.css?browserId=firefox&themeld=1	stylesheet	css	cacheado	133.92 KB	Content-Type: text/css					
200	GET		main.css?browserId=firefox&themeld=1	stylesheet	css	cacheado	133.92 KB	Date: Fri, 28 Feb 2020 09:27:09 GMT					
								ETag: "19ba08f1"					
								filter-class: com.liferay.portal.servlet.filters.header.HeaderFilter					
								Keen-Alive: timenut=15, max=98					

6 solicitudes | 1,20 MB / 0 B transferido | Finalizado: 135 ms

INFORMACIÓN DE LAS WEBS Y CVEs

- Entonces ¿*Hay webs que listan los problemas de seguridad de muchos programas conocidos?*
 - Sí, ¡y es legal!
- Se usan para saber cuándo toca actualizar el software si tiene problemas serios
 - Pero también se puede usar para descubrir si una web está usando software inseguro
- ¡Pero no entiendo que es toda esta información!
 - No importa, los errores se puntúan de 0 (broma 😂) a 10 (sal corriendo ya 😱)
 - El código de colores ya indica cositas 😊🚩
 - ¿*La web que estás mirando tiene algo de 7 para arriba?*
No le des ni los buenos días
 - ¿*Puedes decir que tiene "red flags*? Pues sí 😊

Source: Apache Software Foundation	Updated	2024-06-10
CVE-2023-31122	Max CVSS EPSS Score	7.5 1.01%
Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server. This issue affects Apache HTTP Server: through 2.4.57.	Published	2023-10-23
Source: Apache Software Foundation	Updated	2024-06-10
CVE-2023-27522	Max CVSS EPSS Score	7.5 1.90%
HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client.	Published	2023-03-07
Source: Apache Software Foundation	Updated	2023-09-08
CVE-2023-25690	Max CVSS EPSS Score	9.8 0.74%
Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?\${1}"; [P] ProxyPassReverse /here/	Published	2023-03-07
Source: Apache Software Foundation	Updated	2024-01-02
CVE-2022-37436	Max CVSS EPSS Score	5.3 0.08%
Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.	Published	2023-01-17
Source: Apache Software Foundation	Updated	2023-09-08
CVE-2022-36760	Max CVSS EPSS Score	9.0 3.27%
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP		

Una cosa te digo, si averiguas de cualquier manera productos y versiones usadas para crear una web tienes MUCHA información que puedes usar para tomar decisiones acerca de si te fías o no de la web. Luego te enseño más formas de sacar esa información...incluida una automática 😊

ERRORES COMO FUENTES DE INFORMACIÓN

- Navegar “mal” apostar puede causar errores que revelen productos y versiones

- Ej.: Añadiendo un carácter extraño “.” a la URL
- Esto nos revela el código de la aplicación y que está usando algo llamado **Yii** (primera imagen)
 - Que tiene vulnerabilidades:
https://www.cvedetails.com/product/38868/Yiiframework-YII.html?vendor_id=13516
 - Sí, otra vez lo mismo...

- Tener este tipo de errores son muy mal indicio de la seguridad de una web

- La segunda imagen es un ejemplo de un desastre
- Todos los errores de esta clase son **otro indicio de que una web “huele mal”**



CHttpException

The system is unable to find the requested action "publishers".

/var/www/html/EraLiteraria/yii/framework/web/CController.php(483)

```

471     return $this->createActionFromMap($map,$actionID,$requestActionID,$config);
472 }
473 
474 /**
475  * Handles the request whose action is not recognized.
476  * This method is invoked when the controller cannot find the requested action.
477  * The default implementation simply throws an exception.
478  * @param string $actionID the missing action name
479  * @throws CHttpException whenever this method is invoked
480  */
481 public function missingAction($actionID)
482 {
483     throw new CHttpException(404,Yii::t('yii','The system is unable to find the request
array('{action}')=>$actionID=='?'&gt;$this->defaultAction:$actionID));
484 }
485 
486 /**
487  * @return CAction the action currently being executed, null if no active action.
488  */
489 public function getAction()
490 {
491     return $this->action;
492 }
```

Server Error in '/' Application.

A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)

Source Error:

```

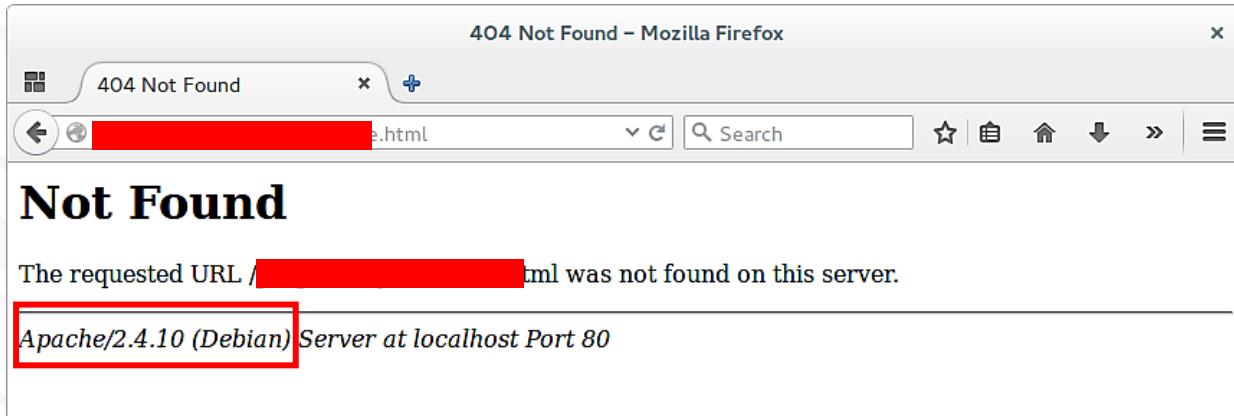
Line 15:         string conString = @"Data Source=[REDACTED];Initial Catalog=[REDACTED];Integrated Security=SSPI";
Line 16:         SqlConnection con = new SqlConnection(conString);
Line 17:         con.Open();
Line 18:         string qry = "select Uname,UPass From UserDetails";
Line 19:
```

Source File: [REDACTED] Line: 17

IP de la base de datos, su nombre, consultas...todo mal 😞

ERRORES COMO FUENTES DE INFORMACIÓN

- Otra forma típica de hacerlo es intentar navegar a páginas que no existen
 - Es el llamado error 404 Not Found
- A veces, los errores derivados pueden dar sorpresas en forma de información de productos usados
 - Y con ella, repetimos el proceso anterior
- ¡Toda información de productos usados debería eliminarse de una web!
 - De no ser así, lo que decimos: “Huele mal”



Como ves, hay varias formas de sacar información de productos y versiones sin hacer nada más que...navegar



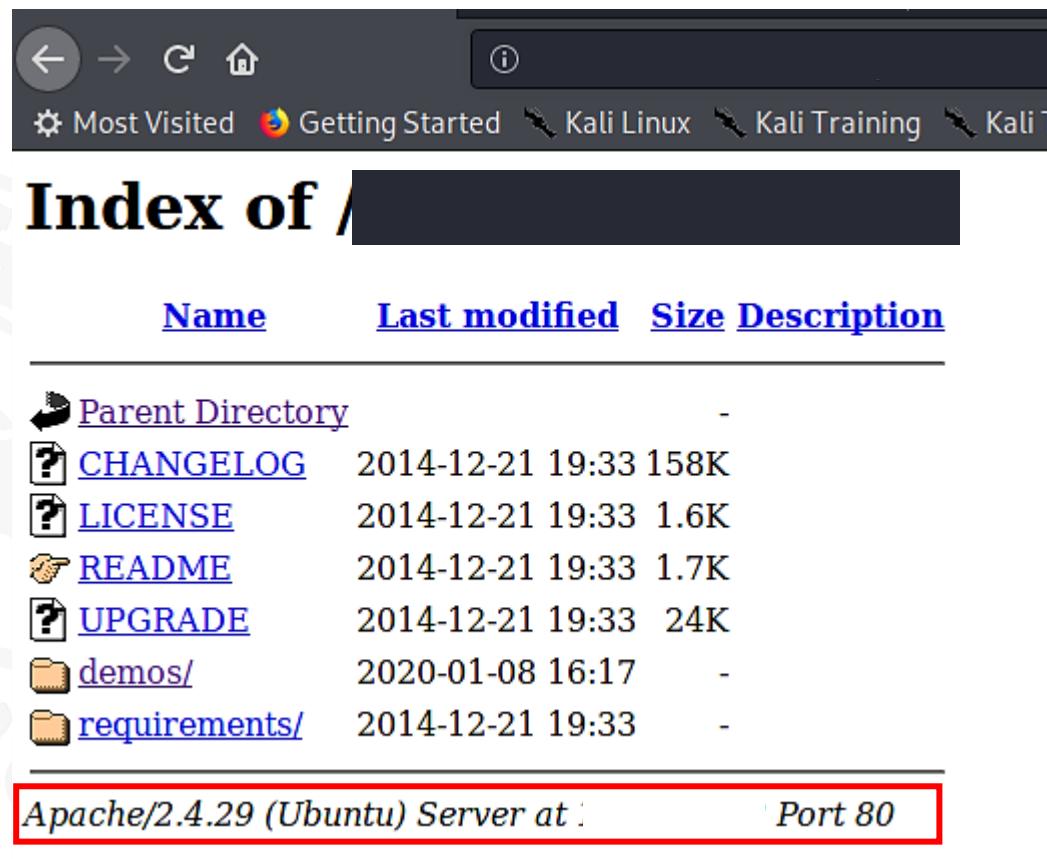
ERRORES COMO FUENTES DE INFORMACIÓN

- Otro error es el 403, cuando se accede a una ruta no permitida, como /

- Muchas veces se redirecciona a una página genérica

- Pero, a veces se genera un listado de directorios

- Esto lista **todos los contenidos la web**
- ¡Sean visibles o no!
- Documentos (con versiones de programas), ficheros ocultos potencialmente descargables...es decir, problemas
- **¡Este es un error gravísimo! Si una web lo tiene, huye de ella CORRIENDO**
- Es síntoma de una dejadez muy grande en temas de seguridad



Name	Last modified	Size	Description
Parent Directory		-	
CHANGELOG	2014-12-21 19:33	158K	
LICENSE	2014-12-21 19:33	1.6K	
README	2014-12-21 19:33	1.7K	
UPGRADE	2014-12-21 19:33	24K	
demos/	2020-01-08 16:17	-	
requirements/	2014-12-21 19:33	-	

Apache/2.4.29 (Ubuntu) Server at : Port 80

Y oooootra vez lo mismo ☺



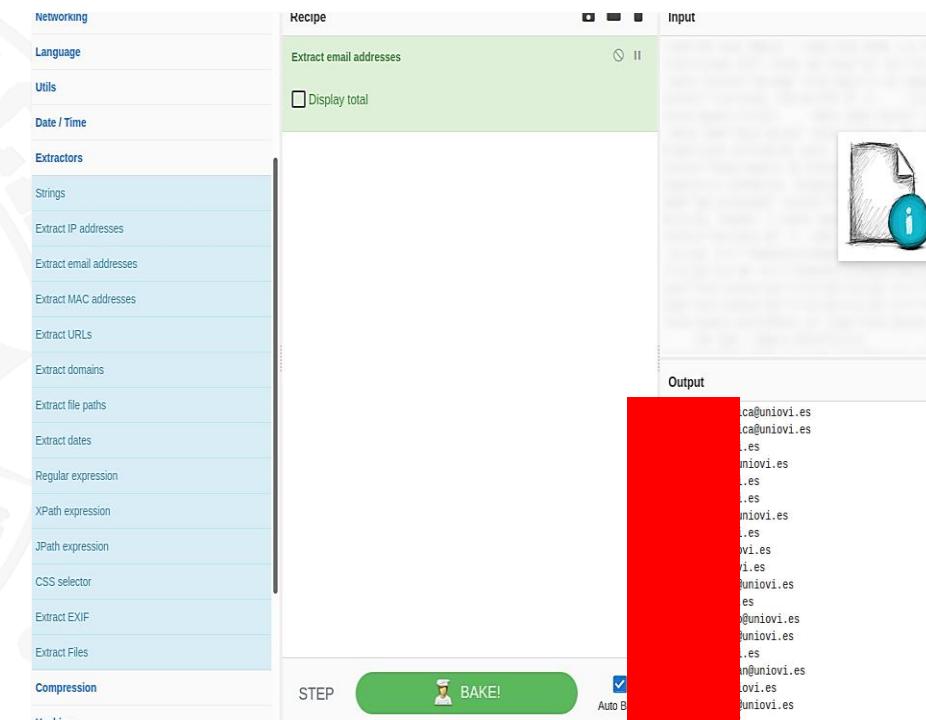
¿TE HAS ENCONTRADO EMAILS?

● El email es uno de los nombres de usuario más típicos en cualquier empresa

- Encontrárselos de forma indiscriminada **puede facilitar ataques de fuerza bruta**
 - Probar claves de ese usuario hasta que encuentres la buena
 - Con programas que permiten probar millones en poco tiempo
- Dependerá de si luego tiene otras medidas en contra de ellos
- También es típico para recolectar emails para **campañas de spam / phishing**

● ¿Es una lata leerse una web para localizarlos? ¿quizá estén en comentarios? No hay problema

- Descarga la página y sube luego el html a CyberChef, que tiene la herramienta que necesitas
- Categoría “Extractors”



¿Es tan horrible como los otros errores? No. ¿Es necesario dar todos los emails posibles? Seguramente tampoco. ¿Ocurre por dejadez? No lo descartes...

EL CERTIFICADO

● Cuando navegas por un sitio, debes tener un icono de un candado

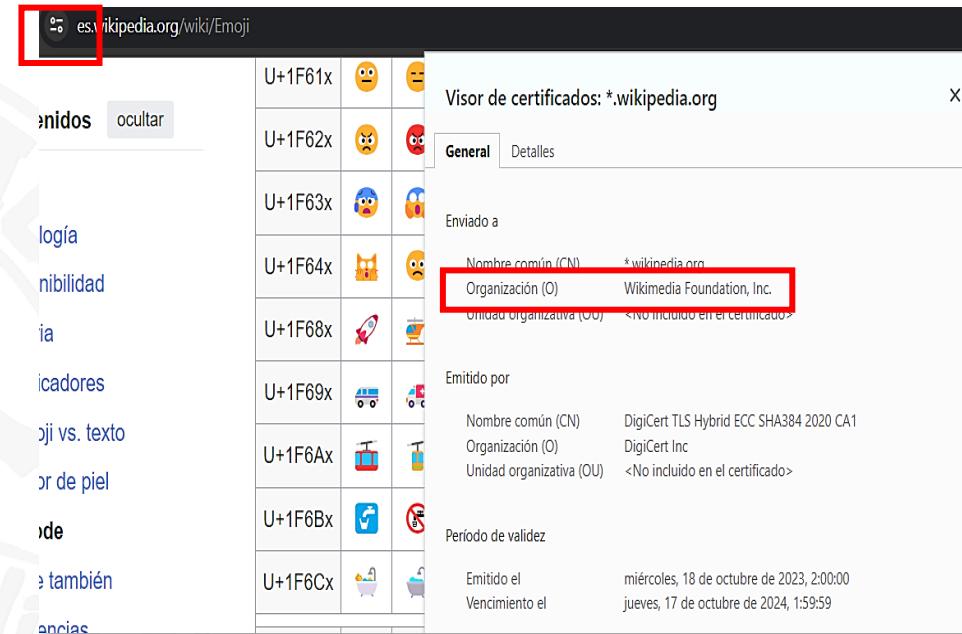
- Si no lo tienes o muestra un error **SAL DE AHÍ YA**
- Hoy día el “candado” es obligatorio prácticamente

● Eso solo garantiza comunicaciones cifradas entre tu PC y la web

- ¡No que la página sea segura!
- Te comunicas de forma secreta...con un delincuente 😊

● También te deja saber de quién es la página

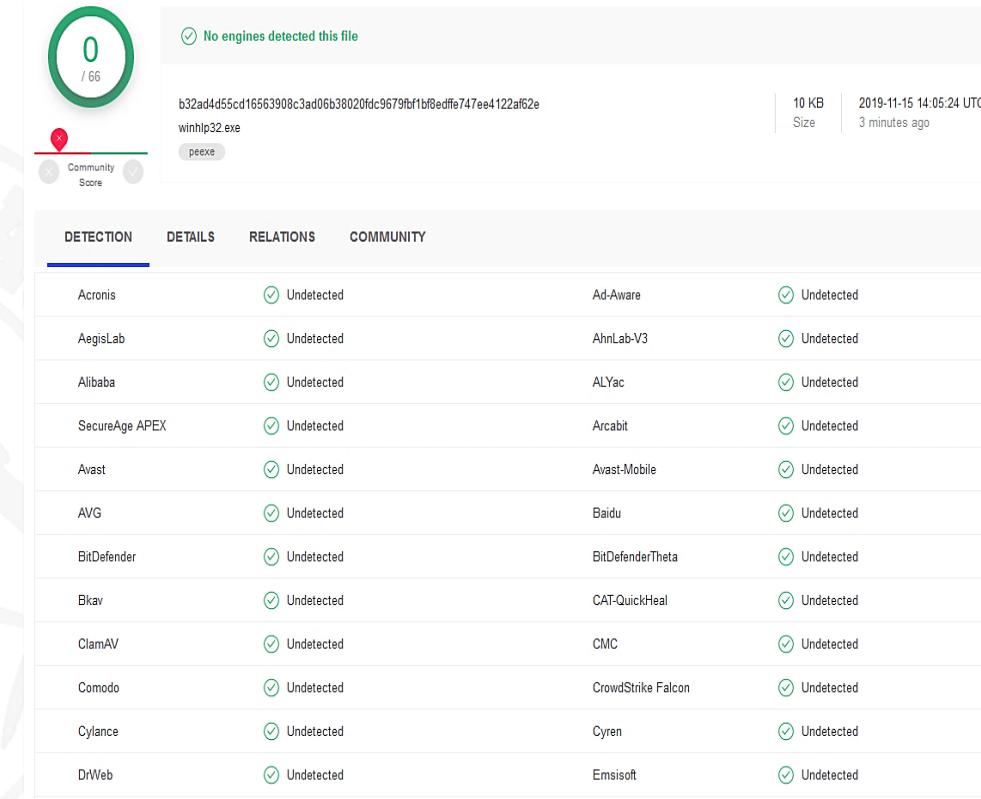
- Puedes consultar más información de la web gracias a él
- ¿La web no es de quien esperas? ¡Es una falsificación!
- Ej.: Vas a la tienda de Rolex, tiene candado, pero el certificado pone que la Organización es “Paco, SL”
 - Sí, aunque sea visualmente igual a la real



De quien es una web normalmente es algo público (y sino usa Google 😊). Si lo que aparece en “Organización” al clicar en donde se indica al lado de la URL no pone lo que esperas, busca qué es. Si no encuentras relación...MUY MALO

¿ES ESTA WEB O SUS DESCARGAS ALGO SEGURO?

- Si una web tiene descargas (documentos, programas...), no te fíes de ellas
 - Descarga siempre programas de sitios oficiales
 - Aun así, pásales un antivirus (Ej.: Caso Solarwinds ☹)
- Si aun así hay dudas, pásale 60+ antivirus 😊
 - Virustotal (<https://www.virustotal.com/gui/home/upload>) analiza cualquier archivo que se le envíe
 - En busca de malware conocido
 - Si pasas sus 60+ antivirus es más probable que el ejecutable esté “limpio”
- ¡Los documentos (Office, PDF...) descargados de una web también pueden ser peligrosos!
 - ¡Mándalos a este servicio también!



The screenshot shows the Virustotal analysis interface. At the top, it says "0 / 66" engines detected. Below that, the file name is listed: "b32ad4d55cd16563908c3ad06b38020fdc9679bf1bf8edffe747ee4122af62e" and "winhlp32.exe". To the right, there are fields for "Size" (10 KB) and "Time" (2019-11-15 14:05:24 UTC, 3 minutes ago). Below this, there are tabs for "DETECTION", "DETAILS", "RELATIONS", and "COMMUNITY". The "DETECTION" tab is selected, showing a table of 15 antivirus engines all reporting "Undetected". Each row includes the engine name, its status, and a green checkmark icon.

Detection Engine	Status	Notes
Acronis	Undetected	Ad-Aware
AegisLab	Undetected	AhnLab-V3
Alibaba	Undetected	ALYac
SecureAge APEX	Undetected	Arcabit
Avast	Undetected	Avast-Mobile
AVG	Undetected	Baidu
BitDefender	Undetected	BitDefenderTheta
Bkav	Undetected	CAT-QuickHeal
ClamAV	Undetected	CMC
Comodo	Undetected	CrowdStrike Falcon
Cylance	Undetected	Cyren
DrWeb	Undetected	Emsisoft

Sí, a veces da falsos positivos. Pero mejor prevenir que lamentar. Si alguno de estos da que es un malware, tiene malas opiniones de la comunidad, etc. no lo abras o instales
Y, por supuesto, no te fíes de la web que lo alojaba

¿ES ESTA WEB SEGURA?

- Al navegar uno puede tener dudas de si una web es o no segura
- **Google Safe Browsing** escanea billones de URL para localizar sitios web inseguros
 - Descubre nuevos sitios inseguros constantemente
 - Muchos de los cuales son sitios web legítimos que han sido robados...
 - Cuando detecta sitios web no seguros, muestra advertencias **en las búsquedas de Google y en los navegadores web que utilizan esta tecnología**
- ¡Pero podemos usarlo para saberlo nosotros mismos sobre sitio que queramos!
 - <https://transparencyreport.google.com/safe-browsing/search>

Comprobar el estado de un sitio web

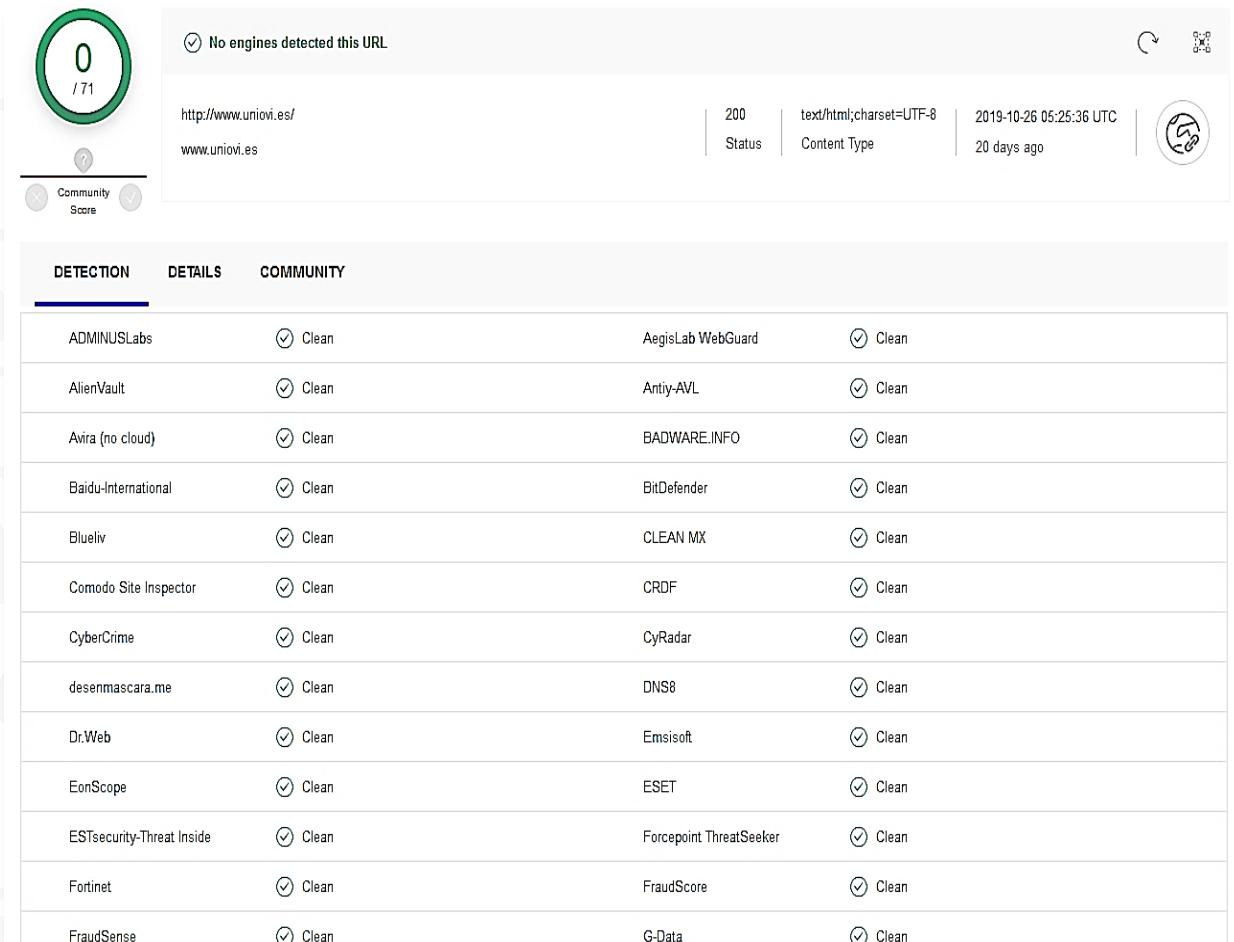
Estado actual

 No se ha detectado contenido no seguro

Aparecer aquí como “sitio no seguro” no deja dudas: Apesta 😊

¿Es esta web segura?

- *¿Necesitas una segunda opinión de una web?*
- Se puede usar la comprobación de URL de **Virustotal**
 - ¡No solo analiza programas! ☺
- Se pone una URL aquí y se mira qué nos dice
 - <https://www.virustotal.com/gui/home/url>
 - Aporta además más detalles acerca de ella,
 - Aunque tampoco es algo importante para lo que queremos conseguir



The screenshot shows the Virustotal interface for the URL <http://www.uniovi.es/>. The main summary indicates "0 / 71 engines detected this URL". Below this, the URL www.uniovi.es is listed with a status of 200 and a content type of text/html; charset=UTF-8. The analysis was performed 20 days ago. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY, with the DETECTION tab currently selected. The DETECTION table lists 15 different security engines, all of which have reported the URL as "Clean".

Engine	Status	Scanner	Status
ADMINUSLabs	Clean	AegisLab WebGuard	Clean
AlienVault	Clean	Antiy-AVL	Clean
Avira (no cloud)	Clean	BADWARE.INFO	Clean
Baidu-International	Clean	BitDefender	Clean
Blueliv	Clean	CLEAN MX	Clean
Comodo Site Inspector	Clean	CRDF	Clean
CyberCrime	Clean	CyRadar	Clean
desenmascara.me	Clean	DNS8	Clean
Dr.Web	Clean	Emsisoft	Clean
EonScope	Clean	ESET	Clean
ESTsecurity-Threat Inside	Clean	Forcepoint ThreatSeeker	Clean
Fortinet	Clean	FraudScore	Clean
FraudSense	Clean	G-Data	Clean

Que te reporte alguna de estas herramientas como "sitio no seguro" tampoco deja dudas: Apesta ☺

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



- *¿Entiendes el sentido de decir que una web “huele bien” o “huele mal” en función de lo que podemos ver en ella?*
- *¿Has entendido que hay cosas que no deberían aparecer en el código de una web, y que merece la pena leer ciertas cosas en él aunque no lo entiendas?*
- *¿Puedes explicarle a alguien que es un CVE y la importancia que tiene para el tema de seguridad?*
- *¿Has entendido la enorme importancia de saber programas y sus versiones que están relacionadas con una web desde el punto de vista de la seguridad?*
- *¿Entiendes cómo provocar errores puede darte pistas de si una web “huele”?*
- *¿Sabes para qué puedes usar los emails que has encontrado en una web o asociados a ella?*
- *¿Entiendes cómo leer el certificado de una web para saber si te engaña o no?*
- *¿Comprendes la enorme utilidad de herramientas como Virustotal o Google Safe Browsing y cómo puedes usarlas para saber cómo “huele” una web?*



Lo que no se ve

Sacando información de cosas que no se ven directamente con un navegador, de nuevo para ver si una web “huele mal”



TÍPICAS RUTAS “DELATORAS” A PROBAR

- Cuando haces clic en un enlace de una web vas a una ruta pública de la misma (Ej.: www.miweb.com/login)
- Pero las hay también no públicas
 - Normalmente porque contienen información que no deben ver los usuarios “normales”
 - Pero al acceder directamente a ellas puedes encontrar información interesante
 - Simplemente escribe www.miweb.com/admin o la que sea
- Si puedes acceder directamente a una ruta no pública, analiza bien la información que muestran
 - En base a ella, puedes fiarte de la web
 - Ejemplos de rutas típicas
 - <https://github.com/v0re/dirb/blob/master/wordlists/common.txt>

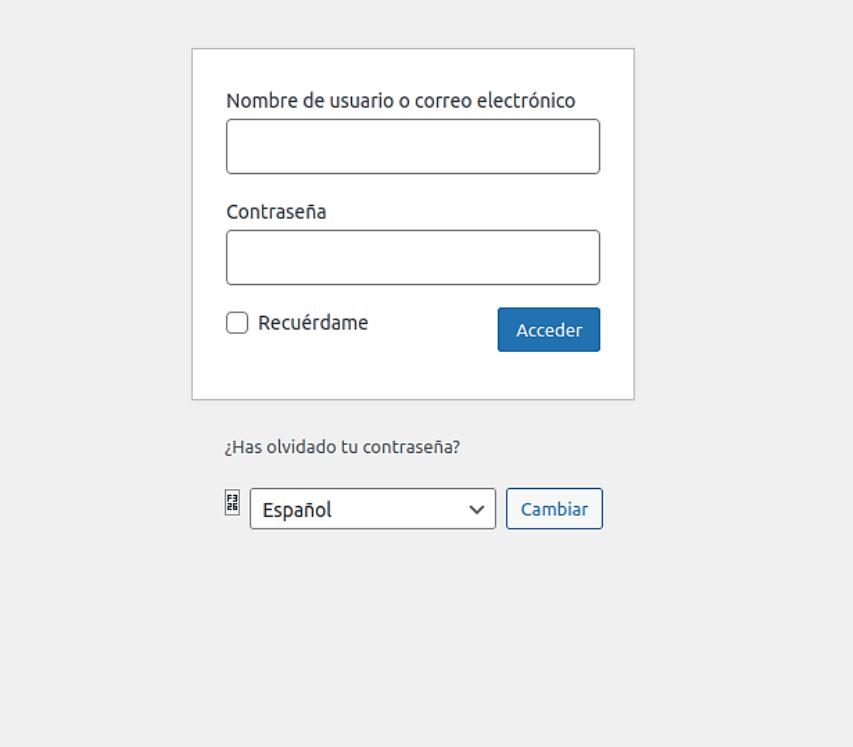
● Ejemplos de rutas ocultas clásicas

- /admin
- /config
- /docs
- /backup
- /external
- /uploads
- /wp-admin
- /phpmyadmin
- ...

TÍPICAS RUTAS “DELATORAS” A PROBAR

● Te lo explico con un ejemplo

- Lo que ves en la imagen aparece si añades /wp-admin a la URL de un partido político (no te digo cuál ☺)
- Indica que **la página está hecha con WordPress**
 - Ahora tienes una pista de **posibles CVEs**
 - Imagina si por otro lado consigues saber la versión concreta...
- Esta página es **la del administrador**
 - Alguien que sepa **usuario y la contraseña**, podría cambiar el contenido de la web por lo que se le antoje
 - El usuario por defecto de WordPress es “admin”
 - Esperemos que lo hayan cambiado y la contraseña sea buena...
 - Bromas, eliminar contenido o engañar a los visitantes...
- *¿Debería ver esta página web yo desde mi casa? **NUNCA***
 - No soy administrador
 - Debería estar **limitado el acceso** sólo a las IPs de los administradores, y no dejar “barra libre”
 - *¿Qué pasa si WordPress tiene un fallo que me permite saltármelo?*



Nombre de usuario o correo electrónico

Contraseña

Recuérdame Acceder

¿Has olvidado tu contraseña?

Español Cambiar

Que alguien pueda ver libremente esta página simplemente sabiendo su ruta es mala señal. Se expone algo que, si se consigue romper, dejaría a la web temblando

EL FICHERO ROBOTS.TXT

• Muchas webs tienen un fichero de estos

- Se usa para indicar a los motores de búsqueda que **no indexen** las rutas indicadas bajo la palabra clave **Disallow**

• Siempre es accesibles usando un patrón

- <http://<La URL>/robots.txt>
- Ej.: www.miweb.com/robots.txt

• El problema es que este archivo es público y accesible

- ¡Declara la existencia de estos contenidos “ocultos” a cualquiera!

• Otra vez es dar demasiada información y “oler mal”

- Al usar un mecanismo como este para ocultar cosas
- Pensando que así se consigue algo de seguridad...

• También puedes probar con rutas `/.well-known/`

- Ej.: <https://www.google.com/.well-known/security.txt>
- Todas las rutas conocidas: https://en.wikipedia.org/wiki/Well-known_URI

```
User-agent: *
Disallow: /cp/bio
Disallow: /cp/top
Disallow: /news
Disallow: /blogtop
Disallow: /blogbio
Disallow: /bh
Disallow: /cp
Disallow: /showblog
Disallow: /index.php
Disallow: /index2.php
Disallow: /jump.php
Disallow: /past-technology-news
Disallow: /klip
Disallow: /?go=
Disallow: /?option=
Disallow: /?q=
Disallow: /?t=
Disallow: /?webmenu=
Disallow: /%22
Disallow: /c/a/Choosing%20
```

Esto y lo de las rutas ocultas de antes tienen algo en común: Si el dueño de la web cree que esto es seguridad, el resto de la web debe ser un desastre. Mejor sal de ella...

LOS METADATOS



- Son datos que se añaden a un archivo, pero no como parte de su contenido

- Mucha gente no sabe que hay programas que los colocan automáticamente en los archivos que generan
- **Y pueden revelar datos interesantes:** Direcciones IP, nombres de personas, empresas, programas usados...

- Se pueden sacar de varias formas

- Botón derecho – Propiedades – Detalles
 - Funciona para documentos e imágenes
- Subiéndolo a webs como Metadata2Go
 - <https://www.metadata2go.com/view-metadata>
- Cyberchef lo permite con Extractors - Extract EXIF

- Si las imágenes o documentos de una web revelan datos interesantes así, es indicio de una seguridad potencialmente débil

Propiedad	Valor
Descripción	EPC. Introducción. Nivel A1
Título	EPC. Introducción. Nivel A1
Asunto	(c) José Manuel Redondo López
Etiquetas	José Manuel Redondo López. D...
Categorías	
Comentarios	
Origen	
Autores	Jose Redondo
Guardado por	JOSE MANUEL REDONDO LOP...
Número de revisión	531
Número de versión	
Nombre del programa	Microsoft Office PowerPoint
Organización	
Administrador	
Contenido creado	30/07/2020 13:09
Guardado el	02/07/2024 10:49
Fecha de impresión	21/01/2022 16:55
Tiempo de edición	401:27:00

[Quitar propiedades e información personal](#)

file_name	3bbae5d2-3280-4dbb-87ac-1157232f4ad8_16-9-aspect-ratio_default_0.jpg
file_size	84 kB
file_type	JPEG
file_type_extension	jpg
mime_type	image/jpeg
jif_version	1.01
exif_byte_order	Little-endian (Intel, II)
orientation	Horizontal (normal)
x_resolution	72
y_resolution	72
resolution_unit	Inches
y_cb_cr_positioning	Centered

Ahora sabes que el fichero es mío, que he usado la plantilla de otro proyecto, que la plantilla original la cree en el 2020 y que trabajo a base de copiar y adaptar un fichero base maestro editado 531 veces durante 401h

METADATOS Y REDES SOCIALES

- La mayoría de las redes sociales y periódicos eliminan los metadatos de las fotos que se suben a las mismas
 - De cara al público, de cara a uso interno ya es otro tema
 - Pueden usarlos para hacerte tracking, como vimos en la F-31 “Descubierta”
- No obstante, no debemos confiar en ello siempre
 - Puede haber **errores**
 - Tras la caída de la red social Parler, hubo una brecha de datos por su baja seguridad
 - Con ella se consiguieron descargar la totalidad de sus videos y fotos históricamente (80Tb)
 - Se encontró que, en muchas ocasiones, estas **tenían sus metadatos sin borrar**
 - Incluyendo dispositivo y coordenadas GPS desde dónde la foto se tomó
 - Si, mediante sus fotos se podía hacer un trazado de la ruta seguida por un asaltante del capitolio
 - Y no tiene que ocurrir lo mismo cuando subes ficheros a páginas “estándar”, salvo que tú lo hagas
 - Por ejemplo, fotos de perfil, de cosas que vendes, documentación a aportar, etc.
 - Por si acaso, **mejor comprueba que no hay metadatos** antes de subir nada a ninguna parte
 - ¿Viste la primera imagen de la página anterior? Abajo hay un enlace que los borra si lo clicas
 - Si una web no elimina los metadatos de la información que tiene o se sube a ella “huele mal”

METADATOS Y REDES SOCIALES

● Pero ahí no queda la cosa...

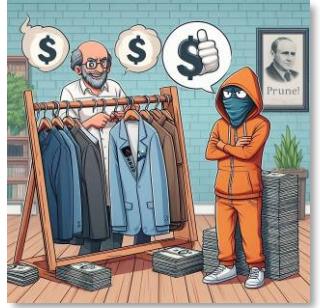
- En Parler, la verificación de cuenta **requería enviar un documento identificativo**,
 - Como, por ejemplo, copia del carnet de conducir
- La red **conservaba ese documento**, una vez verificada la cuenta
 - También todos los mensajes borrados
- Así que un asaltante del capitolio con una supuesta cuenta anónima (se supone que la verificación era interna) pudo
 - Ser perfectamente **identificado**, y con un exceso de datos personales (¡el carnet!)
 - **Tener su ruta de asalto trazada**, más cuantas más fotos haya tomado
 - Y, con esa información, **detenido y procesado**



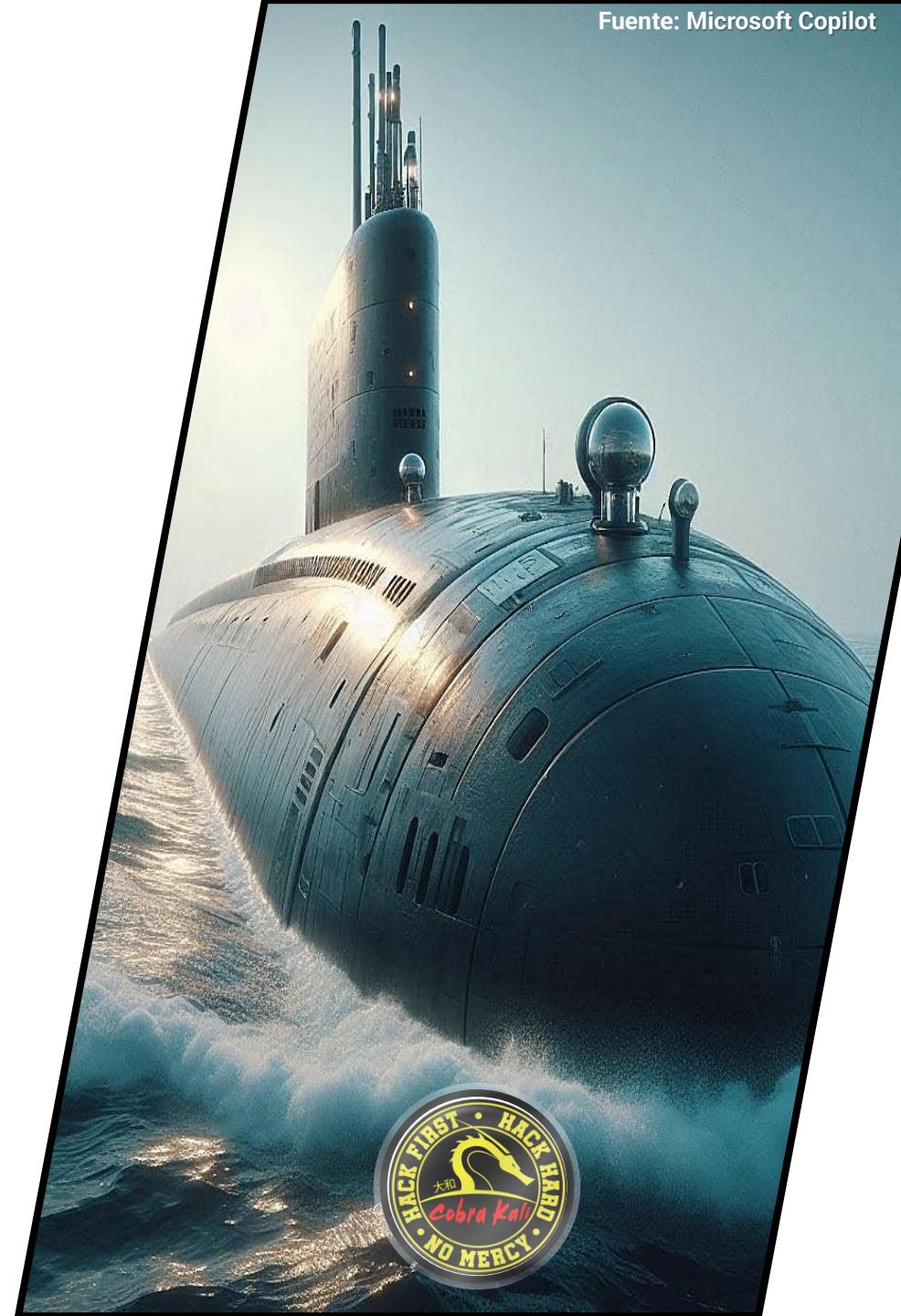
Muchas web y redes sociales te piden subir el DNI o similar para verificar tu edad. No lo hagas. Si se lo roban, puedes meterte en un problema importante...

● Moraleja

- **No te fíes** de los sitios donde subes cosas, pueden tener errores
- Si una web (que no sea un banco) te pide subir el DNI, **no lo hagas**: es muy peligroso y seguramente vulnera las leyes de protección de datos



¿Se toma en serio una web su seguridad?



¿QUÉ PUEDE HACER PARA AVERIGUAR ESTO?

- *¿Preocupado porque algunas webs pueden tratar tu información fatal?*
 - Hay una serie de pruebas no invasivas para ver si una web está bien o mal hecha en ese sentido
- *¿Confiarías en un servicio del que tienes pruebas de que algo va mal?*
 - Ahora tú puedes hacer esas pruebas



Hay una norma no escrita que dice que las webs con aspecto cutre tienen seguridad cutre. Ahora puedes ir más allá de lo que ven tus ojos

SHODAN EL DESTRUCTOR

- Shodan (<http://www.shodanhq.com/>) es un motor de búsqueda capaz de encontrar dispositivos en Internet: routers, servidores, cámaras, semáforos, impresoras...
 - Revela qué tipo de servicio/aparato es, su versión, etc.
 - Y mucha información que se puede usar para encontrar problemas relacionados con los mismos o si representan un peligro
 - Si tienen software al que se puede acceder y, por lo tanto, atacar
- Localizarlos es legal, entrar en ellos **NO** ¿Qué puedo hacer con esto entonces?
 - A partir de una IP de una web, mirar si **encuentra CVEs asociados a la misma**
 - La IP de una web la puedes averiguar aquí: <https://www.nslookup.io/website-to-ip-lookup/>
 - *¿Aparecen CVEs?* La web (y la empresa en general) “apesta”
 - No se han preocupado mínimamente de su **mantenimiento / actualización**
 - En la **F-83 “Numancia”** veremos cómo sacarle más partido a Shodan ☺
- Más información
 - <https://danielmiessler.com/study/shodan/>
 - <https://hacking-etico.com/2016/02/12/4979/>

Esto es un submarino,
y Shodan su sónar ☺





SHODAN EL DESTRUCTOR

- Shodan es poderoso: no sólo te dice el tipo de dispositivo asociado a una IP

- Dónde cree que está (**geolocalizar**)
- Te cuenta **las tecnologías que usa**
- Y también **¡las vulnerabilidades públicas** que cree que tienen esas tecnologías!
 - Detecta **productos y versiones** y busca sus vulnerabilidades conocidas
 - Lo que vimos antes, ¡pero **automáticamente!**

- Es decir, una lista de todos los CVEs de todos los productos que la web usa

- Si una web reporta cosas graves en Shodan, ¡márchate corriendo!
- ¿*No te marca la puntuación?* Prueba a buscar el código del CVE + “CVE Details” en Google

Yo no pondría mis datos en una web que tenga CVEs activos...

UFFFF 😊

Vulnerability ID	Description
CVE-2019-0215	In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.
CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2019-0217	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0196	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts

¿PROTEGE UNA WEB MI IDENTIDAD DE USUARIO?

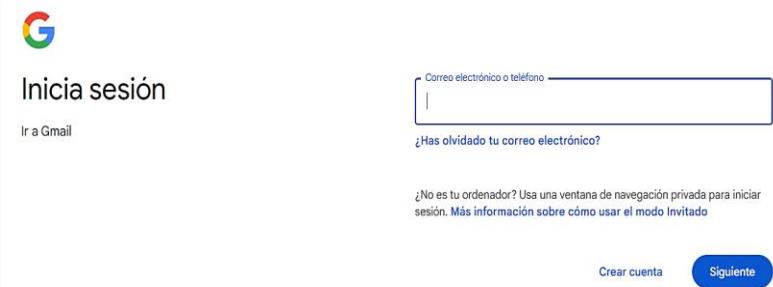
- Los ataques de fuerza bruta prueban combinaciones de nombres de usuario hasta que se da con uno adecuado
 - Luego se prueban distintas claves (de un diccionario, de una lista de claves más usadas...) sobre esa cuenta de usuario averiguada
 - Es necesario saber el nombre de usuario primero para poder intentar averiguar su clave
- ¿Qué pasaría si la web delatase nombres de usuario existentes?
 - Que el atacante tendría la mitad del trabajo hecho ☹
- Un nombre puede usarse para averiguar otros válidos si siguen una secuencia
 - Ej.: Los nombres de usuario se crean usando el correo de la empresa
 - O si se identifican por números consecutivos



¡Las páginas de “Nuestro equipo” o “Conócenos” pueden ser peligrosas!

¿CÓMO SE DETECTA SI SE PROTEGEN LOS USUARIOS?

- Lo primero es determinar qué webs pueden ser débiles a este ataque
 - Formularios de **inicio de sesión**
 - Formularios de **registro** (Nuevo usuario)
 - Formularios de **restablecer la contraseña**
- Para detectar si es posible obtener una lista de usuarios válidos se debe observar cómo responde la propia aplicación y el servidor
 - Se deben de realizar las pruebas introduciendo datos válidos e inválidos
 - Si el servidor responde igual para todas las peticiones que provocan un error y la aplicación muestra un mensaje genérico no sería posible obtener información así
- Es necesario saber si la web bloquea la cuenta temporalmente si se hacen 3-5 intentos de acceso fallidos
 - ¿No lo hace? Es vulnerable a ataques de fuerza bruta: “Huele mal”



Como se comporta el login de una web ante estas pruebas dice mucho más de lo que crees... No hace falta que hagas la prueba de intentos fallidos: busca alguien que lo haya hecho ya ☺

¿CÓMO SE DETECTA SI SE PROTEGEN LOS USUARIOS?

- Si probamos con un usuario no registrado y una contraseña cualquiera y obtenemos lo siguiente...

- Por el mensaje podemos **ver qué ha fallado** a la hora de acceder sesión
 - Es decir, distingue entre cuando metes mal el usuario y cuando metes mal la contraseña
 - Una web seria no debería...
- Así sabemos que ese usuario no existe
- **Es más común de lo que se cree**
- *¿Te registras en una red social y tu identificador no se da por bueno? Ya sabes por qué*

- También puede mostrarse una página de error concreta

- Debemos observar esa página y guardarla para compararla con otras que salgan al meter otros datos mal

Accede a tu cuenta

Los campos marcados con * son obligatorios.

Usuario incorrecto

Correo electrónico *

Contraseña *

LOGIN

Si no tienes cuenta [Regístrate aquí](#)

Gracias por decir que el usuario no existe... A veces no lo puedes evitar (como en redes sociales) pero en una web típica seguramente sí

¿CÓMO SE DETECTA?

- Si ahora probamos a introducir un usuario registrado y una contraseña no válida...
 - El mensaje nos revela que el usuario es válido, pero no la contraseña
 - *¿Y si nos devuelve un error?* Debemos compararlo con el anterior
 - *¿Y si en este caso fuese una página de error ligeramente diferente a la anterior?*
- El formulario del registro puede tener exactamente los mismos problemas

Accede a tu cuenta

Los campos marcados con * son obligatorios.

Contraseña incorrecta

Correo electrónico *

Contraseña *

LOGIN

Si no tienes cuenta [Regístrate aquí](#)

Ahora sé que el usuario existe.
¿Cuántas contraseñas deja probar sin bloquearme?

CÓMO SE GUARDA NUESTRA CLAVE EN UNA WEB

- Otra de las cosas a evitar son webs que guardan nuestras contraseñas en texto plano

- Para evitar ser víctimas directas de robos de clave

- *¿Cómo lo sabemos? Fingiendo que olvidamos nuestra clave*

- *¿La web no tiene opción de recuperar claves?* Huele mal

- Normalmente recibimos un email al correo que hemos registrado

- Con un enlace / botón para meter una nueva clave
- Es muy probable que nuestra clave se guarde mediante una técnica llamada **hash**
 - No voy a entrar en detalles, pero te basta saber que, aunque roben las claves no pueden simplemente usarlas y ya ☺
- No al 100%, pero es un **buen indicio** ☺

Hi Damien,

We received a request to reset your password for your [REDACTED] account:
[REDACTED] We're here to help!

Simply click on the button to set a new password:

[Set a New Password](#)

If you didn't ask to change your password, don't worry! Your password is still safe and you can delete this email.

Cheers,

Recibes un mensaje así en el email que registraste cuando hiciste la cuenta *¿El botón te lleva a una web que te deja poner una clave nueva?* Es correcto, la web lo hace bien 🙌⭐👍

CÓMO SE GUARDA NUESTRA CLAVE EN UNA WEB

● Pero podemos recibir un email donde se nos recuerda nuestra clave tal cual

- Si es así, es mejor **NO USAR** esa web
- Es indicio que la clave no se guarda en forma de hash
- Si se roba, **cualquiera puede leerla sin esfuerzo**
- Los administradores de la página también

● Si esa clave la usamos en otras partes, comprometemos varias cuentas

- Si ya hemos cometido este error, **es mejor cambiar las claves de las cuentas donde la reutilicemos**
- Las webs que hacen esto también suelen tener más problemas de seguridad
 - Si tienes este problema de seguridad básico, tendrás muchos más 🛡️

To log in when visiting our site just click [Login](#) or [My Account](#) at the top of every page, and then enter your email address and password.

Use the following values when prompted to log in:
Email: [REDACTED]
Password: [REDACTED]

When you log in to your account, you will be able to do the following:

- Proceed through checkout faster when making a purchase
- Check the status of orders
- View past orders
- Make changes to your account information
- Change your password
- Store alternative addresses (for shipping to multiple family members and friends!)

Hello [REDACTED]

Thank you for your order with [REDACTED]

You can login to our billing system at [REDACTED], using the email address we sent this email to, and the password T[REDACTED].
Shared Plan: Hatchling
Your Control Panel: [REDACTED]
Username: [REDACTED]
Domain: [REDACTED]
Password: T[REDACTED]
1st Nameserver: [REDACTED]
2nd Nameserver: [REDACTED]
Server IP: [REDACTED]

Recibir esta clase de emails es algo terrible 😞

[REDACTED] is a cryptocurrency exchange with the most favorable rates and the fairest terms. Your exchange has never been so smooth.

Please proceed under the following credentials.

[https://\[REDACTED\].com](https://[REDACTED].com)
Login: [REDACTED]
Password: [REDACTED]

Best Regards,
[REDACTED] team.

Follow us on [Twitter](#) and [Facebook](#)!

LA CALIDAD DEL CIFRADO

- Hay páginas que nos dejan examinar la calidad del cifrado de comunicaciones de cualquier web

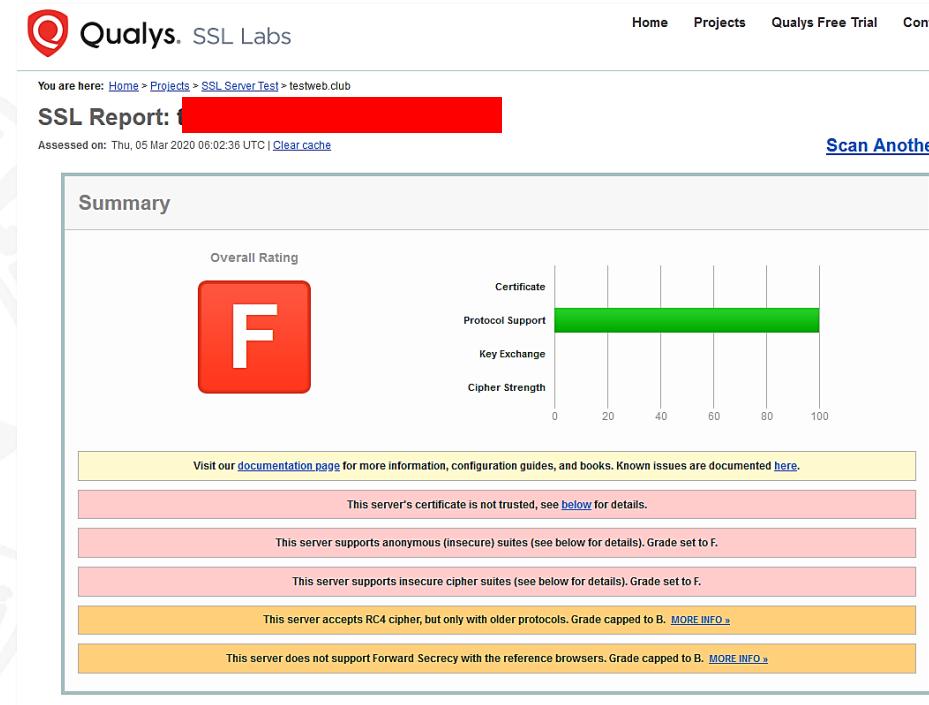
- Es otra forma de saber si puede o no tener problemas técnicos de seguridad

- Se puede saber metiendo su URL aquí

- <https://www.ssllabs.com/ssltest/>
- Da una nota de A+ (mejor) a F (terrible) o T (Not Trusted, web directamente evitable)
- Dice además los problemas que tiene y porqué esa nota
 - Pero es un tema técnico que excede lo que pretendemos

- Notas bajas suelen indicar poco cuidado técnico sobre seguridad

- ¡Indicio claro de que “huele” mal!



¿Evaluada con la peor nota posible? El mantenimiento de esta web “huele mal”. Y su seguridad suele ir de la mano... Como ves, se pueden saber cosas sin tener tampoco una idea al 100% de lo que está pasando por debajo 😊

EVALUACIÓN DE CABECERAS

● ¿Te acuerdas de las cabeceras de antes?

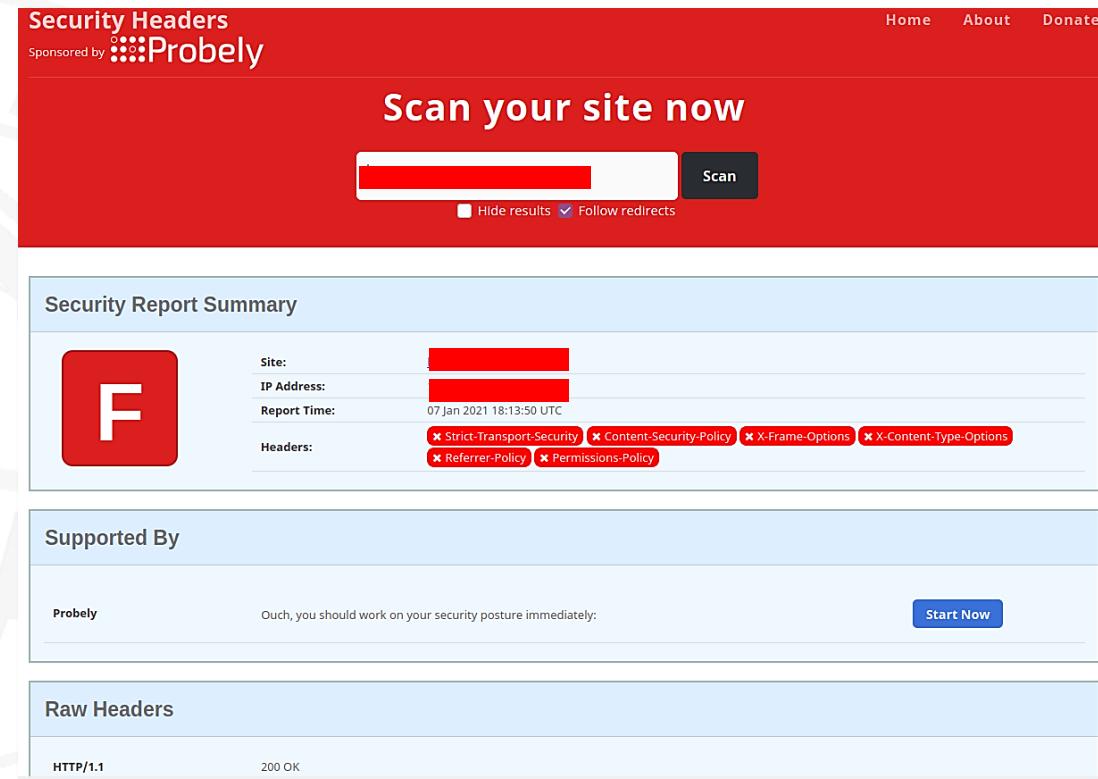
- Además de las que vimos, hay algunas que se usan para seguridad
- Algunas webs no las usan (normalmente porque ignoran que existen)
- Si no las usan, es otro indicio de que “huele mal”

● ¿Pero yo como se si las usan o no?

- Preguntando a <https://securityheaders.com/>
- Evalúa su uso por nosotros y nos da una nota de A logan F, como antes

● Aunque no sepamos qué significa, que una web saque una nota baja (F, E...) indica que tiene carencias de seguridad

- *¿Nos fiamos de ella?*



The screenshot shows a red header bar with the text "Security Headers" and "Sponsored by Probely". Below it is a large red button with the text "Scan your site now". Underneath the button are two checkboxes: "Hide results" and "Follow redirects", with the latter being checked. The main content area has a light blue background and is titled "Security Report Summary". It features a large red square with a white letter "F". To the right of the "F" are fields for "Site", "IP Address", and "Report Time" (07 Jan 2021 18:13:50 UTC). Below these fields is a list of missing headers: "Strict-Transport-Security", "Content-Security-Policy", "X-Frame-Options", "X-Content-Type-Options", "Referrer-Policy", and "Permissions-Policy". Below this section is another titled "Supported By" which includes the "Probely" logo and a message: "Ouch, you should work on your security posture immediately:". At the bottom is a section titled "Raw Headers" showing the response "HTTP/1.1 200 OK".

Otra nota terrible, otro indicio de que algo en esta web “huele mal”

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

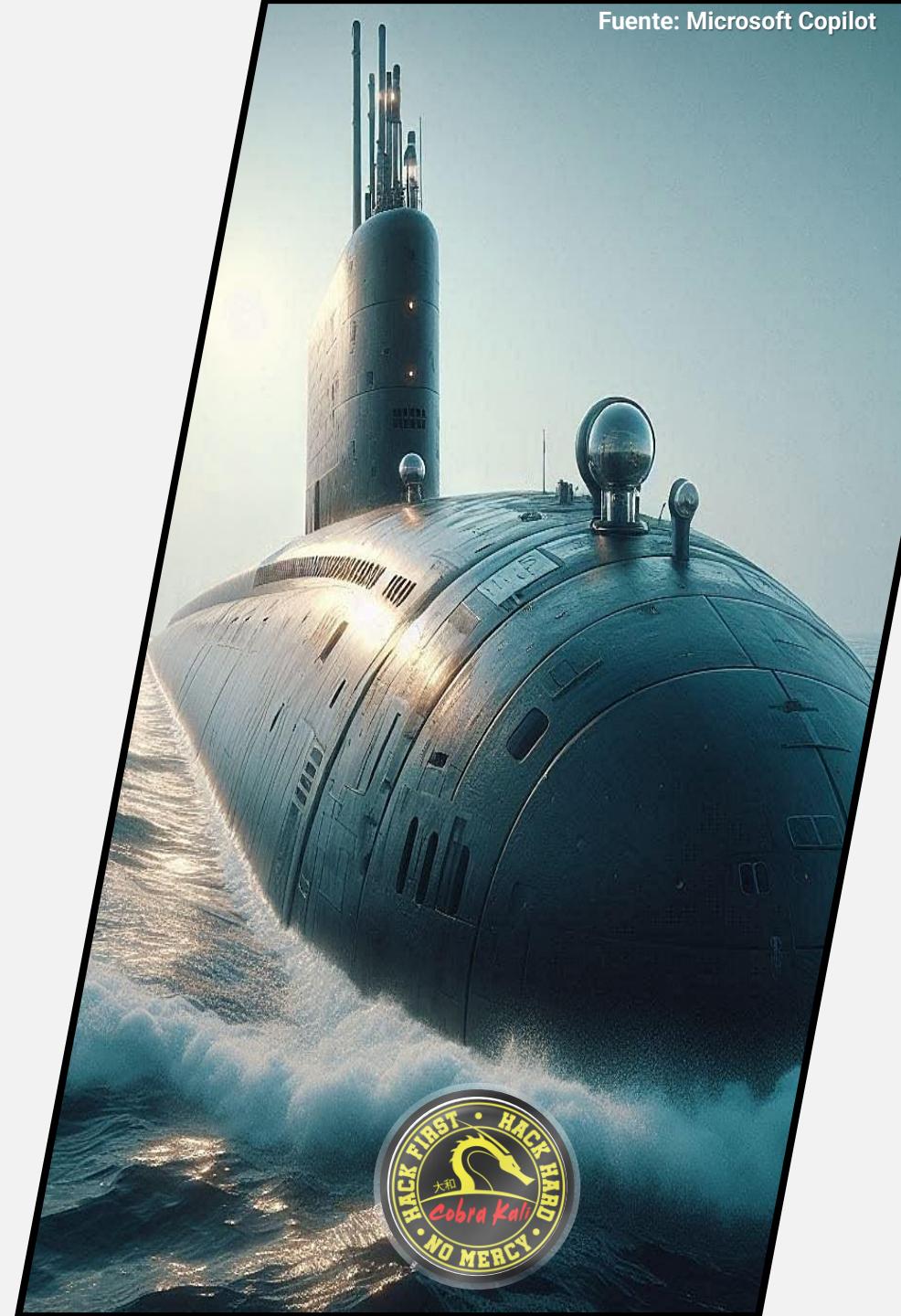


- *¿Entiendes por qué ocultar información en la web no es un sistema de seguridad, ya que te acabo de enseñar a sacarlo la típica información que se oculta?*
- *¿Has entendido que muchas de esas cosas ocultas son realmente indicativos de que la web “apesta”?*
- *¿Entiendes lo que es un metadato de un fichero y cómo se puede usar para saber más cosas de lo que hay en una web, aunque no se vean a simple vista?*
- *¿Has entendido la utilidad de Shodan para sacarle los CVEs automáticamente a una web, y con eso tomar decisiones acerca de si haces negocios con ella o no?*
- *¿Entiendes que dar información acerca de si has metido mal tu nombre de usuario tu contraseña es algo malo para la seguridad?*
- *¿Entiendes también que si pides recordar tu contraseña y te la mandan tal cual la has metido, es un muy mal indicio acerca de la seguridad general de la web?*
- *¿Has entendido que las páginas que te marcan la calidad del cifrado y el uso de elementos de seguridad con letras de la A la F son buenos indicativos de si la web está o no bien hecha, aunque no sepas qué significan estas pruebas?*



Lo que se vio

El pasado de la web

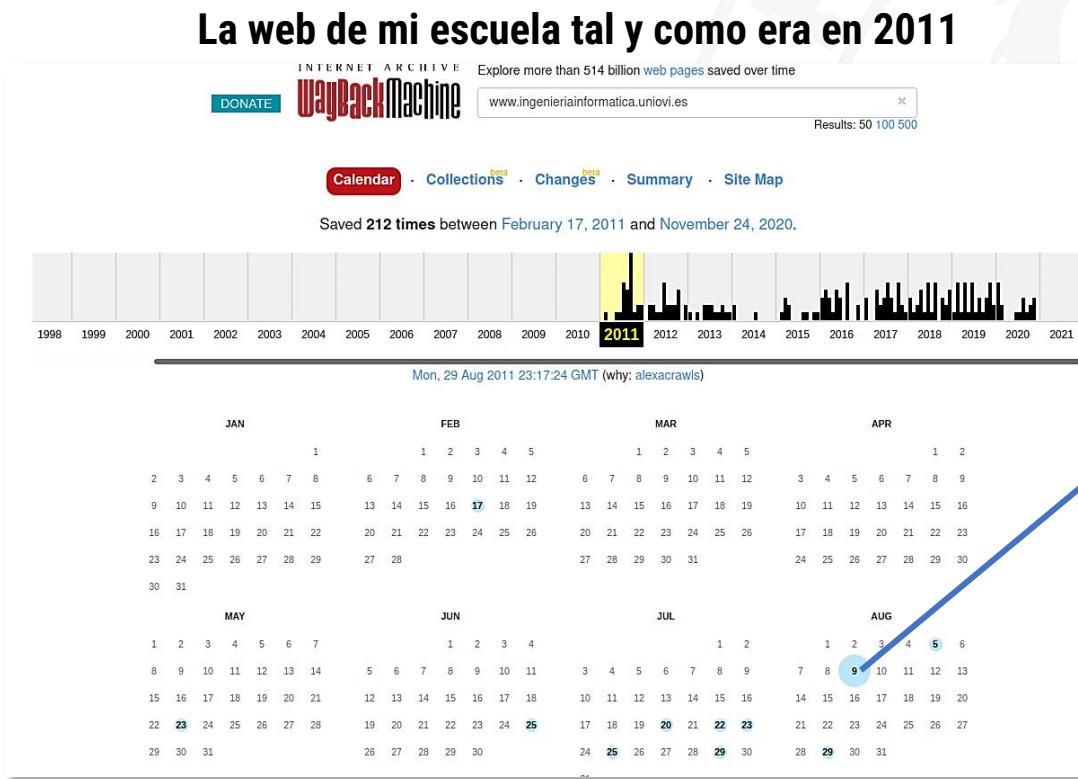


¿QUÉ ES ESTO?

- Mucha gente se centra en investigar la web que ve, pero no se para a pensar en la web que FUÉ
 - Es decir, en cómo era la web hace días/semanas/meses/años
- *¿Qué utilidad tiene esto? Una web puede tener un error de seguridad y se puede haber eliminado de la web actual, pero no de la web pasada*
- *¿Y saber cómo era una web hace tiempo?*
 - Hay una página que hace de “museo de Internet”: “The Wayback Machine” (o The Internet Archive):
 - <https://archive.org/web/>
- **Es un archivo ENORME de cómo eran webs públicas hace tiempo**
 - Mostrándotelas tal cual se navegaba por ellas (incluso las que desaparecieron)
 - Por curiosidad (“ciber-arqueología” 😊)
 - Ver si los responsables se preocuparon de eliminar errores también de sus versiones pasadas
 - Porque igual tenemos formas erróneas de acceder a datos que aún existen...
 - O simplemente **no saben que esta web existe** (mal por su parte)

COMO VER LAS WEBS DEL PASADO

- Basta con buscar una dirección y, si la tiene capturada, saldrá un calendario por años y fechas que te permite saber cómo era esa web ese día/hora
 - ¡No captura todas las fechas posibles!
 - A más popular sea una web (visitas), más “capturas” tendrá



Go JUN AUG SEP 09 2010 2011 2012

ESCUEDA DE INGENIERÍA INFORMÁTICA UNIVERSIDAD DE OVIEDO

Inicio Nuestro Centro Estudios Trabajo FAQ > Inicio Actualidad ComputingOviedo: La Convocatoria de la Comisión de Becas Colaboración de Servicios Informáticos 1 de septiembre de 2011. http://t.co/8JOipEx (Fri, 29 Jul 2011 10:55:17 +0000)

Estudios

Grado en Ingeniería Informática del Software

Grado base para la formación de Ingenieros Informáticos expertos el desarrollo de Software Profesional. Dura 4 años y no tiene restricciones de acceso.



Máster y Doctorado en Ingeniería Web

Formación avanzada para profesionales e investigadores de tecnologías web. Carrera dual con especialización en desarrollo (título de Máster) o en investigación (título de Doctor).



Centro Internacional

Nuestros estudiantes pueden cursar parte de su carrera en los siguientes centros (más información en 'Nuestro Centro').



José Manuel
Redondo López

¿QUÉ NOS PERMITE SABER ESTA TÉCNICA?

- Quién estaba vinculado a la web históricamente
 - Podemos luego buscarlo en LinkedIn u otras redes sociales
- Tecnologías que se usaron a lo largo del tiempo
 - A lo mejor ahora no se revelan, pero ¿seguirán en uso?
- Fallos de seguridad que delaten cosas que ahora no se delatan
 - Todo lo que hemos visto: comentarios, errores...
- Metadatos de imágenes o archivos que estaban, pero ya no están
 - Y con ello IPs, personas, información privada...
- Documentos que ahora revelan demasiada información (y a lo mejor en su día no)
 - Si se publica de más, se suele borrar en la web, pero no en la copia del “museo”
- Identificar bulos (“nosotros nunca”, “este sitio jamás”...)
- ¿Sabes qué otra cosa sale? Posts de gente en redes sociales en ciertas fechas (aunque se hayan borrado): Busca la URL de su perfil y me cuentas ☺



Esta página es más peligrosa
de lo que parece....

ENLACE AL PASADO...

- Para eso tenemos que hacer algo potencialmente aún más comprometedor
 - Obtener **todas las URLs archivadas de una web (documentos incluidos)**
- ¿Cómo se hace esto?
 - Haz una búsqueda como `http://web.archive.org/web/*/<URL>/*`
 - (Ej. http://web.archive.org/web/*/http://www.uniovi.es/*)
 - **Tarda bastante en cargar** si es una página bastante “movida”
 - Con esto podemos **filtrar archivos interesantes** que estuvieron ahí en algún momento y ya no están
 - `robots.txt`, `backup.zip`, PDFs, documentos Office, imágenes...todo lo que se te ocurra
 - *¿Qué pasa ahora si me da por mirar lo que tienen estos archivos “olvidados”?*
 - *¿O sus metadatos?*
 - Es decir, podemos **desenterrar errores del pasado**
 - También se encuentran frecuentemente muchas cosas que **no respetan el RGPD actual**
 - En esas fechas no había tanta preocupación por la **protección de datos...**
 - Con todo esto podemos evaluar si la web se ha preocupado de la seguridad a fondo, o no
 - Y si hay vinculación **con cuentas de redes sociales** actuales...o pasadas
 - Cuentas actuales o abandonadas que **puedes explorar** con lo que se ve en la **F-31 “Descubierta”**

ENLACE AL PASADO...



José Manuel
Redondo López

- Una vez tienes todos los enlaces, puedes filtrar por tipo (Ej.: PDF)

100,000 URLs have been captured for this domain.

¿Qué hay dentro de estos PDFs? ¿Personas? ¿Datos? ¿Metadatos? Puedes ir a redes sociales para completar la investigación. ¡Ciber-marujeo extremo!

100,000 URLs have been captured for this domain.

Filter results (i.e. '.txt')						
URL	MIME TYPE	FROM	TO	CAPTURES	DUPликATES	UNIQUEs
http://www.uniovi.es/	text/html	Jun 16, 2013	Jul 15, 2013	2	0	2
http://www.uniovi.es/	text/html	Jun 16, 2013	Jul 15, 2013	2	0	2
http://www.uniovi.es/	text/html	Jun 16, 2013	Jul 15, 2013	2	0	2
http://www.uniovi.es/	text/html	Jun 16, 2013	Jul 15, 2013	2	0	2
http://www.uniovi.es/	text/html	Jun 6, 2011	Dec 15, 2018	7	6	1
junto+Plantilla+Solic	text/plain	Sep 4, 2014	Sep 4, 2014	1	0	1
http://www.uniovi.es/	text/html	Sep 8, 2014	Sep 8, 2014	1	0	1
blisher/v9UAvM9qJp						
82/243104/INSTANCE						
028.pdf/d7cdc975-d5						
http://www.uniovi.es/	text/html	Jan 19, 2012	Apr 12, 2012	2	1	1
http://www.uniovi.es/	unk	Nov 11, 2014	Nov 11, 2014	1	0	1
stigacionaerodinami						
http://www.uniovi.es/	unk	Apr 12, 2017	Apr 12, 2017	1	0	1
uras/maquinas_de_f						
http://www.uniovi.es/	unk	Apr 12, 2017	Apr 12, 2017	1	0	1
uras/maquinas_de_f						
http://www.uniovi.es/	unk	Jul 29, 2015	Jul 29, 2015	1	0	1
uras/mecanica_de_f						
pdf						

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

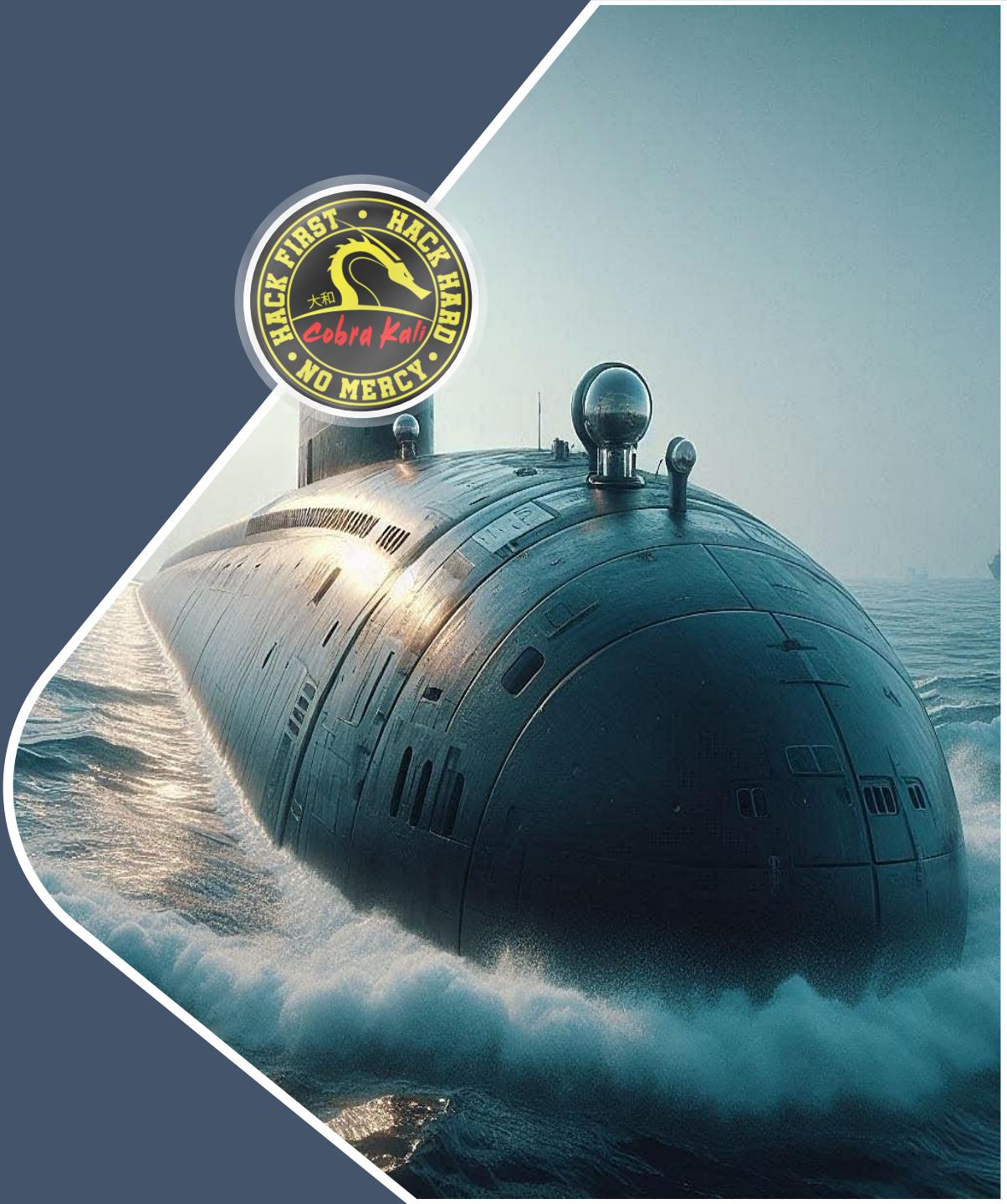
?

- *¿Te ha quedado claro el uso que puedes darle a lo que te ofrece el “museo de Internet” relativo a una web y su seguridad?*
- *¿Te das cuenta de que puedes tener un histórico de cómo ha ido evolucionando la web a lo largo de los años?*
- *¿Y que puedes sacar de él más información de lo que inicialmente parece?*
- *¿Te das cuenta de que si eres capaz de sacar todos los documentos pasados vinculados a una web tienes realmente una enorme cantidad de información a consultar?*
- *¿Entiendes como eso se puede combinar con los metadatos para sacar muchas cosas hola accionadas con una web?*



INVESTIGANDO LO QUE HAY DETRÁS DE UNA WEB

Las empresas y las personas vinculadas a ella



¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?



- En esta sección vas a aprender que detrás de una web hay empresas personas y máquinas
- También que cada uno de esos elementos puede ser una fuente de información que te enseñe a saber cosas de una web y cómo “huele”
- Y, en el caso de las personas, abrir la puerta a investigar su vida en Internet
 - Y con ello poder responder aún más preguntas acerca de la web y del contenido que hay en ella
- Nuevamente es un ejemplo del dicho “el conocimiento es poder” 😎



Las empresas detrás de una web

No solo el propietario, sino los negocios que dependen del mismo



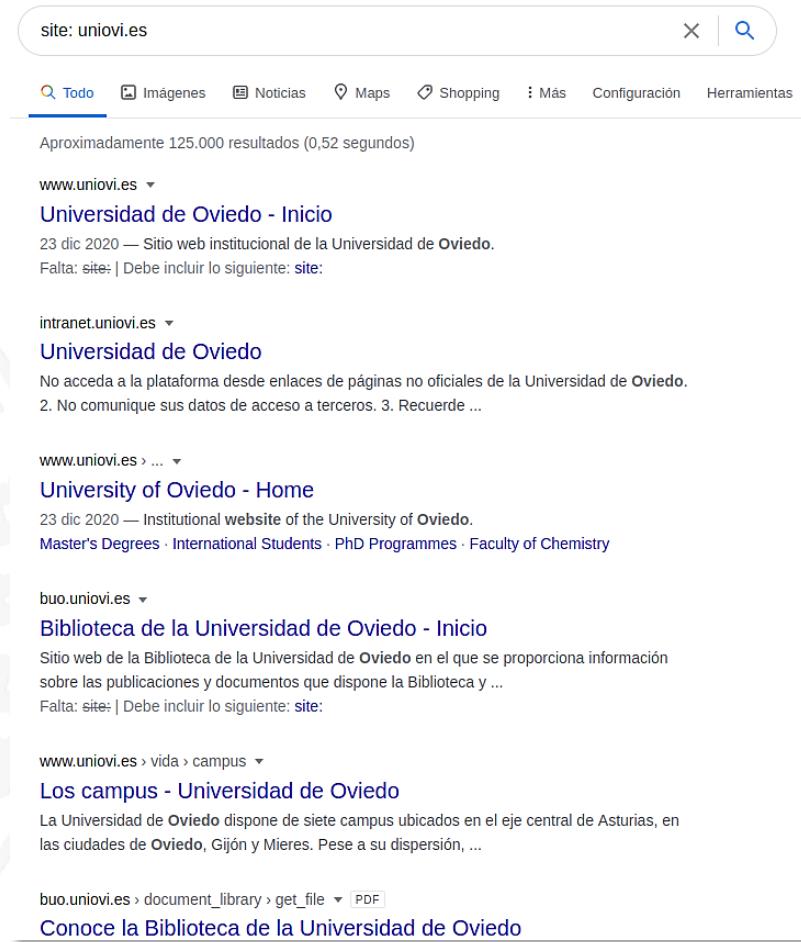
DOMINIOS Y SUBDOMINIOS

● ¿Te acuerdas que al principio de la presentación hablábamos de nombre de dominio de una web?

- Pues el dominio bajo el que se aloja una web puede tener “hijos” (**subdominios**)
 - www.uniovi.es pertenece al dominio uniovi.es
 - Pero pueden existir más subdominios xxxx.uniovi.es
- Lo que puede implicar más web a explorar

● ¿Cómo averiguamos si una web usa subdominios?

- Hay herramientas, pero la más fácil de usar es **Google**
- Buscamos **site: uniovi.es** (o cualquier dominio que queramos)
- Recorriendo los resultados aparecen subdominios si los tiene
 - buo.uniovi.es, colab.uniovi.es...
- Puedes ahora **tratar cada uno de ellos independientemente** para estudiar que hacen



site: uniovi.es

Todo Imágenes Noticias Maps Shopping Más Configuración Herramientas

Aproximadamente 125.000 resultados (0,52 segundos)

[www.uniovi.es](#) Universidad de Oviedo - Inicio 23 dic 2020 — Sitio web institucional de la Universidad de Oviedo. Falta: site: | Debe incluir lo siguiente: site:

[intranet.uniovi.es](#) Universidad de Oviedo No acceda a la plataforma desde enlaces de páginas no oficiales de la Universidad de Oviedo. 2. No comunique sus datos de acceso a terceros. 3. Recuerde ...

[www.uniovi.es](#) University of Oviedo - Home 23 dic 2020 — Institutional website of the University of Oviedo. Master's Degrees · International Students · PhD Programmes · Faculty of Chemistry

[buo.uniovi.es](#) Biblioteca de la Universidad de Oviedo - Inicio Sitio web de la Biblioteca de la Universidad de Oviedo en el que se proporciona información sobre las publicaciones y documentos que dispone la Biblioteca y ... Falta: site: | Debe incluir lo siguiente: site:

[www.uniovi.es](#) > vida > campus Los campus - Universidad de Oviedo La Universidad de Oviedo dispone de siete campus ubicados en el eje central de Asturias, en las ciudades de Oviedo, Gijón y Mieres. Pese a su dispersión, ...

buo.uniovi.es > document_library > get_file PDF Conoce la Biblioteca de la Universidad de Oviedo

A lo mejor los subdominios están hechos con lo mismo que el dominio principal y no hay nada donde rascar... o son cada uno de su padre y de su madre y entonces sí...

● Es una web que analiza las URLs que le damos

- Y nos devuelve información que indica si cree que es oficial, no oficial o falsa
- <https://desenmascara.me/>

● Analiza cosas que ya hemos visto: metadatos, cabeceras, si se sabe que ha sido comprometido

- No es infalible (ninguna herramienta lo es)
- Pero en caso de salir que la web es falsa, mejor no usarla...

● Además de Virustotal y Google Safe Browsing ya vistos, otra que podemos usar es PhishTank

- <https://phishtank.org/>
- Mejor tener una segunda (o tercera, o cuarta...) opinión de un sitio, por si "oliere mal"

¿Es este un sitio web fraudulento?

("Kudos!, this service has picked up stuff we missed." Well-known sportswear company)

<https://www.lne.es>

VeriFakes

The most comprehensive database of counterfeit-related webs

All good!



<https://www.lne.es> does looks trustworthy (Don't you agree?, Contact me)

Helping users to keep them ahead of online counterfeiters.

[Seguir a @desenmascarame](#)

Cuidado! Twittear

<http://www.goodug...> does NOT looks trustworthy -TAKE CARE!! (Don't you agree?, Contact me)

Eres una Marca preocupada por las falsificaciones online?



(Detalles ocultos para prevenir bots recopilar dicha información, contacta conmigo si necesitas estos datos)

Follow @desenmascarame

DESENMASCARAME otra vez (contacta conmigo si necesitas esto)

Principal

INFORME DEL SITIO

(valoración basada en los siguientes datos desenmascarados):

Sitio Web

<http://www.goodug...>

FALSO, WEB FRAUDULENTA

Suele detectar webs que venden falsificaciones

THE BLACK LIGHT



- En la F-31 “Descubierta” vimos que muchas páginas usan nuestros datos personales para hacer negocio
 - Recopilan nuestros datos de navegación y los venden a 3ºs (tracking)
- Muchas veces “pasamos” del tema, pero *¿nunca os ha picado la curiosidad si lo hacen mucho o poco?*
 - Blacklight (<https://themarkup.org/blacklight>) es una web que escanea otras webs y revela las **tecnologías de tracking** de usuarios que usa
 - Es decir, quien obtiene tus datos cuando navegas por ella
- Webs que abusan de estas técnicas “huelen” peor
 - Puedes verlo también en el **aviso de consentimiento de cookies**
 - “Colaboramos con nuestros 752 partners para...” (real): Pasan tus datos a ese nº de empresas

The screenshot shows the Blacklight inspection result for the website elmundo.es. At the top, there is a redacted URL bar and a "Scan Site" button. Below that, it says "Visited elmundo.es on Oct. 19, 2020, 03:43 ET" and "Learn more ▾". The main section is titled "Blacklight Inspection Result" and contains the following information:

- 10 Ad trackers found on this site.** This is **more than** the average of **seven** that we found on popular sites.
- 13 Third-party cookies were found.** This is **more than** the average of **three** that we found on popular sites.
- Fingerprinting**: Tracking that evades cookie blockers wasn't found.
- Session recording**: Session recording services not found on this website.
- Keylogger**: We did not find this website capturing keystrokes.
- Facebook tracking**: When you visit this site, it tells Facebook — even if you block cookies.
- Google Analytics**: Google Analytics' "remarketing audiences" feature not found.

Análisis de conocido periódico español. 10 trackers sacando tus datos para venderlos a muchos sitios distintos

¿Y SI LA WEB OFRECE UNA APP?

- Hoy día muchas webs intentan que te instales su “app móvil” asociada
 - Algunas con MUCHA insistencia
- En gran parte es porque así pueden hacerte más tracking aún que en su web
- *¿Quieres saber cuánto y si, por tanto, te la instalas?*
 - O lo usas para ver si te fías de esa web...
- Prueba Exodus Privacy (<https://reports.exodus-privacy.eu.org/es/>)
 - Pon un nombre de app y analízala
 - *¿Muchos rastreadores?*
 - *¿Pide a tu juicio demasiados permisos para lo que hace?*
 - Ya sabes...huele ☺

11 rastreadores

39 permisos

Versión 3.12.0 - [ver otras versiones](#)

Fuente: Google Play

Informe creado el 18 de Abril de 2024 a las 12:16

[Ver en Google Play >](#)

11 rastreadores

Hemos encontrado firma de código de los siguientes rastreadores en la aplicación:

[Adobe Experience Cloud >](#)

[AltBeacon >](#)

[Appdynamics >](#)

[analytics](#) [profiling](#)

[Facebook Login >](#)

[identification](#)

[Facebook Share >](#)

[fullstory >](#)

[analytics](#)

[Google CrashLytics >](#)

[crash reporting](#)

[Google Firebase Analytics >](#)

[analytics](#)

Análisis de app de conocido comercio español. Aunque la app no tiene por qué usar los 39 permisos de mano (puede ir pidiéndotelos según los necesite) ¿Por qué necesita tantos? Y además ¿11 rastreadores?

¿Y CÓMO SE LO QUE OPINAN LOS DEMÁS DE LA WEB?

- Muchas webs tienen sitios donde la gente opina de ellas, sus servicios y otros comportamientos
 - Algunos usuarios son expertos y te pueden mencionar detalles técnicos como los que mencionamos
- Pero necesitamos un sitio fiable
 - Hay mercado comprando opiniones positivas de uno mismo...
- Uno de ellos es TrustPilot (<https://es.trustpilot.com/>)
 - Busca la web ahí (aparecerá si es una empresa o comercio) y mira lo que opinan
 - TrustPilot vive de que las opiniones que muestra sean fiables
- Depende del tipo de web también
 - Si una página de noticias aparece muy a menudo en Maldito Bulo (<https://maldita.es/malditobulo/>) pues...



Valoraciones de conocido centro de formación privado Español. Las opiniones van justo debajo, lee, analiza y toma una decisión.
Las empresas suelen tener gente registrada en TrustPilot contestando las opiniones negativas. Valora también sus argumentos (¡hay review-bombing!)



Las personas detrás de una web

La gente tras la empresa o negocio que representa



SOBRE LO QUE VAMOS A VER A CONTINUACIÓN...

- Averiguar información pública de una web o su gente en sí no es delito
 - Es saber mirar mejor lo que recibes en el navegador
 - Puede usarse para saber **si se puede confiar o no en ella o la empresa propietaria**
- Pero **lo que hagas** con esa información, **sí puede serlo** (y penal, es decir, cárcel)
 - Como divulgar la información comprometedora que has encontrado
- **¿Para qué te enseño esto? Para que “veas” mejor**
 - Ves a alguien haciendo muy buenas revisiones de un negocio y te extraña
 - *¿Es el propietario o un familiar suyo?*
 - Ves a una empresa siempre recomendando los productos de otra
 - *¿Pertenecen a la misma persona? ¿O a un familiar?*
 - Ves a personas recomendando ciertos servicios o ideas
 - *¿Pertenece lo que recomienda a su familia? (o a la persona)*
 - Esas ideas *¿Son porque esa persona pertenece a cierta organización / partido?*
- En otras palabras, quiero ayudarte a que encuentres explicaciones a lo que leas

¿QUIÉN ES EL PROPIETARIO DE UNA WEB?

- Todas las webs tienen que estar registradas a nombre de un propietario / responsable

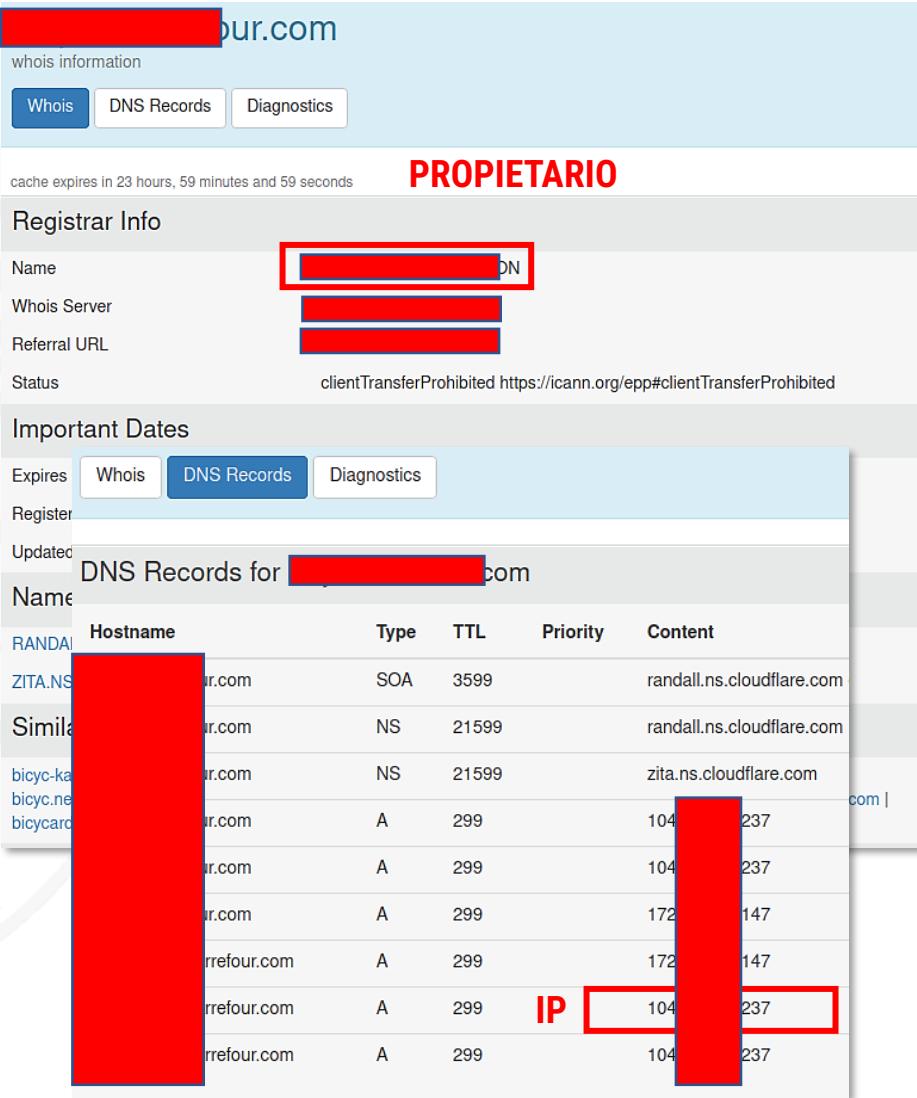
- El servicio que recoge esta información se llama **WHOIS**
- Hay servicios de consulta (Ej.: <https://who.is/>)

- Muchas veces aparece el nombre de una empresa de hosting, no el de una persona o empresa real

- Pero otras veces si, y con ello podemos ir a redes sociales para saber más de él/ella...y sus contactos ☺

- También podemos detectar fraudes así

- La imagen muestra una tienda cuya dirección contiene el nombre de un comercio famoso
- Pero está registrada por MAT BAO CORPORATION, una empresa Vietnamita ¿Nos fiamos?
- Ante la mínima duda: **NO COMPRAR**



The screenshot shows a WHOIS search result for a domain. At the top, it says "Whois information" with tabs for Whois, DNS Records, and Diagnostics. The Whois tab is selected. It displays the following details:

PROPIETARIO

Name	Value
Name	[REDACTED]
Whois Server	[REDACTED]
Referral URL	[REDACTED]
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates

Expires	Whois	DNS Records	Diagnostics
Updated			

DNS Records for [REDACTED].com

Name	Hostname	Type	TTL	Priority	Content
ZITA.NS	[REDACTED].com	SOA	3599		randall.ns.cloudflare.com
Similar	[REDACTED].com	NS	21599		randall.ns.cloudflare.com
bicy-ka	[REDACTED].com	NS	21599		zita.ns.cloudflare.com
bicy-ne	[REDACTED].com	A	299		104.24.237
bicycard	[REDACTED].com	A	299		104.24.237
	[REDACTED].com	A	299		172.24.147
	[REDACTED].com	A	299		172.24.147
	[REDACTED].com	A	299		IP [REDACTED]
	[REDACTED].com	A	299		104.24.237
	[REDACTED].com	A	299		104.24.237

- La página anterior solo vale para webs .com, .edu y algunas más

- Para consultar esta información de webs de países concretos, es mejor recurrir al servicio WHOIS de cada país

- En el caso de España, podemos acceder a <https://www.dominios.es/>

- Es lo mismo: obtener datos de personas y las IPs usadas en máquinas que sirven la web
- ¿Quieres la IP de una web concreta solamente? Mete la URL en Virustotal



The screenshot shows two pages from the Dominios.es website:

- Dominios disponibles:** A table showing domain availability for various suffixes. All shown domains are registered (indicated by a red 'X').

DOMINIO	DISPONIBLE	REGISTRAR CON ...
uniovi.es	✗	Registrado. Ver datos
uniovi.com.es	✗	Registrado. Ver datos
uniovi.nom.es	✗	Registrado. Ver datos
uniovi.org.es	✗	Registrado. Ver datos
uniovi.gob.es	✗	Registrado. Ver datos
uniovi.edu.es	✗	
- Información de Dominio:** Detailed WHOIS information for uniovi.edu.es.
 - DATOS DEL TITULAR:** Nombre del Dominio: uniovi.es, Estado: Activado, Identificador: E26F-MIG1, Titular: Universidad de Oviedo, Fecha de Alta: 10-06-1991, Fecha de Caducidad: 10-06-2021, Agente Registrador: NOMINALIA.
 - PERSONA DE CONTACTO ADMINISTRATIVO:** Identificador: 960F5F-ESNIC-F5, Nombre: Javier.
 - PERSONA DE CONTACTO TECNICO:** Identificador: 2C3EEB-ESNIC-F5, Nombre: [redacted].
 - SERVIDORES DNS:** chico.rediris.es, enol.si.uniovi.es, sun.rediris.es, zeus.etsimo.uniovi.es, coruxa.epsig.uniovi.es, vci.uniovi.es.
 - IPS ASOCIADAS:** IP: 64.2.160.1, 64.2.162.1, 64.2.160.8, 64.2.162.4, 64.2.160.70.

Notes: The contact information for the domain owner is hidden. The page states: "Los datos de contacto de este dominio están ocultos. Si desea comunicarse con el Titular y el PCA pulse [aqui](#)".

¿HAN ROBADO ALGUNA CUENTA DE LA WEB?

- **Tus cuentas de email podrían haber sido ya comprometidas sin saberlo**
 - Habitualmente por robos de datos en sitios web que las tienen guardadas como no deben
- **Have I been pwned? (<https://haveibeenpwned.com/>) es un sitio que, si le das un email**
 - Te dice qué **contraseñas asociadas a él** han sido robadas
 - **Cuándo y dónde** (las webs vulneradas, vamos)
 - Puedes además ver la **lista de sitios que han sido vulnerados** en “Who’s been pwnd”
 - <https://haveibeenpwned.com/PwnedWebsites>
 - Si te aparece una web que quieras examinar en sus bases de datos, es que **ha sufrido una filtración**
 - Hoy en día es demasiado común, pero así al menos ya sabes un dato más que te ayuda a decidir

Pwned websites

Breached websites that have been loaded into Have I Been Pwned

Here's an overview of the various breaches that have been consolidated into this Have I Been Pwned. These are accessible programmatically via the HIBP API and also via the RSS feed.

000webhost
In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed almost 15 million customer records. The data was sold and traded before 000webhost was alerted in October. The breach included names, email addresses and plain text passwords.
Breach date: 1 March 2015
Date added to HIBP: 26 October 2015
Compromised accounts: 14,936,670
Compromised data: Email addresses, IP addresses, Names, Passwords
[Permalink](#)

123RF
In March 2020, the stock photo site 123RF suffered a data breach which impacted over 8 million subscribers and was subsequently sold online. The breach included email, IP and physical addresses, names, phone numbers and passwords stored as MD5 hashes. The data was provided to HIBP by dehashed.com.
Breach date: 22 March 2020
Date added to HIBP: 15 November 2020
Compromised accounts: 8,661,578
Compromised data: Email addresses, IP addresses, Names, Passwords, Phone numbers, Physical addresses, Usernames
[Permalink](#)

126
In approximately 2012, it's alleged that the Chinese email service known as 126 suffered a data breach that impacted 6.4 million subscribers. Whilst there is evidence that the data is legitimate, due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified". The data in the breach contains email addresses and plain text passwords. Read more about Chinese data breaches in Have I Been Pwned.
Breach date: 1 January 2012
Date added to HIBP: 8 October 2016
Compromised accounts: 6,414,191
Compromised data: Email addresses, Passwords
[Permalink](#)

17
In April 2016, customer data obtained from the streaming app known as "17" appeared listed for sale on a Tor hidden service marketplace. The data contained over 4 million unique email addresses along

YOU HAVE BEEN PWNED...

● Imagina que ahora poner el email de alguien que sabes que está registrado en la web que investigas

- ¿Te acuerdas de que antes *hablamos de cómo sacar los emails asociados a una web?* Pues ahora ya sabes por qué ☺

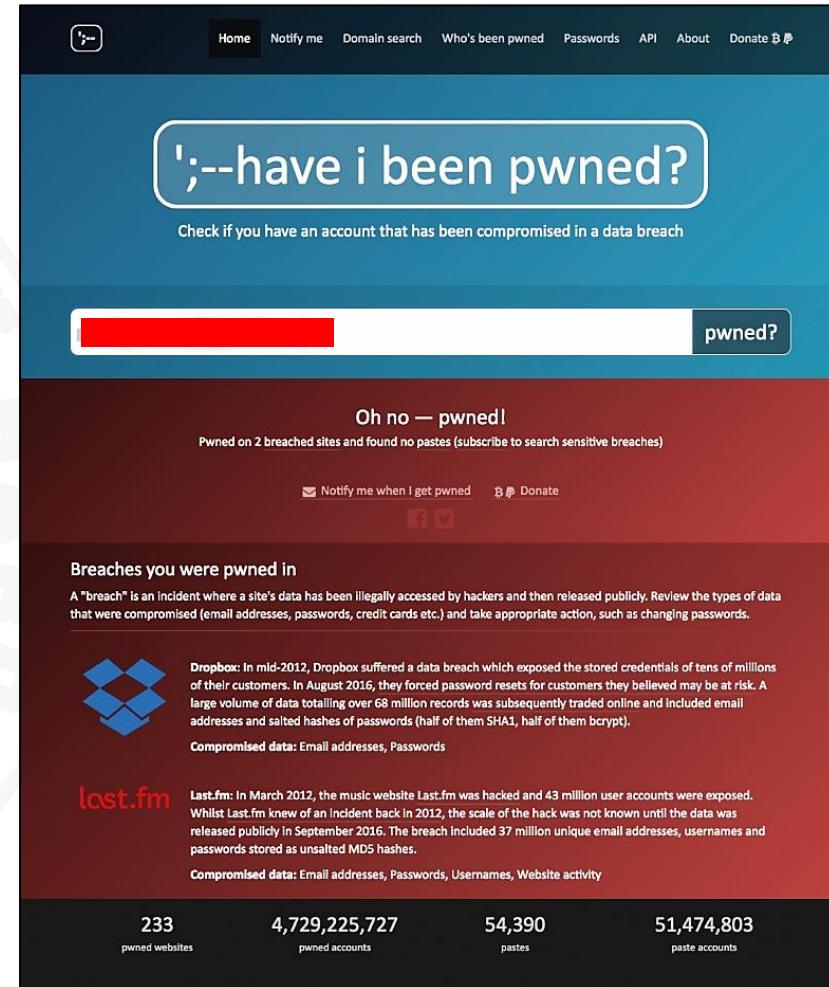
● ¿Aparece como origen de filtraciones?

- Es posible que las claves estén circulando por sitios indebidos
- Este sitio te explica qué se ha robado y como
- Y, por tanto, si entrar en la cuenta es cuestión poco tiempo

● ¿Y el email cuya clave ha sido filtrada es la de una web en la que voy a comprar, o de sus responsables? ☹

- Direcciones de contacto, soporte de una web...

● Si el afectado eres tú, no entres en pánico y cambia ya la clave



The screenshot shows the HIBP homepage with a search bar containing a redacted email address. Below the search bar, a message says "Oh no — pwned!" and "Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)". There are links to "Notify me when I get pwned" and "Donate". The main content area displays two breach entries:

- Dropbox**: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt). Compromised data: Email addresses, Passwords.
- Last.fm**: In March 2012, the music website Last.fm was hacked and 43 million user accounts were exposed. Whilst Last.fm knew of an incident back in 2012, the scale of the hack was not known until the data was released publicly in September 2016. The breach included 37 million unique email addresses, usernames and passwords stored as unsalted MD5 hashes. Compromised data: Email addresses, Passwords, Usernames, Website activity.

At the bottom of the page, there are summary statistics: 233 pwned websites, 4,729,225,727 pwned accounts, 54,390 pastes, and 51,474,803 paste accounts.

Lo cierto es que esta página es más versátil de lo que inicialmente parece...

¿DÓNDE ESTÁ LA WEB?

- Con el servicio WHOIS puedes sacar la IP de una web, no solo el propietario

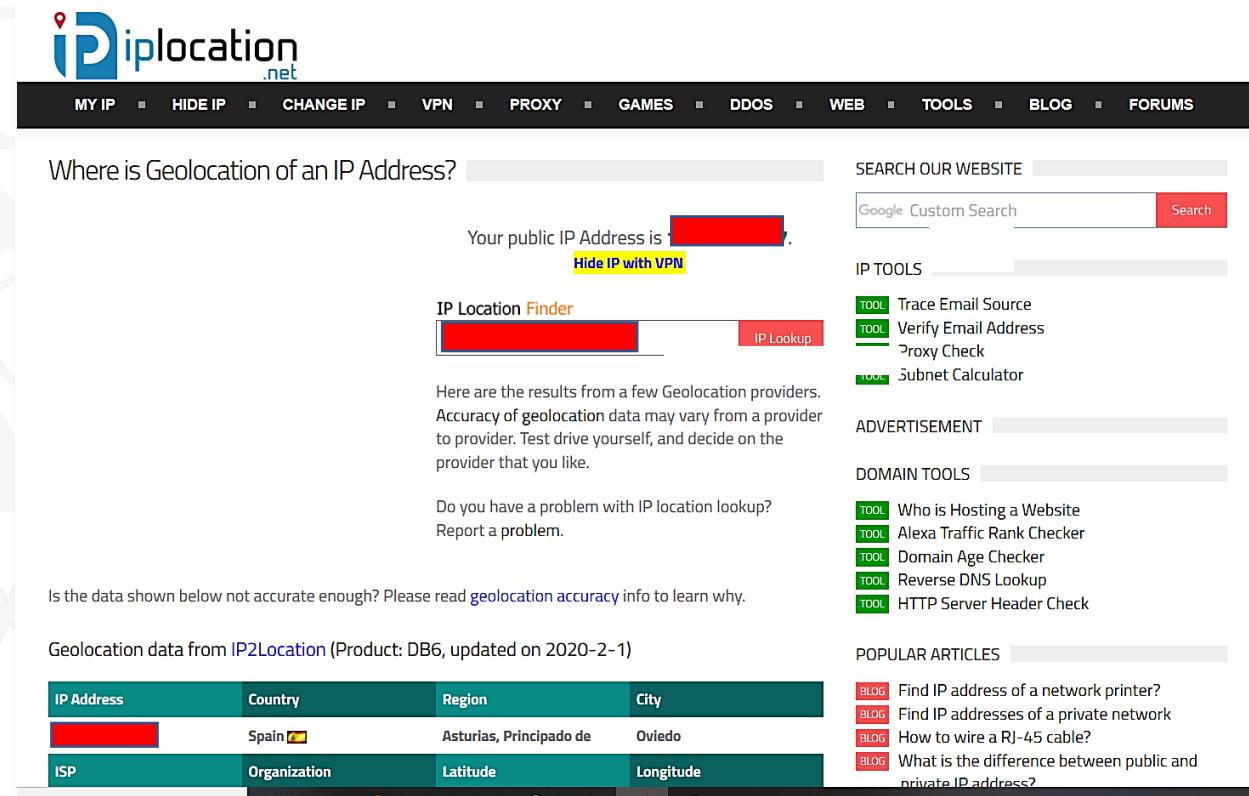
- Bueno, y de otras formas que hemos visto ☺

- Si tienes la IP de algo, puedes tratar de geolocalizarla en el mundo

- Con servicios como <https://www.iplocation.net/>

- Estos servicios localizan de forma más o menos precisa

- En función de si es una IP pública o pertenece a un proveedor de Internet
- Mucha gente contrata su servidor en nube y entonces **puede aparecer en sitios atípicos**
 - No es la panacea, pero si una ➤



The screenshot shows the iplocation.net homepage. At the top, there's a navigation bar with links like MY IP, HIDE IP, CHANGE IP, VPN, PROXY, GAMES, DDOS, WEB, TOOLS, BLOG, and FORUMS. Below the navigation is a search bar for "Where is Geolocation of an IP Address?" followed by a redacted IP address. A button labeled "Hide IP with VPN" is visible. The main content area has a heading "IP Location Finder" with a redacted IP address input field and a "IP Lookup" button. It displays results from several providers, noting that accuracy varies. A "Report a problem" link is present. At the bottom, it shows geolocation data from IP2Location: IP Address (redacted), Country (Spain), Region (Asturias, Principado de), City (Oviedo), ISP (redacted), Organization (redacted), Latitude, and Longitude.

Una web de empanadillas artesanas de Extremadura que esté alojada en Sebastopol ya te digo yo que no va a vender empanadillas ☺. El único arte que tendrá es el de copiar el aspecto de la real para timarte... PRO TIP: Las webs públicas de un ministerio, hacienda, etc. SIEMPRE deben estar alojadas en España. Si te sale que no, **es un fraude**

¿QUIÉN ES EL PROPIETARIO DE UNA WEB?

- Los datos devueltos nos permiten averiguar cosas (ver imagen)

- Página alojada en Oviedo, Asturias, España
- Universidad de Oviedo (entidad pública)
- Y una latitud y longitud...

- Google Earth y ... ¡hola! ☺

- No obstante, la precisión de localización habitualmente es solo a **nivel de código postal**
- Sería una máquina en algún sitio dentro del código postal indicado
- Muy impreciso, pero puede revelar fraudes con webs impostoras

- También sirve Google Maps vía web

- <https://www.google.es/maps/>

Geolocation data from IP2Location (Product: DB6, updated on 2021-1-1)

IP Address	Country	Region	City
[REDACTED]	Spain 	Asturias, Principado de	Oviedo
ISP	Organization	Latitude	Longitude
Universidad de Oviedo	Not Available	43.3603	-5.8448

Geolocation data from ipinfo.io (Product: API, real-time)

IP Address	Country	Region	City
[REDACTED]	Spain 	Asturias	Oviedo
ISP	Organization	Latitude	Longitude
Entidad Publica Empresarial Red.es	Universidad de Oviedo (uniovi.es)	43.3603	-5.8448

Geolocation data from DB-IP (Product: Full, 2021-1-1)

IP Address	Country	Region	City
[REDACTED]	Spain 	Asturias	Oviedo
ISP	Organization	Latitude	Longitude
Entidad Publica Empresarial Red.es	Uniovi	43.363	-5.84396

Geolocation data from IPGeolocation.io (Product: API, real-time)

IP Address	Country	Region	City
[REDACTED]	Spain 	Principality of Asturias	
ISP	Organization	Latitude	Longitude
Entidad Publica Empresarial Red.es	Entidad Publica Empresarial Red.es	43.36269	-5.84768

En esta web se canta el “Asturias patria querida” fijo ☺

▼ Buscar

43.3693°,-5.8448°

Buscar

por ejemplo: Restaurantes

Obtener indicaciones Historial

A 43°22'09.5"N 5°50'41.3"W
33011 Oviedo, Asturias
★★★☆☆

Mis sitios

- Mis sitios
- Tour de lugares destacados
Asegúrate de que la capa de edificios 3D está activada.

- Sitios temporales

Capas

- Base de datos principal
- Anuncios
- Fronteras y etiquetas
- Lugares
- Fotografías
- Carreteras
- Edificios 3D
- Océanos
- Tiempo
- Galería
- Concienciación global
- Más



43°22'09.5"N 5°50'41.3"W

© 2020 Google

Google Earth

¿QUIÉN ES EL PROPIETARIO DE UNA WEB?

● Recuerda que esto tiene limitaciones

- Como decíamos, si la web está alojada en un proveedor de nube la cosa cambia
- Nos dirá dónde está el servidor que el propietario ha comprado para alojar su web
- Y eso puede ser cualquier parte del mundo...

● Por tanto, no sabremos dónde está realmente el propietario

- Aunque si es un proveedor “raro” (no el típico Amazon, Microsoft, Google...), es motivo de sospecha

● En la imagen vemos una web alojada en la nube de Microsoft

- ¡Aparece en Washington! (nada relacionable con el propietario, que era uno de mis alumnos)

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2020-2-1)

IP Address	Country	Region	City
	United States of America 	Washington	Redmond
ISP	Organization	Latitude	Longitude
	Microsoft Corporation	47.6829	-122.1209

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

IP Address	Country	Region	City
	United States 	Washington	Redmond
ISP	Organization	Latitude	Longitude
	Not Available	47.6740	-122.1215

Geolocation data from [DB-IP](#) (Product: Full, 2020-2-1)

IP Address	Country	Region	City
	United States 	New Jersey	Newark
ISP	Organization	Latitude	Longitude
	Microsoft Corporation	40.7357	-74.1724

Sí, es probar suerte. Pero al menos ahora puedes comprar ese billete de lotería a ver si te toca, ¿no? ☺

¡PERSONAS! ¿QUÉ SE HACE CON LAS PERSONAS?

● ¿Sacamos el nombre de una persona asociada a la web con alguna técnica de las vistas?

- Vamos a redes sociales para **intentar averiguar muchas cosas de esa persona**
 - De qué trabaja exactamente y su cargo
 - Sitios donde vive/trabaja/acostumbra a ir
 - Amigos y relaciones
 - Aficiones, manías, gustos personales, grupos, afiliaciones políticas/religiosas, rutinas...
 - Horarios de trabajo, vacaciones, qué coche tiene, ...
 - ...

● ¿Sabéis que se consigue con estas cosas?

- ¡Responder a las preguntas que nos hicimos antes!
 - Y a muchas más ☺
- **Estafas: Phising y Spear phising**
 - No viene mal por tanto mirar si nosotros mismos estamos dando demasiada información...



The screenshot shows a LinkedIn profile page. At the top, there's a search bar with 'Buscar' and a blue 'in' logo. Below it, a banner reads 'A 10,000% ROI pre-IPO? - TransparentBusiness is a \$1Billion Unicorn pre-IPO Opportunity'. The main profile area has a large red circular placeholder for the photo. To the right of the photo are three buttons: 'Conectar' (Connect), 'Enviar mensaje' (Send message), and 'Más...' (More...). Below the photo, the user's name is redacted. Underneath, it says 'Jefe de Área Técnica de Informática y Comunicaciones en Universidad de Oviedo, Oviedo, Principado de Asturias, España · 140 contactos · Información de contacto'. There are also two 'Universidad de Oviedo' links.

Si hacemos un poco de "marujeo" (al final de la F-31 "Descubierta" tienes materiales para hacerlo) podemos sacar MUCHA información de la gente asociada a una web...y su entorno personal y laboral P.D.: LinkedIn es especialmente bueno para estas cosas ;)



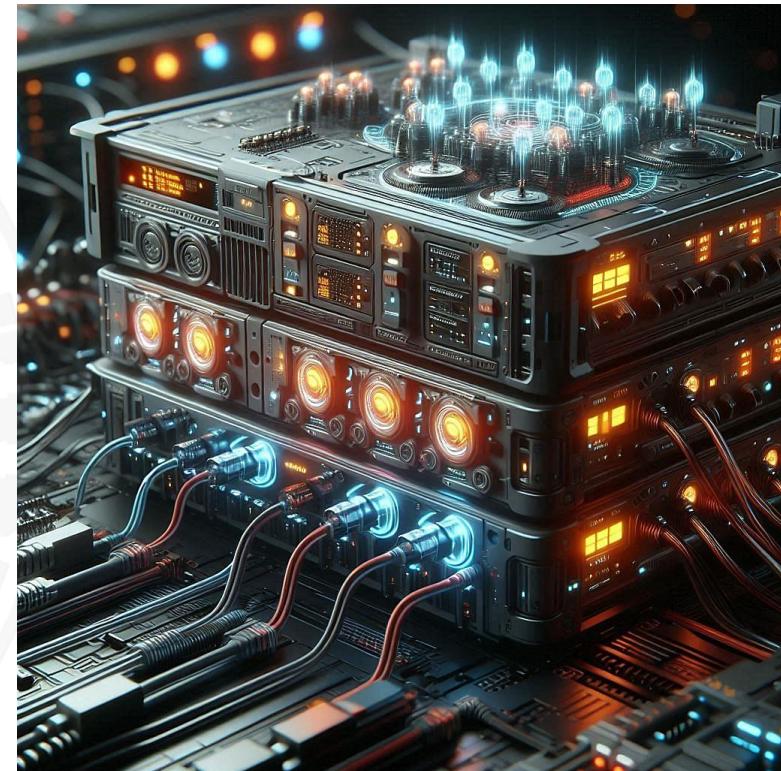
Las máquinas

Las páginas web se alojan en máquinas, y estas ofrecen otra clase de información



¿QUÉ INFORMACIÓN PUEDO SACAR DE UNA MÁQUINA?

- Una vez sabes la IP de una máquina, puedes averiguar qué puertos tiene abiertos
 - Son “puertas” detrás de las cuales la máquina ofrece algo (**un servicio**) a los demás
 - Cada una de esas “puertas” **tiene un nº asociado** (nº de puerto)
- Todo esto requiere conocimientos de redes para sacarle al máximo partido
 - Eso los veremos en la **F-83 “Numancia”**



PUERTOS DE RED

● Un puerto completa el acceso a un servicio ofrecido por una máquina

- ¡La misma máquina puede ofrecer muchos servicios! (**uno por puerto**)
- La IP es la dirección de la máquina a la que nos conectamos
- El puerto decide **qué servicio** (de todos los que ofrece la máquina) de esa dirección IP se va a usar
 - "Se llegar al aeropuerto, pero al final, tendré que elegir un vuelo concreto" 😊
 - Por ejemplo, si el sitio web de nuestra escuela está en la IP **156.35.94.1**
 - Para navegar por el necesitamos un cliente adecuado que se conecte al puerto **80** o al **443** (servicios HTTP(S))
 - Y para conectarse de forma segura como usuario, usar el puerto **22** (**servicio SSH**)

● Hay 65.536 puertos diferentes posibles en una máquina

- Los primeros 1.024 se conocen como "**puertos comunes**", **reservados para servicios típicos**
 - El resto se puede utilizar para crear programas que "escuchen" conexiones y den diversos servicios
- Los números de puerto más utilizados aparecen en la siguiente diapositiva
- "**Abrir un puerto**" significa ofrecer un servicio a máquinas de fuera desde la tuya
 - Por ejemplo: servidor web, servidor Minecraft ...
- **¡No se pueden abrir puertos bajo CG-NAT! (¡cuidado!)**



José Manuel
Redondo López

packetlife.net

ACERCA DE LOS PUERTOS...

● Los puertos del 1 al 1024 son reservados

- Para servicios conocidos
- Por ejemplo, cada vez que nos conectamos a `https://<lo que sea>` estamos accediendo al **puerto 443** de la máquina que tiene esa web
- Es el reservado para **webs con conexión cifrada**

● Los puertos > 1024 "normalmente" tienen los servicios de la imagen

- Pero a diferencia de los reservados, no es obligatorio
- Usa esta lista como una aproximación

● Los puertos se pueden inspeccionar con herramientas

- Pero en nuestro caso nos lo dice Shodan

COMMON PORTS

TCP/UDP Port Numbers			
7 Echo	554 RTSP	2745 Bagle.H	6891-6901 Windows Live
19 Chargen	546-547 DHCPv6	2967 Symantec AV	6970 Quicktime
20-21 FTP	560 rmonitor	3050 Interbase DB	7212 GhostSurf
22 SSH/SCP	563 NNTP over SSL	3074 XBOX Live	7648-7649 CU-SeeMe
23 Telnet	587 SMTP	3124 HTTP Proxy	8000 Internet Radio
25 SMTP	591 FileMaker	3127 MyDoom	8080 HTTP Proxy
42 WINS Replication	593 Microsoft DCOM	3128 HTTP Proxy	8086-8087 Kaspersky AV
43 WHOIS	631 Internet Printing	3222 GLBP	8118 Privoxy
49 TACACS	636 LDAP over SSL	3260 iSCSI Target	8200 VMware Server
53 DNS	639 MSDP (PIM)	3306 MySQL	8500 Adobe ColdFusion
67-68 DHCP/BOOTP	646 LDP (MPLS)	3389 Terminal Server	8767 TeamSpeak
69 TFTP	691 MS Exchange	3689 iTunes	8866 Bagle.B
70 Gopher	860 iSCSI	3690 Subversion	9100 HP JetDirect
79 Finger	873 rsync	3724 World of Warcraft	9101-9103 Bacula
80 HTTP	902 VMware Server	3784-3785 Ventrilo	9119 MXit
88 Kerberos	989-990 FTP over SSL	4333 mSQL	9800 WebDAV
102 MS Exchange	993 IMAP4 over SSL	4444 Blaster	9898 Dabber
110 POP3	995 POP3 over SSL	4664 Google Desktop	9988 Rbot/Spybot
113 Ident	1025 Microsoft RPC	4672 eMule	9999 Urchin
119 NNTP (Usenet)	1080 SOCKS Proxy	4899 Radmin	10000 Webmin
123 NTP	1080 MyDoom	5000 UPnP	10000 BackupExec
135 Microsoft RPC	1194 OpenVPN	5001 Slingbox	10113-10116 NetIQ
137-139 NetBIOS	1214 Kazaa	5001 iperf	11371 OpenPGP
143 IMAP4	1241 Nessus	5004-5005 RTP	12035-12036 Second Life
161-162 SNMP	1311 Dell OpenManage	5050 Yahoo! Messenger	12345 NetBus
177 XDMCP	1337 WASTE	5060 SIP	13720-13721 NetBackup
179 BGP	1433-1434 Microsoft SQL	5190 AIM/ICQ	14567 Battlefield
201 AppleTalk	1512 WINS	5222-5223 XMPP/Jabber	15118 Dipnet/Oddbob
264 BGMP	1589 Cisco VQP	5432 PostgreSQL	19226 AdminSecure
318 TSP	1701 L2TP	5500 VNC Server	19638 Ensim
381-383 HP Openview	1723 MS PPTP	5554 Sasser	20000 Usermin
389 LDAP	1725 Steam	5631-5632 pcAnywhere	24800 Synergy
411-412 Direct Connect	1741 CiscoWorks 2000	5800 VNC over HTTP	25999 Xfire
443 HTTP over SSL	1755 MS Media Server	5900+ VNC Server	27015 Half-Life
445 Microsoft DS	1812-1813 RADIUS	6000-6001 X11	27374 Sub7
464 Kerberos	1863 MSN	6112 Battle.net	28960 Call of Duty
465 SMTP over SSL	1985 Cisco HSRP	6129 DameWare	31337 Back Orifice
497 Retrospect	2000 Cisco SCCP	6257 WinMX	33434+ traceroute
500 ISAKMP	2002 Cisco ACS	6346-6347 Gnutella	Legend
512 rexec	2049 NFS	6500 GameSpy Arcade	Chat
513 rlogin	2082-2083 cPanel	6566 SANE	Encrypted
514 syslog	2100 Oracle XDB	6588 AnalogX	Gaming
515 LPD/LPR	2222 DirectAdmin	6665-6669 IRC	Malicious
520 RIP	2302 Halo	6679/6697 IRC over SSL	Peer to Peer
521 RIPng (IPv6)	2483-2484 Oracle DB	6699 Napster	Streaming
540 UUCP		6881-6999 BitTorrent	

IANA port assignments published at <http://www.iana.org/assignments/port-numbers>

by Jeremy Stretch

v1.1

SERVICIOS

- **Programas que están funcionando asociados a un puerto de red**
 - Ellos "escuchan" en ese puerto
 - ¿*El qué?* Peticiones de clientes en otras máquinas, claro
- **Estos programas se ejecutan en el equipo de destino y esperan las conexiones entrantes de clientes**
 - Cuando un cliente se conecta a ellos, el servicio procesa la solicitud del cliente y envía una respuesta
 - O un error si la solicitud no es válida
 - O contiene cualquier tipo de datos / comandos inesperados ...
 - De esta manera, cualquier máquina puede proporcionar un servicio a otras
- **¡Y esta es la base de las comunicaciones entre máquinas hoy en día! 😊**
 - Ver una web en tu navegador es **localizar la máquina** donde está alojada (**su IP**)
 - El navegador entonces **va automáticamente al puerto 443** (donde sabe qué están las webs)
 - Y el servicio de la máquina localizada registrado en el puerto 443 (**servidor web**) nos manda esa web
 - Y, si no la tiene, nos manda una página de error: **Error 404 Not Found 😊**

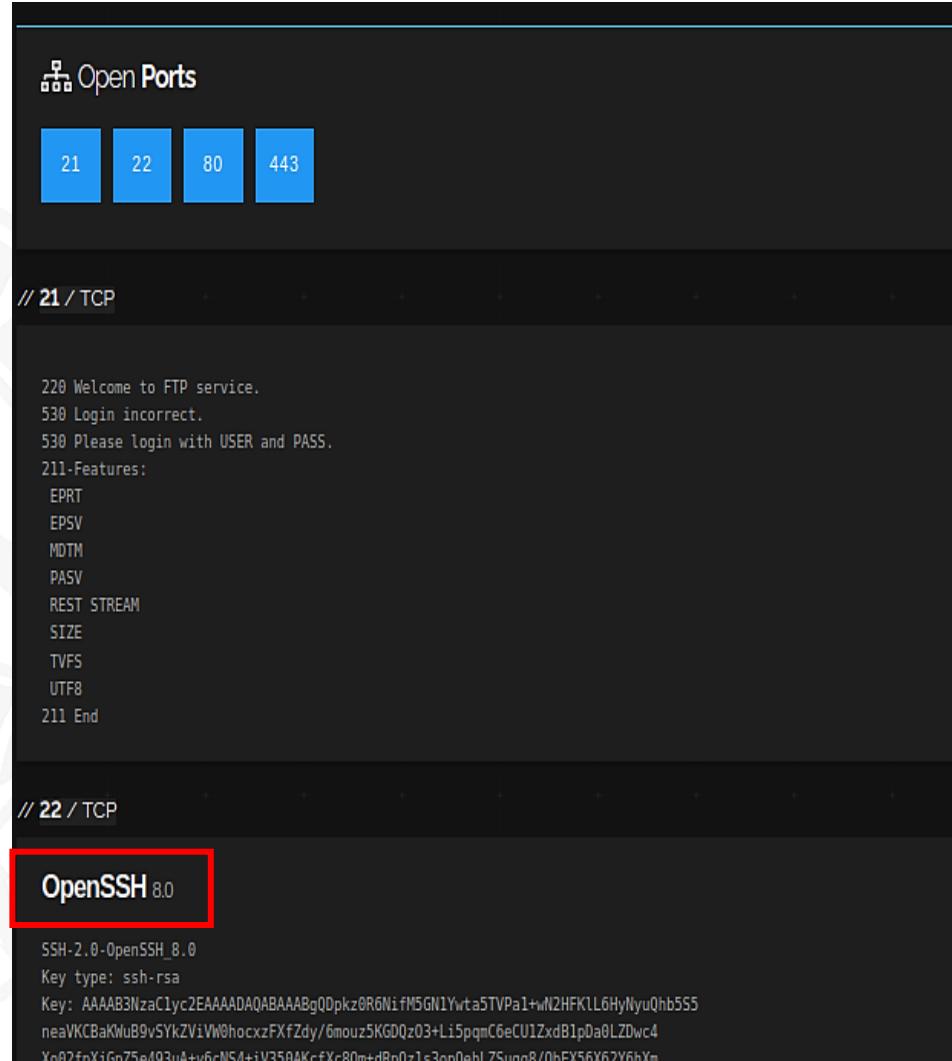
PONIÉNDODO TODO JUNTO...

● Los puertos son extremos de comunicación

- Las conexiones físicas e inalámbricas terminan en puertos de un dispositivo
- Identifican un **proceso** o un **servicio** de red
- Así una misma IP puede ofrecer varias cosas dentro de una misma máquina

● Shodan nos pinta cada puerto en un cuadro azul con su nº dentro

- Debajo muestra información de los servicios que están a la escucha
- A veces en esa información aparecen productos y versiones de los mismos
- *¿Recuerdas que se hace con esa información?* 😊 😊



The screenshot shows a Shodan search interface. At the top, it lists "Open Ports" with four blue boxes containing the numbers 21, 22, 80, and 443. Below this, under the heading "// 21 / TCP", there is a block of text from an FTP service:
220 Welcome to FTP service.
530 Login incorrect.
530 Please login with USER and PASS.
211-Features:
EPRT
EPSV
MDTM
PASV
REST STREAM
SIZE
TVFS
UTF8
211 End

Below this, under the heading "// 22 / TCP", there is a box containing the text "OpenSSH 8.0", which is highlighted with a red border. Underneath this box, there is more detailed information:
SSH-2.0-OpenSSH_8.0
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAQABAAABgQDpkz0R6Ni:fM5GN1Yvta5TPa1+wN2HFkLL6HyNyUhb555
neAVKCBaKwJB9vSYkZViWb0hocxzFXfZdy/6mouz5KGQz03+Li5pqmC6eCU1ZxdB1pDa0LZDwc4
Xo82feXiGn75e493uA+y6cN54+iV350AKcfXc80m+dRp0zls3op0ehl75uon8/0bEX56X62Y6hXm

Nada es más satisfactorio cuando aprendes algo que aprender a “leer” cosas nuevas ;)

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



- *¿Entiendes cuál es el concepto de subdominio?*
- *¿Has entendido que existen páginas web que te pueden hablar de la reputación de la empresa vinculada a una web, y con eso tomar decisiones acerca de si te fías o no?*
- *¿Qué opinas de las empresas que abusan de los métodos de tracking?*
- *¿Qué opinas ahora de las empresas que intentan por todos los medios que este instalas su aplicación vinculada? ¿entiendes ahora mejor por qué lo hacen?*
- *¿Has entendido la utilidad de páginas de opiniones como Trustpilot?*
- *¿Te das cuenta de que cualquier persona que está vinculada a una web es una vía de investigación tirando de redes sociales o de búsquedas en internet?*
- *¿Entiendes lo relevante que es saber si una web ha sido vulnerada o no desde el punto de vista de lo que pretendemos?*
- *¿Sabías que se podían geolocalizar IPs y lo que implica para la seguridad?*
- *¿Entiendes que es el concepto de puerto y de servicio, y cómo están ambos relacionados?*
- *¿Te das cuenta entonces que es otro sitio donde mirar productos y versiones y con ello sacar CVEs, siendo por tanto otra forma de saber si una web es o no fiable?*

INVESTIGANDO LA WEB

