WebSockets con ZAP

Lic. Cristian Borghello, CISSP – CSSK – MVP
www.segu-info.com.ar
info@segu-info.com.ar
@SeguInfo

SEGU-INFO
SEGURIDAD DE LA INFORMACION

OWASP LATAM TOUR 2014

Sobre Cristian Borghello

- Licenciado en Sistemas UTN desde 2000
- Desarrollador desde los 8 años
- CISSP (Certified Information Systems Security Professional) desde 2008
- Microsoft MVP Security (Most Valuable Professional) desde 2010
- CCSK (Certificate Cloud Security Knowledge) desde 2014
- Creador y Director de **Segu-Info**
- Consultor independiente en Seguridad de la Información

Segu-Info .com.ar

Historia de la Web

1991	HTML	WEB 1.0 HTML
1994	HTML 2	
1996	CSS 1 + JavaScript	
1997	HTML 4	
1998	CSS 2	
2000	XHTML 1	WEB 2.0 LAMP
2002	Tableless Web Design	
2005	AJAX	
2009	HTML 5	

HTML5 ~= HTML + CSS + JS

Tiempo real
Asincronía

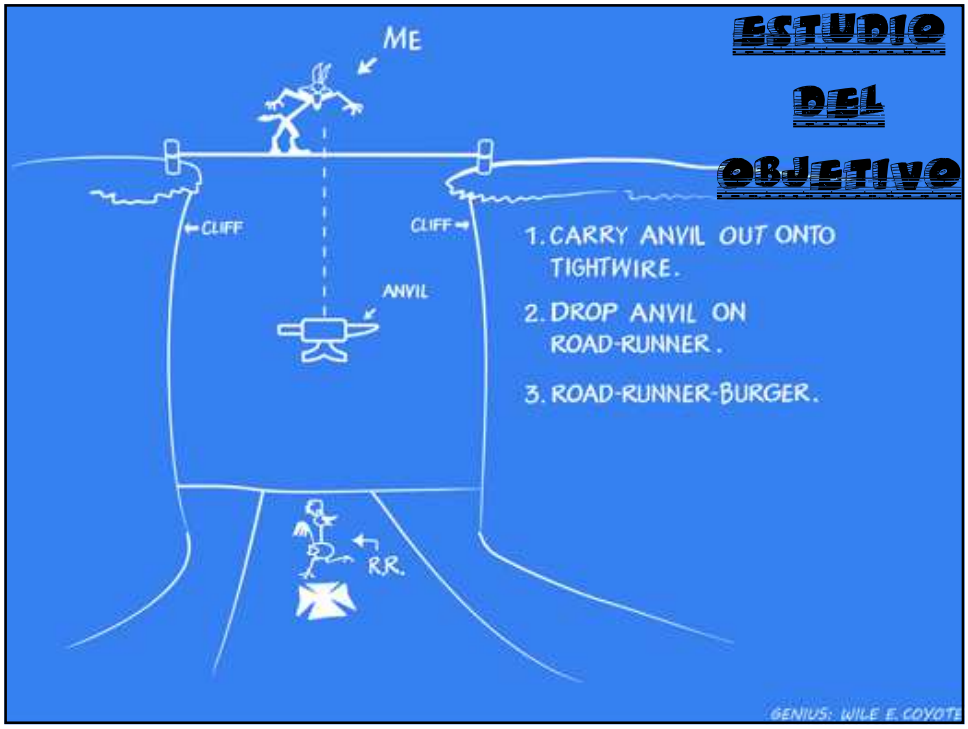
http://slides.html5rocks.com/#title-slide

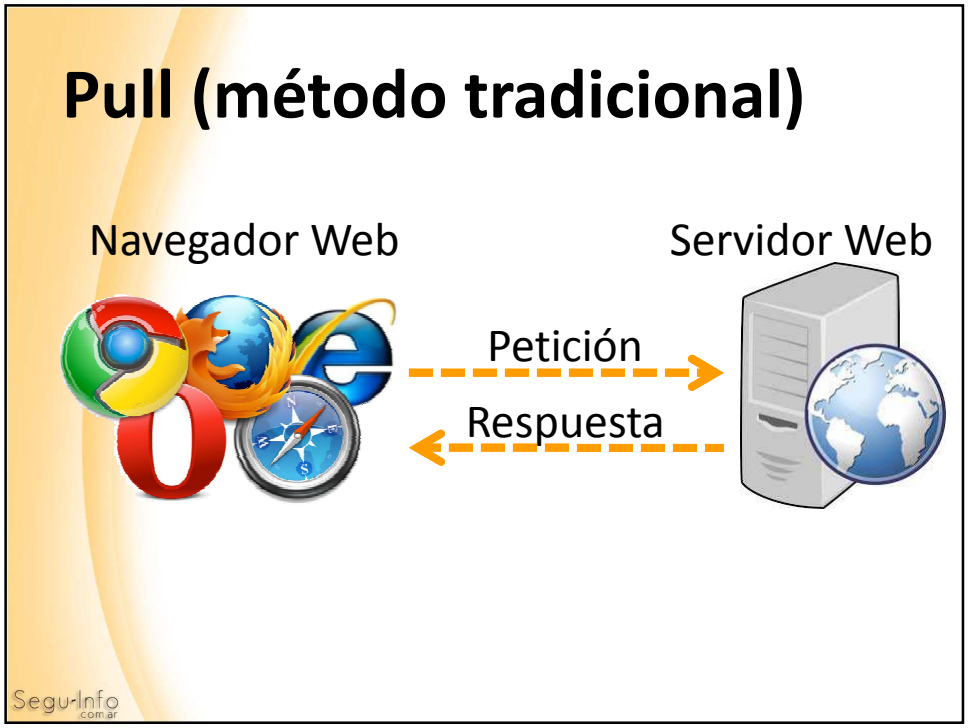
Segu-Info .com.ar

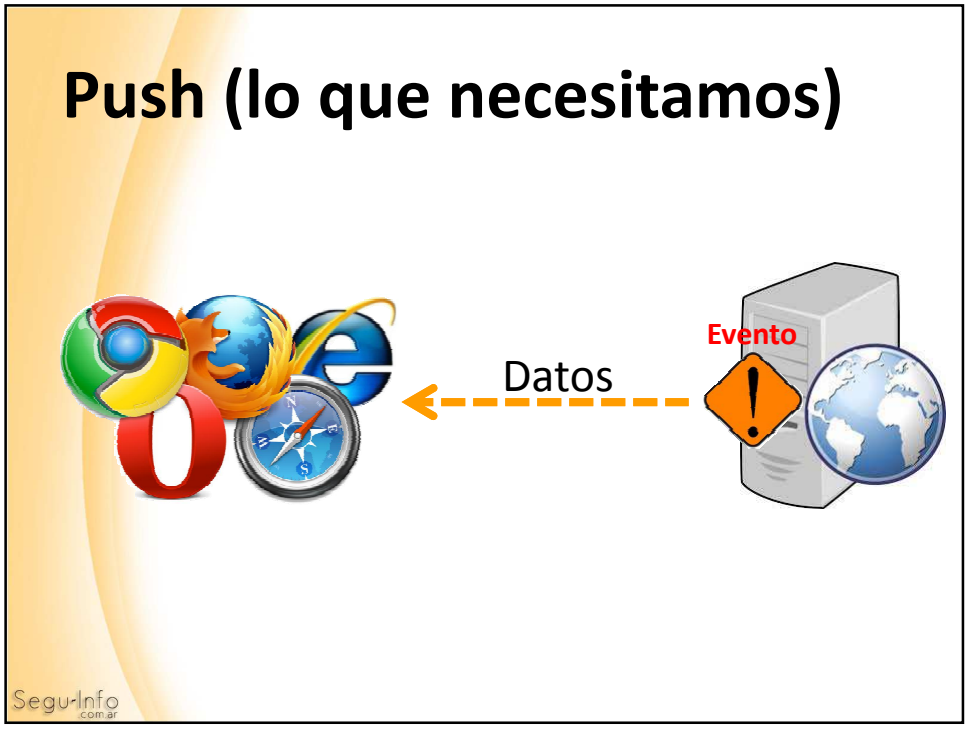
El protocolo HTTP es…

- Diseñando para transferir “documentos”
- Comunicación bi-direccional
- Comunicación *half-dúplex (*TCP es *full-dúplex)*
- Cada requerimiento envía y recibe cabeceras
- Las cabeceras agregan sobrecarga

Segu-Info .com.ar

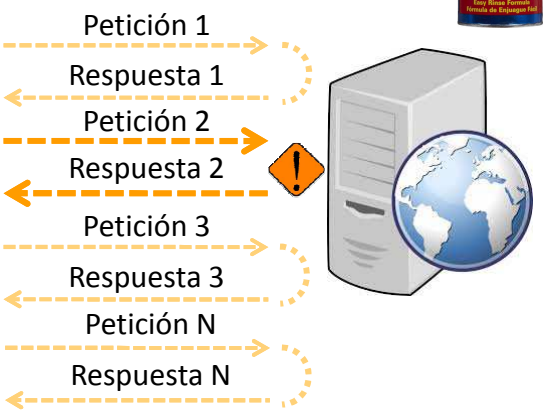

ESTUDIO
DEL
OBJETIVO
ME
CLIFF
CLIFF
ANVIL
RR.
1. CARRY ANVIL OUT ONTO TIGHTWIRE.
2. DROP ANVIL ON ROAD-RUNNER.
3. ROAD-RUNNER-BURGER.
GENIUS: WILE E. COYOTE


Pull (método tradicional)
Navegador Web
Servidor Web
Petición
Respuesta
Segu-Info
.com.ar


Push (lo que necesitamos)
Datos
Evento
Segu-Info
.com.ar


ACME

Ajax (Polling)

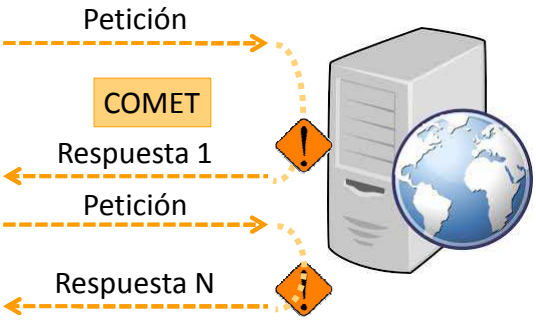


En **XMLHttpRequest (XHR)** en realizan peticiones HTTP y los datos son transferidos vía XML, JSON…

¡Pero sigue siendo exceso de HTTP!

Segu-Info .com.ar

Comet (Long Polling)

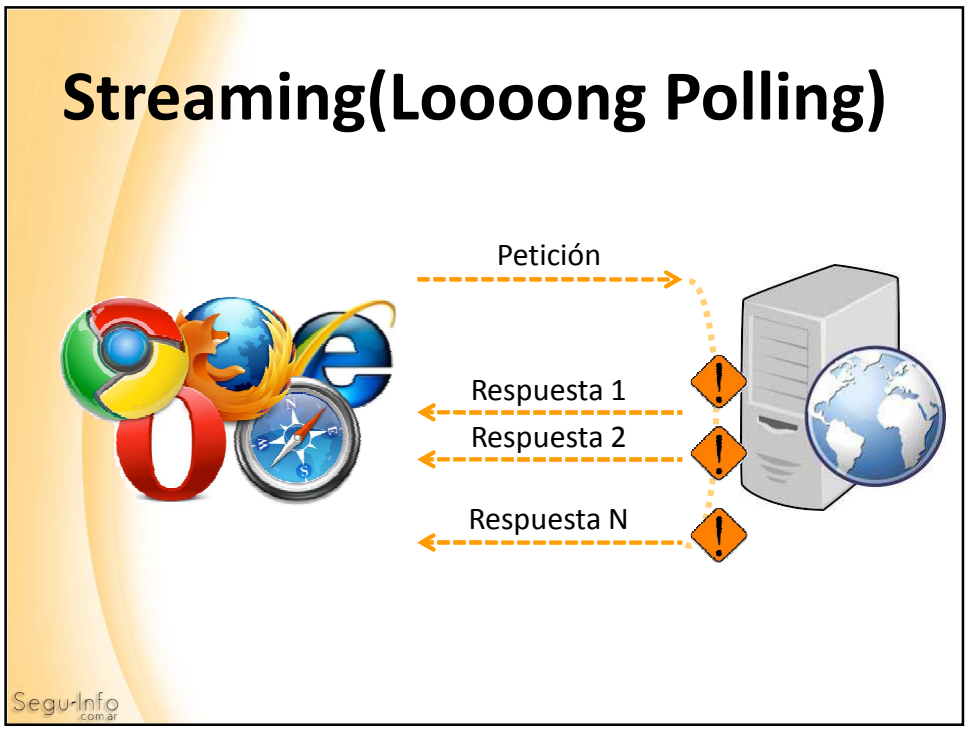


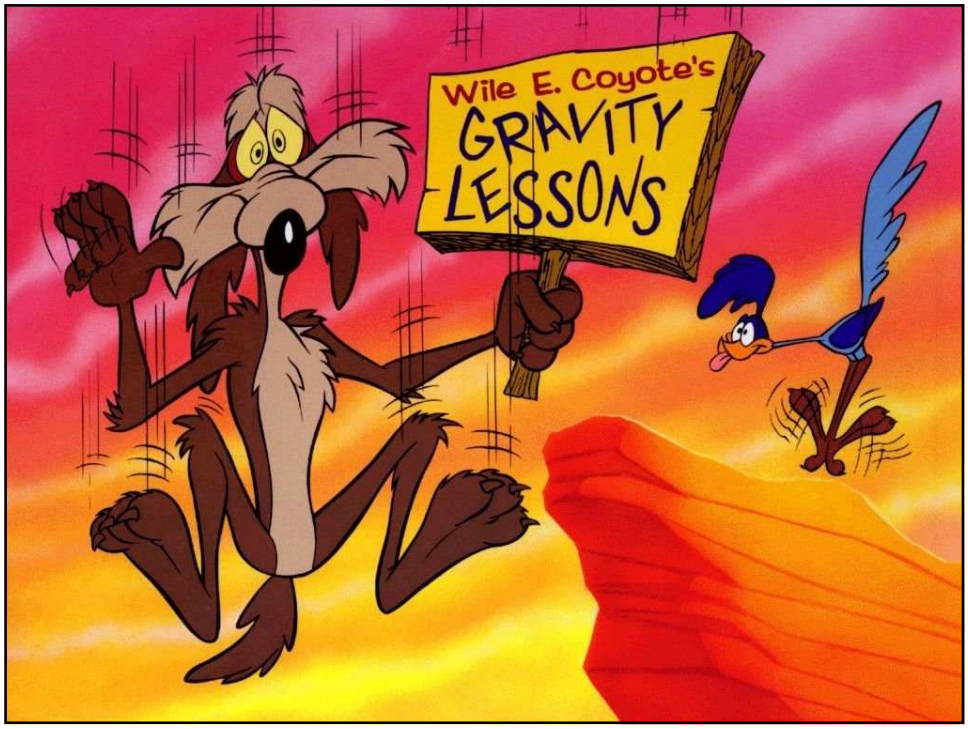
Comet usa AJAX con una petición prolongada

¡Pero sigue siendo exceso de HTTP!

Alex Russell de www.DojoToolkit.org definió la técnica
Dojo es el primer *Framework* que implementa Comet

Segu-Info .com.ar


Streaming(Loooong Polling)
Petición
Respuesta 1
Respuesta 2
Respuesta N
Segu-Info
.com.ar


Wile E. Coyote's
GRAVITY
LESSONS

WebSocket (I)

- La especificación **WebSocket** (RFC 6455) es parte de la iniciativa de HTML5
- WebSockets define una API que permite a las páginas web, la comunicación en dos vías con un *host*
- WebSocket define un canal de comunicación de texto *full-duplex* y bidereccional que opera a través de un solo conector TCP/HTTP
- WebSockets proporcionan una enorme reducción de tráfico de red

http://websocket.org/
http://socket.io/
http://pusher.com/

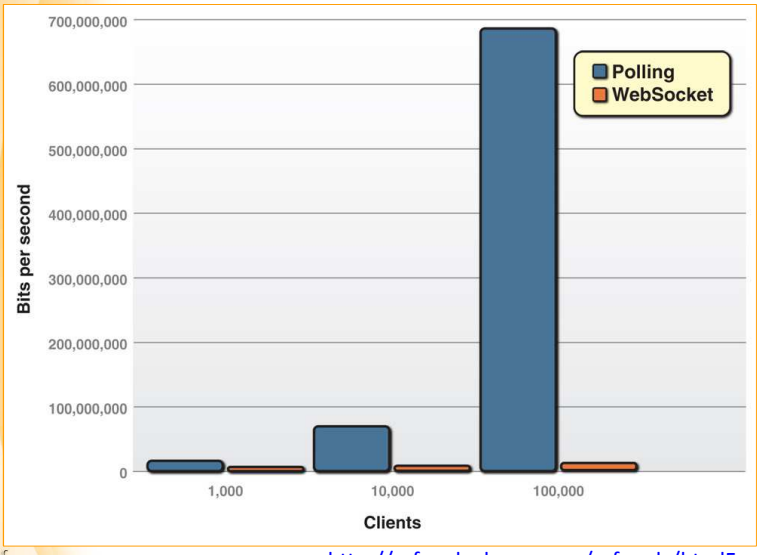
Segu-Info .com.ar

WebSocket (II)

- WebSocket simplifica la complejidad en la administración de conexiones
- Representa la evolución en la comunicación web, en comparación con Ajax y Comet
- Tanto el servidor como el cliente pueden enviar datos en cualquier momento, y al mismo tiempo
- Sólo los datos son enviados, sin sobrecarga de cabeceras HTTP, lo que reduce drásticamente el ancho de banda
- Baja latencia entre el cliente y el servidor

Segu-Info .com.ar

Reducción de Tráfico



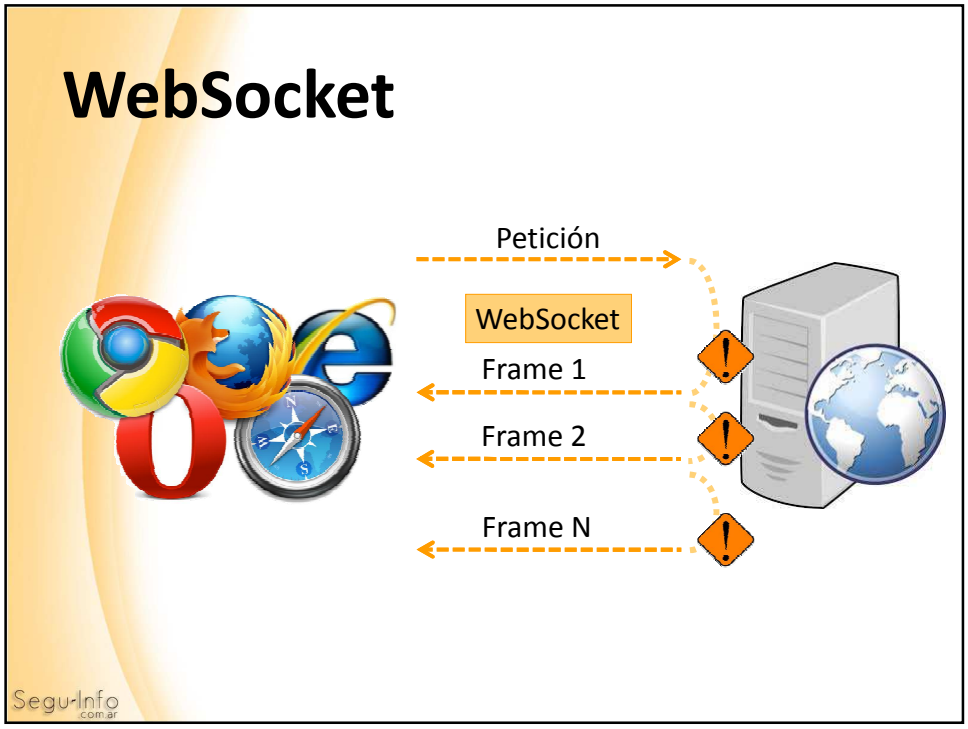
http://refcardz.dzone.com/refcardz/html5-websocket

Segu-Info .com.ar

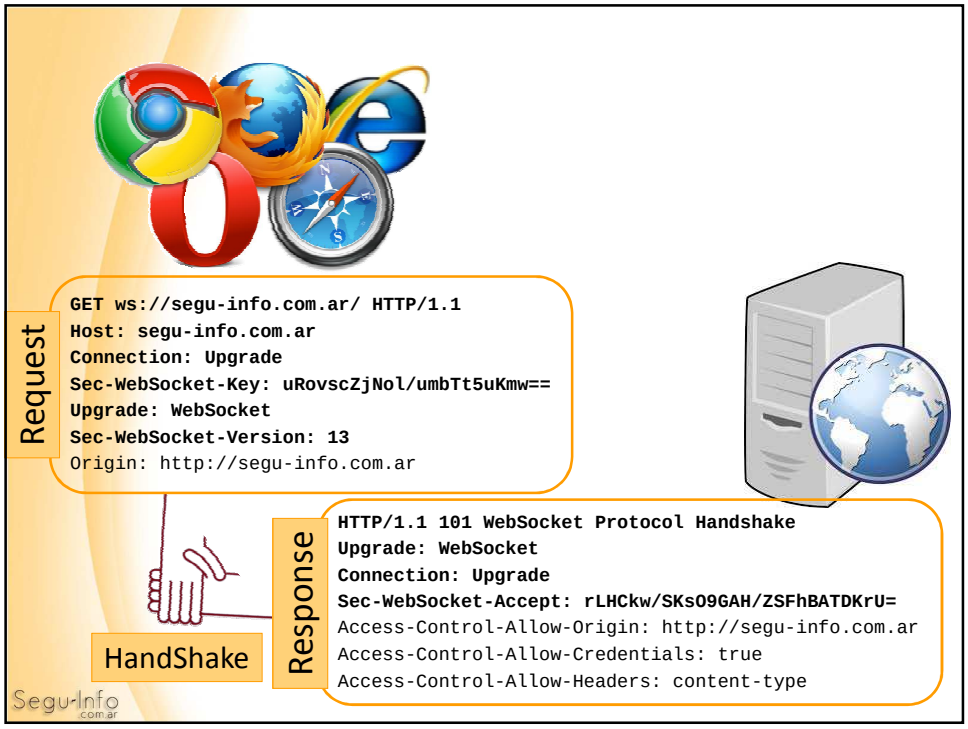
WebSocket (III)

- Para conectarse desde un cliente, se crea una instancia WebSocket a través de la dirección **ws://... (80) o wss://... (443)**
- La nueva conexión se establece a través de un *"Upgrade"* del protocolo HTTP durante el *handshake* del cliente y el servidor y sobre la misma conexión de TCP/IP existente

Segu-Info .com.ar


WebSocket
Petición
WebSocket
Frame 1
Frame 2
Frame N
Segu-Info
.com.ar


Welcome, Matt
Level 69
$7,031,478
GET CHIPS
Send Chips
Leaderboard
Gifts
Fold
Fold
$7000
$155
Raise
$8,875
Call
$9,509
$950
$50
$45
$50
$50
Raise
$2,450,900
Call
$1,127
$100
Chris Cranky
$1,410
Call
$100
$4,500
All-In
$0
Fold
Check
Chris Cranky: Howdy
Wilfred: Hi everybody
Snowman: Going all in. LOL!
Call
Raise
Check/Fold
I love playing Zynga Poker!
Call Any



Implementaciones en Servidor

PHP

Rachet – http://socketo.me

Node.js

http://socket.io/

https://github.com/Worlize/WebSocket-Node

https://github.com/einaros/ws

Java

http://www.eclipse.org/jetty/

Ruby

http://github.com/igrigorik/em-websocket

Python

http://code.google.com/p/pywebsocket/

https://github.com/facebook/tornado

.NET

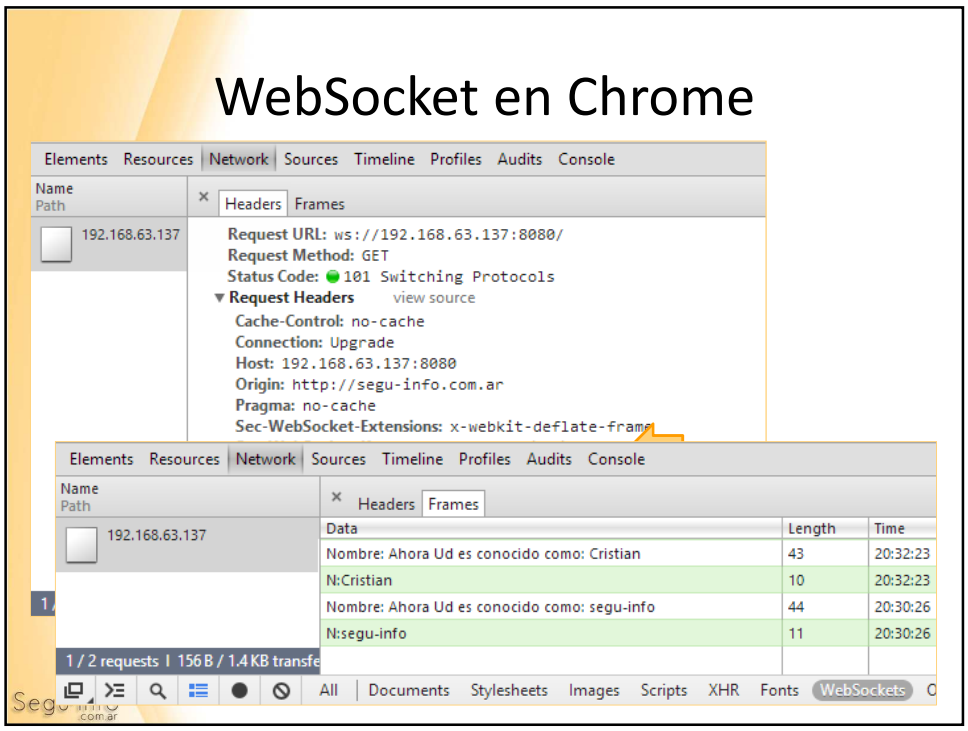
http://git.warmcat.com/cgi-bin/cgit/libwebsockets/

http://superwebsocket.codeplex.com/

http://msdn.microsoft.com/en-us/library/system.net.websockets(v=vs.110).aspx

Segu-Info

WebSocket en Chrome



WebSocket en ZAP

- El Proxy OWASP ZAP es una herramienta fácil de usar y permite la búsqueda de vulnerabilidades en aplicaciones web
- ZAP ofrece escáneres automáticos, así como conjunto de herramientas que permiten encontrar vulnerabilidades de seguridad
- **ZAP ~~es~~ era el <u>único</u>* Proxy que permite análisis de WebSocket**

* Ya no. Acaba de publicarse BURP 1.5.21 y 1.6
http://releases.portswigger.net/2014/01/v1521.html

Segu-Info .com.ar

WebSocket en ZAP

Segu-Info .com.ar

¿Quiénes lo soportan?

Web Sockets - Candidate Recommendation

Bidirectional communication technology for web apps

*Usage stats:	Global
Support:	72.24%
Partial support:	1.94%
Total:	74.18%

Show all versions	IE	Firefox	Chrome	Safari	Opera	iOS Safari	Opera Mini	Android Browser	Blackberry Browser	IE Mobile
								2.1		
								2.2		
						3.2		2.3		
						4.0-4.1		3.0		
	8.0		31.0			4.2-4.3		4.0		
	9.0		32.0			5.0-5.1		4.1		
	10.0	27.0	33.0			6.0-6.1		4.2-4.3	7.0	
Current	11.0	28.0	34.0	7.0	20.0	7.0	5.0-7.0	4.4	10.0	10.0
Near future		29.0	35.0		21.0					
Farther future		30.0	36.0		22.0					
3 versions ahead		31.0	37.0							

Segu-Info .com.ar

http://caniuse.com/#feat=websockets

Gracias

Lic. Cristian Borghello
www.segu-info.com.ar
info@segu-info.com.ar
@SeguInfo

SEGU.INFO
SEGURIDAD DE LA INFORMACION

OWASP LATAM TOUR 2014