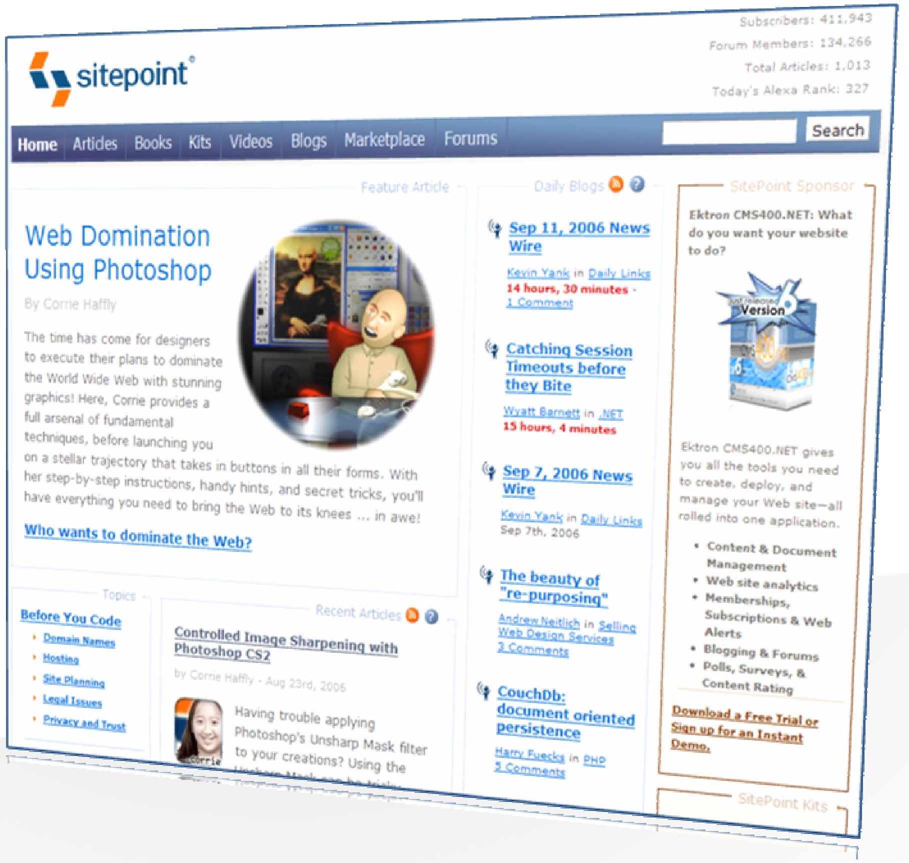
COPING WITH THE NEW WEB

on the server side

Kevin Yank
http://sitepoint.com/
kevin@sitepoint.com

ABOUT SITEPOINT

- publishing
  - articles
  - newsletters
  - books
  - kits
  - videos
  - marketplace
  - forums



Subscribers: 411,943
Forum Members: 134,266
Total Articles: 1,013
Today's Alexa Rank: 327

Feature Article

Web Domination Using Photoshop

By Corrie Haffly

The time has come for designers to execute their plans to dominate the World Wide Web with stunning graphics! Here, Corrie provides a full arsenal of fundamental techniques, before launching you on a stellar trajectory that takes in buttons in all their forms. With her step-by-step instructions, handy hints, and secret tricks, you'll have everything you need to bring the Web to its knees ... in awe!

Who wants to dominate the Web?

Topics

Before You Code
- Domain Names
- Hosting
- Site Planning
- Legal Issues
- Privacy and Trust

Recent Articles

Controlled Image Sharpening with Photoshop CS2

by Corrie Haffly - Aug 23rd, 2006

Having trouble applying Photoshop's Unsharp Mask filter to your creations? Using the

Daily Blogs

Sep 11, 2006 News Wire
Kevin Yank in Daily Links
14 hours, 30 minutes - 1 Comment

Catching Session Timeouts before they Bite
Wyatt Barnett in .NET
15 hours, 4 minutes

Sep 7, 2006 News Wire
Kevin Yank in Daily Links
Sep 7th, 2006

The beauty of "re-purposing"
Andrew Neitlich in Selling Web Design Services
3 Comments

CouchDb: document oriented persistence
Harry Fuecks in PHP
5 Comments

SitePoint Sponsor

Ektron CMS400.NET: What do you want your website to do?

Ektron CMS400.NET gives you all the tools you need to create, deploy, and manage your Web site—all rolled into one application.

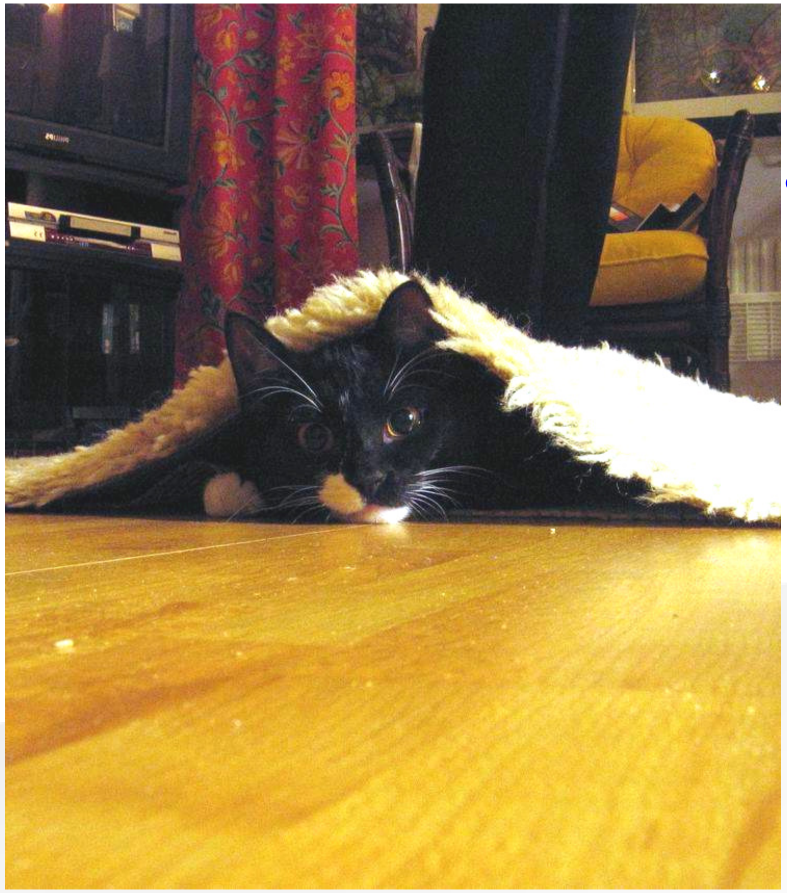
- Content & Document Management
- Web site analytics
- Memberships, Subscriptions & Web Alerts
- Blogging & Forums
- Polls, Surveys, & Content Rating

Download a Free Trial or Sign up for an Instant Demo.

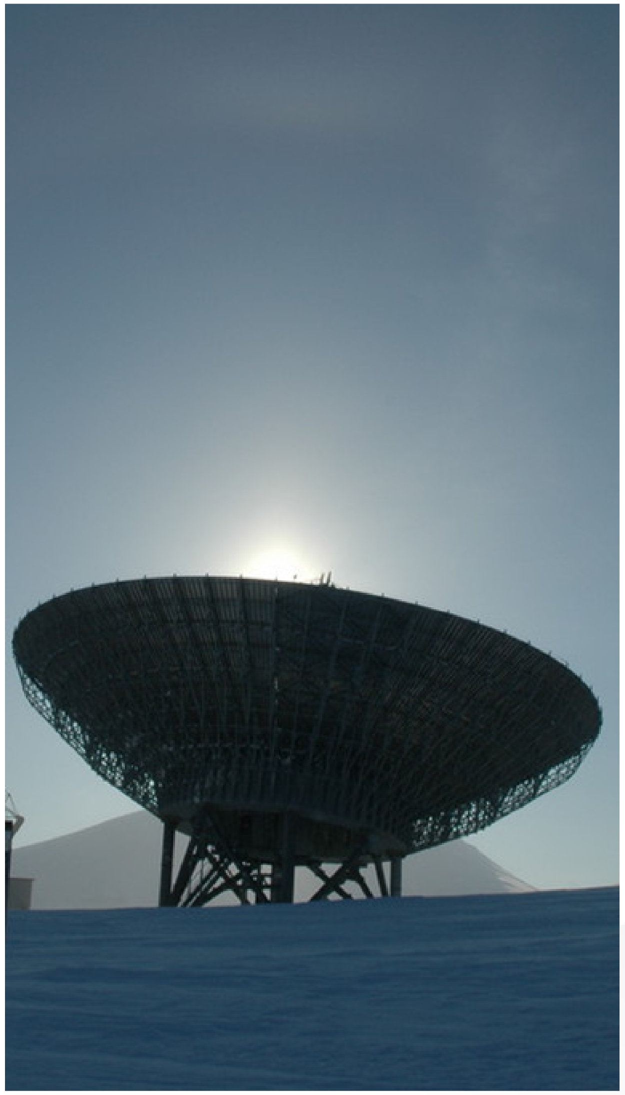
SitePoint Kits

WEB STANDARDS AND THE NEW WEB

- AJAX etc.
  - W3C standard
  - accessible?
- enhance, don't replace
- server-side
  - multiple client interfaces
  - problems, both old and new



ON THE RADAR



- server side architecture
- rethinking security
- character encoding with AJAX
- high-level solutions

coping with the new web on the server side

SERVER-SIDE WEB APPLICATION ARCHITECTURE

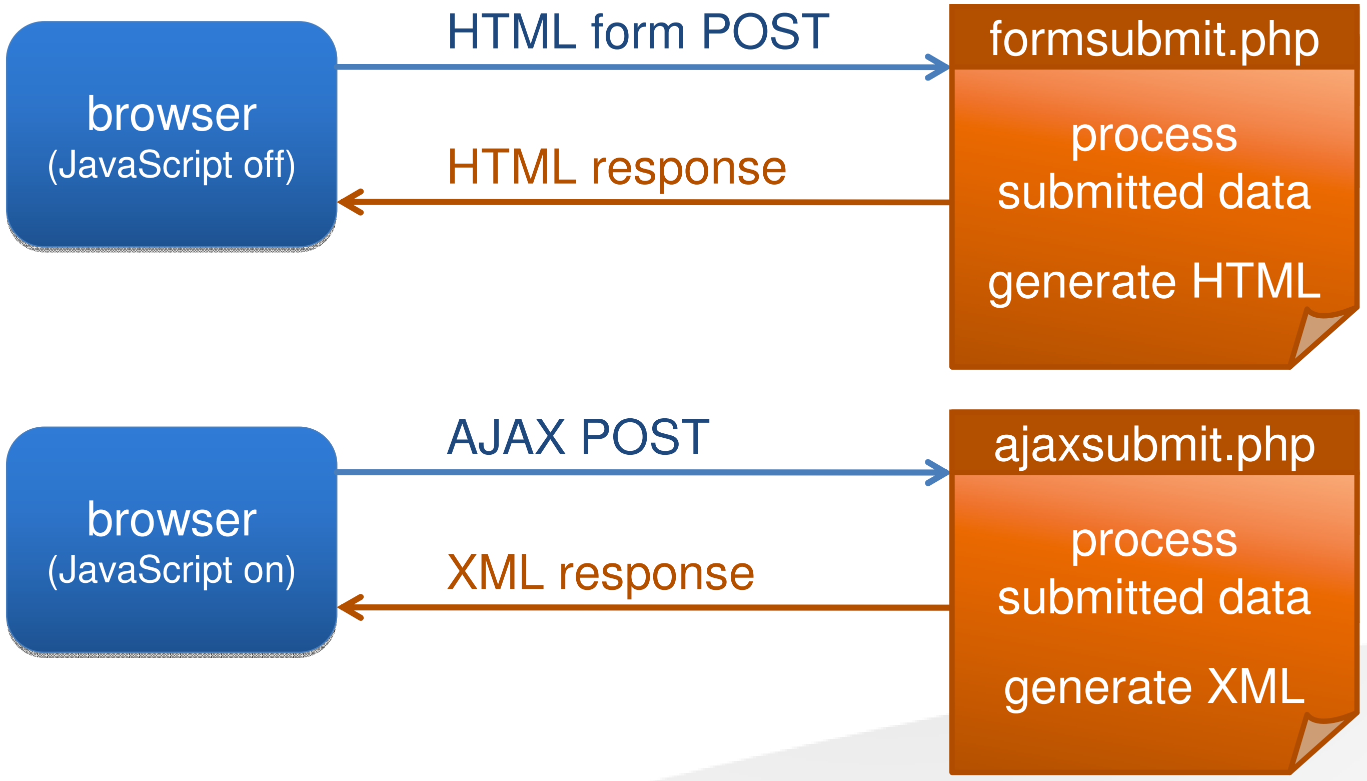
4 October 2006

Kevin Yank
Fundamentos Web 06

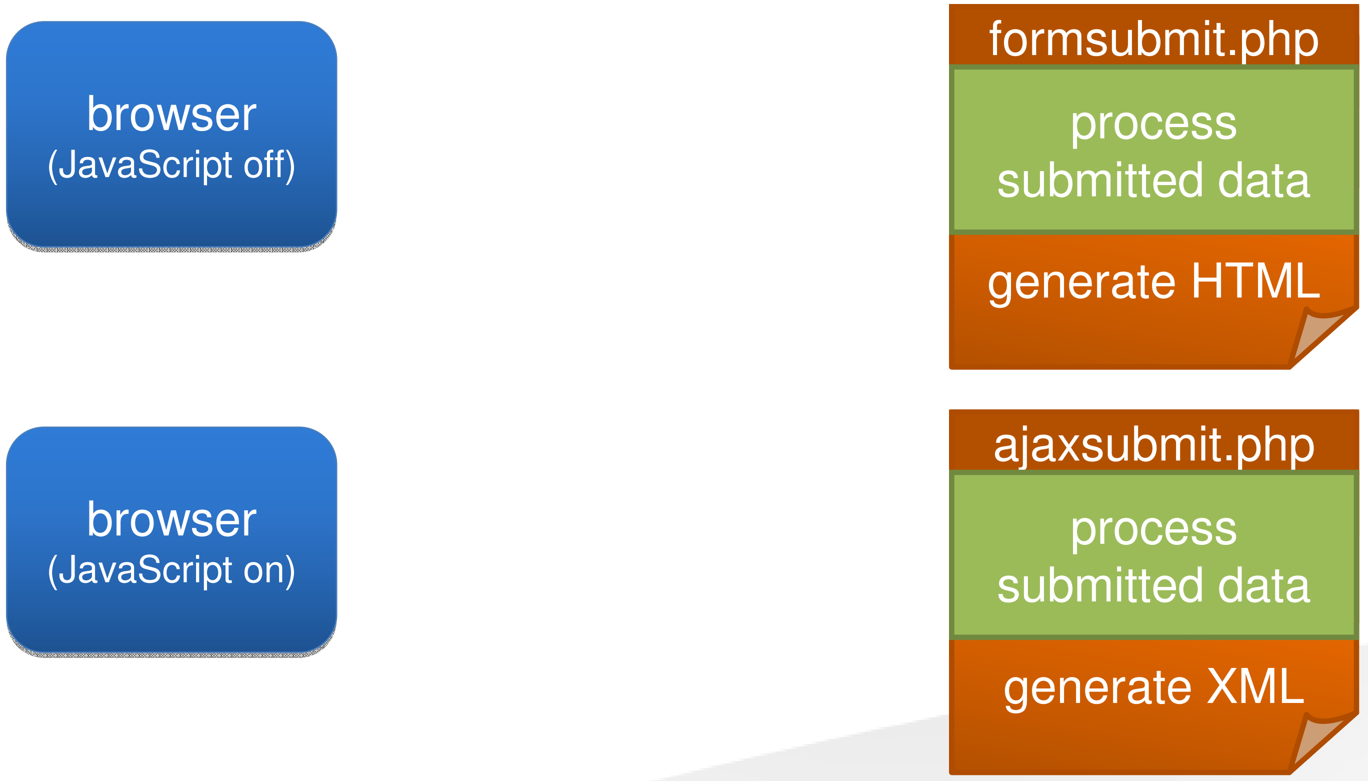
SERVER-SIDE ARCHITECTURE

- is this your PHP code?
- AJAX can cause this

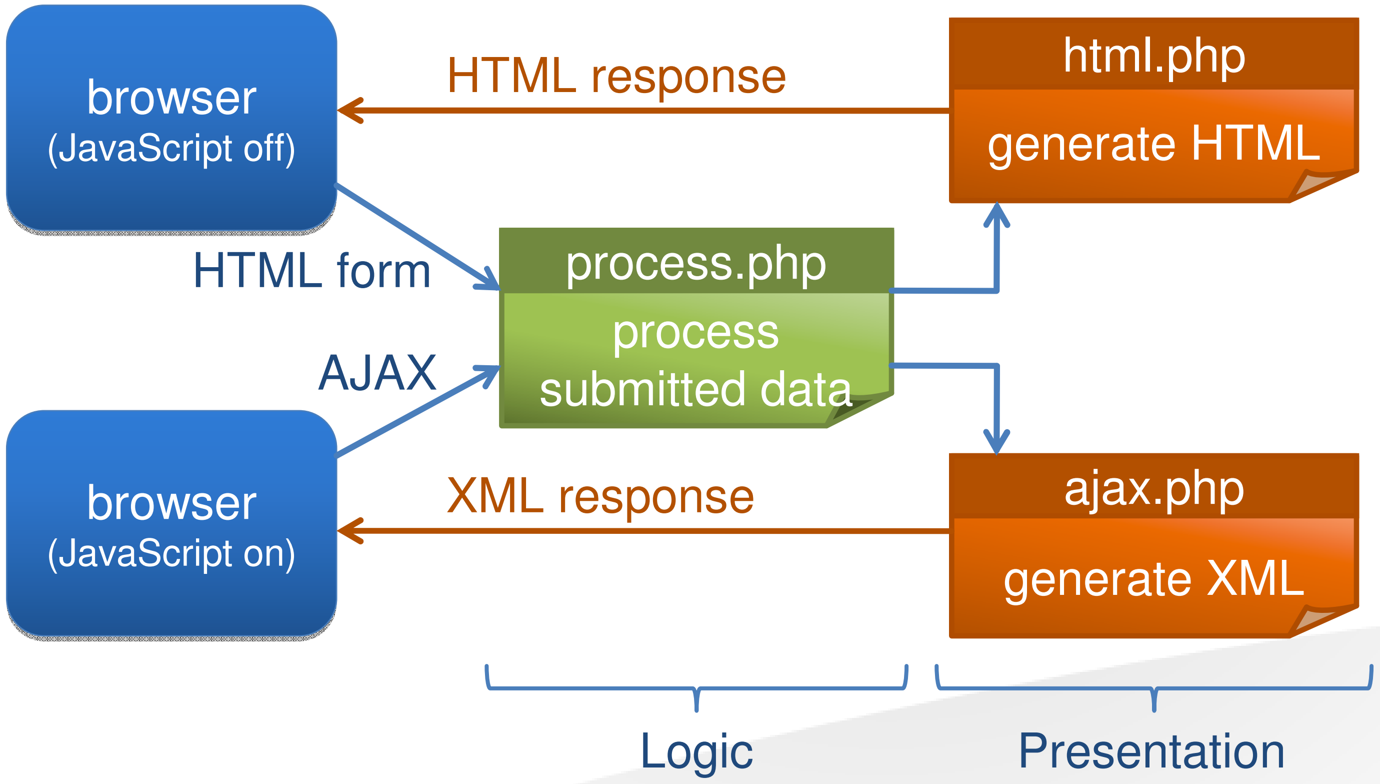
Leo Reynolds



SERVER-SIDE ARCHITECTURE



SERVER-SIDE ARCHITECTURE



SERVER-SIDE ARCHITECTURE

SERVER-SIDE ARCHITECTURE

- is this your PHP code?
- AJAX can cause this
- separate presentation
  - Ruby on Rails
  - Zend Framework
  - CakePHP

coping with the new web on the server side

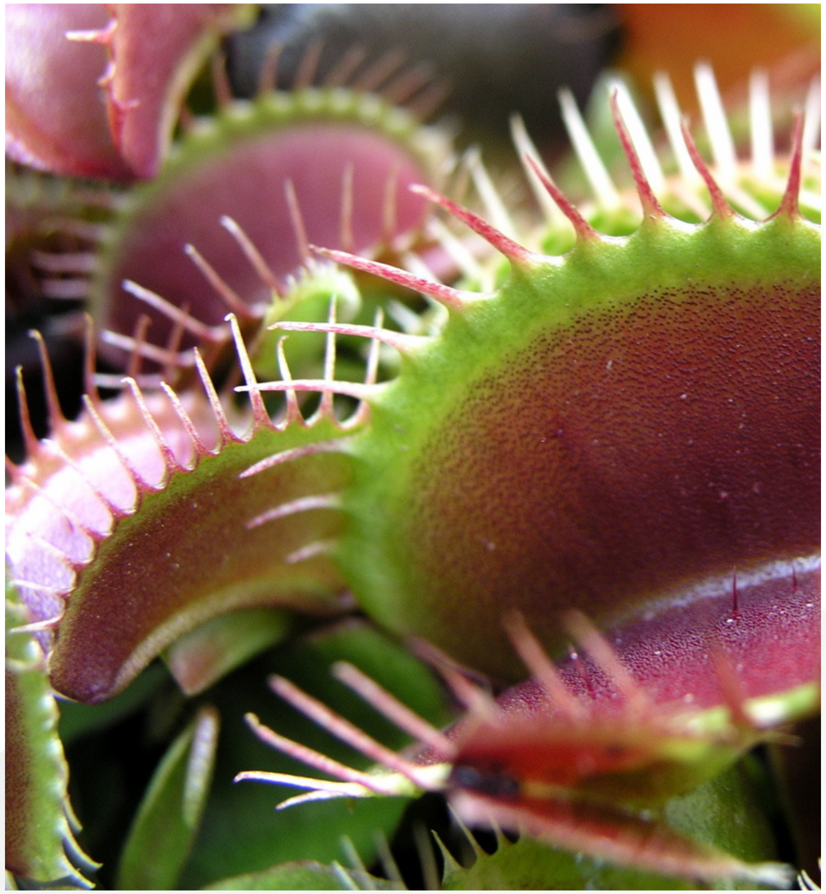
RETHINKING SECURITY

4 October 2006

Kevin Yank
Fundamentos Web 06

OLD TRAPS

- trusting user input
  AJAX is user input too
- secure data exposure
  AJAX readable =
  user readable



© David Midgley

4 October 2006

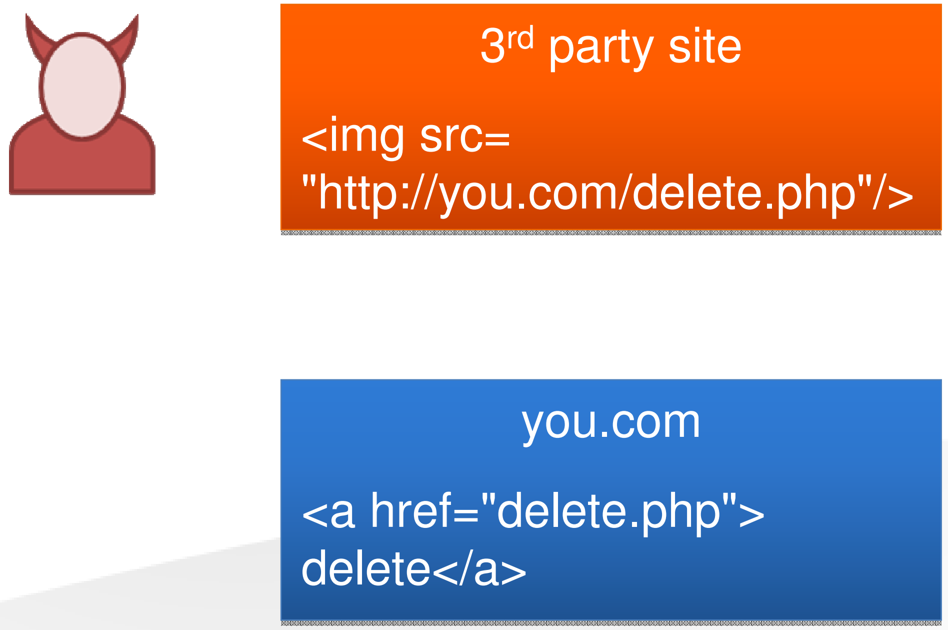
GET VS. POST

- GET for retrieval
- POST, PUT, DELETE for actions
- “delete” links are bad
- security exploits trivial
  `<img src="delete.php"/>`

> “GET and HEAD methods SHOULD NOT have the significance of taking an action other than retrieval. These methods ought to be considered “safe”.”
>
> RFC 2616 HTTP/1.1

CROSS-SITE REQUEST FORGERIES

1. attack on 3rd party site

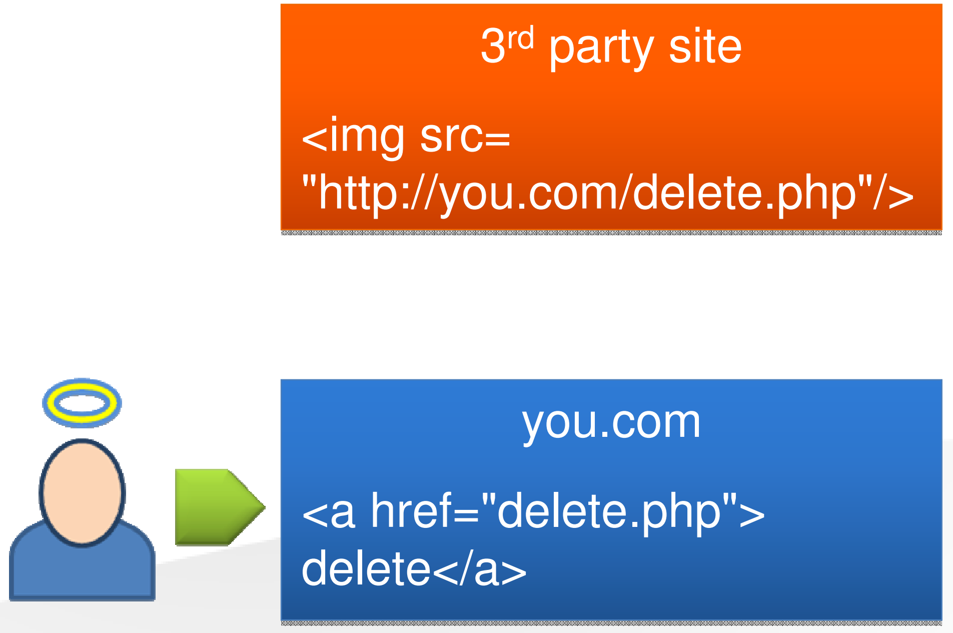


```
<img src=
"http://you.com/delete.php"/>
```

```
<a href="delete.php">
delete</a>
```

CROSS-SITE REQUEST FORGERIES

1. attack on 3rd party site
2. user visits your site
3. user logs in

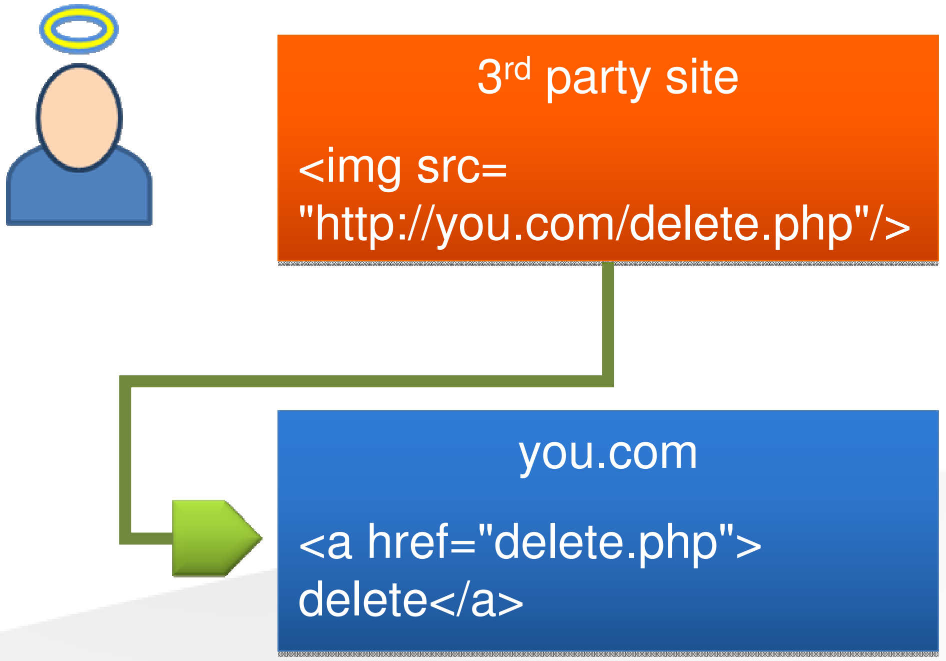


```
<img src=
"http://you.com/delete.php"/>
```

```
<a href="delete.php">
delete</a>
```

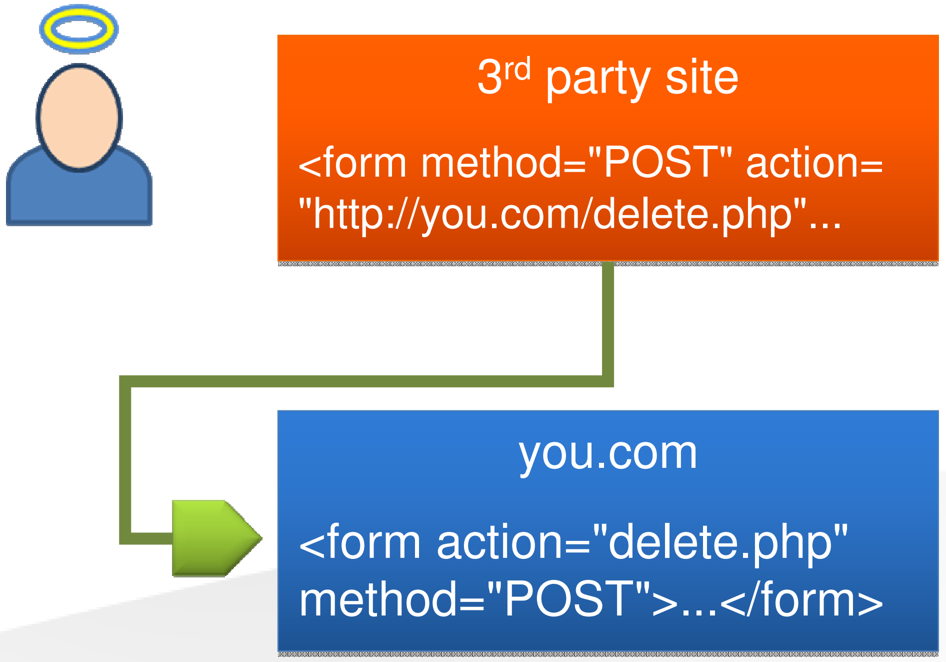
CROSS-SITE REQUEST FORGERIES

1. attack on 3rd party site
2. user visits your site
3. user logs in
4. user visits 3rd party site
5. attack triggered



CROSS-SITE REQUEST FORGERIES

1. attack on 3rd party site
2. user visits your site
3. user logs in
4. user visits 3rd party site
5. attack triggered

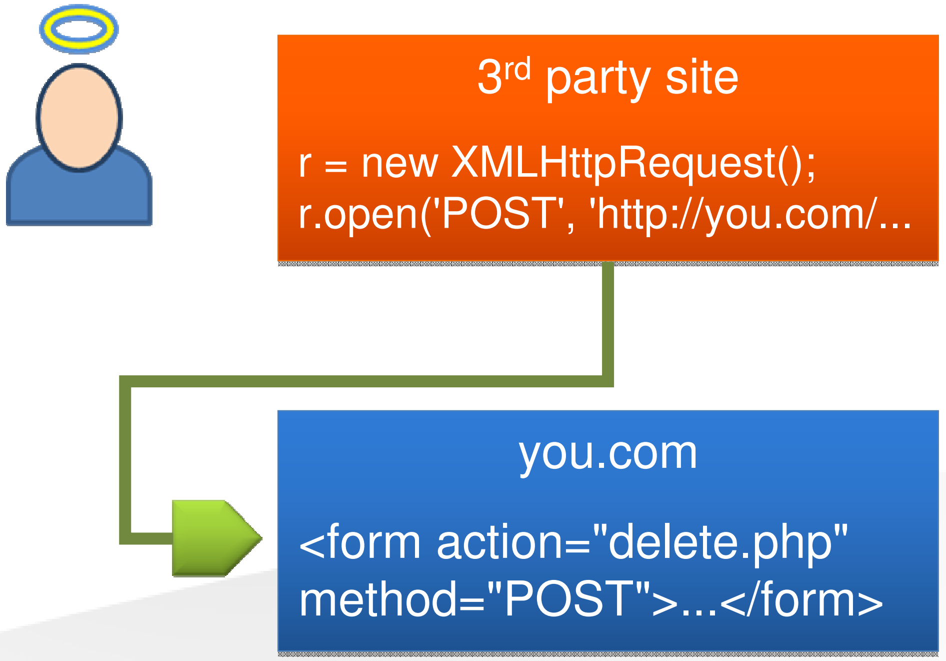


```
<form method="POST" action=
"http://you.com/delete.php"...
```

```
<form action="delete.php"
method="POST">...</form>
```

CROSS-SITE REQUEST FORGERIES

1. attack on 3rd party site
2. user visits your site
3. user logs in
4. user visits 3rd party site
5. attack triggered



3rd party site

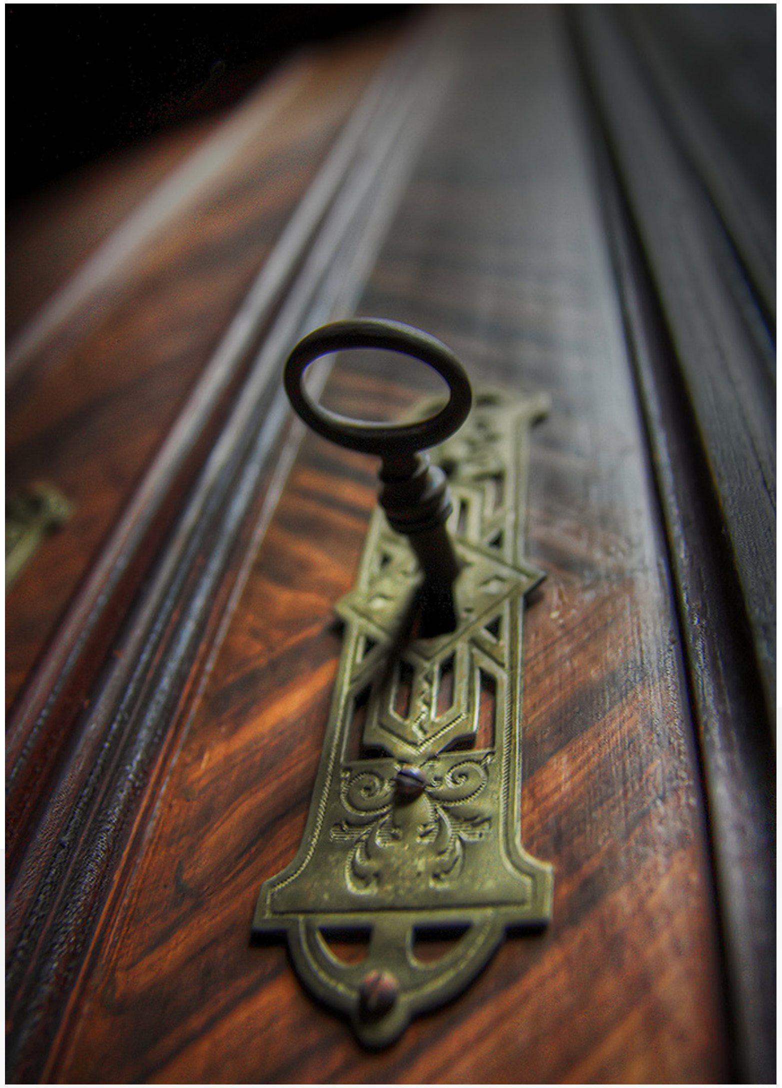
```
r = new XMLHttpRequest();
r.open('POST', 'http://you.com/...
```

you.com

```
<form action="delete.php"
method="POST">...</form>
```

PREVENTING CSRF

- form token
  - per user
  - per session
  - time limited
- CAPTCHA
  - full paranoia



coping with the new web on the server side

CHARACTER ENCODING WITH AJAX

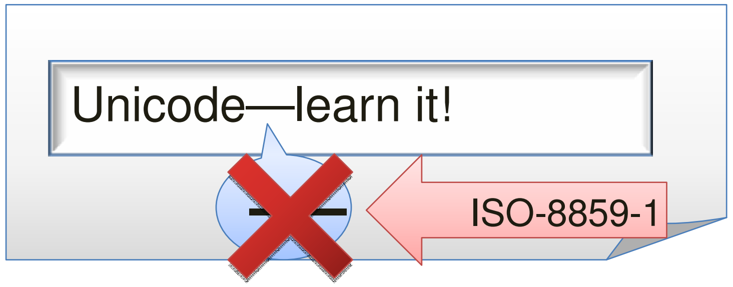
http://www.w3.org/International/tutorials/tutorial-char-enc/

4 October 2006

Kevin Yank
Fundamentos Web 06

HTML FORMS ENCODING

- form encoding = page encoding

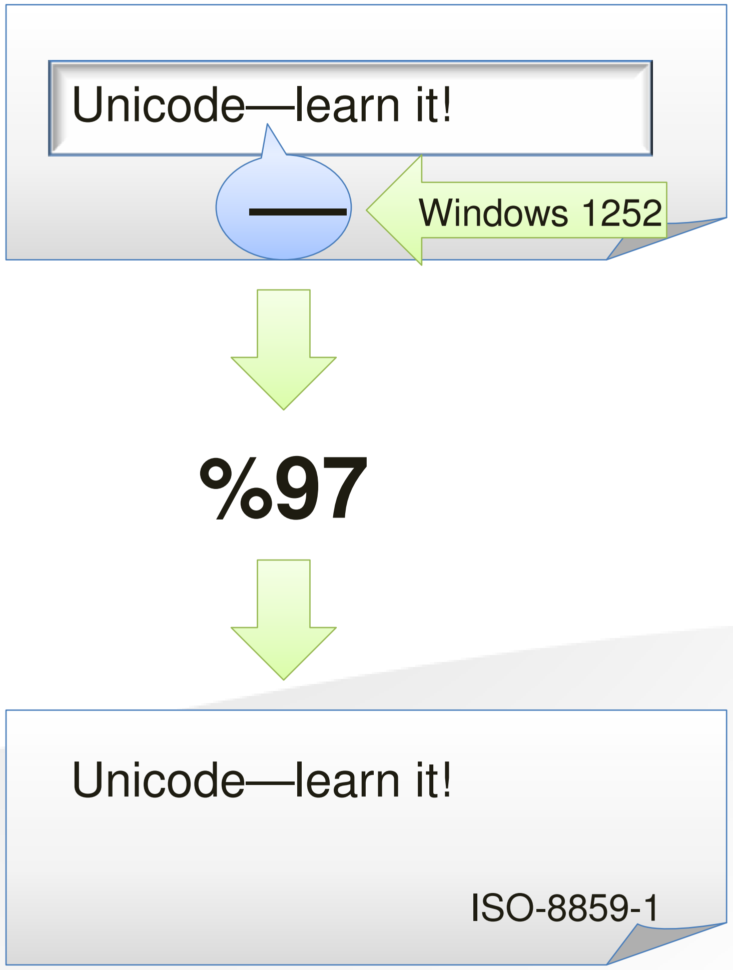


4 October 2006

Kevin Yank
Fundamentos Web 06

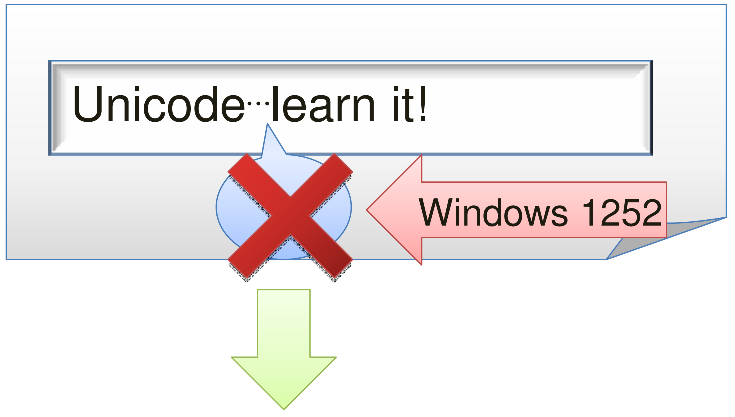
HTML FORMS ENCODING

- form encoding = page encoding
- characters outside encoding handled as Windows 1252
  - older browsers break



HTML FORMS ENCODING

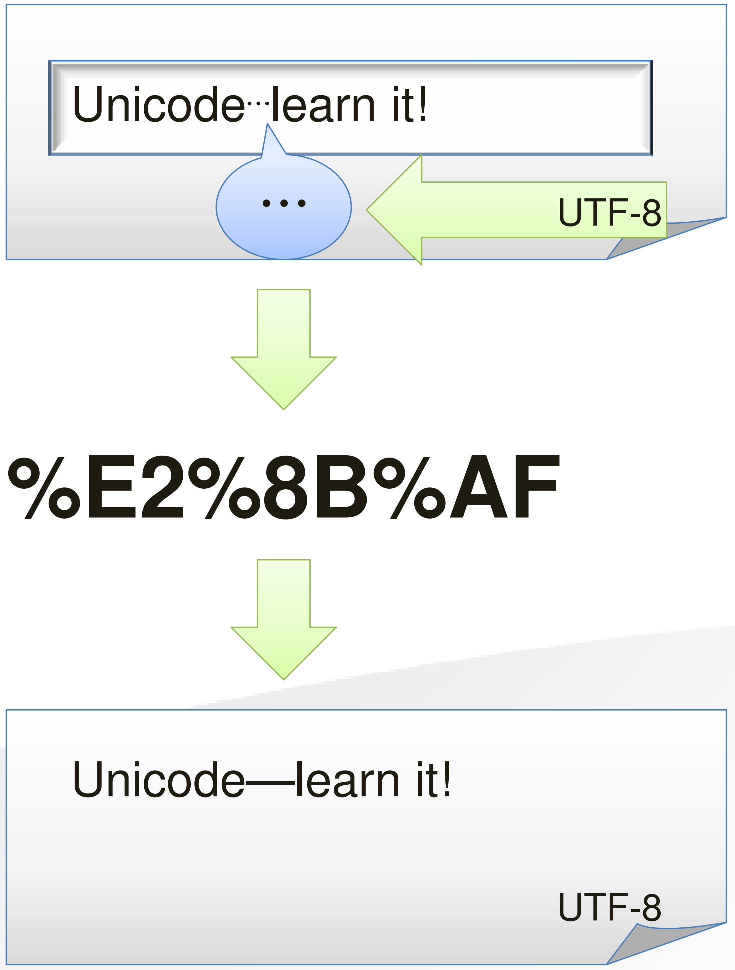
- form encoding = page encoding
- characters outside encoding handled as Windows 1252
  - older browsers break
- characters outside Windows 1252 break



%26%238943%3B
(&#8943;)

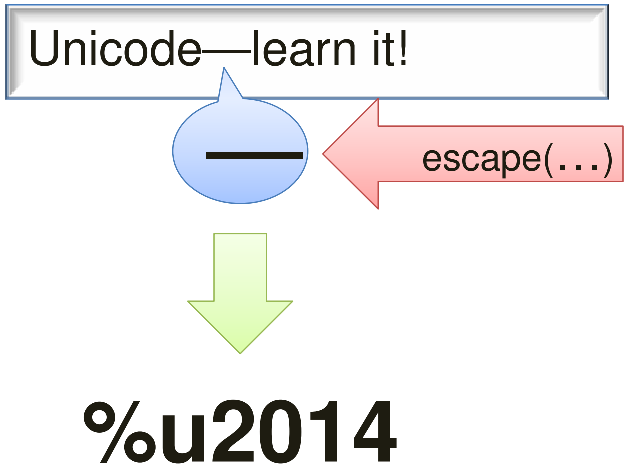
HTML FORMS ENCODING

- form encoding = page encoding
- characters outside encoding handled as Windows 1252
  - older browsers break
- characters outside Windows 1252 break
- Unicode—learn it!



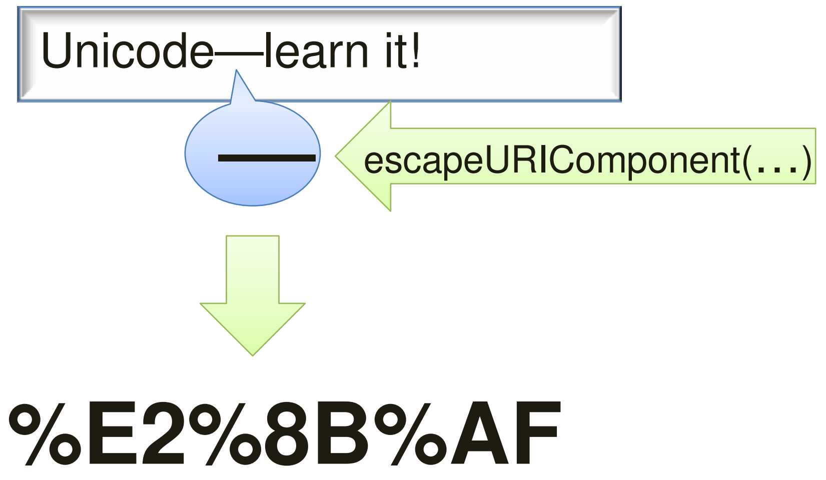
AJAX REQUIRES UTF-8

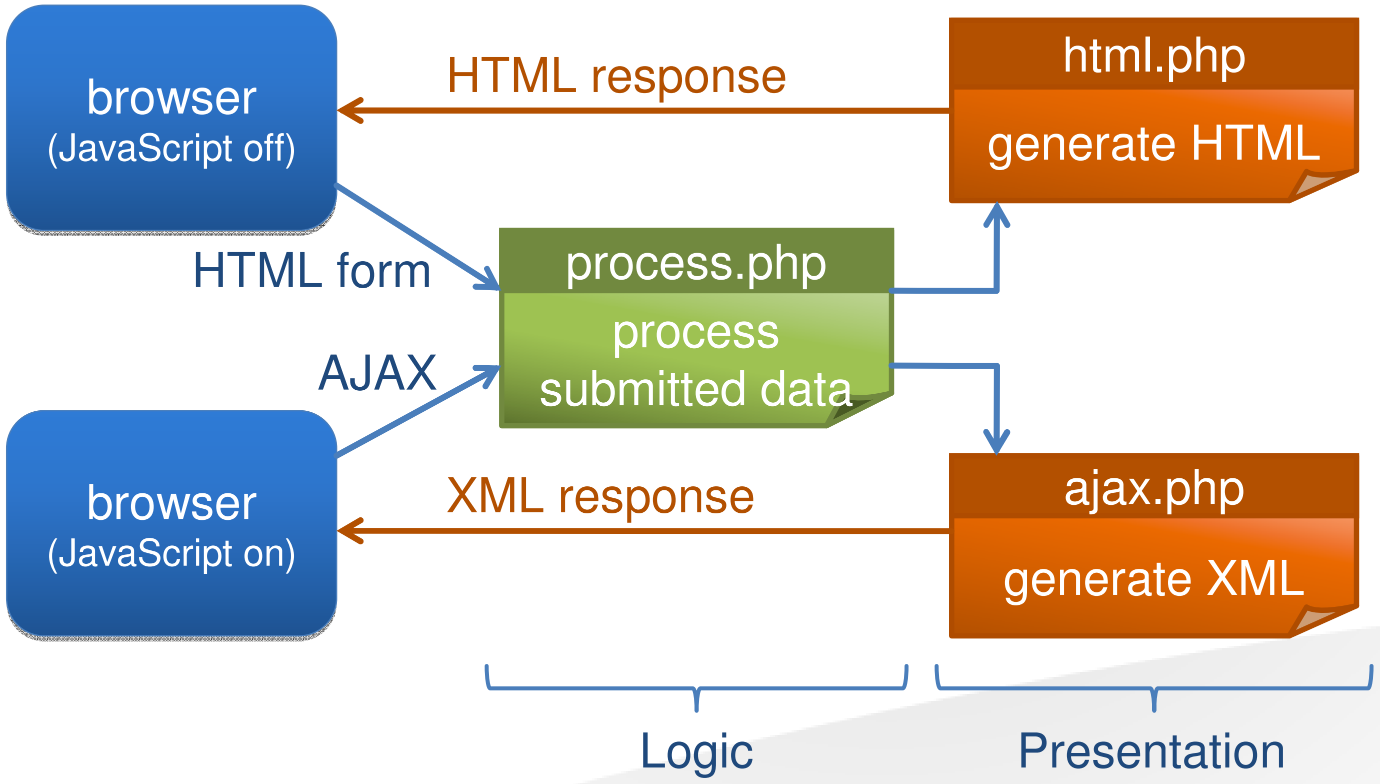
- AJAX encoding ≠ page encoding
  - JavaScript controls the encoding
- escape(…)
  - ISO-8859-1 encoding
  - other characters break



AJAX REQUIRES UTF-8

- AJAX encoding ≠ page encoding
  - JavaScript controls the encoding
- escape(…)
  - ISO-8859-1 encoding
  - other characters break
- encodeURIComponent(…)
  - UTF-8 encoding





SERVER-SIDE ARCHITECTURE

PHP, ROR AND UNICODE

- no native support for Unicode
- UTF-8 direct input and output works
- most string manipulation will break
  - strlen("ñ") → 2
  - strlen("—") → 3
- PHP: mbstring, other libraries, PHP 6
- Ruby on Rails: partial fixes only
  - http://wiki.rubyonrails.org/rails/pages/HowToUseUnicodeStrings

coping with the new web on the server side

HIGH-LEVEL SOLUTIONS

4 October 2006

Kevin Yank
Fundamentos Web 06

TAKING YOUR SKILLS TO THE CLIENT SIDE

- do I have to learn JavaScript?
- short answer: yes
  - standards compliance
  - accessibility
- options
  - Google Web Toolkit
  - Ruby on Rails RJS
  - ASP.NET 2.0 AJAX Extensions (Atlas)

THE NEXT STEP

true HTML/AJAX application frameworks

- abandon JavaScript accessibility
- formalize interaction patterns

the web returns to its roots

- the page paradigm
- web-enabled desktop applications (XUL, XAML, Apollo, etc.)

accessibility tools support AJAX

- extend JavaScript/DOM with accessibility features
- accessibility as a first-class citizen

coping with the new web on the server side

QUESTIONS?

Kevin Yank
http://sitepoint.com/
kevin@sitepoint.com