Seguridad de Recursos y Aplicaciones Web
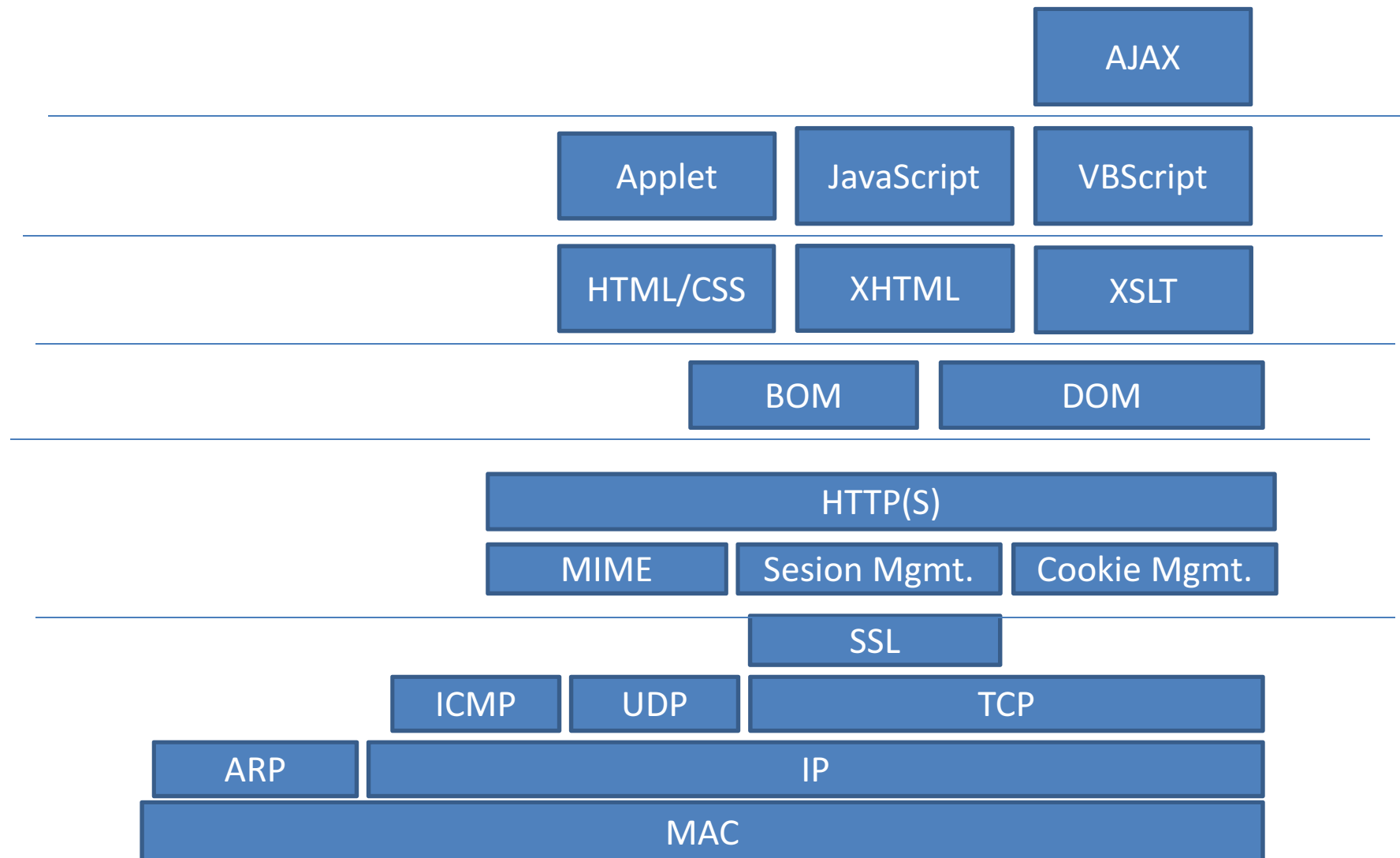
Web Technologies

Web Client-Side Stack
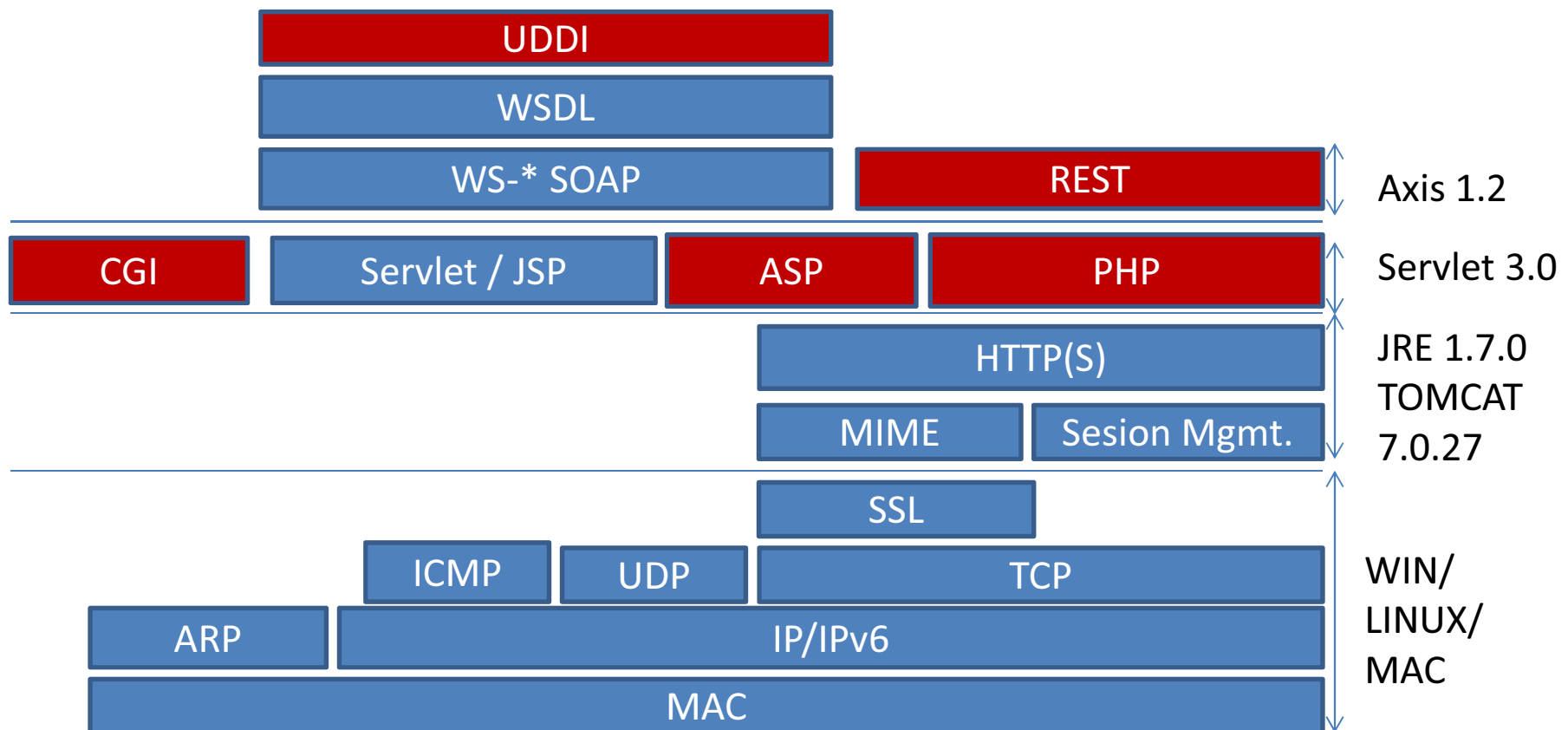
Web Server-Side Stack

UDDI

WSDL

WS-* SOAP	REST

CGI	Servlet / JSP	ASP	PHP

HTTP(S)

MIME	Sesion Mgmt.

SSL

ICMP	UDP	TCP

ARP	IP/IPv6

MAC
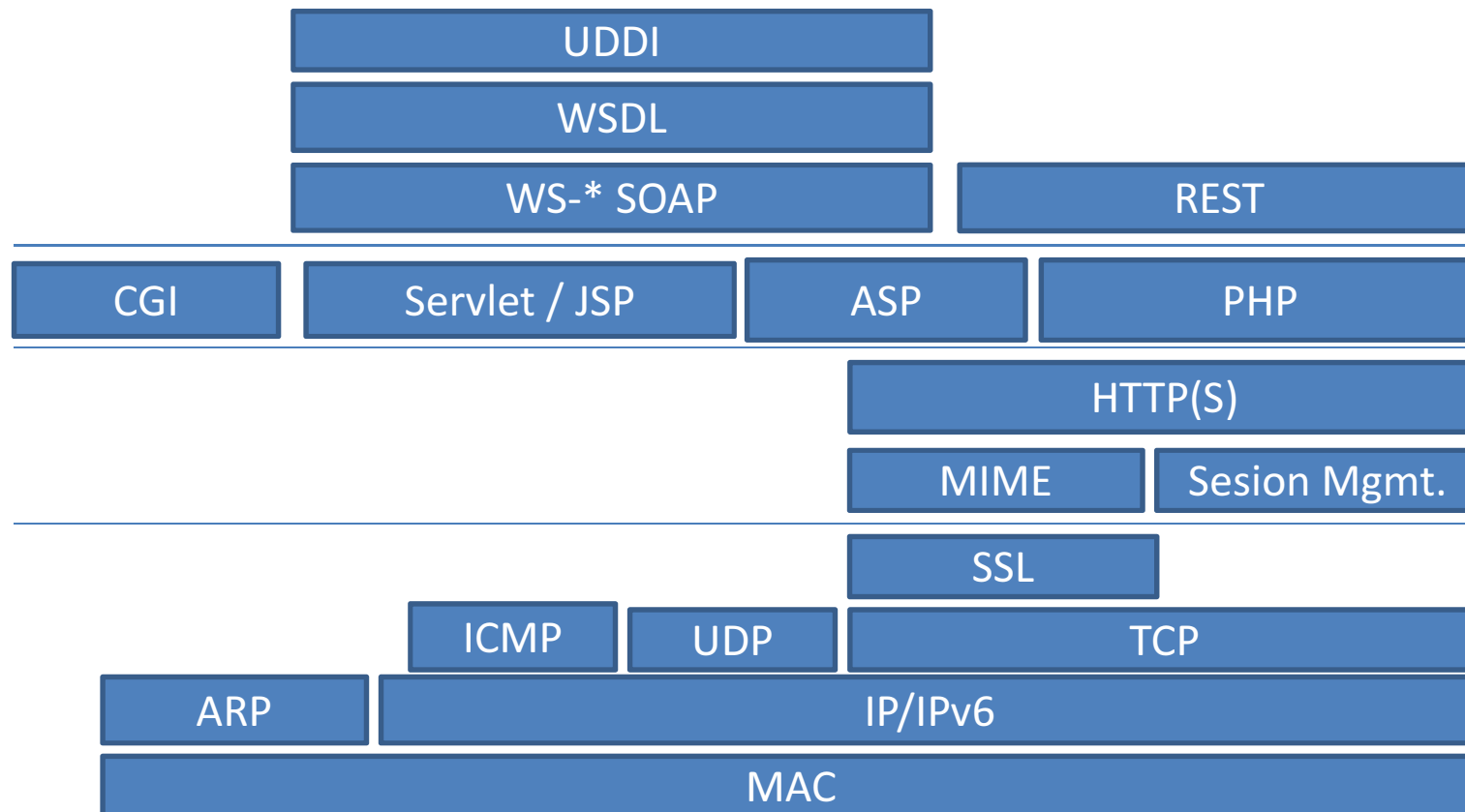
WEBGoat v5.4 J2EE Server

- A J2EE "Intentionally Insecure"
- https://code.google.com/p/webgoat/

UDDI	
WSDL	
WS-* SOAP	REST

Axis 1.2

CGI	Servlet / JSP	ASP	PHP

Servlet 3.0

HTTP(S)
MIME	Sesion Mgmt.

JRE 1.7.0
TOMCAT
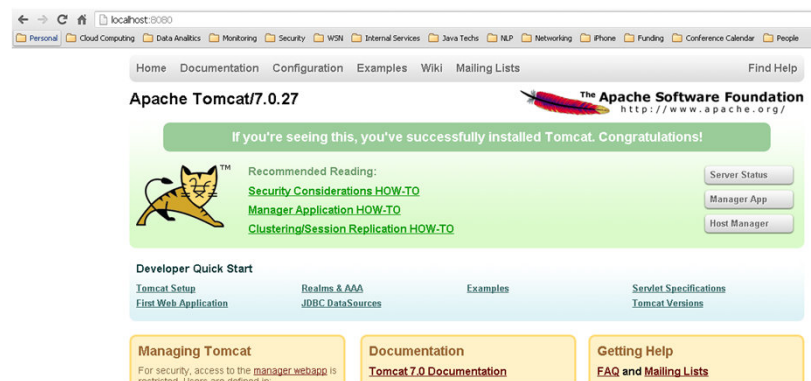7.0.27

SSL
ICMP	UDP	TCP
ARP	IP/IPv6
MAC

WIN/
LINUX/
MAC

Setting up our TestBed

Setting up WebGoat

- Instalation
  - Just download, uncompress and that's all!
- Execution
  - Just run the script: /webgoat_8080.bat (.sh)
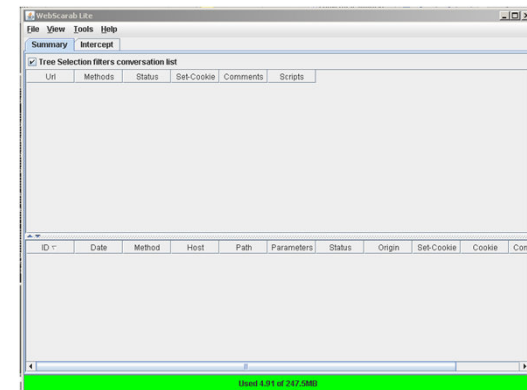 - Open the web browser
  - http://localhost:8080

WebScarab

- WebScarab is a framework for analysing applications that communicate using the HTTP and HTTPS protocols.
- WebScarab operates as an intercepting proxy, allowing the operator to review and modify requests created by the browser before they are sent to the server, and to review and modify responses returned from the server before they are received by the browser.
- WebScarab is able to intercept both HTTP and HTTPS communication.
- The operator can also review the conversations (requests and responses) that have passed through WebScarab.

Setting up WebScarab

- Installation
  - Just double click on the installer and Next, Next, Next …
  - http://sourceforge.net/projects/owasp/files/WebScarab/20070504-1631/webscarab-installer-20070504-1631.jar/download

- Execution
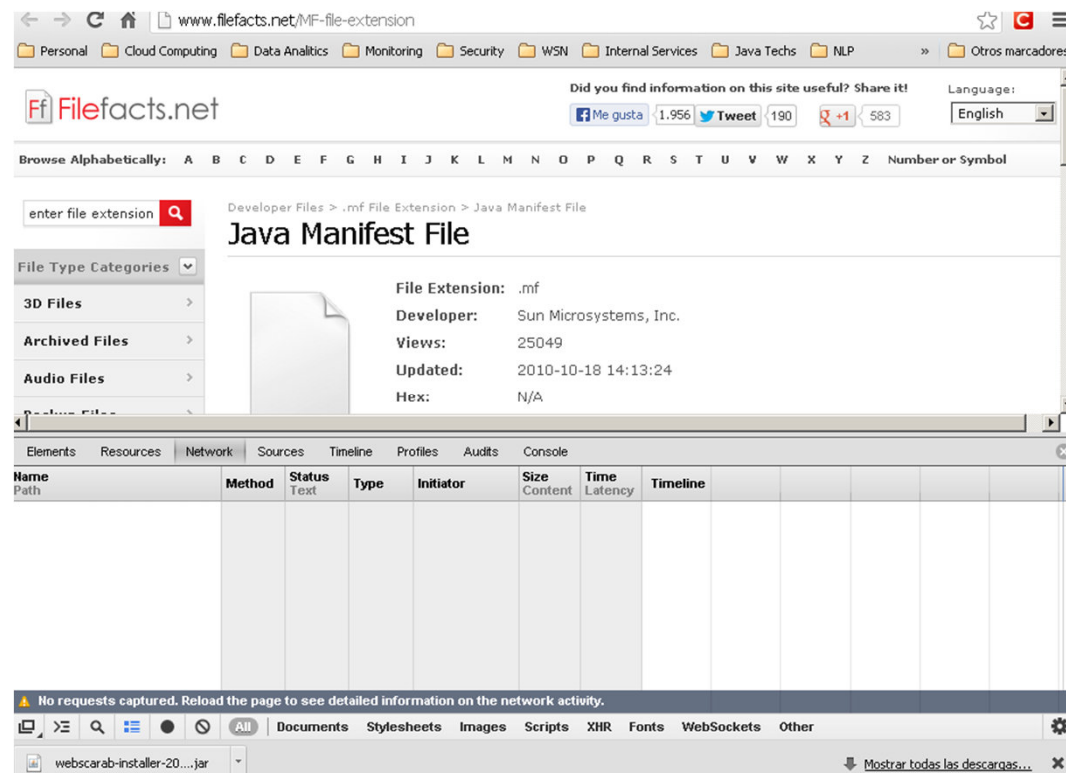 - Open "webscarab.jar" with java

Placing WebScarab between your Browser and WebGOAT

- TBD

Setting up your browser (Chrome)

- Ensure that you have in Google Chrome
  - Tools -> Tools for Developers
  - If click on "rec" -> Record all the traffic

Set up some favorite URLs

- Charset Decoder Online
    - http://yehg.net/encoding/
- Set of Chrome Plugins for Hacking
    - http://bl0g.yehg.net/2012/06/google-chrome-add-ons-for-web-app.html
- WebGoat Tutorial
    - http://localhost:8080/WebGoat/attack