



• The Browser Exploitations Google Chrome

Richard Villca Apaza

@SixP4ck3r



OWASP

The Open Web Application Security Project

Santa Cruz - Bolivia, Abril 2016



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

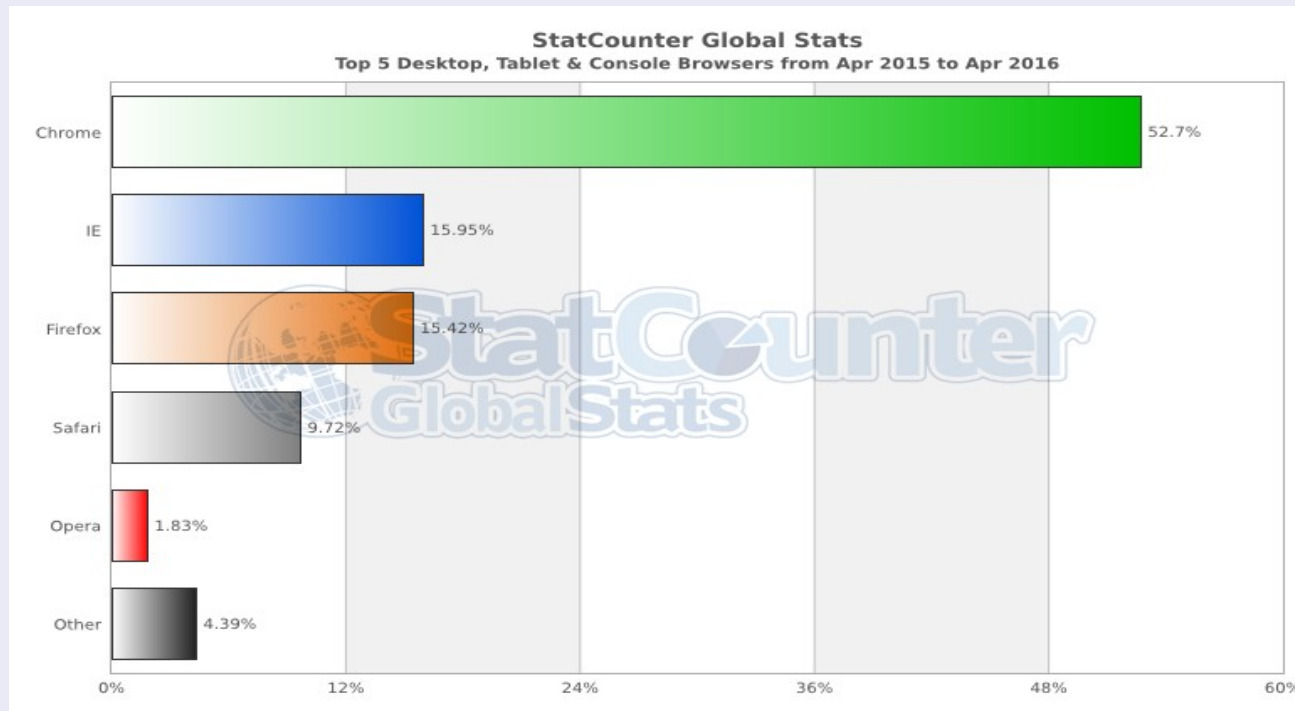


OWASP

The Open Web Application Security Project

- Google Chrome como Navegador Web

Google Chrome 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 desarrolladores 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?

The screenshot displays the Chrome Web Store interface. On the left is a navigation sidebar with categories like 'Aplicaciones', 'Juegos', 'Extensiones', and 'Temas'. The main content area features a 'Destacado' section with a large banner for 'SELECT AND SPEAK' (Any Text, Spoken Aloud). Below this is a grid of 'Extensiones nuevas y actualizadas'. Each extension card includes an icon, name, star rating, and price (all are 'GRATIS').

Extension Name	Rating	Price
Google Cast	★★★★☆ (1,2588)	GRATIS
Apaga las luces	★★★★☆ (2,4257)	GRATIS
MEGA	★★★★☆ (4138)	GRATIS
Showgoers	★★★★☆ (284)	GRATIS
Papier	★★★★☆ (77)	GRATIS
LastPass: Free Password Manager	★★★★☆ (16790)	GRATIS
Dress By Weather What to wea...	★★★★☆ (3)	GRATIS
Email Hunter	★★★★☆ (1,320)	GRATIS



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 Chrome quitara algunas de las funciones gradualmente.

En el año 2015 dispuso que ya no se podrían más usar extensiones que no estén 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."



OWASP

The Open Web Application Security Project

¿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.**



REVERSE ENGINEERING



BELEBZE ENGINEERING



OWASP

The Open Web Application Security Project

¿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.

The screenshot shows the Chrome DevTools documentation page for the `chrome.cookies` API. The page header includes the Chrome logo, the word "chrome", and navigation links for "DEVTOOLS" and "MULTI-DEVICE". The main heading is "chrome.cookies". Below this is a table with three rows: "Description", "Availability", and "Permissions".

Description:	Use the <code>chrome.cookies</code> API to query and modify cookies, and to be notified w
Availability:	Since Chrome 6.
Permissions:	<code>"cookies"</code> <code>host permissions</code>

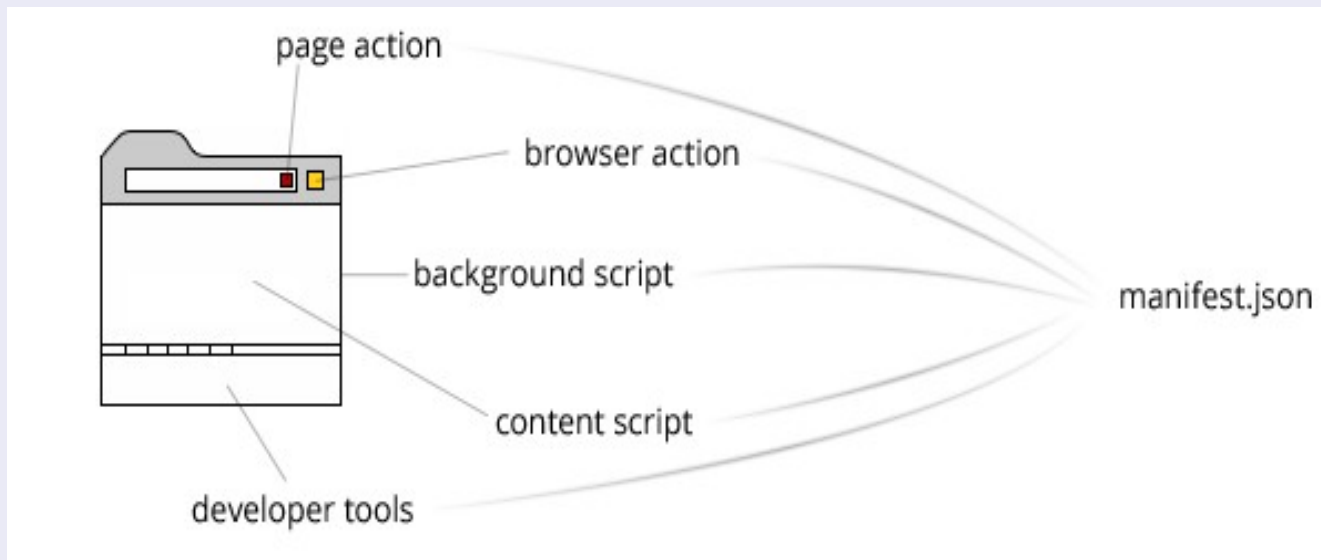


OWASP

The Open Web Application Security Project

Desarrollo de extensiones

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





OWASP

The Open Web Application Security Project

Características y APIs ofrecidas

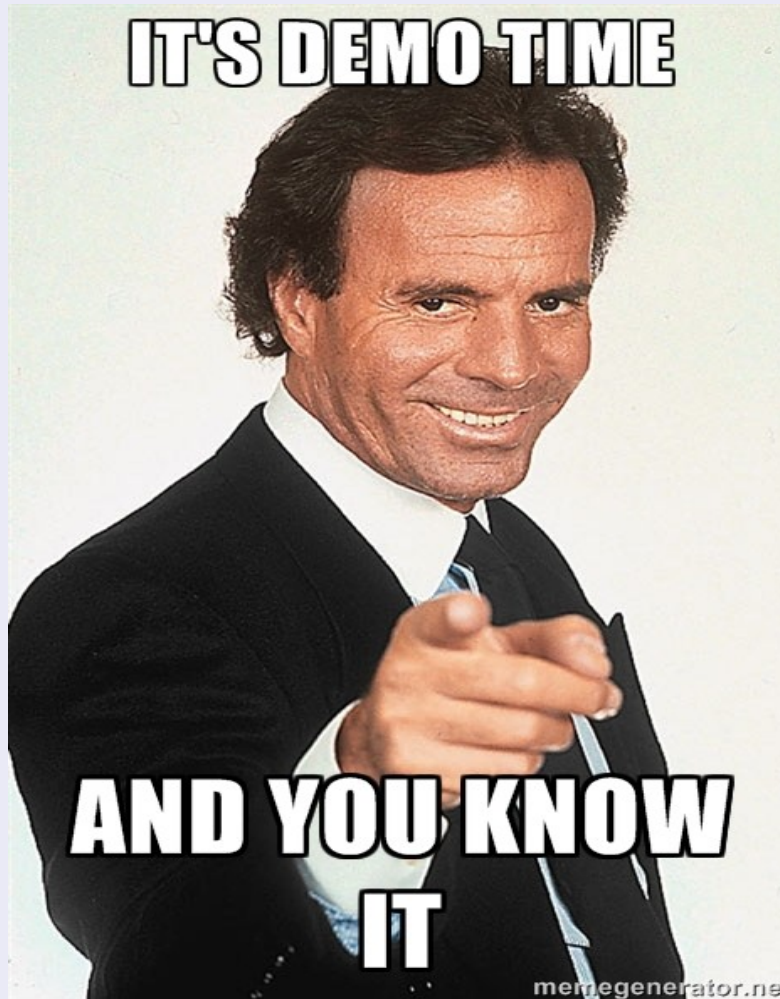
accessibilityFeatures | alarms | automation | bookmarks |
browserAction | browsingData | certificateProvider | commands |
contentSettings | contextMenus | cookies | debugger |
declarativeContent | declarativeWebRequestdesktopCapture |
devtools.inspectedWindow | devtools.network | devtools.panels |
documentScan | 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



OWASP

The Open Web Application Security Project

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



OWASP

The Open Web Application Security Project

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.





OWASP

The Open Web Application Security Project

RAT - Prueba de Concepto

830034&exec=1

The screenshot displays a web-based interface for a Remote Access Tool (RAT). At the top, there is a navigation bar with several buttons: Information, TabsOpened, Passwords, POST-MITM, Keylogger, OpenTab, Screenshot, LogOut, Clone, ExecJS, and History. Below the navigation bar, the user-agent string is shown: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.110. The browser is identified as Google Chrome 49.0.2623.110 on a Windows operating system. The user's public IP is redacted with a grey box, and the local IP is also redacted. The user's location is identified as Slough, England, United Kingdom, with a timezone of Europe/London. The screen resolution is 1256 x 730, and the color depth is 24 bits. The interface also shows that cookies are enabled, and Java, Flash, and WebGL are all supported.

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.110
Browser: Google Chrome 49.0.2623.110
Os: Windows
Public Ip: [Redacted]
Local Ip: [Redacted]
Country: United Kingdom
City: Slough
Region Name: England
Timezone: Europe/London
Lat: 51.5
Long: -0.5833
Screen resolution: 1256 x 730
Color depth: 24
Cookies enabled: Yes
Java: Yes
Flash: 19.0.0
WebGL: Yes



OWASP

The Open Web Application Security Project

RAT - ONLINE

<https://consejotech.com/>





OWASP

The Open Web Application Security Project

¿Preguntas?





OWASP

The Open Web Application Security Project

Contacto

Email: rithchard@gmail.com

Twitter: [@SixP4ck3r](https://twitter.com/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>