The Browser Exploitations
Google Chrome

Richard Villca Apaza

@SixP4ck3r

OWASP
The Open Web Application Security Project

Santa Cruz - Bolivia, Abril 2016

About Me

OWASP
The Open Web Application Security Project

DISCLOSURE

La siguiente presentación obedece a necesidades estrictamente educativos, ni el presentador ni OWASP se hacen responsables del mal uso que pudieran dar con la presente información.

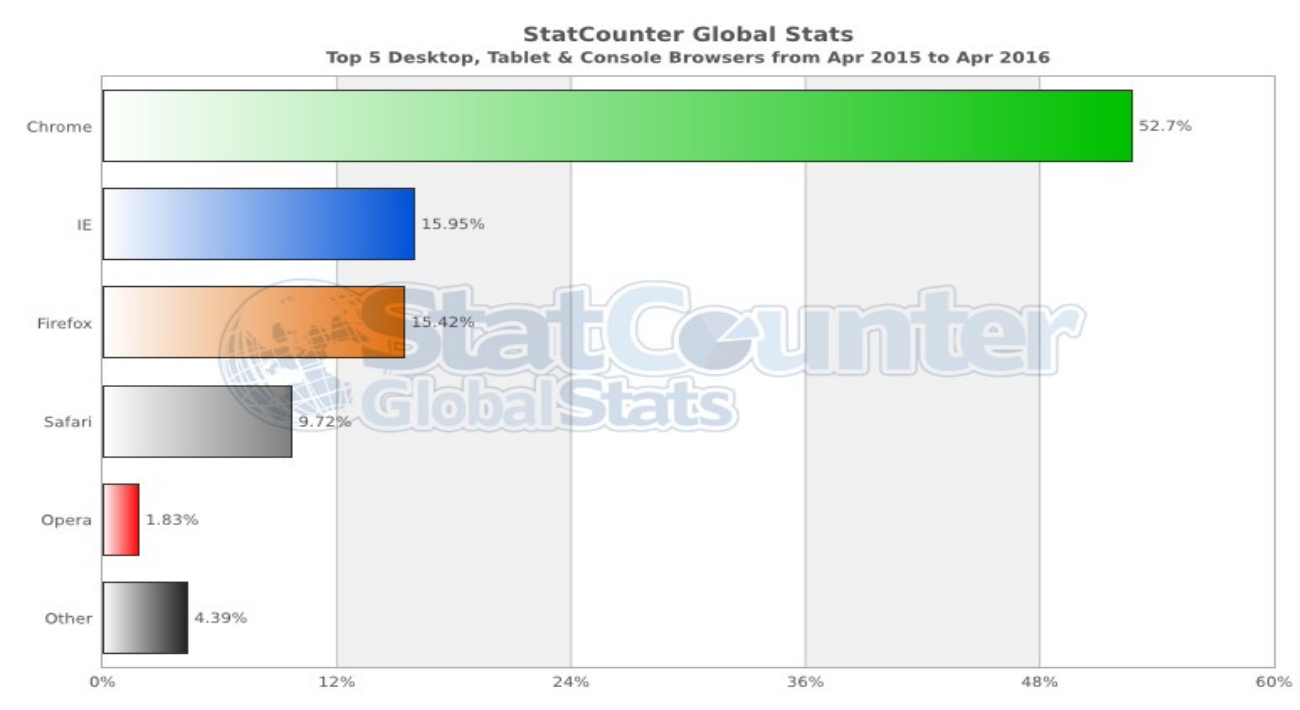
OWASP
The Open Web Application Security Project

Lo que veremos...

- Extensiones
- La Seguridad en las extensiones de Google Chrome
- Debilidades... ¿y como explotarlo?
- Demos (Cookies, MiTM-GET-POST, Keylogger)
- Creando un RAT basado en extensiones.
- ¿Entonces como puedo protegerme?
- Conclusión

- Google Chrome como Navegador Web

  Google Chome es el navegador más usado.



OWASP
The Open Web Application Security Project

¿Que son las Extensiones en Google Chrome?

Las extensiones son pequeños programas auxiliares o dispositivos de hardware que permiten a sistemas mayores extender sus capacidades normales o aportar una función, generalmente muy específica.

Gracias a sus miles de extensiones hacen a Google Chrome una navegador aun más potente.

OWASP
The Open Web Application Security Project

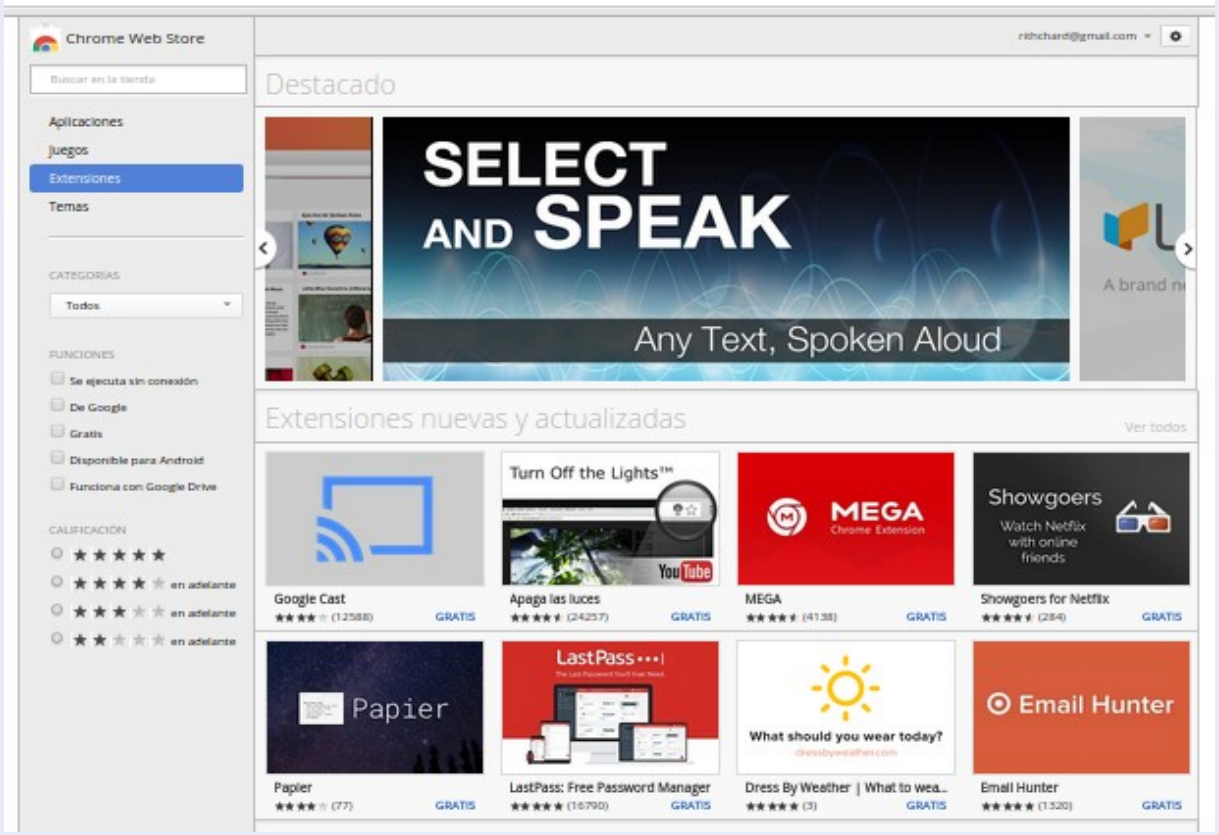
¿Que son las Extensiones en Google Chrome?

Google Chrome sabe de la importancia de las extensiones, Google Chrome ofrece a los desarolladores un Dashboard para que pueda subir y gestionar sus extensiones, por un pago unico de 5 USD.

Para el usuario ofrece **Chrome Web Store** para que pudieran descargar y usarlo de manera sencilla.

OWASP
The Open Web Application Security Project

¿Que son las Extensiones en Google Chrome?



OWASP
The Open Web Application Security Project

La Seguridad en las extensiones de Google Chrome

Inicialmente Google Chrome dotó de muchas funcionalidades que muchas veces fue aprovechado por los atacantes y eso conllevó que Google Chorme quitara algunas de las funciones gradualmente.

En el año 2015 dispuso que ya no se podrian mas usar extensiones que no esten en el market (Extensiones Offline).

OWASP
The Open Web Application Security Project

La Seguridad en las extensiones de Google Chrome

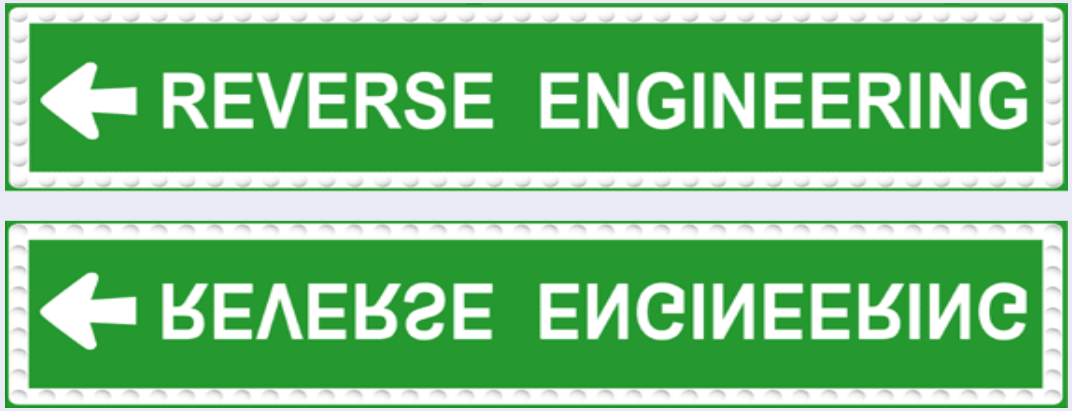
Actualmente hast abril del 2016, se puede instalar extensiones que no esten en market de Google Chrome(Conocidas como Extensiones Offline), en **Modo Developer**.

''For any problem, there are hundreds of excuses as to why, and how it can't, and shouldn't be done.. But in this infinite universe, it's really just a matter of determination as to whether YOU will make it happen.''

¿Como explotarlo?

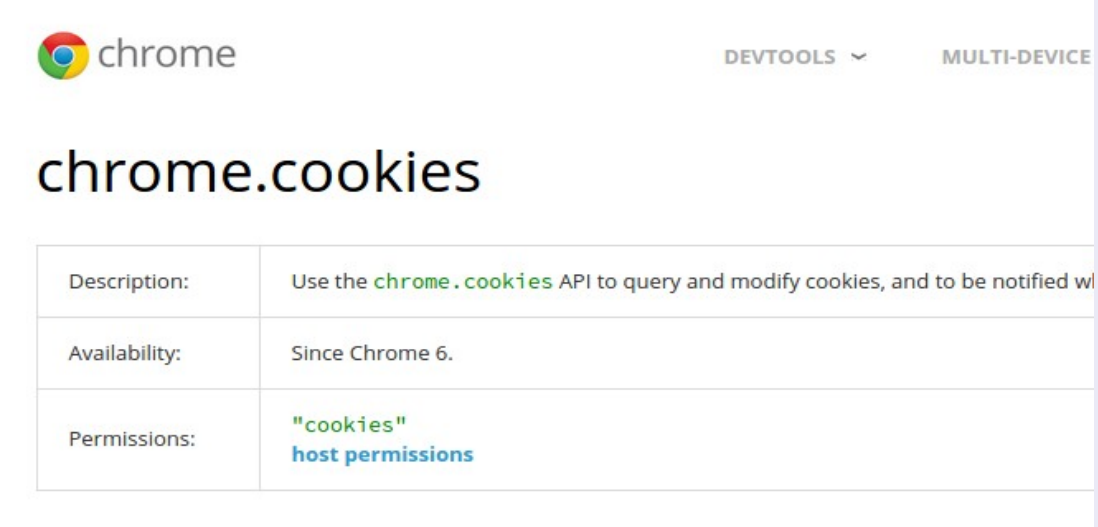
Para explotar algun software es sugerible estudiar el objetivo hasta llegar a un punto de usar esas funcionalidades de manera **Particular**.

Es conocida en tambien como **reverse engineering**.



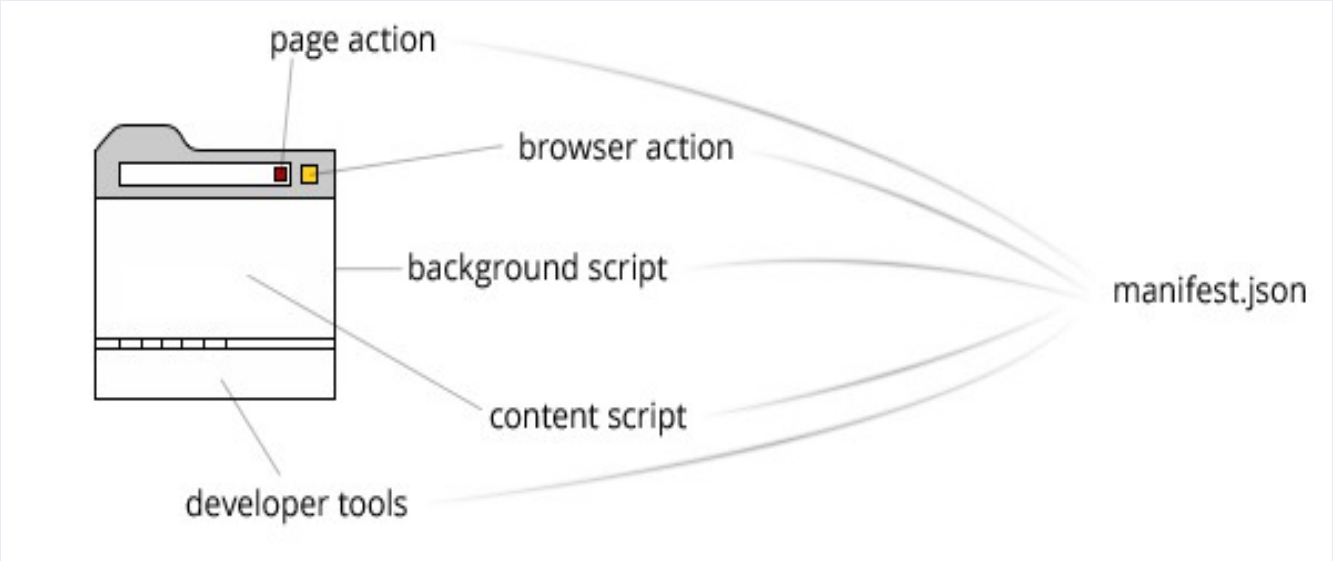
¿Como explotarlo?

Todas las funciones que Google Chrome dá al desarrollador estan documentadas en su pagina oficial, muchas de ellas con ejemplos en forma de extensiones para instalar y probar.



Desarrollo de extensiones

Para desarollar extensiones es necesario tener un navegador Google Chrome, saber los archivos de estructura de una extension para Google Chrome, Javacript y HTML.



OWASP
The Open Web Application Security Project

Caracteristicas y APIs ofrecidas

accessibilityFeatures | alarms | automation | bookmarks | browserAction | browsingData | certificateProvider | commands | contentSettings | contextMenus | cookies | debugger | declarativeContent | declarativeWebRequestdesktopCapture | devtools.inspectedWindow | devtools.network | devtools.panels | documentScan | downloads | enterprise.deviceAttributes | enterprise.platformKeys | events | experimental.devtools.audits | experimental.devtools.consoleextension | extensionTypes | fileBrowserHandler | fileSystemProvider | fontSettings | gcm | history | i18n | identity | idle | input.ime | instanceID | management | networking.config | notifications | omnibox | pageAction | pageCapture | permissions | platformKeys | power | printerProvider | privacy | processes | proxy | runtime | sessions | signedInDevicesstorage | system.cpu | system.memory | system.storage | tabCapture | tabs | topSites | tts | ttsEngine | types | vpnProvider | wallpaper | webNavigation | webRequest | webstore | windows

Google Chrome APIs en acción

OWASP
The Open Web Application Security Project

Tool - Compartiendo tu Navegador

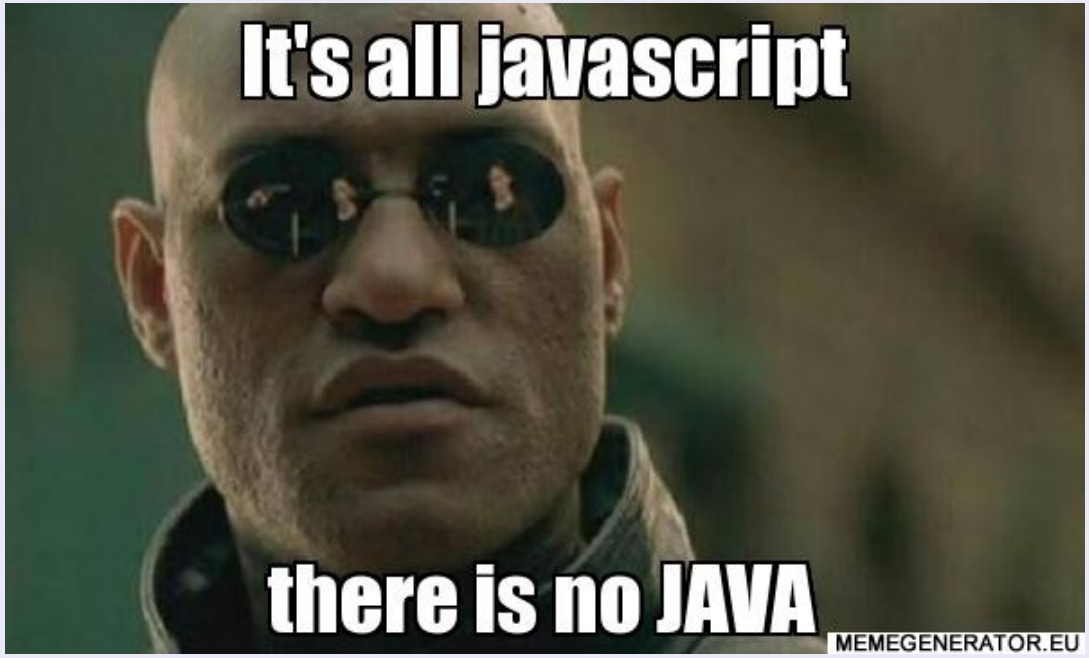
- **chrome.tabs.captureVisibleTab**

  Lo que hace esta función es de tomar la actual pestaña, sacar un captura y devolver la captura en base64, se necesita el permiso en el manifest, TABS.

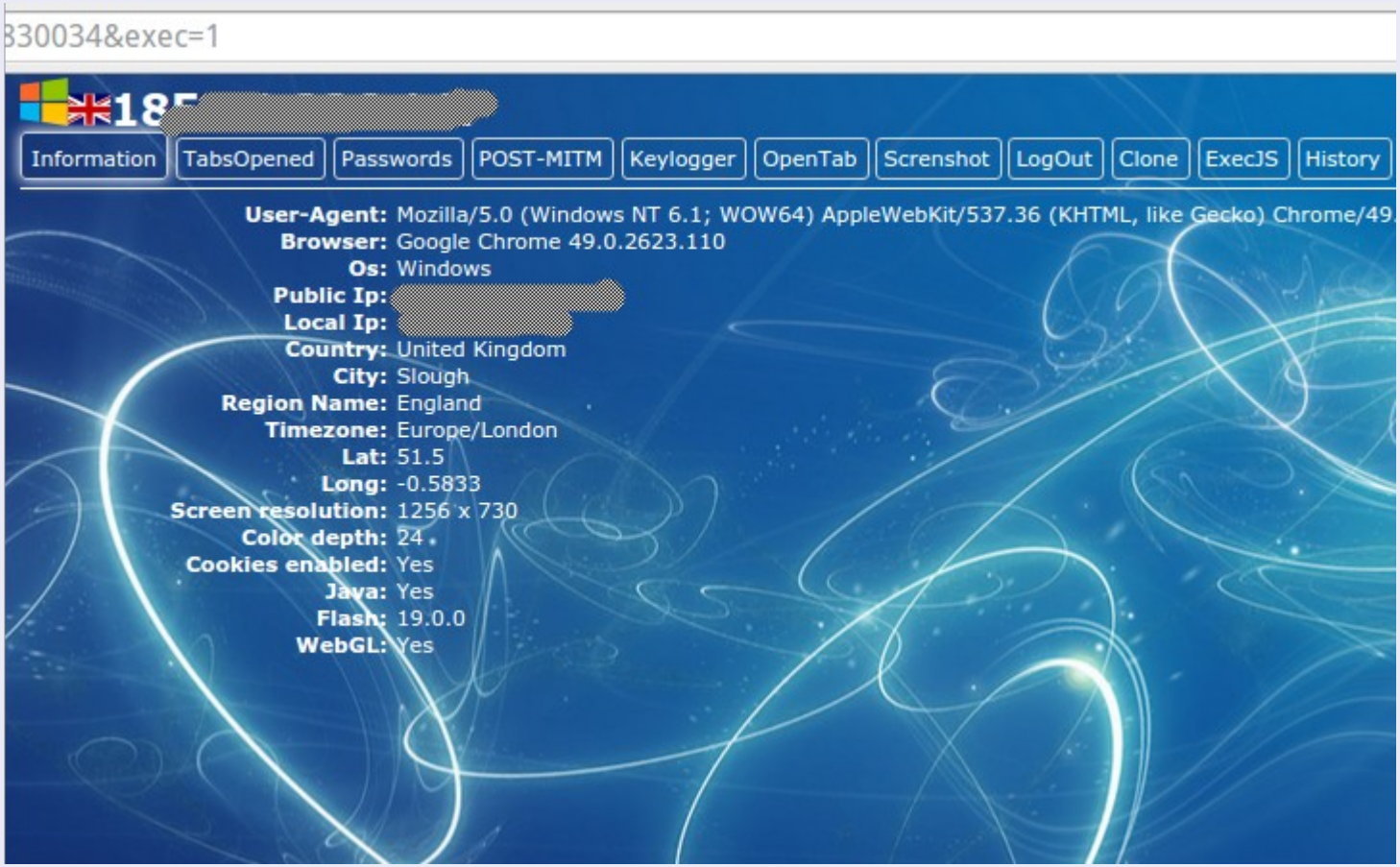
  Se podria convinar con la potencia de **NodeJS** y pedir a la extension que envie las capturas cada x segundos, y en el frontend, dibujar esa captura y mostrar. De esta forma conseguiremos el Tab Sharing deseado.

Creando un RAT basado en extension

- El objetivo es usar estas funciones como lo haria un atacante que quiere sacarle cierta ventaja usando las extensiones.



RAT – Prueba de Concepto



OWASP
The Open Web Application Security Project

RAT - ONLINE

https://consejostech.com/

¿Preguntas?

OWASP
The Open Web Application Security Project

Contacto

Email: rithchard@gmail.com

Twitter: @SixP4ck3r

Blog: http://sixp4ck3r.blogspot.com/

OWASP
The Open Web Application Security Project

Referencias

https://developer.chrome.com/extensions/api_index#stable_apis

https://developer.chrome.com/extensions/samples

http://stackoverflow.com/

http://sixp4ck3r.blogspot.com/

https://www.exploit-db.com/author/?a=2745