[Cyber Webinar]
Protocolo HTTP y Webservers

Entendamos como funcionan las cosas!

Presentación

- Miguel Díaz
- Especialista en Seguridad informática
- Trabajo en CSIRT

www.linkedin.com/in/mdiazcl

- **Especialidad:** Romper sitios Seguridad en sitios web

Conceptos básicos

- Definiciones importantes
- HTTP
- Aplicaciones Web

Definiciones importantes

Protocolo: Conjunto de reglas y acuerdos de comunicación entre ambas partes (ej: HTTP, FTP, TELNET, etc...)

WebServer: Es un software capaz de entregar un servicio de WebApp

WebApp: Es un software “Cliente-Servidor” el cual su entorno gráfico es procesado por un WebClient y la lógica reside en el servidor (****)

WebClient (Web Browser): Es un software que solicita a un WebServer y presenta (*) los recursos de una WebApp en el cliente.

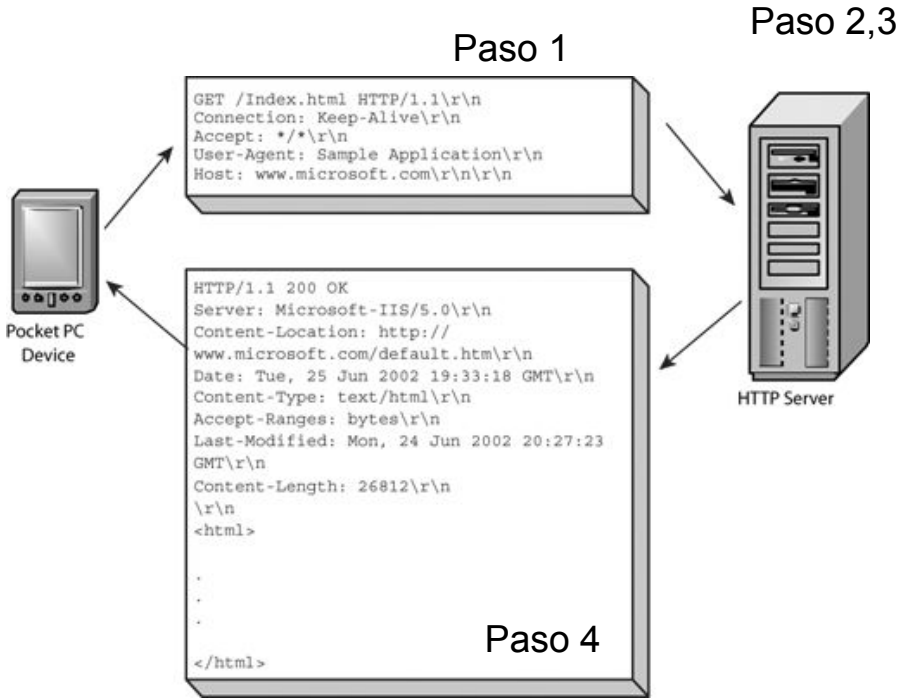
Definiciones importantes

Protocolo: Conjunto de reglas y acuerdos de comunicación entre ambas partes (ej: HTTP, FTP, TELNET, etc...)

HTML: Es un lenguaje de marcado (***lo lamento @RA_cl***) el cual permite definir la estructura de la capa de presentación de una aplicación Web

PHP/Python/Ruby/Etc: Es un lenguaje computacional formal para comunicar instrucciones a una maquina

Protocolo HTTP

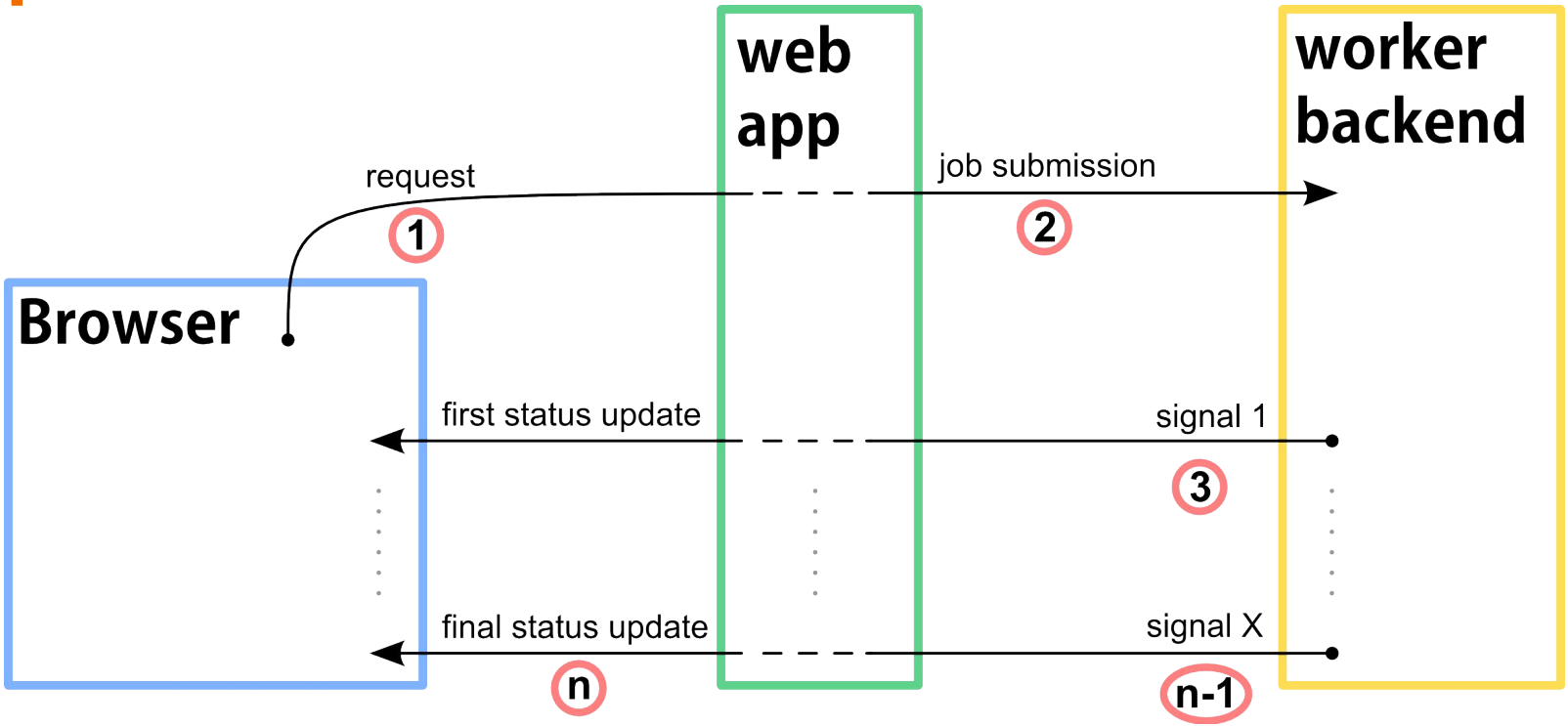


Fuente: etutorials.org

- **Paso 1:** Petición HTTP por parte del Cliente
- **Paso 2:** Servidor procesa la petición
- **Paso 3:** Servidor procesa un HTML
- **Paso 4:** Servidor entrega al servidor (con código 200)

- **Métodos HTTP:**
  - **GET**
  - **POST**
  - **OTROS**

Aplicaciones Web

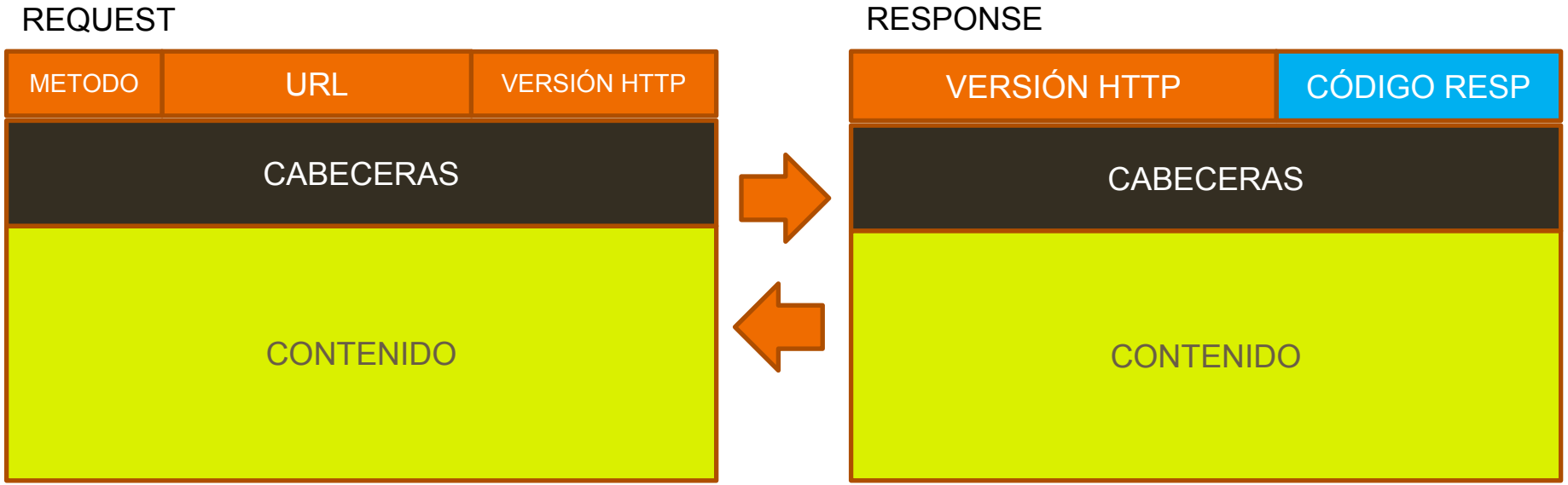


Fuente: http://stackoverflow.com/questions/12733985/job-processing-via-web-application-real-time-status-updates-and-backend-messagi/

Protocolo HTTP Y WebServers

- Estructura de una petición y respuesta HTTP
- Procesamiento por parte del WebServer
- Manejo de sesiones persistentes

Estructura petición HTTP



Request > método, url y versión

METODO

- OPTIONS
- GET
- POST
- HEAD
- PUT
- DELETE
- TRACE
- CONNECT

URL

Uniform Resource Locator

ej:
/wiki/Localizador_de_recursos_uniforme

VERSIÓN HTTP

Versión del protocolo que utilizarán ambos extremos

Request > cabeceras y contenido

CABECERAS

https://en.wikipedia.org/wiki/List_of_HTTP_header_fields

CONTENIDO

```
Host: pocae.tstgo.cl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=2293467E24BC6BA1EAC9BBFBF69463DF
Connection: close
```

Response > versión y código de respuestas

VERSIÓN HTTP

CODIGO RESP

Response > cabeceras y contenido

CABECERAS

CONTENIDO

Ejemplo Response HTTP

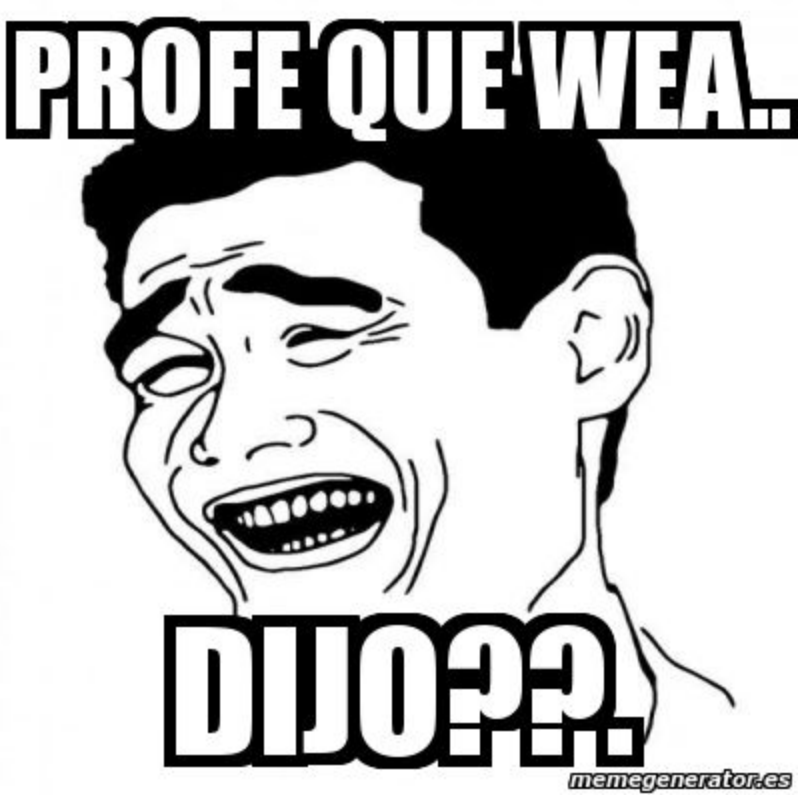
```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=F07210ADFF037B15033E3E4948F4766C; Path=/PortalCAE-WAR-MODULE
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 29 Dec 2016 23:36:35 GMT
Connection: close
Content-Length: 26755
```

```
<html>

        <head>
            <title>bip! en línea - tarjeta bip! - transantiago</title>
            <style type="text/css">
                <!--
                        body {
                                background-image: url(imagenes/bkng-page.gif);
                                margin-left: 1px;
                                margin-top: 1px;
                                margin-right: 1px;
                                margin-bottom: 1px;
                        }
                -->
                </style>
                <link href="general/estilos.css" rel="stylesheet" type="text/css">
                <script language="javascript" src="general/utilcli.js"></script>
                <script language="javascript" src="general/mm_menu.js"></script>
                <script type="text/javascript" src="general/jquery.js"></script>
            <script type="text/javascript" src="general/interface.js"></script>
            <script type="text/javascript" src="general/jquery.realperson.js"></script>
            <link href="general/jquery.realperson.css" rel="stylesheet" type="text/css">
        </head>

        <style type="text/css">
        #formInicioSesion br {
                margin-top: 0px;
```

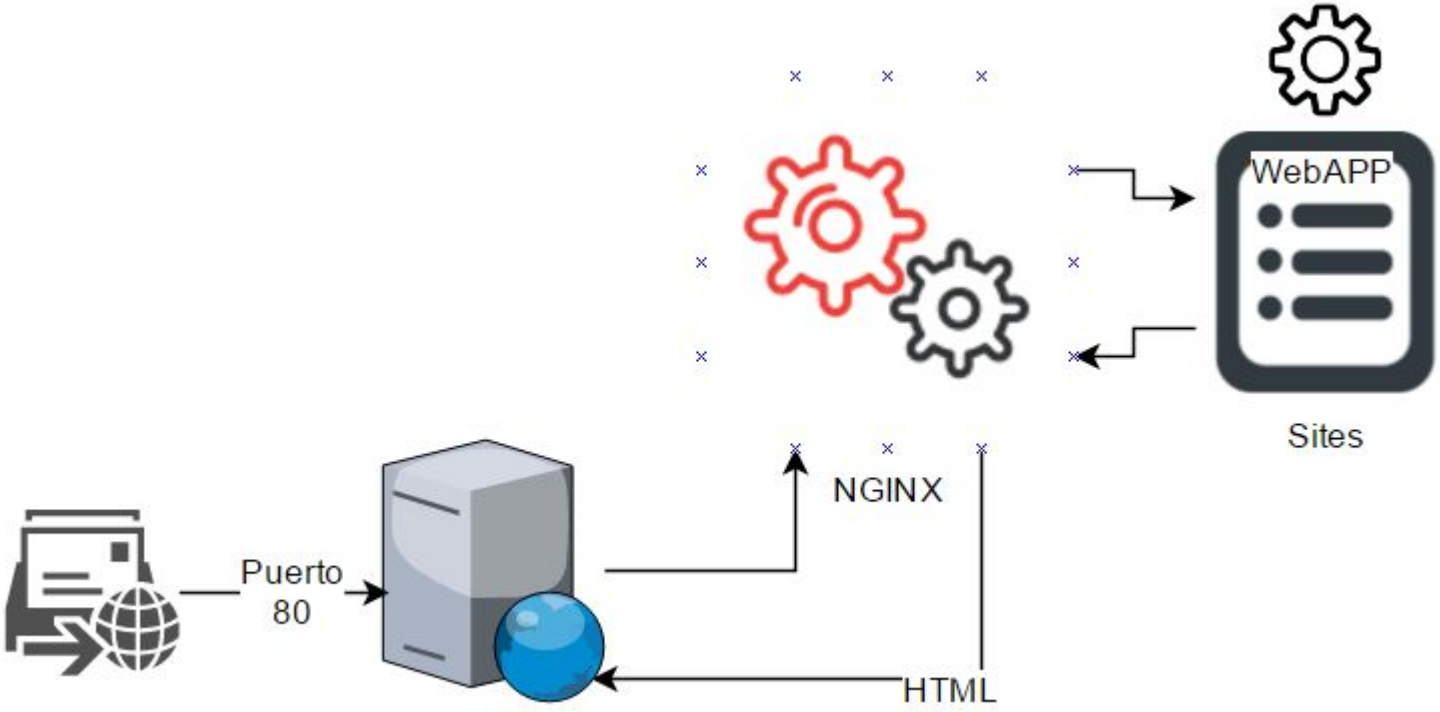
El protocolo HTTP es Stateless...


PROFE QUE WEA..
DIJO?.?.
memegenerator.es

Las conexiones son únicas, no guardan relación entre sí y no identifican al usuario...

Solución? Las malditas cookies...

Procesamiento WebServer



Veamos bajo el capó