Security of Web Applications

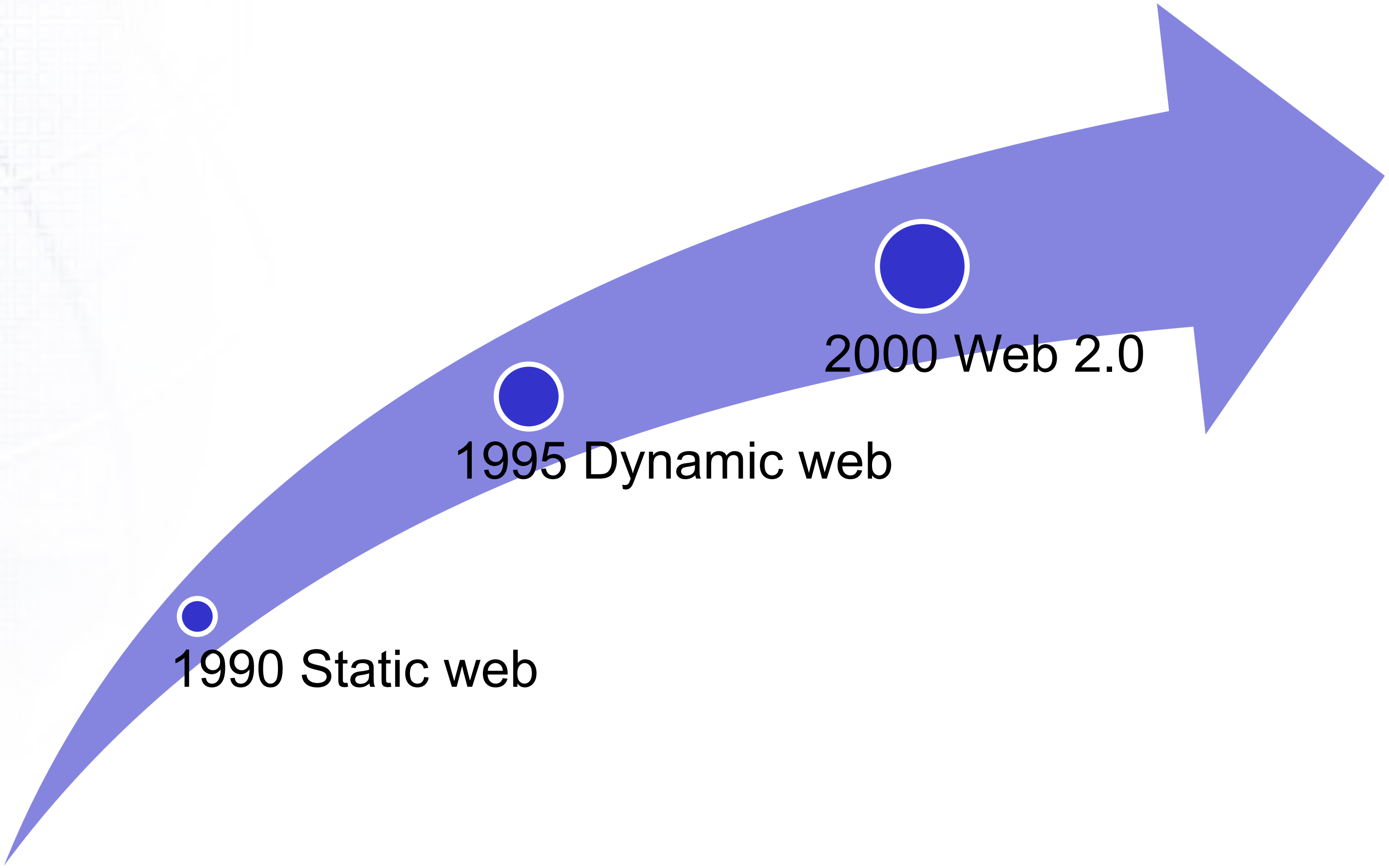
Lecture 1

Tamara Rezk

Objectives of this course

- Get the basis to understand web attacks and defenses
- Get acquainted with the top-ten most popular web vulnerabilities (OWASP top ten)

Web Evolution

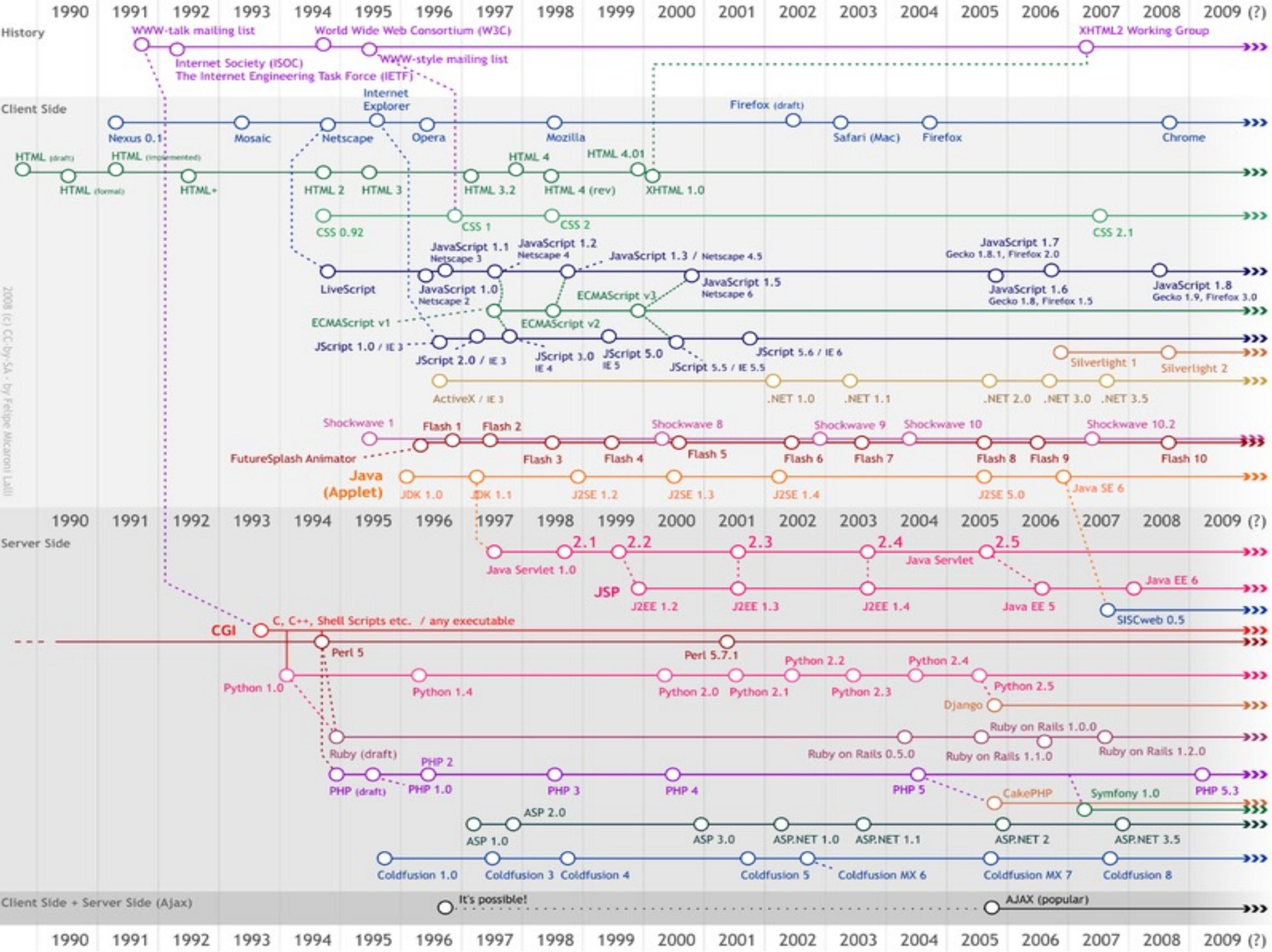


1990 Static web

1995 Dynamic web

2000 Web 2.0

see evolutionoftheweb.com


1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 (?)
History
WWW-talk mailing list
World Wide Web Consortium (W3C)
XHTML2 Working Group
Internet Society (ISOC)
The Internet Engineering Task Force (IETF)
WWW-style mailing list
Client Side
Internet Explorer
Firefox (draft)
Nexus 0.1
Mosaic
Netscape
Opera
Mozilla
Safari (Mac)
Firefox
Chrome
HTML (draft)
HTML (implemented)
HTML 4
HTML 4.01
HTML (formal)
HTML+
HTML 2
HTML 3
HTML 3.2
HTML 4 (rev)
XHTML 1.0
CSS 0.92
CSS 1
CSS 2
CSS 2.1
JavaScript 1.1 Netscape 3
JavaScript 1.2 Netscape 4
JavaScript 1.3 / Netscape 4.5
JavaScript 1.7 Gecko 1.8.1, Firefox 2.0
LiveScript
JavaScript 1.0 Netscape 2
JavaScript 1.5 Netscape 6
JavaScript 1.6 Gecko 1.8, Firefox 1.5
JavaScript 1.8 Gecko 1.9, Firefox 3.0
ECMAScript v3
ECMAScript v1
ECMAScript v2
JScript 1.0 / IE 3
JScript 2.0 / IE 3
JScript 3.0 IE 4
JScript 5.0 IE 5
JScript 5.5 / IE 5.5
JScript 5.6 / IE 6
Silverlight 1
Silverlight 2
ActiveX / IE 3
.NET 1.0
.NET 1.1
.NET 2.0
.NET 3.0
.NET 3.5
Shockwave 1
Flash 1
Flash 2
Shockwave 8
Shockwave 9
Shockwave 10
Shockwave 10.2
FutureSplash Animator
Flash 3
Flash 4
Flash 5
Flash 6
Flash 7
Flash 8
Flash 9
Flash 10
Java (Applet)
JDK 1.0
JDK 1.1
J2SE 1.2
J2SE 1.3
J2SE 1.4
J2SE 5.0
Java SE 6
2008 (c) CC-by-SA - by Felipe Micaroni Lalli
1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 (?)
Server Side
2.1
2.2
2.3
2.4
2.5
Java Servlet 1.0
Java Servlet
JSP
J2EE 1.2
J2EE 1.3
J2EE 1.4
Java EE 5
Java EE 6
SISCweb 0.5
CGI
C, C++, Shell Scripts etc. / any executable
- - -
Perl 5
Perl 5.7.1
Python 1.0
Python 1.4
Python 2.0
Python 2.1
Python 2.2
Python 2.3
Python 2.4
Python 2.5
Django
Ruby (draft)
Ruby on Rails 0.5.0
Ruby on Rails 1.0.0
Ruby on Rails 1.1.0
Ruby on Rails 1.2.0
PHP (draft)
PHP 2
PHP 1.0
PHP 3
PHP 4
PHP 5
CakePHP
Symfony 1.0
PHP 5.3
ASP 1.0
ASP 2.0
ASP 3.0
ASP.NET 1.0
ASP.NET 1.1
ASP.NET 2
ASP.NET 3.5
Coldfusion 1.0
Coldfusion 3
Coldfusion 4
Coldfusion 5
Coldfusion MX 6
Coldfusion MX 7
Coldfusion 8
Client Side + Server Side (Ajax)
It's possible!
AJAX (popular)
1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 (?)

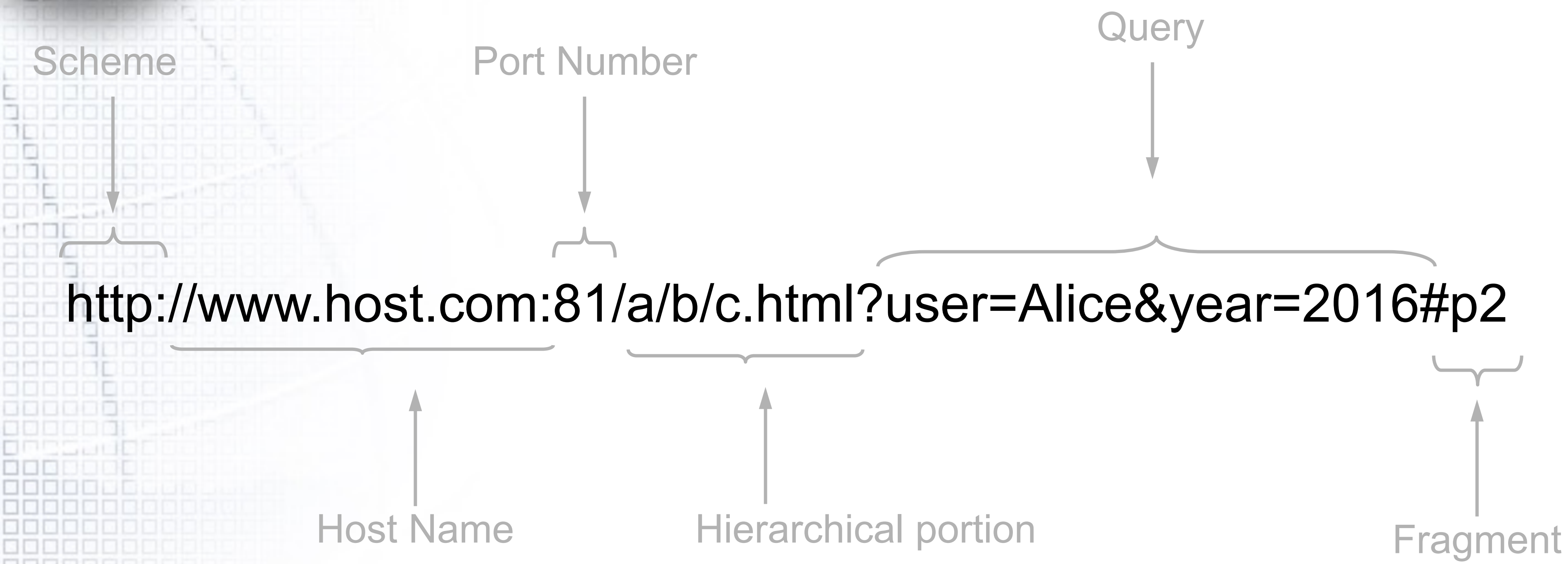
Web 1.0 The static web

1990:

First Server:
httpd
running at
Info.cern.ch
(NeXT computer)

First Browser:
WorldWideWeb

Uniform Resource Locators (URLs)



Query

Scheme

Port Number

http://www.host.com:81/a/b/c.html?user=Alice&year=2016#p2

Host Name

Hierarchical portion

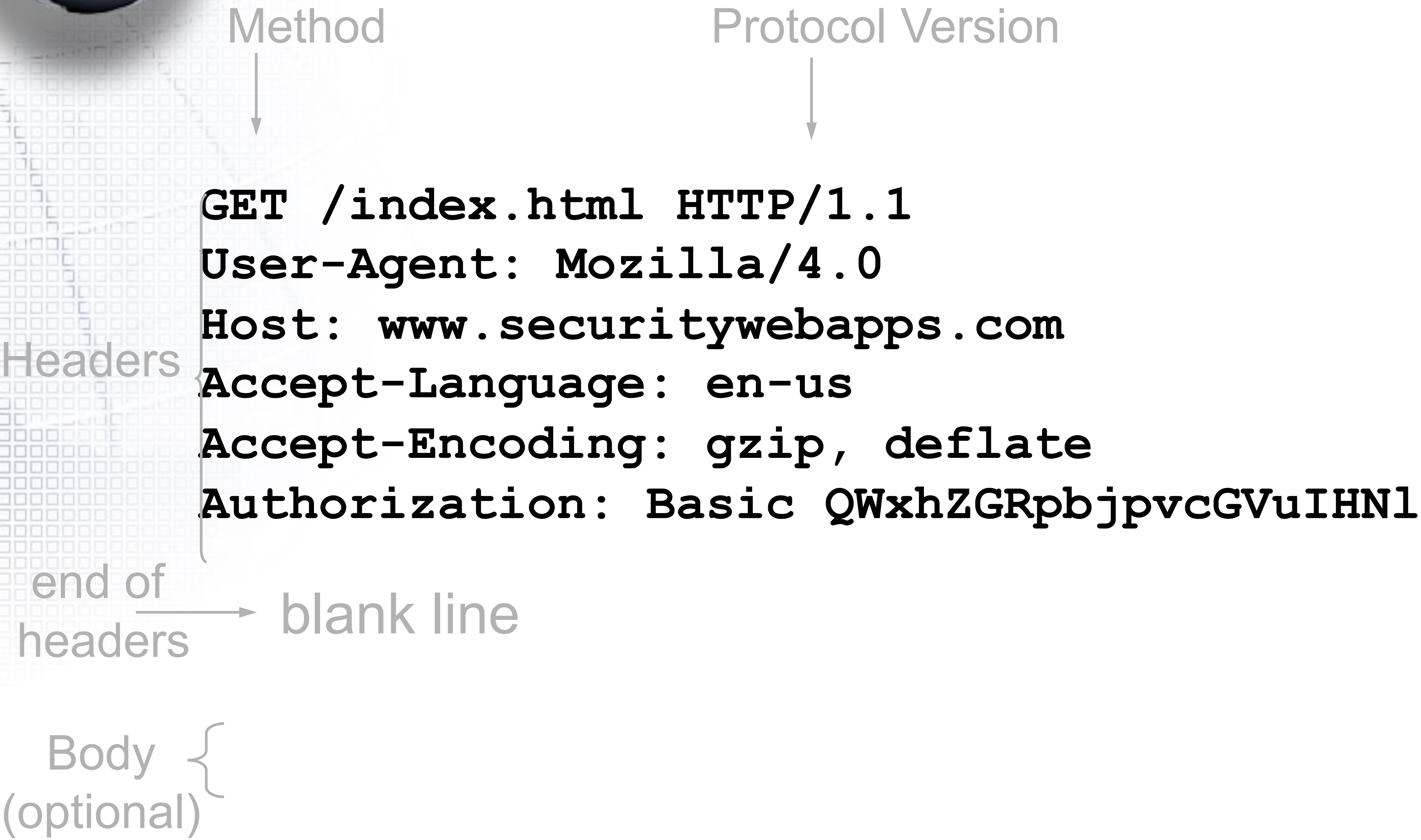
Fragment

HTTP: HyperText Transfer Protocol

- HTTP important characteristic: **no state**
- request/response - each request is independent

- HTTP header: header section of requests and responses, parameters of the HTTP transaction

HTTP Request Message



Method

Protocol Version

```
GET /index.html HTTP/1.1
User-Agent: Mozilla/4.0
Host: www.securitywebapps.com
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Authorization: Basic QWxhZGRpbjpvcGVuIHNl
```

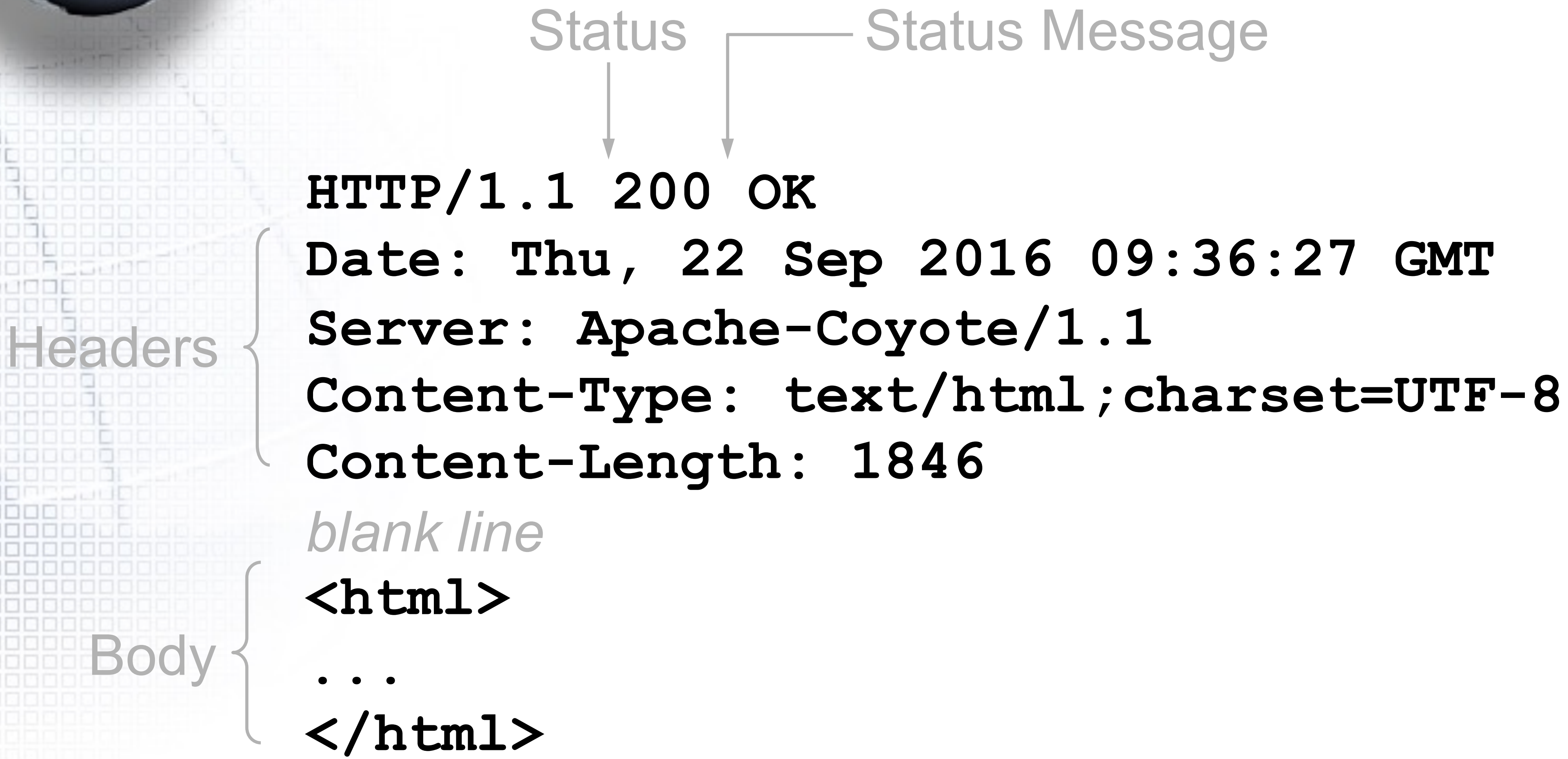
Headers

end of headers

blank line

Body (optional)

HTTP Response Message



Status

Status Message

```
HTTP/1.1 200 OK
Date: Thu, 22 Sep 2016 09:36:27 GMT
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 1846
```

Headers

blank line

```
<html>
...
</html>
```

Body

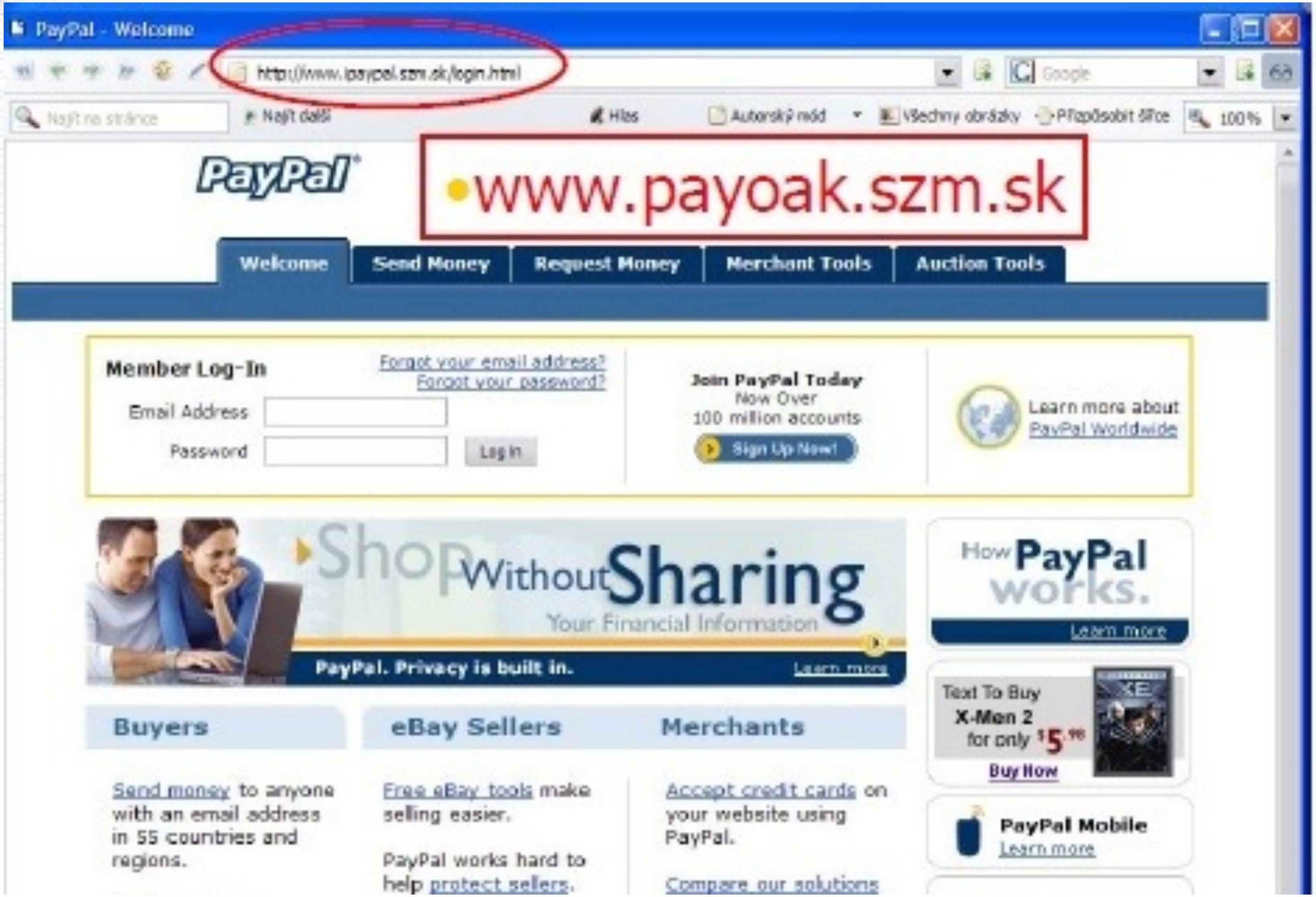
Phishing attacks

www.paypal.com

www.payoak.szm.sk

- Be aware of URLs that are shown in the browser
- or links that are clicked!

Phishing attacks



http://www.ipaypal.szm.sk/login.html

•www.payoak.szm.sk

Member Log-In

Forgot your email address?
Forgot your password?

Email Address

Password

Join PayPal Today
Now Over
100 million accounts

Learn more about
PayPal Worldwide

Shop Without Sharing
Your Financial Information

PayPal. Privacy is built in.

How PayPal works.

Text To Buy
X-Men 2
for only $5.98

PayPal Mobile

Buyers

Send money to anyone with an email address in 55 countries and regions.

eBay Sellers

Free eBay tools make selling easier.

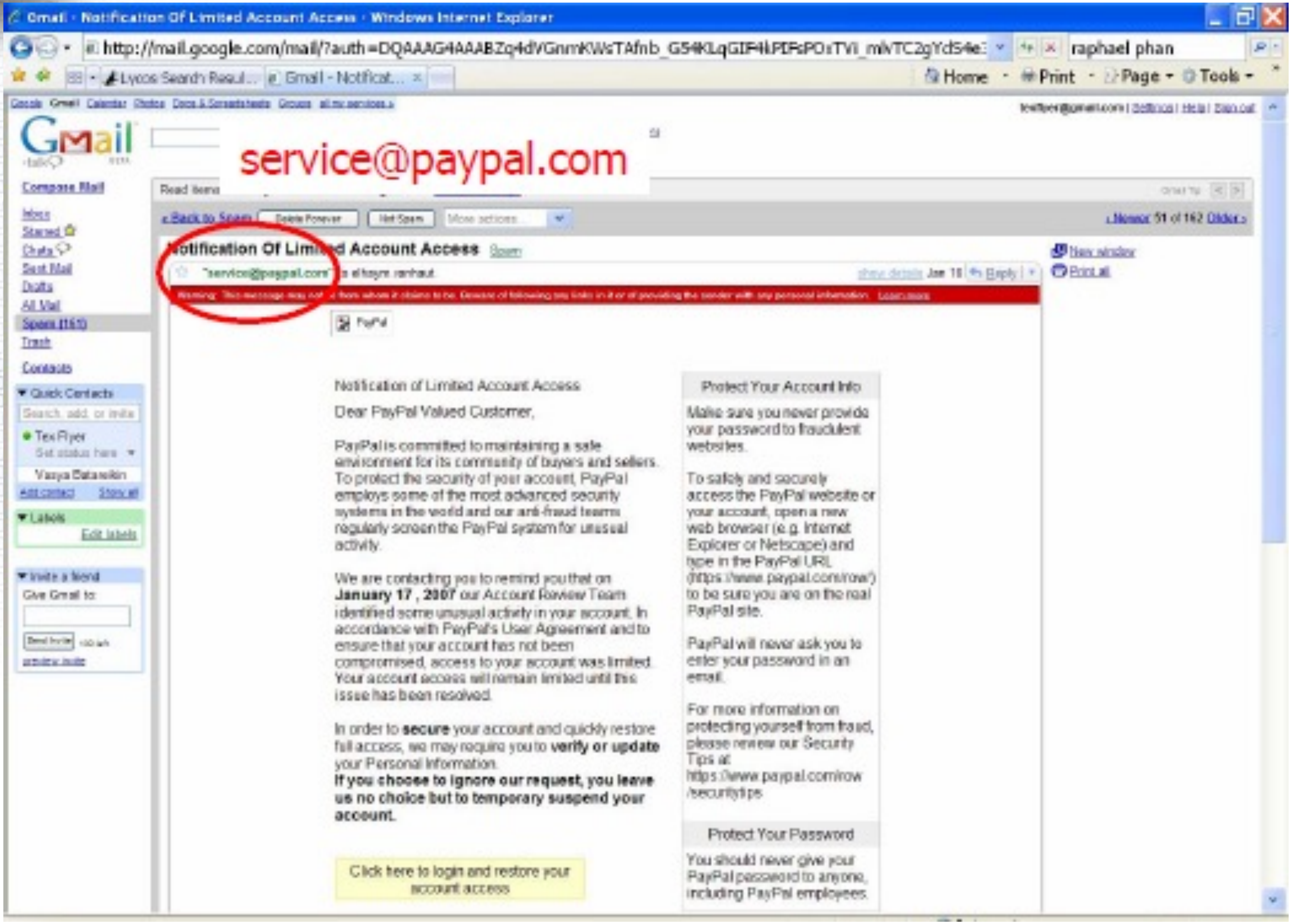
PayPal works hard to help protect sellers.

Merchants

Accept credit cards on your website using PayPal.

Compare our solutions

Phishing attacks: also emails with false senders



service@paypal.com

Notification Of Limited Account Access Spam

"service@paypal.com"

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. Learn more

Notification of Limited Account Access

Dear PayPal Valued Customer,

PayPal is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account, PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

We are contacting you to remind you that on **January 17 , 2007** our Account Review Team identified some unusual activity in your account. In accordance with PayPal's User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved.

In order to **secure** your account and quickly restore full access, we may require you to **verify or update** your Personal Information.
If you choose to ignore our request, you leave us no choice but to temporary suspend your account.

Click here to login and restore your account access

Protect Your Account Info

Make sure you never provide your password to fraudulent websites.

To safely and securely access the PayPal website or your account, open a new web browser (e.g. Internet Explorer or Netscape) and type in the PayPal URL (https://www.paypal.com/row/) to be sure you are on the real PayPal site.

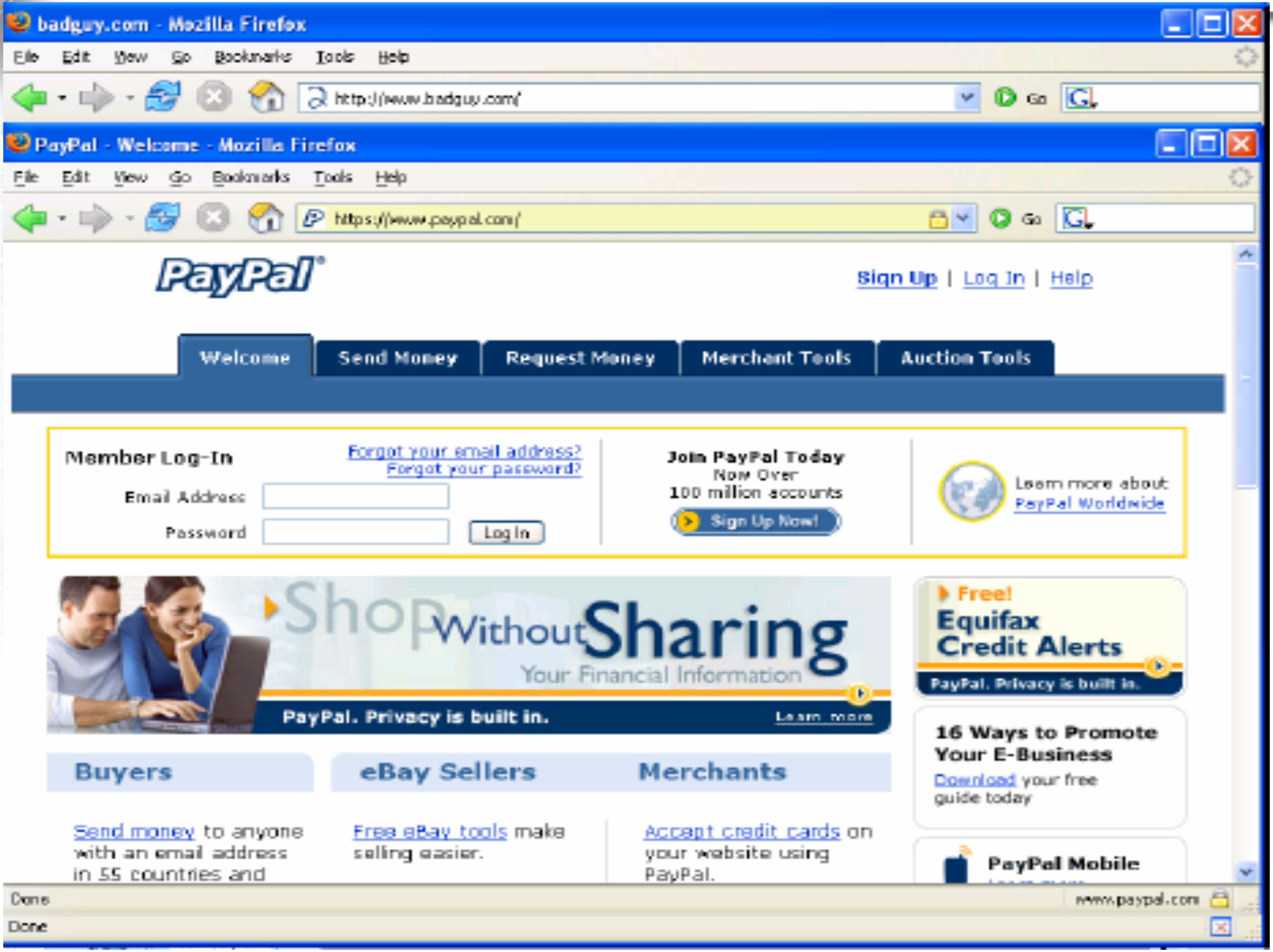
PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at https://www.paypal.com/row/securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

And even this!



badguy.com - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.badguy.com/

PayPal - Welcome - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://www.paypal.com/

Member Log-In

Forgot your email address?
Forgot your password?

Email Address

Password

Log In

Join PayPal Today
Now Over
100 million accounts

Sign Up Now!

Learn more about PayPal Worldwide

Shop Without Sharing
Your Financial Information
PayPal. Privacy is built in.
Learn more
Free!
Equifax
Credit Alerts
PayPal. Privacy is built in.

16 Ways to Promote Your E-Business

Download your free guide today

PayPal Mobile

Buyers

eBay Sellers

Merchants

Send money to anyone with an email address in 55 countries and

Free eBay tools make selling easier.

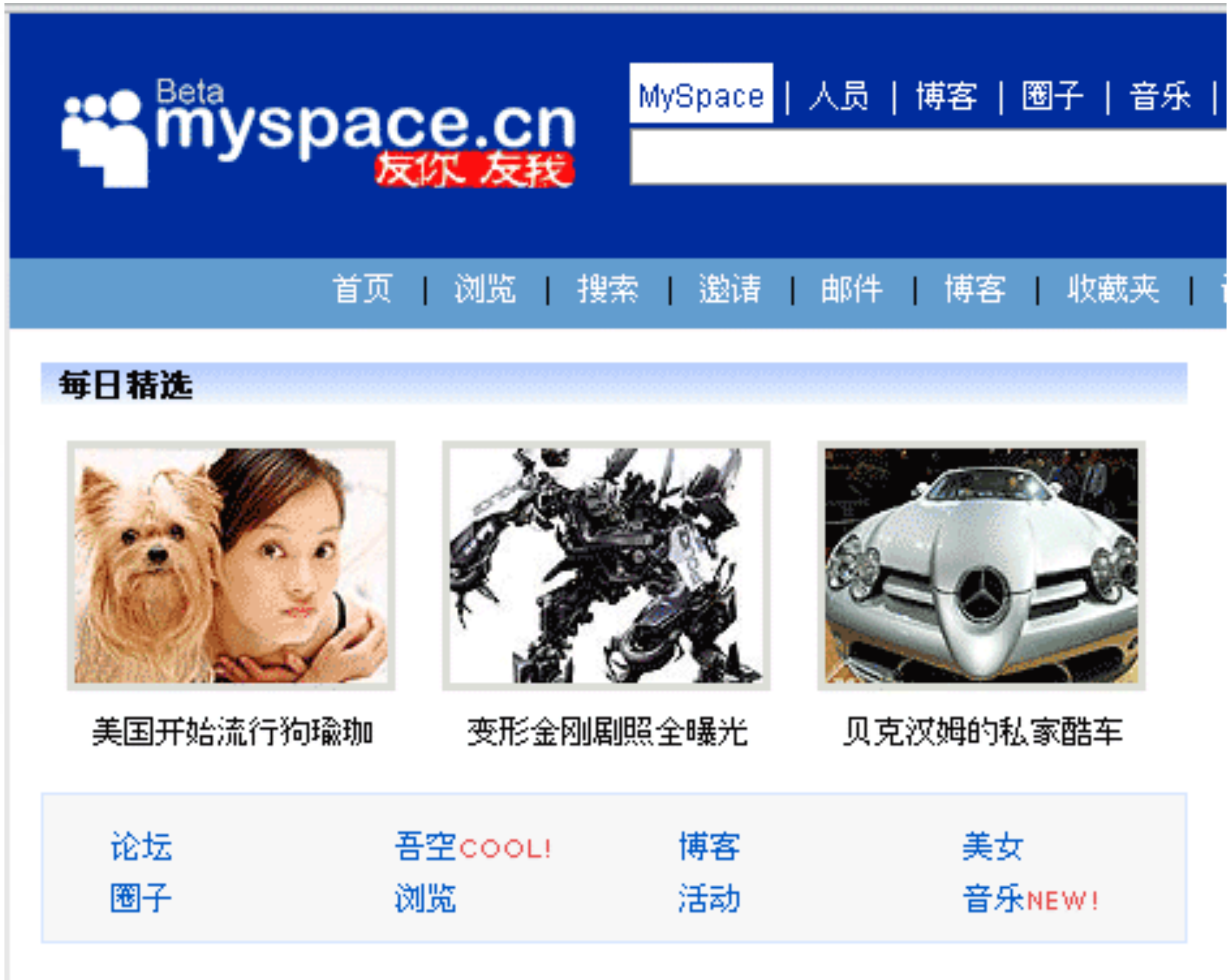
Accept credit cards on your website using PayPal.

Done

www.paypal.com

Done

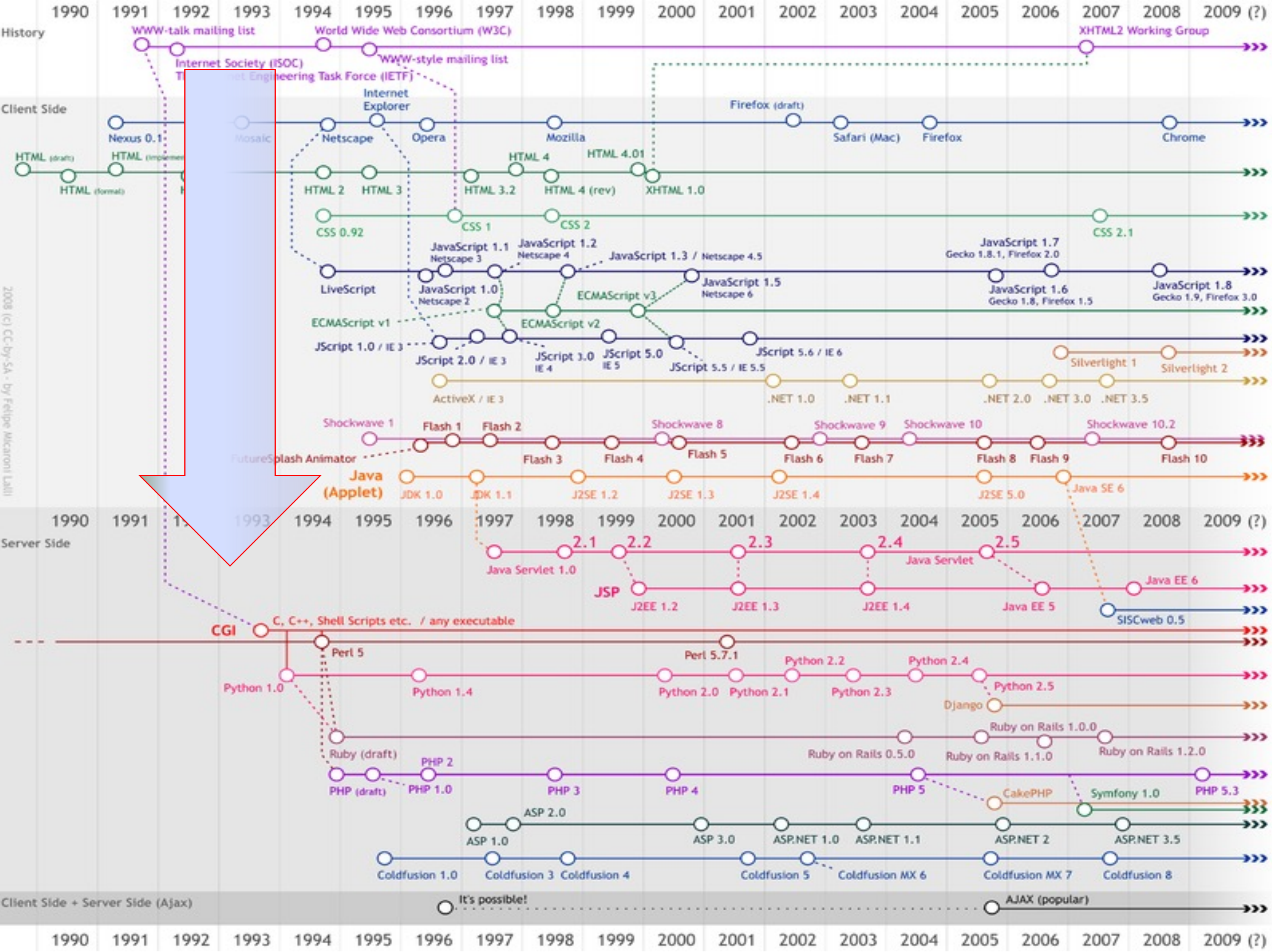
A phishing attack to MySpace



In 2006, a worm altered links to direct MySpace users to evil websites

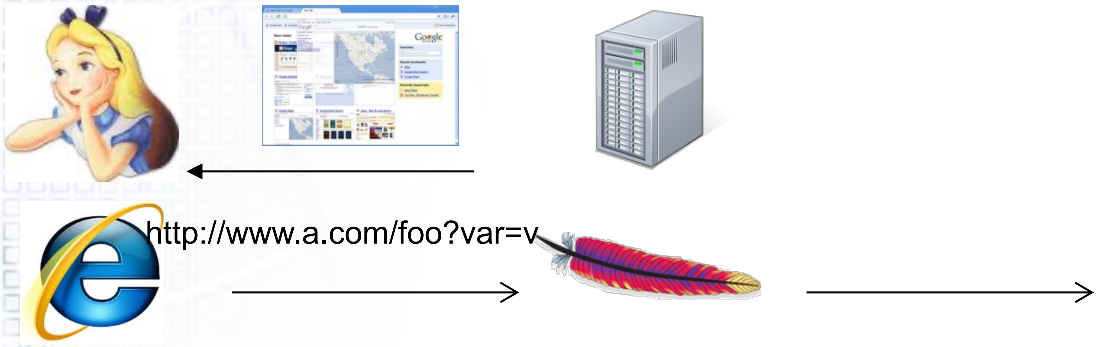
Phishing Solutions

- Use https (created in 1994 by Netscape)
- Verify carefully the URL


1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 (?)
History
WWW-talk mailing list
World Wide Web Consortium (W3C)
XHTML2 Working Group
Internet Society (ISOC)
The Internet Engineering Task Force (IETF)
WWW-style mailing list
Client Side
Internet Explorer
Firefox (draft)
Nexus 0.1
Mosaic
Netscape
Opera
Mozilla
Safari (Mac)
Firefox
Chrome
HTML (draft)
HTML (implemented)
HTML (formal)
HTML 2
HTML 3
HTML 3.2
HTML 4
HTML 4 (rev)
HTML 4.01
XHTML 1.0
CSS 0.92
CSS 1
CSS 2
CSS 2.1
JavaScript 1.1 Netscape 3
JavaScript 1.2 Netscape 4
JavaScript 1.3 / Netscape 4.5
JavaScript 1.7 Gecko 1.8.1, Firefox 2.0
LiveScript
JavaScript 1.0 Netscape 2
JavaScript 1.5 Netscape 6
JavaScript 1.6 Gecko 1.8, Firefox 1.5
JavaScript 1.8 Gecko 1.9, Firefox 3.0
ECMAScript v1
ECMAScript v2
ECMAScript v3
JScript 1.0 / IE 3
JScript 2.0 / IE 3
JScript 3.0 IE 4
JScript 5.0 IE 5
JScript 5.5 / IE 5.5
JScript 5.6 / IE 6
Silverlight 1
Silverlight 2
ActiveX / IE 3
.NET 1.0
.NET 1.1
.NET 2.0
.NET 3.0
.NET 3.5
Shockwave 1
Flash 1
Flash 2
Shockwave 8
Shockwave 9
Shockwave 10
Shockwave 10.2
FutureSplash Animator
Flash 3
Flash 4
Flash 5
Flash 6
Flash 7
Flash 8
Flash 9
Flash 10
Java (Applet)
JDK 1.0
JDK 1.1
J2SE 1.2
J2SE 1.3
J2SE 1.4
J2SE 5.0
Java SE 6
2008 (c) CC-by-SA - by Felipe Micaroni Lalli
Server Side
2.1
2.2
2.3
2.4
2.5
Java Servlet 1.0
Java Servlet
JSP
J2EE 1.2
J2EE 1.3
J2EE 1.4
Java EE 5
Java EE 6
SISCweb 0.5
CGI
C, C++, Shell Scripts etc. / any executable
- - -
Perl 5
Perl 5.7.1
Python 1.0
Python 1.4
Python 2.0
Python 2.1
Python 2.2
Python 2.3
Python 2.4
Python 2.5
Django
Ruby (draft)
Ruby on Rails 0.5.0
Ruby on Rails 1.0.0
Ruby on Rails 1.1.0
Ruby on Rails 1.2.0
PHP (draft)
PHP 1.0
PHP 2
PHP 3
PHP 4
PHP 5
CakePHP
Symfony 1.0
PHP 5.3
ASP 1.0
ASP 2.0
ASP 3.0
ASP.NET 1.0
ASP.NET 1.1
ASP.NET 2
ASP.NET 3.5
Coldfusion 1.0
Coldfusion 3
Coldfusion 4
Coldfusion 5
Coldfusion MX 6
Coldfusion MX 7
Coldfusion 8
Client Side + Server Side (Ajax)
It's possible!
AJAX (popular)

Web 1.0 Applications

1993: The Web becomes less static

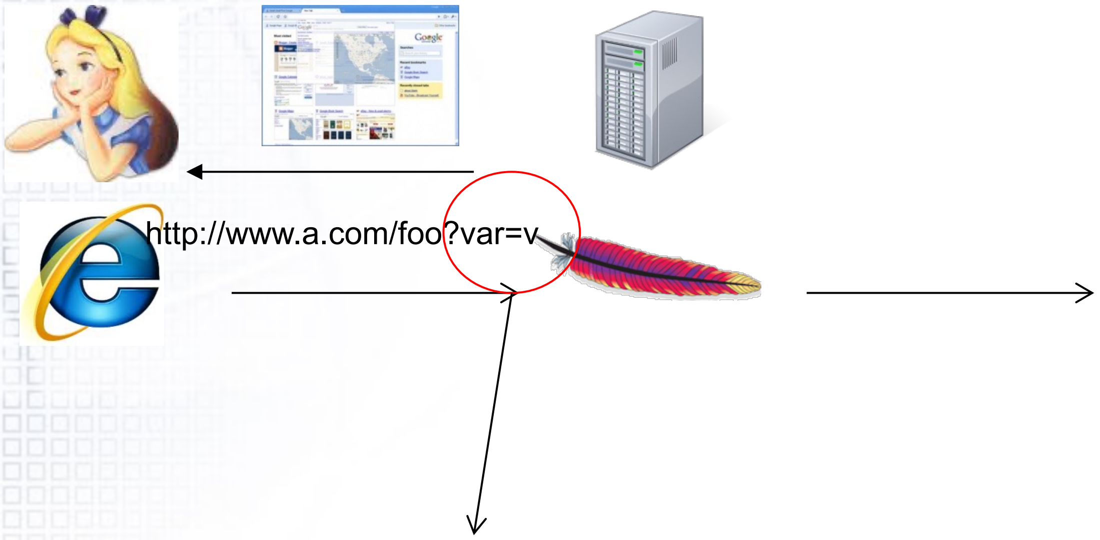


http://www.a.com/foo?var=v

http://www.a.com	a.cgi
http://www.b.com	b.cgi
http://www.c.com	c.cgi

Web 1.0 Applications

1993: The Web becomes less static



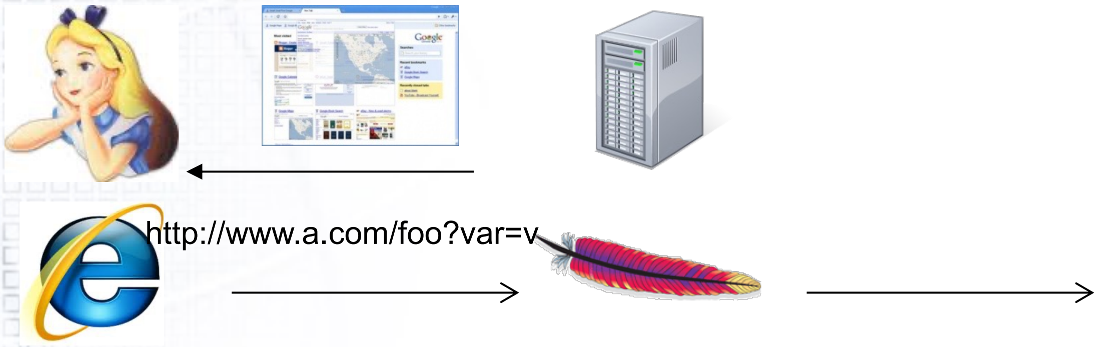
parameters

http://www.a.com	a.cgi
http://www.b.com	b.cgi
http://www.c.com	c.cgi

Example hello2.php

Web 1.0 Applications

1993: The Web becomes less static



http://www.a.com	a.cgi
http://www.b.com	b.cgi
http://www.c.com	c.cgi

Technologies:
Web Browser, Web Server,
HTTP , HTML
CGI: Common Gateway Interface

1994: World Wide Web Consortium (W3C)
http://validator.w3.org/

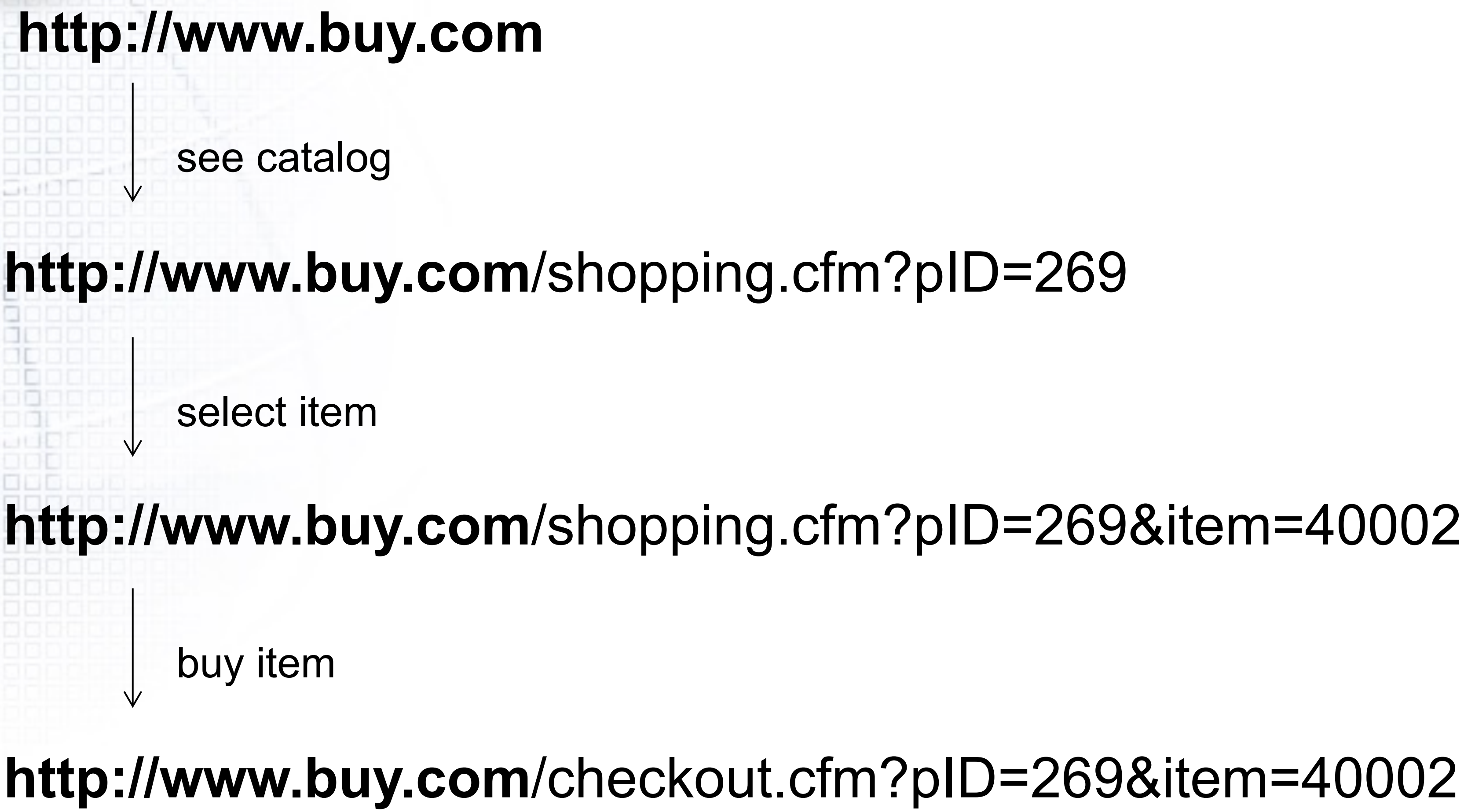
HTTP is stateless

HOW TO KEEP STATE INFORMATION ON SESSIONS?

How to keep state on sessions?

- URL
- HTML
- COOKIES

HTTP: Session in URL Example



http://www.buy.com

↓ see catalog

http://www.buy.com/shopping.cfm?pID=269

↓ select item

http://www.buy.com/shopping.cfm?pID=269&item=40002

↓ buy item

http://www.buy.com/checkout.cfm?pID=269&item=40002

Since HTTP is stateless all session information is saved in the URL

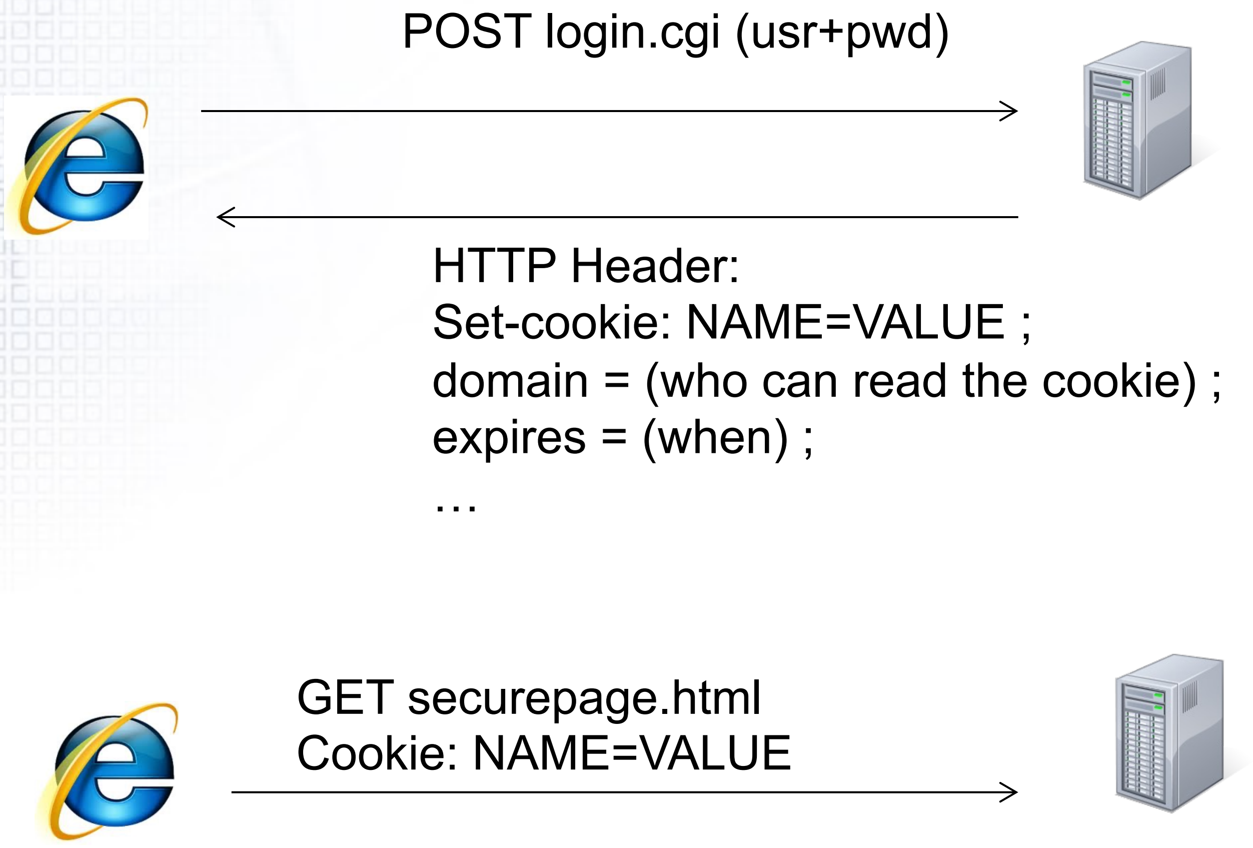
HTTP: Session in hidden field Example

Why not to store sensitive information on the client side?
Integrity violation: Dansie Shopping Cart (2006)

```
<FORM METHOD=POST
ACTION="http://www.dansie.net/cgi-bin/scripts/cart.pl">
Black Leather purse with leather straps<BR>Price:
$20.00<BR>
<INPUT TYPE=HIDDEN NAME=name VALUE="Black leather purse">
<INPUT TYPE=HIDDEN NAME=price VALUE="20.00">
<INPUT TYPE=HIDDEN NAME=sh VALUE="1">
<INPUT TYPE=HIDDEN NAME=img VALUE="purse.jpg">
<INPUT TYPE=HIDDEN NAME=custom1 VALUE="Black leather
purse
with leather straps">
<INPUT TYPE=SUBMIT NAME="add" VALUE="Put in Shopping
Cart">
</FORM>
```

HTTP : COOKIES

A cookie resides in the disk and is created by the web browser



POST login.cgi (usr+pwd)

HTTP Header:
Set-cookie: NAME=VALUE ;
domain = (who can read the cookie) ;
expires = (when) ;
…

GET securepage.html
Cookie: NAME=VALUE

HTTP : COOKIES

- HTTP does not have state, cookies add state
- Cookies are useful for:
  - Authentication
    - to know if a user has authenticated in the past
  - Personalization
    - recognize the user since last visit
  - Tracking
    - analyze the behaviour of the user

HTTP : COOKIES

Only the site that creates the cookie can read it

HTTP : COOKIES

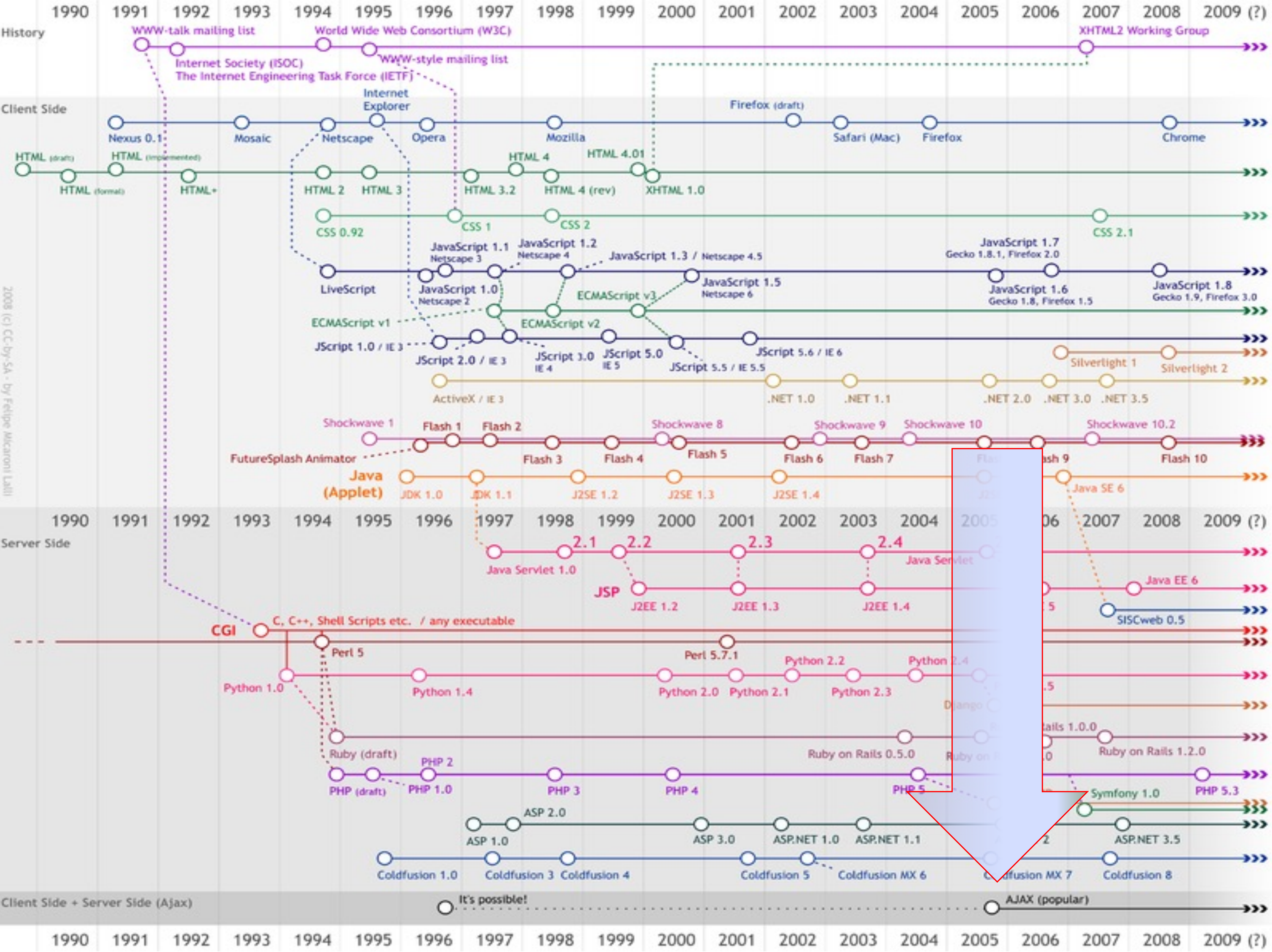
```
set-cookie(“amount”,$amount);
```

```
Content-type:text/html
Cookie: Amount = 20$
```

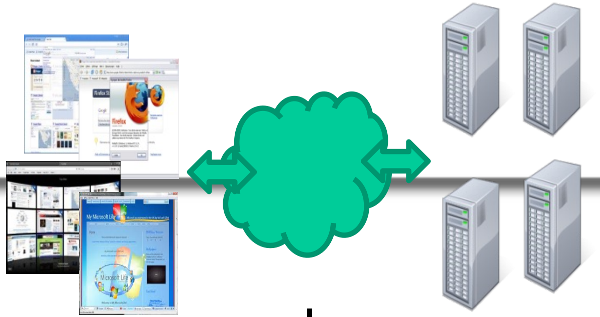
To make it secure it is necessary to add a “MAC” (message authenticated code) to the amount:

```
Cookie: Amount = 20$; HMAC(ServerKey, 20)
```

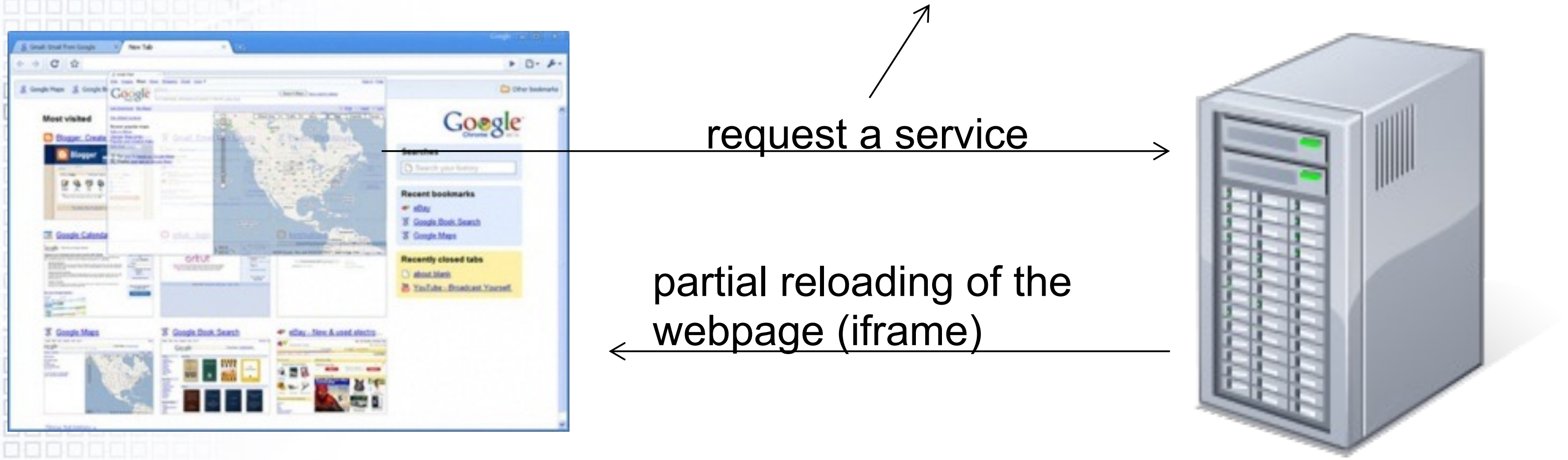
Example
cookie.php/2


1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 (?)
History
WWW-talk mailing list
World Wide Web Consortium (W3C)
XHTML2 Working Group
Internet Society (ISOC)
The Internet Engineering Task Force (IETF)
WWW-style mailing list
Client Side
Internet Explorer
Firefox (draft)
Nexus 0.1
Mosaic
Netscape
Opera
Mozilla
Safari (Mac)
Firefox
Chrome
HTML (draft)
HTML (implemented)
HTML 4
HTML 4.01
HTML (formal)
HTML+
HTML 2
HTML 3
HTML 3.2
HTML 4 (rev)
XHTML 1.0
CSS 0.92
CSS 1
CSS 2
CSS 2.1
JavaScript 1.1 Netscape 3
JavaScript 1.2 Netscape 4
JavaScript 1.3 / Netscape 4.5
JavaScript 1.7 Gecko 1.8.1, Firefox 2.0
LiveScript
JavaScript 1.0 Netscape 2
JavaScript 1.5 Netscape 6
JavaScript 1.6 Gecko 1.8, Firefox 1.5
JavaScript 1.8 Gecko 1.9, Firefox 3.0
ECMAScript v3
ECMAScript v1
ECMAScript v2
JScript 1.0 / IE 3
JScript 2.0 / IE 3
JScript 3.0 IE 4
JScript 5.0 IE 5
JScript 5.5 / IE 5.5
JScript 5.6 / IE 6
Silverlight 1
Silverlight 2
ActiveX / IE 3
.NET 1.0
.NET 1.1
.NET 2.0
.NET 3.0
.NET 3.5
Shockwave 1
Flash 1
Flash 2
Shockwave 8
Shockwave 9
Shockwave 10
Shockwave 10.2
FutureSplash Animator
Flash 3
Flash 4
Flash 5
Flash 6
Flash 7
Flash 9
Flash 10
Java (Applet)
JDK 1.0
JDK 1.1
J2SE 1.2
J2SE 1.3
J2SE 1.4
Java SE 6
Server Side
2.1
2.2
2.3
2.4
Java Servlet 1.0
Java Servlet
JSP
J2EE 1.2
J2EE 1.3
J2EE 1.4
Java EE 6
SISCweb 0.5
CGI
C, C++, Shell Scripts etc. / any executable
Perl 5
Perl 5.7.1
Python 1.0
Python 1.4
Python 2.0
Python 2.1
Python 2.2
Python 2.3
Python 2.4
Django
Ruby (draft)
Ruby on Rails 0.5.0
Rails 1.0.0
Ruby on Rails 1.2.0
PHP 2
PHP (draft)
PHP 1.0
PHP 3
PHP 4
PHP 5
Symfony 1.0
PHP 5.3
ASP 2.0
ASP 1.0
ASP 3.0
ASP.NET 1.0
ASP.NET 1.1
ASP.NET 3.5
Coldfusion 1.0
Coldfusion 3
Coldfusion 4
Coldfusion 5
Coldfusion MX 6
Coldfusion MX 7
Coldfusion 8
Client Side + Server Side (Ajax)
It's possible!
AJAX (popular)
2008 (c) CC-by-SA - by Felipe Micaroni Lalli

Web 2.0 Applications



2004: AJAX (Asynchronous Javascript and XML) becomes popular, social sites emerge



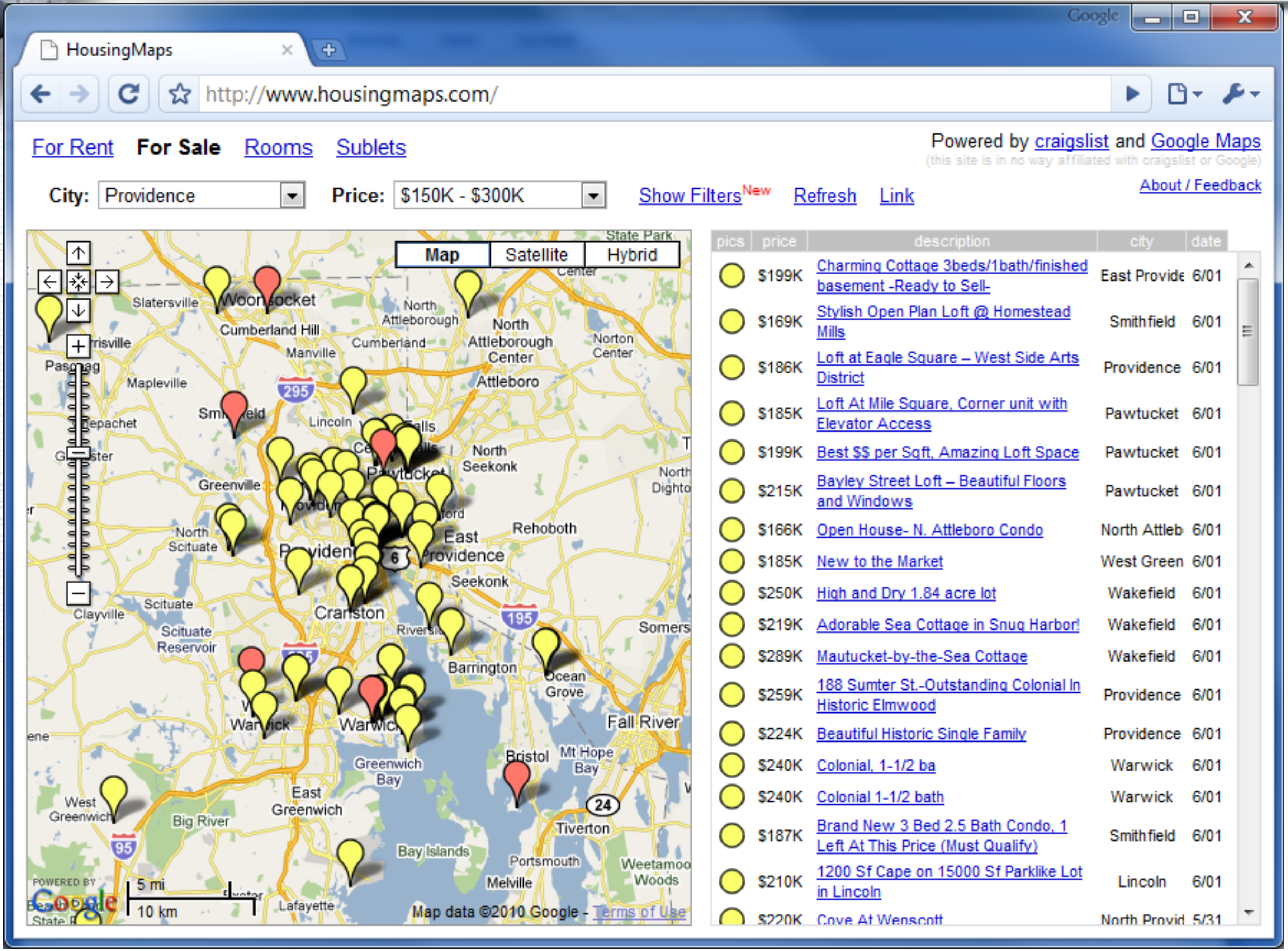
XMLHttpRequest object for asynchronous communication

request a service

partial reloading of the webpage (iframe)

Technologies:
Web Browser, Web Server,
HTTP , HTML
CGI: Common Gateway Interface
AJAX : Javascript, CSS, XML, DOM, XMLHttpRequest

Mashups: HousingMaps, 2005



For Rent **For Sale** Rooms Sublets

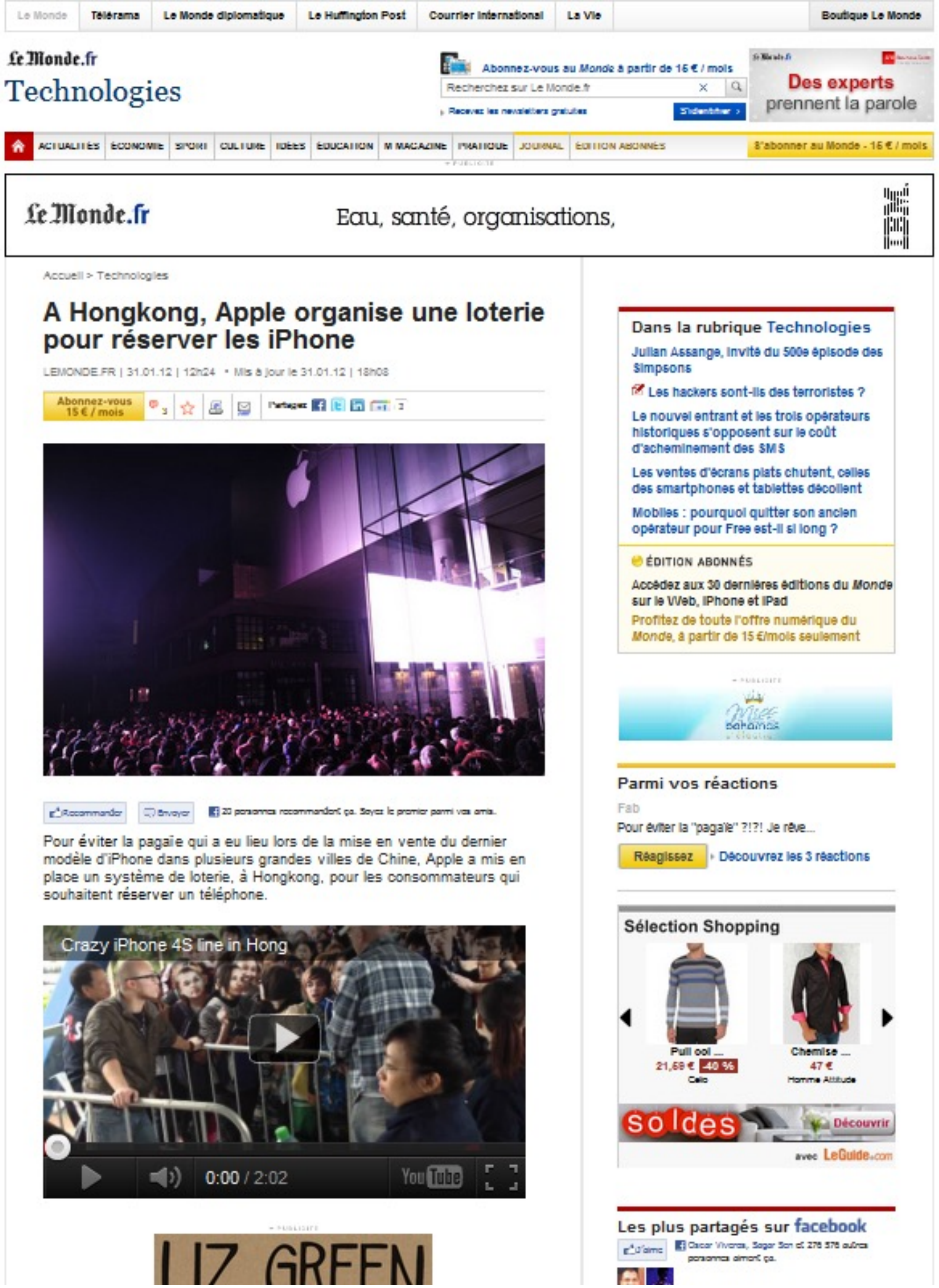
Powered by craigslist and Google Maps
(this site is in no way affiliated with craigslist or Google)

City: Providence Price: $150K - $300K Show Filters New Refresh Link

About / Feedback

pics	price	description	city	date
○	$199K	Charming Cottage 3beds/1bath/finished basement -Ready to Sell-	East Provide	6/01
○	$169K	Stylish Open Plan Loft @ Homestead Mills	Smithfield	6/01
○	$186K	Loft at Eagle Square – West Side Arts District	Providence	6/01
○	$185K	Loft At Mile Square, Corner unit with Elevator Access	Pawtucket	6/01
○	$199K	Best $$ per Sqft, Amazing Loft Space	Pawtucket	6/01
○	$215K	Bayley Street Loft – Beautiful Floors and Windows	Pawtucket	6/01
○	$166K	Open House- N. Attleboro Condo	North Attleb	6/01
○	$185K	New to the Market	West Green	6/01
○	$250K	High and Dry 1.84 acre lot	Wakefield	6/01
○	$219K	Adorable Sea Cottage in Snug Harbor!	Wakefield	6/01
○	$289K	Mautucket-by-the-Sea Cottage	Wakefield	6/01
○	$259K	188 Sumter St.-Outstanding Colonial In Historic Elmwood	Providence	6/01
○	$224K	Beautiful Historic Single Family	Providence	6/01
○	$240K	Colonial, 1-1/2 ba	Warwick	6/01
○	$240K	Colonial 1-1/2 bath	Warwick	6/01
○	$187K	Brand New 3 Bed 2.5 Bath Condo, 1 Left At This Price (Must Qualify)	Smithfield	6/01
○	$210K	1200 Sf Cape on 15000 Sf Parklike Lot in Lincoln	Lincoln	6/01
○	$220K	Cove At Wenscott	North Provid	5/31

Le Monde is a mashup



Le Monde | Télérama | Le Monde diplomatique | Le Huffington Post | Courrier international | La Vie | Boutique Le Monde

Le Monde.fr
Technologies

Abonnez-vous au *Monde* à partir de 15 € / mois

Recherchez sur Le Monde.fr

Recevez les newsletters gratuites

S'identifier ›

Des experts prennent la parole

ACTUALITÉS | ÉCONOMIE | SPORT | CULTURE | IDÉES | ÉDUCATION | M MAGAZINE | PRATIQUE | JOURNAL | ÉDITION ABONNÉS | S'abonner au Monde - 15 € / mois

PUBLICITÉ

Le Monde.fr Eau, santé, organisations,

Accueil > Technologies

A Hongkong, Apple organise une loterie pour réserver les iPhone

LEMONDE.FR | 31.01.12 | 12h24 • Mis à jour le 31.01.12 | 18h08

Abonnez-vous 15 € / mois | 3 | Partagez

Recommander | Envoyer | 20 personnes recommandent ça. Soyez le premier parmi vos amis.

Pour éviter la pagaie qui a eu lieu lors de la mise en vente du dernier modèle d'iPhone dans plusieurs grandes villes de Chine, Apple a mis en place un système de loterie, à Hongkong, pour les consommateurs qui souhaitent réserver un téléphone.

Crazy iPhone 4S line in Hong

0:00 / 2:02

PUBLICITÉ

LIZ GREEN

Dans la rubrique Technologies

Julian Assange, invité du 500e épisode des Simpsons

Les hackers sont-ils des terroristes ?

Le nouvel entrant et les trois opérateurs historiques s'opposent sur le coût d'acheminement des SMS

Les ventes d'écrans plats chutent, celles des smartphones et tablettes décollent

Mobiles : pourquoi quitter son ancien opérateur pour Free est-il si long ?

ÉDITION ABONNÉS

Accédez aux 30 dernières éditions du *Monde* sur le Web, iPhone et iPad

Profitez de toute l'offre numérique du *Monde*, à partir de 15 €/mois seulement

PUBLICITÉ

Parmi vos réactions

Fab

Pour éviter la "pagaïe" ?!?! Je rêve...

Réagissez › Découvrez les 3 réactions

Sélection Shopping

Pull col ...	Chemise ...
21,59 € -40 %	47 €
Celio	Homme Attitude

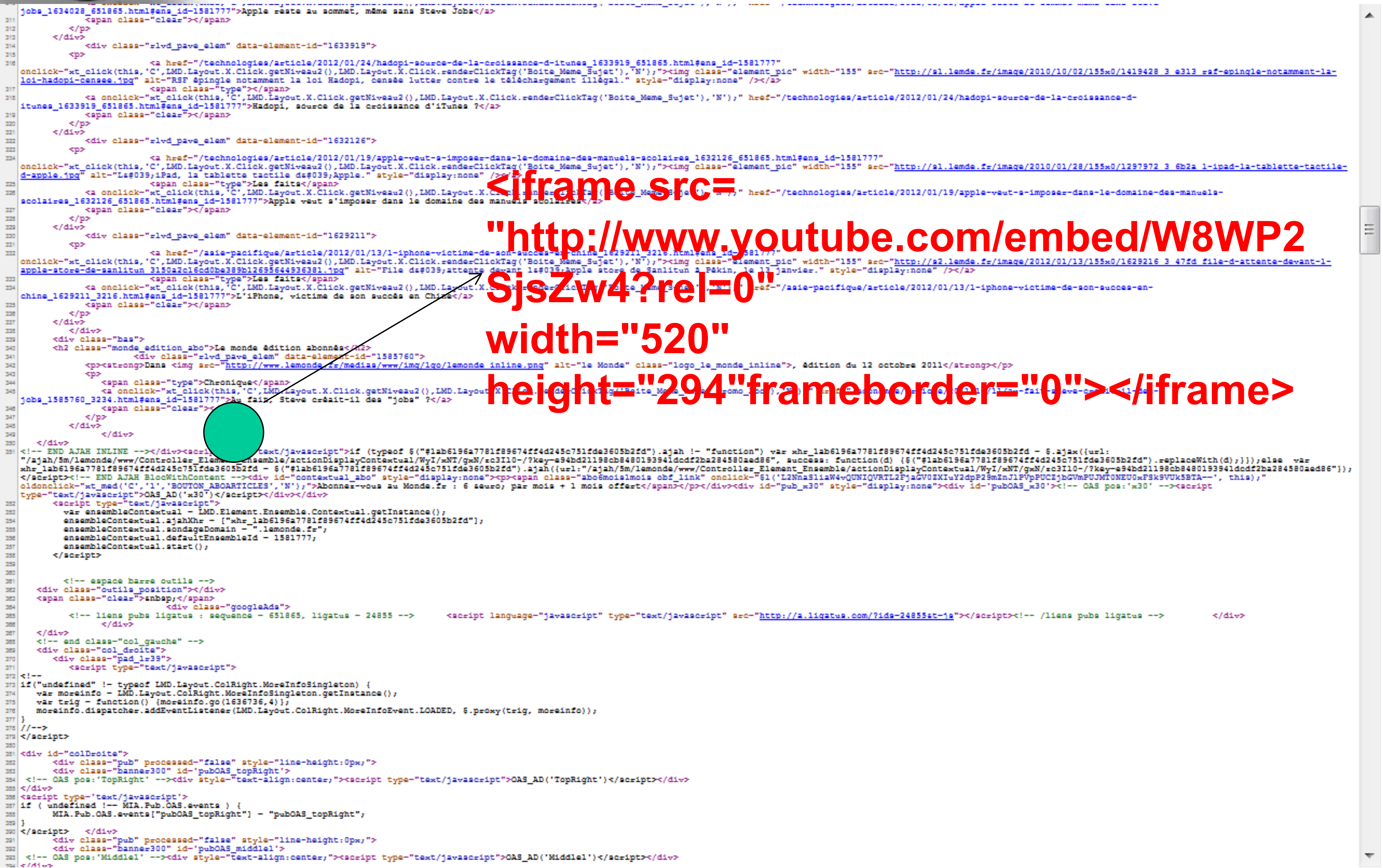
soldes Découvrir

avec LeGuide.com

Les plus partagés sur facebook

J'aime | Oscar Viveros, Sagar Son et 276 576 autres personnes aiment ça.

Code of Le Monde



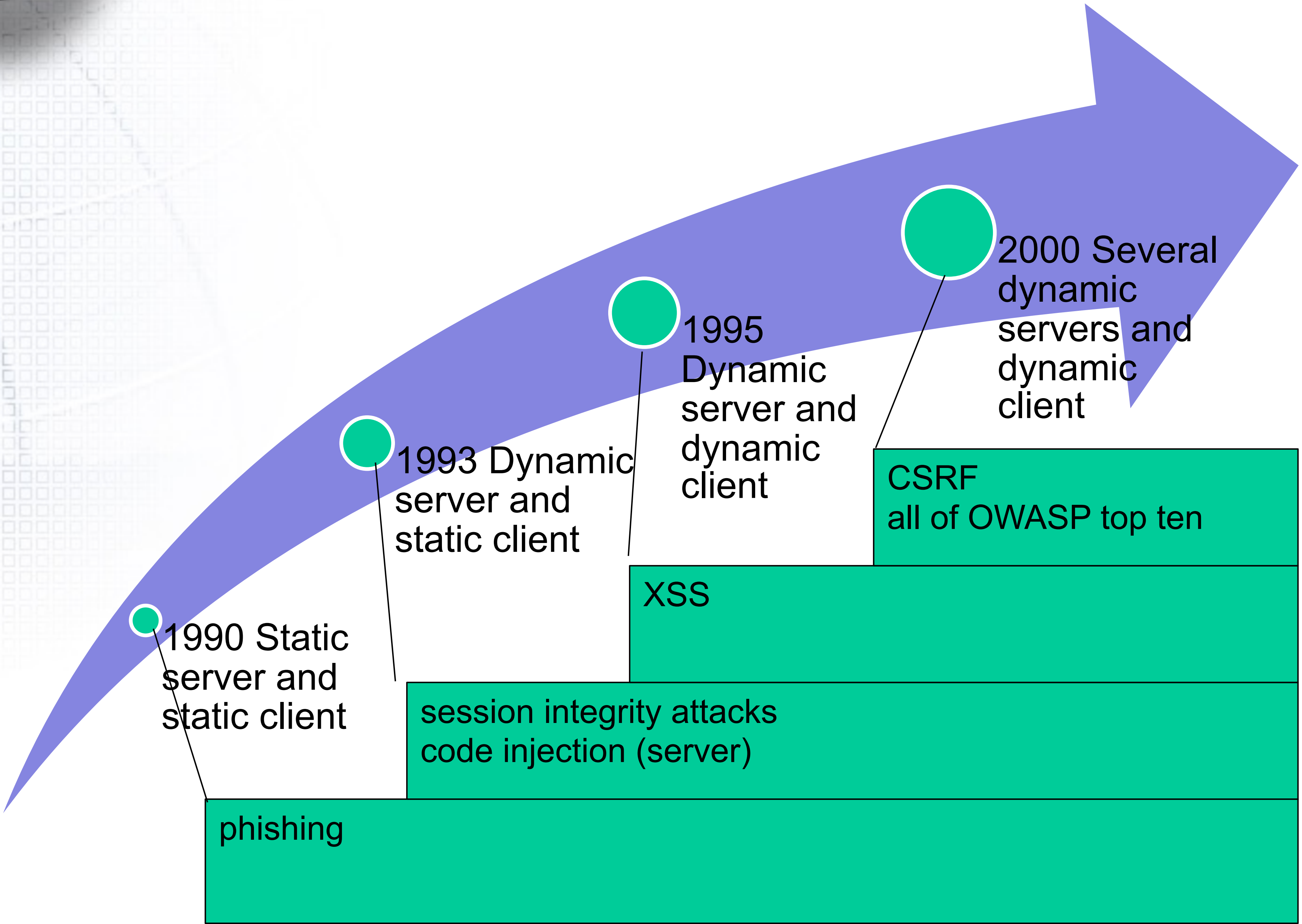
```
jobs_1634028_651865.html#ens_id-1581777">Apple reste au sommet, même sans Steve Jobs</a>
                <span class="clear"></span>
            </p>
        </div>
                <div class="rlvd_pave_elem" data-element-id="1633919">
            <p>
                                <a href="/technologies/article/2012/01/24/hadopi-source-de-la-croissance-d-itunes_1633919_651865.html#ens_id-1581777"
onclick="xt_click(this,'C',LMD.Layout.X.Click.getNiveau2(),LMD.Layout.X.Click.renderClickTag('Boite_Meme_Sujet'),'N');"><img class="element_pic" width="155" src="http://s1.lemde.fr/image/2010/10/02/155x0/1419428_3_e313_rsf-epingle-notamment-la-
loi-hadopi-censee.jpg" alt="RSF épingle notamment la loi Hadopi, censée lutter contre le téléchargement illégal." style="display:none" /></a>
                                <span class="type"></span>
                <a onclick="xt_click(this,'C',LMD.Layout.X.Click.getNiveau2(),LMD.Layout.X.Click.renderClickTag('Boite_Meme_Sujet'),'N');" href="/technologies/article/2012/01/24/hadopi-source-de-la-croissance-d-
itunes_1633919_651865.html#ens_id-1581777">Hadopi, source de la croissance d'iTunes ?</a>
                <span class="clear"></span>
            </p>
        </div>
                <div class="rlvd_pave_elem" data-element-id="1632126">
            <p>
                                <a href="/technologies/article/2012/01/19/apple-veut-s-imposer-dans-le-domaine-des-manuels-scolaires_1632126_651865.html#ens_id-1581777"
onclick="xt_click(this,'C',LMD.Layout.X.Click.getNiveau2(),LMD.Layout.X.Click.renderClickTag('Boite_Meme_Sujet'),'N');"><img class="element_pic" width="155" src="http://s1.lemde.fr/image/2010/01/28/155x0/1297972_3_6b2a_l-ipad-la-tablette-tactile-
d-apple.jpg" alt="L&#039;iPad, la tablette tactile d&#039;Apple." style="display:none" /></a>
                                <span class="type">Les faits</span>
                <a onclick="xt_click(this,'C',LMD.Layout.X.Click.getNiveau2(),LMD.Layout.X.C[illegible]('Boite_Meme_Sujet'),'N');" href="/technologies/article/2012/01/19/apple-veut-s-imposer-dans-le-domaine-des-manuels-
scolaires_1632126_651865.html#ens_id-1581777">Apple veut s'imposer dans le domaine des manuels scolaires</a>
                <span class="clear"></span>
            </p>
        </div>
                <div class="rlvd_pave_elem" data-element-id="1629211">
            <p>
                                <a href="/asie-pacifique/article/2012/01/13/l-iphone-victime-de-son-succes-en-chine_1629211_3216.html#ens_id-1581777"
onclick="xt_click(this,'C',LMD.Layout.X.Click.getNiveau2(),LMD.Layout.X.Click.renderClickTag('Boite_Meme_Sujet'),'N');"><img class="element_pic" width="155" src="http://s2.lemde.fr/image/2012/01/13/155x0/1629216_3_47fd_file-d-attente-devant-l-
apple-store-de-sanlitun_3150a2c16cd0be389b12695644936381.jpg" alt="File d&#039;attente devant l&#039;Apple store de Sanlitun à Pékin, le 13 janvier." style="display:none" /></a>
                                <span class="type">Les faits</span>
                <a onclick="xt_click(this,'C',LMD.Layout.X.Click.getNiveau2(),LMD.Layout.X.C[illegible]('Boite_Meme_Sujet'),'N');" href="/asie-pacifique/article/2012/01/13/l-iphone-victime-de-son-succes-en-
chine_1629211_3216.html#ens_id-1581777">L'iPhone, victime de son succès en Chine</a>
                <span class="clear"></span>
            </p>
        </div>
            </div>
        <div class="bas">
        <h2 class="monde_edition_abo">Le monde édition abonnés</h2>
                        <div class="rlvd_pave_elem" data-element-id="1585760">
                <p><strong>Dans <img src="http://www.lemonde.fr/medias/www/img/lgo/lemonde_inline.png" alt="le Monde" class="logo_le_monde_inline">, édition du 12 octobre 2011</strong></p>
                <p>
                    <span class="type">Chronique</span>
                    <a onclick="xt_click(this,'C',LMD.Layout.X.Click.getNiveau2(),LMD.Layout[illegible]
jobs_1585760_3234.html#ens_id-1581777">Au fait, Steve créait-il des "jobs" ?</a>
                    <span class="clear">[illegible]
                </p>
            </div>
                    </div>
    </div>
<!-- END AJAH INLINE --></div><scri[illegible]text/javascript">if (typeof $("#lab6196a7781f89674ff4d245c751fde3605b2fd").ajah != "function") var xhr_lab6196a7781f89674ff4d245c751fde3605b2fd = $.ajax({url:
"/ajah/5m/lemonde/www/Controller_Elem[illegible]nsemble/actionDisplayContextual/WyI/xNT/gxN/rc3I10-/?key=a94bd21198cb8480193941dcdf2ba284580aed86", success: function(d) {$("#lab6196a7781f89674ff4d245c751fde3605b2fd").replaceWith(d);}});else  var
xhr_lab6196a7781f89674ff4d245c751fde3605b2fd = $("#lab6196a7781f89674ff4d245c751fde3605b2fd").ajah({url:"/ajah/5m/lemonde/www/Controller_Element_Ensemble/actionDisplayContextual/WyI/xNT/gxN/rc3I10-/?key=a94bd21198cb8480193941dcdf2ba284580aed86"});
</script><!-- END AJAH BlocWithContent --><div id="contextual_abo" style="display:none"><p><span class="abo6mois1mois obf_link" onclick="$1('L2NnaS1iaW4vQUNIQVRTL2FjaGV0ZXIuY2dpP29mZnJlPVpPUCZjbGVmPUJMT0NEU0xFSk9VUk5BTA==', this);"
oldonclick="xt_med('C','1','BOUTON_ABOARTICLES','N');">Abonnez-vous au Monde.fr : 6 &euro; par mois + 1 mois offert</span></p></div><div id="pub_x30" style="display:none"><div id='pubOAS_x30'><!-- OAS pos:'x30' --><script
type="text/javascript">OAS_AD('x30')</script></div></div>
        <script type="text/javascript">
          var ensembleContextual = LMD.Element.Ensemble.Contextual.getInstance();
          ensembleContextual.ajahXhr = ["xhr_lab6196a7781f89674ff4d245c751fde3605b2fd"];
          ensembleContextual.sondageDomain = ".lemonde.fr";
          ensembleContextual.defaultEnsembleId = 1581777;
          ensembleContextual.start();
        </script>


          <!-- espace barre outils -->
    <div class="outils_position"></div>
    <span class="clear">&nbsp;</span>
                              <div class="googleAds">
            <!-- liens pubs ligatus : sequence = 651865, ligatus = 24855 -->      <script language="javascript" type="text/javascript" src="http://a.ligatus.com/?ids=24855&t=js"></script><!-- /liens pubs ligatus -->         </div>
                  </div>
    </div>
    <!-- end class="col_gauche" -->
    <div class="col_droite">
       <div class="pad_lr39">
          <script type="text/javascript">
<!--
if("undefined" != typeof LMD.Layout.ColRight.MoreInfoSingleton) {
   var moreinfo = LMD.Layout.ColRight.MoreInfoSingleton.getInstance();
   var trig = function() {moreinfo.go(1636736,4)};
   moreinfo.dispatcher.addEventListener(LMD.Layout.ColRight.MoreInfoEvent.LOADED, $.proxy(trig, moreinfo));
}
//-->
</script>

<div id="colDroite">
       <div class="pub" processed="false" style="line-height:0px;">
       <div class="banner300" id='pubOAS_topRight'>
 <!-- OAS pos:'TopRight' --><div style="text-align:center;"><script type="text/javascript">OAS_AD('TopRight')</script></div>
</div>
<script type='text/javascript'>
if ( undefined !== MIA.Pub.OAS.events ) {
       MIA.Pub.OAS.events["pubOAS_topRight"] = "pubOAS_topRight";
}
</script>   </div>
       <div class="pub" processed="false" style="line-height:0px;">
       <div class="banner300" id='pubOAS_middle1'>
 <!-- OAS pos:'Middle1' --><div style="text-align:center;"><script type="text/javascript">OAS_AD('Middle1')</script></div>
</div>
```

<iframe src= "http://www.youtube.com/embed/W8WP2SjsZw4?rel=0" width="520" height="294"frameborder="0"></iframe>

Web Attacks Evolution



1990 Static server and static client

1993 Dynamic server and static client

1995 Dynamic server and dynamic client

2000 Several dynamic servers and dynamic client

CSRF
all of OWASP top ten

XSS

session integrity attacks
code injection (server)

phishing

TP

Exercises

https://play.picoctf.org/

Insp3c0r, don’t-use-client-side, InspectHTML

where are the robots

logon