ISSA/OWASP Oyrgpuyrl Cnex

Graveyards & Zombies:

How HTML5 Improves Security. Mostly.

Mike Shema, Director of Engineering

May 10th, 2012

QUALYS®

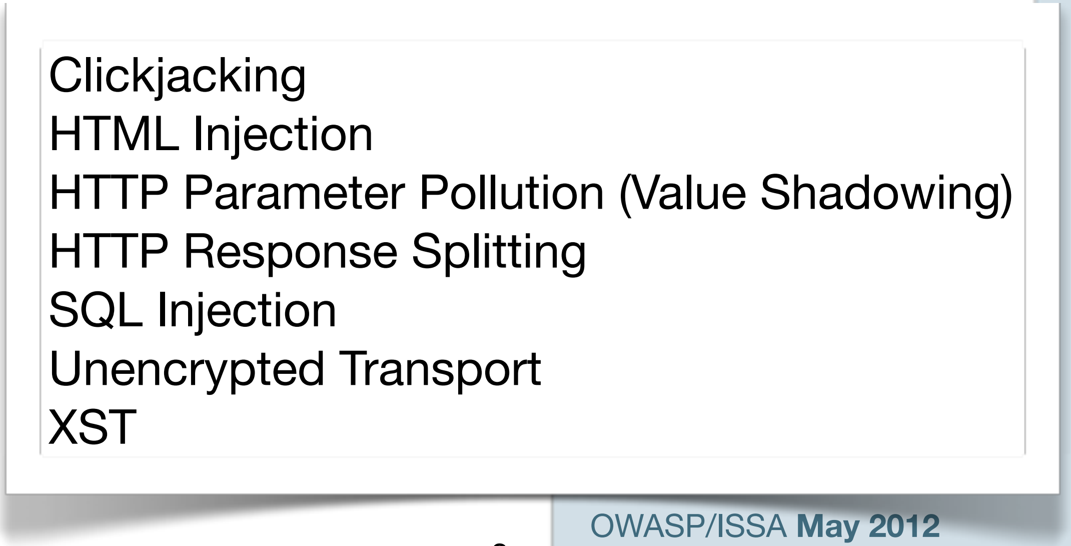
Vuln Sematary

"This specification defines the 5th major revision of the core language of the World Wide Web: the Hypertext Markup Language (HTML). In this version, new f to help Web application au e introduced based on resear vailing authoring practices, and s ntion has been given to defining clear conformance criteria for user agents in an effort to improve interoperability."

Is my ~~Geocities~~ site secure?

“They’re coming to get you, Barbara.”

- Death Throes
  - Server-side/browser design available
- Graveyard
  - Server-side/browser design implemented
- Zombies
  - Developers’ brains
- Undying
  - No design available

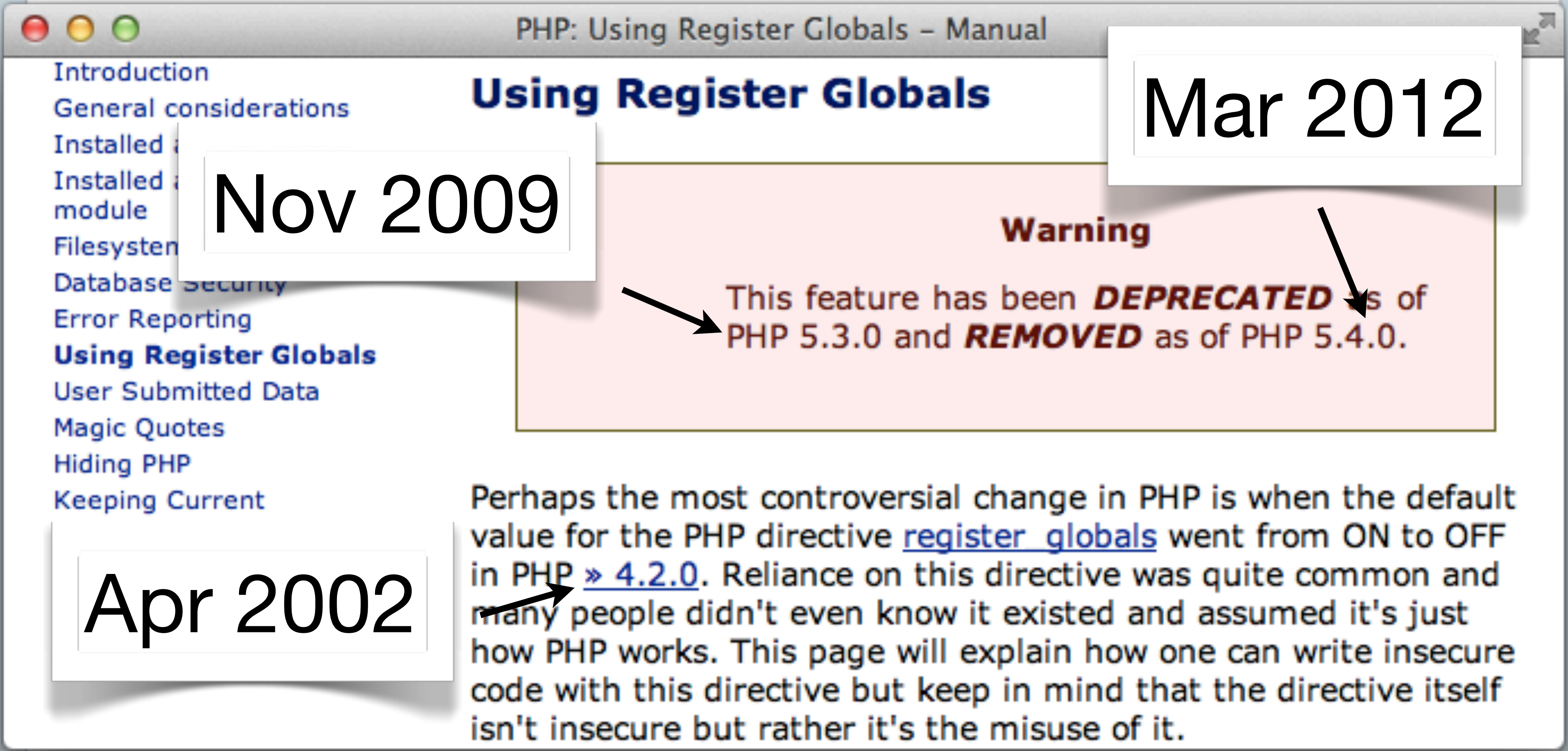


Clickjacking
HTML Injection
HTTP Parameter Pollution (Value Shadowing)
HTTP Response Splitting
SQL Injection
Unencrypted Transport
XST

The Path to HTML5

3350 B.C.	Cuneiform enables stone markup languages.
July 1984	"Cyberspace. A consensual hallucination..." *Neuromancer,* p. 0x33.
Nov 1988	The Morris Worm
Dec 1990	CERN httpd starts serving HTML.
Nov 1995	HTML 2.0 standardized in RFC 1866.
Sep 1999	"Perl CGI Problems" in Phrack 55
Dec 1999	HTML 4.01 finalized.

“Default Secure” Takes Time



PHP: Using Register Globals - Manual

- Introduction
- General considerations
- Installed
- Installed module
- Filesystem
- Database Security
- Error Reporting
- **Using Register Globals**
- User Submitted Data
- Magic Quotes
- Hiding PHP
- Keeping Current

Using Register Globals

Warning

This feature has been ***DEPRECATED*** as of PHP 5.3.0 and ***REMOVED*** as of PHP 5.4.0.

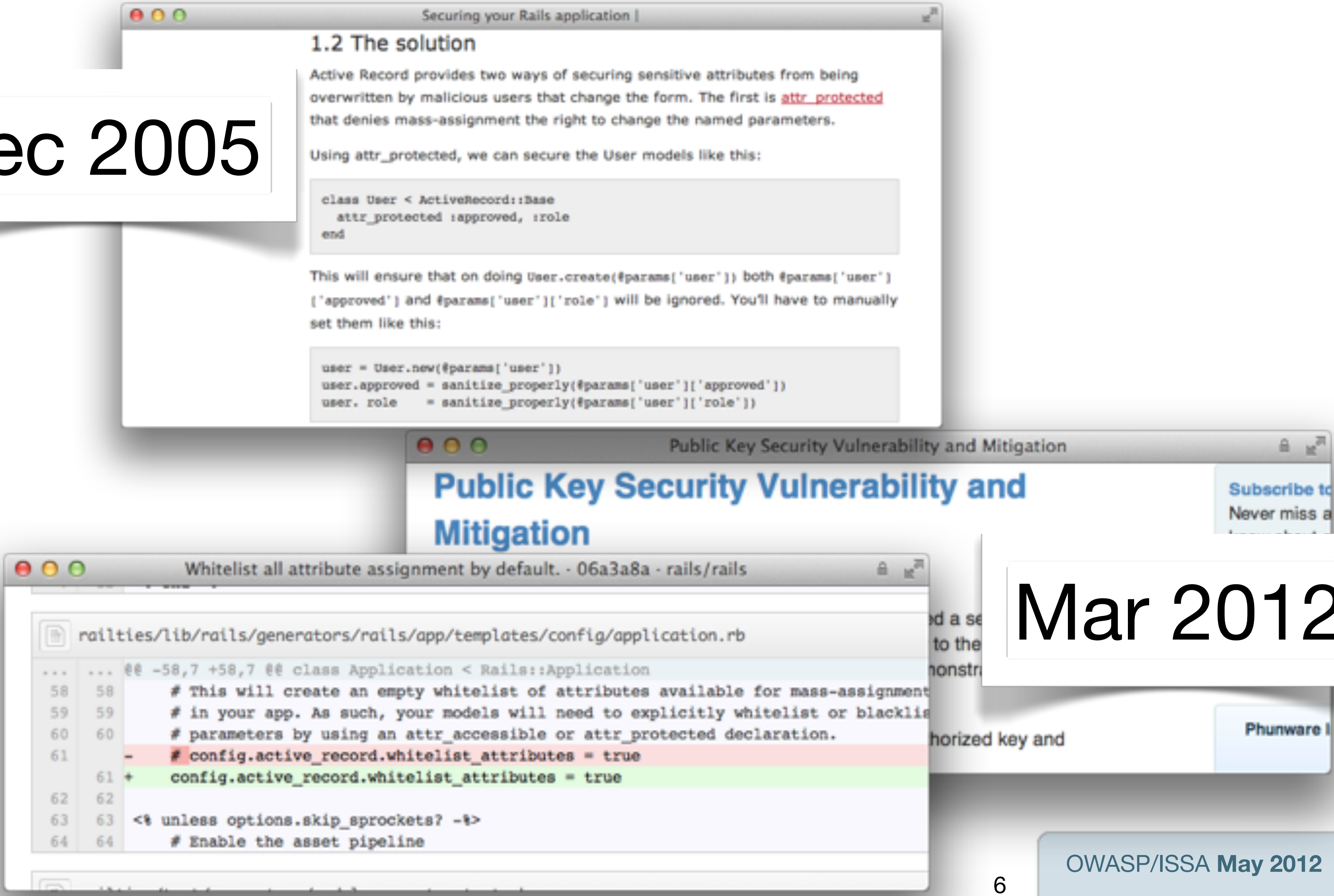
Perhaps the most controversial change in PHP is when the default value for the PHP directive register_globals went from ON to OFF in PHP » 4.2.0. Reliance on this directive was quite common and many people didn't even know it existed and assumed it's just how PHP works. This page will explain how one can write insecure code with this directive but keep in mind that the directive itself isn't insecure but rather it's the misuse of it.

Mar 2012

Nov 2009

Apr 2002

“Default Insecure” Is Enduring



Dec 2005

1.2 The solution

Active Record provides two ways of securing sensitive attributes from being overwritten by malicious users that change the form. The first is attr_protected that denies mass-assignment the right to change the named parameters.

Using attr_protected, we can secure the User models like this:

```
class User < ActiveRecord::Base
  attr_protected :approved, :role
end
```

This will ensure that on doing `User.create(@params['user'])` both `@params['user']['approved']` and `@params['user']['role']` will be ignored. You'll have to manually set them like this:

```
user = User.new(@params['user'])
user.approved = sanitize_properly(@params['user']['approved'])
user. role    = sanitize_properly(@params['user']['role'])
```

Public Key Security Vulnerability and Mitigation

Whitelist all attribute assignment by default. - 06a3a8a - rails/rails

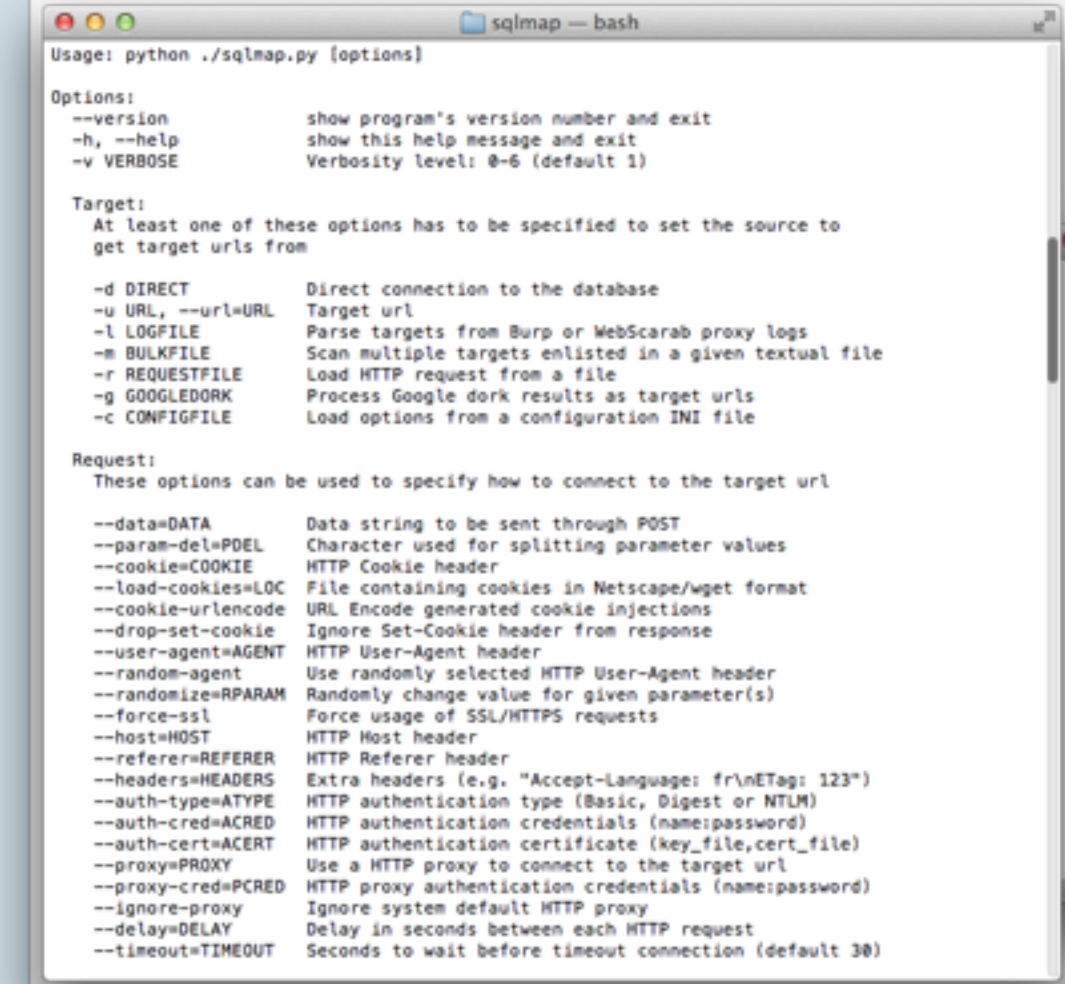
railties/lib/rails/generators/rails/app/templates/config/application.rb

```
@@ -58,7 +58,7 @@ class Application < Rails::Application
     # This will create an empty whitelist of attributes available for mass-assignment
     # in your app. As such, your models will need to explicitly whitelist or blacklis
     # parameters by using an attr_accessible or attr_protected declaration.
-    # config.active_record.whitelist_attributes = true
+    config.active_record.whitelist_attributes = true

 <% unless options.skip_sprockets? -%>
     # Enable the asset pipeline
```

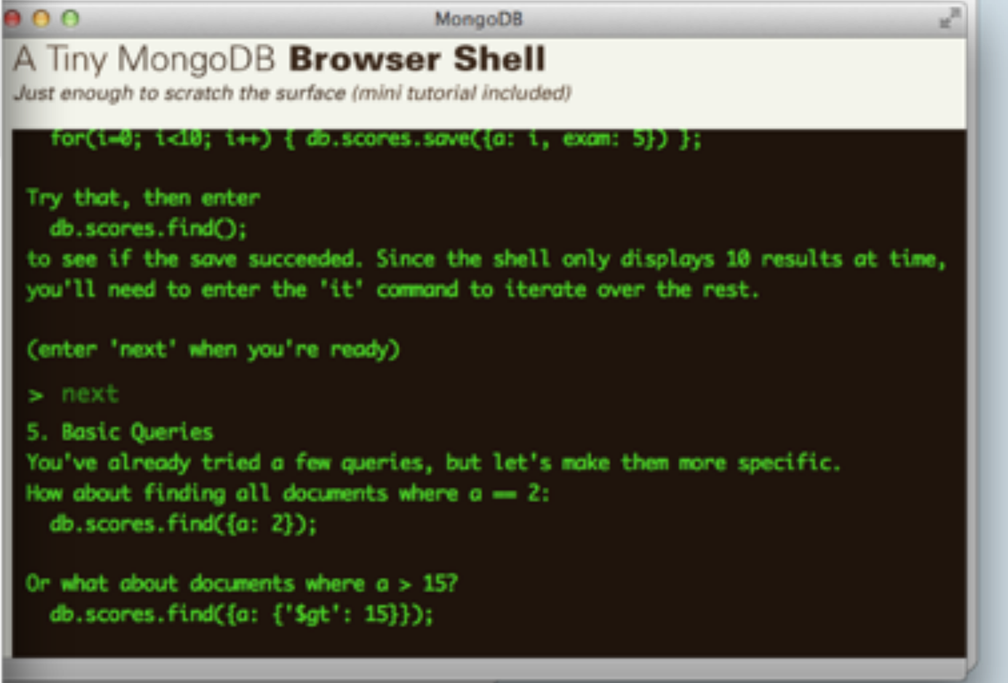
Mar 2012

“Developer Insecure” Is Eternal

- Advanced Persistent Ignorance



```
Usage: python ./sqlmap.py [options]

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be specified to set the source to
    get target urls from

    -d DIRECT           Direct connection to the database
    -u URL, --url=URL   Target url
    -l LOGFILE          Parse targets from Burp or WebScarab proxy logs
    -m BULKFILE         Scan multiple targets enlisted in a given textual file
    -r REQUESTFILE      Load HTTP request from a file
    -g GOOGLEDORK       Process Google dork results as target urls
    -c CONFIGFILE       Load options from a configuration INI file

  Request:
    These options can be used to specify how to connect to the target url

    --data=DATA         Data string to be sent through POST
    --param-del=PDEL    Character used for splitting parameter values
    --cookie=COOKIE     HTTP Cookie header
    --load-cookies=LOC  File containing cookies in Netscape/wget format
    --cookie-urlencode  URL Encode generated cookie injections
    --drop-set-cookie   Ignore Set-Cookie header from response
    --user-agent=AGENT  HTTP User-Agent header
    --random-agent      Use randomly selected HTTP User-Agent header
    --randomize=RPARAM  Randomly change value for given parameter(s)
    --force-ssl         Force usage of SSL/HTTPS requests
    --host=HOST         HTTP Host header
    --referer=REFERER   HTTP Referer header
    --headers=HEADERS   Extra headers (e.g. "Accept-Language: fr\nETag: 123")
    --auth-type=ATYPE   HTTP authentication type (Basic, Digest or NTLM)
    --auth-cred=ACRED   HTTP authentication credentials (name:password)
    --auth-cert=ACERT   HTTP authentication certificate (key_file,cert_file)
    --proxy=PROXY       Use a HTTP proxy to connect to the target url
    --proxy-cred=PCRED  HTTP proxy authentication credentials (name:password)
    --ignore-proxy      Ignore system default HTTP proxy
    --delay=DELAY       Delay in seconds between each HTTP request
    --timeout=TIMEOUT   Seconds to wait before timeout connection (default 30)
```



A Tiny MongoDB **Browser Shell**

Just enough to scratch the surface (mini tutorial included)

```
  for(i=0; i<10; i++) { db.scores.save({a: i, exam: 5}) };

Try that, then enter
  db.scores.find();
to see if the save succeeded. Since the shell only displays 10 results at time,
you'll need to enter the 'it' command to iterate over the rest.

(enter 'next' when you're ready)

> next
5. Basic Queries
You've already tried a few queries, but let's make them more specific.
How about finding all documents where a == 2:
  db.scores.find({a: 2});

Or what about documents where a > 15?
  db.scores.find({a: {'$gt': 15}});
```

JavaScript: Client(?!) Code

- The global scope of superglobals
- The prototypes of mass assignment
- The eval() of SQL injection
- The best way to create powerful browser apps
- The main accomplice to HTML5

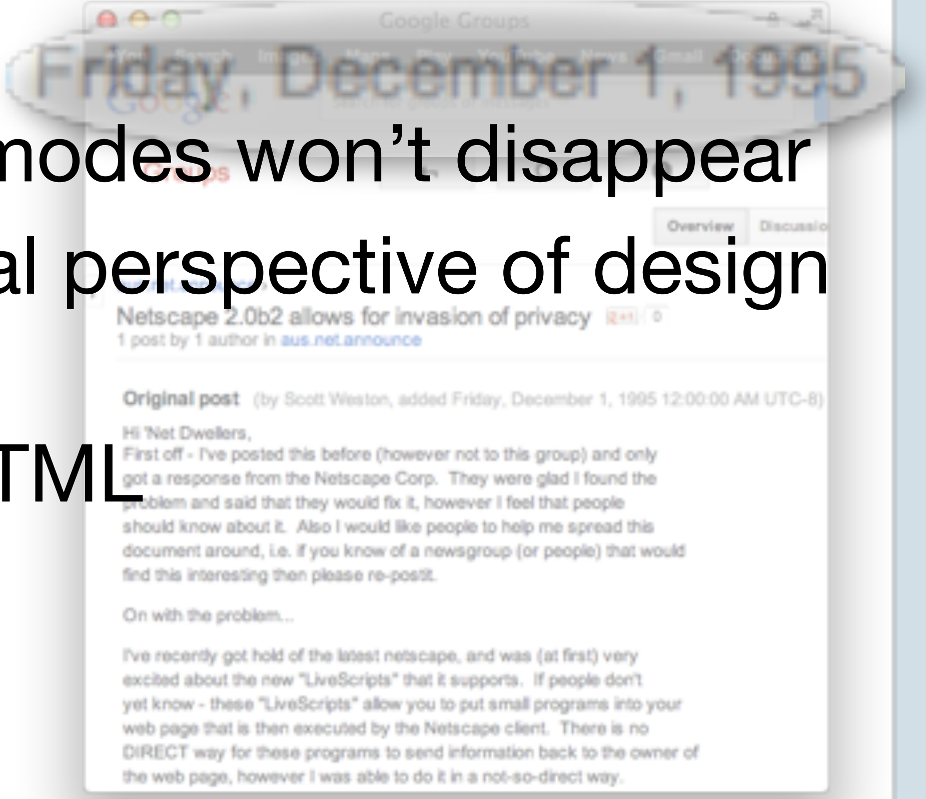
Node.js is a platform built on Chrome's JavaScript runtime for easily building fast, scalable network applications. Node.js uses an event-driven, non-blocking I/O model that makes it lightweight and efficient, perfect for data-intensive real-time applications that run across distributed devices.

Scattered Security

- Cookies
  - Implementation by fiat, not by standard
  - A path of ornamentation, not origin
  - HTTP/HTTPS, JavaScript/non-JavaScript
- Same Origin Policy
  - Access everything, read some things
  - No privilege or all privilege, not least privilege
- HTTPS
  - Not the default
  - Relies on DNS

HTML5 Injection

- Legacy and “non-standard” modes won’t disappear
- Look at this from the historical perspective of design and implementation
- Section 8.2 unifies parsing HTML
  - Still unsettled implementations
- Same old same origin



Friday, December 1, 1995

Netscape 2.0b2 allows for invasion of privacy
1 post by 1 author in aus.net.announce

Original post (by Scott Weston, added Friday, December 1, 1995 12:00:00 AM UTC-8)

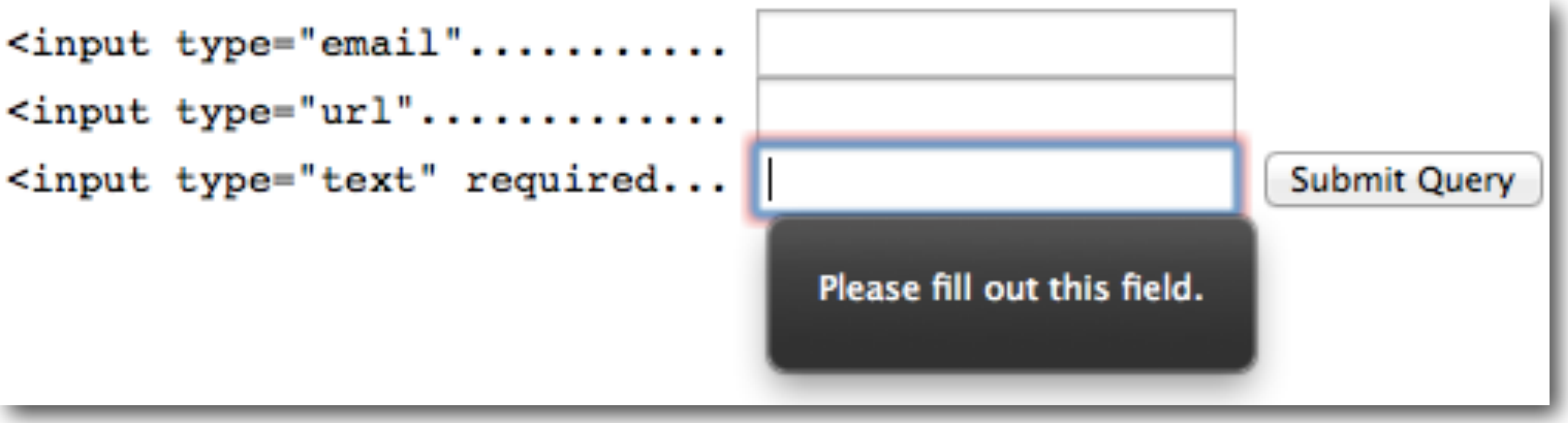
Hi 'Net Dwellers,
First off - I've posted this before (however not to this group) and only got a response from the Netscape Corp. They were glad I found the problem and said that they would fix it, however I feel that people should know about it. Also I would like people to help me spread this document around, i.e. if you know of a newsgroup (or people) that would find this interesting then please re-postit.

On with the problem...

I've recently got hold of the latest netscape, and was (at first) very excited about the new "LiveScripts" that it supports. If people don't yet know - these "LiveScripts" allow you to put small programs into your web page that is then executed by the Netscape client. There is no DIRECT way for these programs to send information back to the owner of the web page, however I was able to do it in a not-so-direct way.

```
<div id=mycode style="BACKGROUND: url('java
script:eval(document.all.mycode.expr)')"
expr="..."></div>
```

HTML5 Form Validation



```
<input type="email"...........
<input type="url".............
<input type="text" required...
```

Please fill out this field.

```
<input pattern="[A-Z]+" name="alpha_only"...

<input ... autofocus onfocus="...
```

"Yes, you can re-add that logic server-side, but why would you want to add that kind of logic twice." -- illustrative mailing list comment from 2011

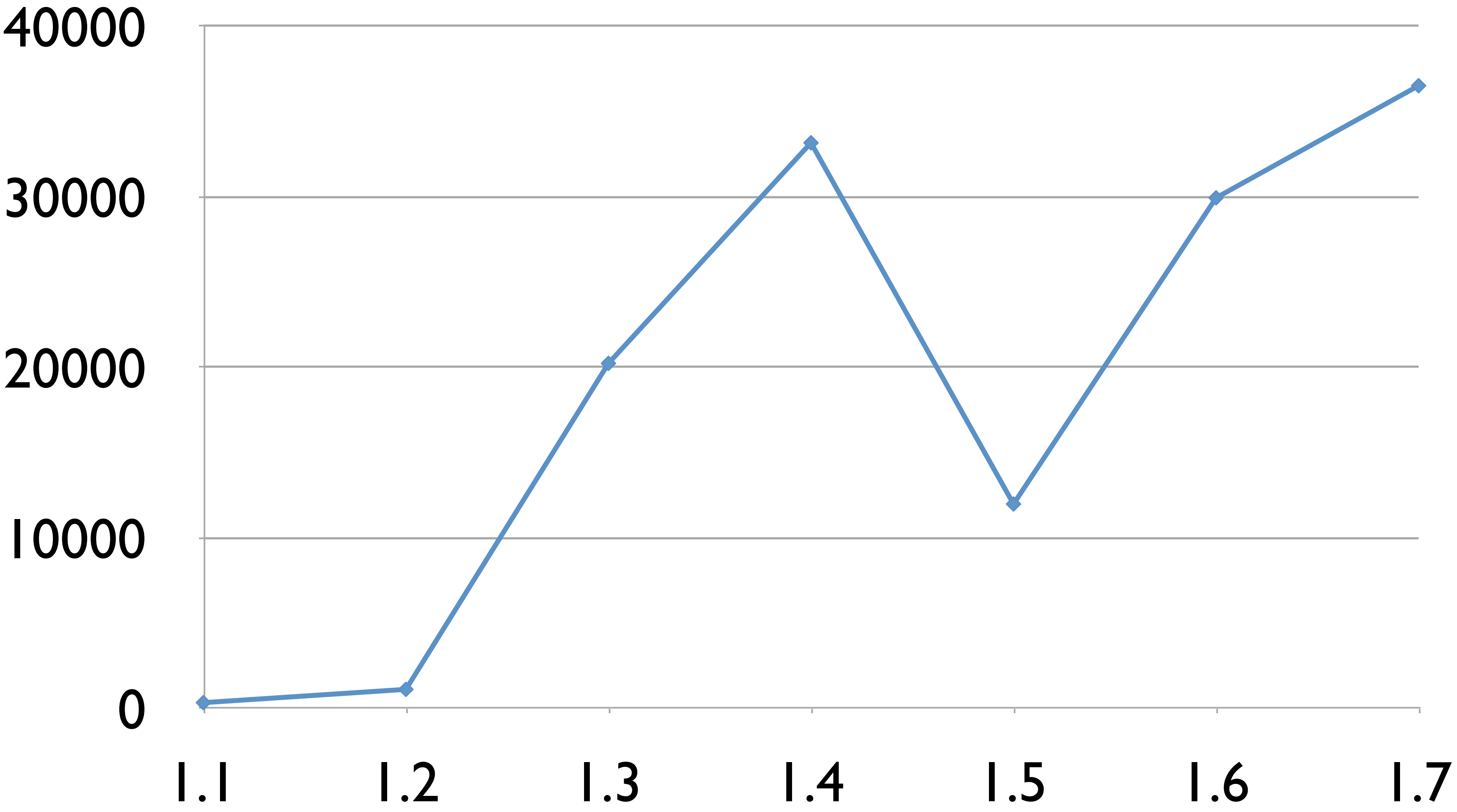
Shift from Implementation to Design

- Sandboxing iframes, form submission, javascript execution
  - Improving granularity of Same Origin Policy
- Cross Origin Resource Sharing
  - Better than JSONP
- Content Security Policy
  - Monitor/enforce eases adoption

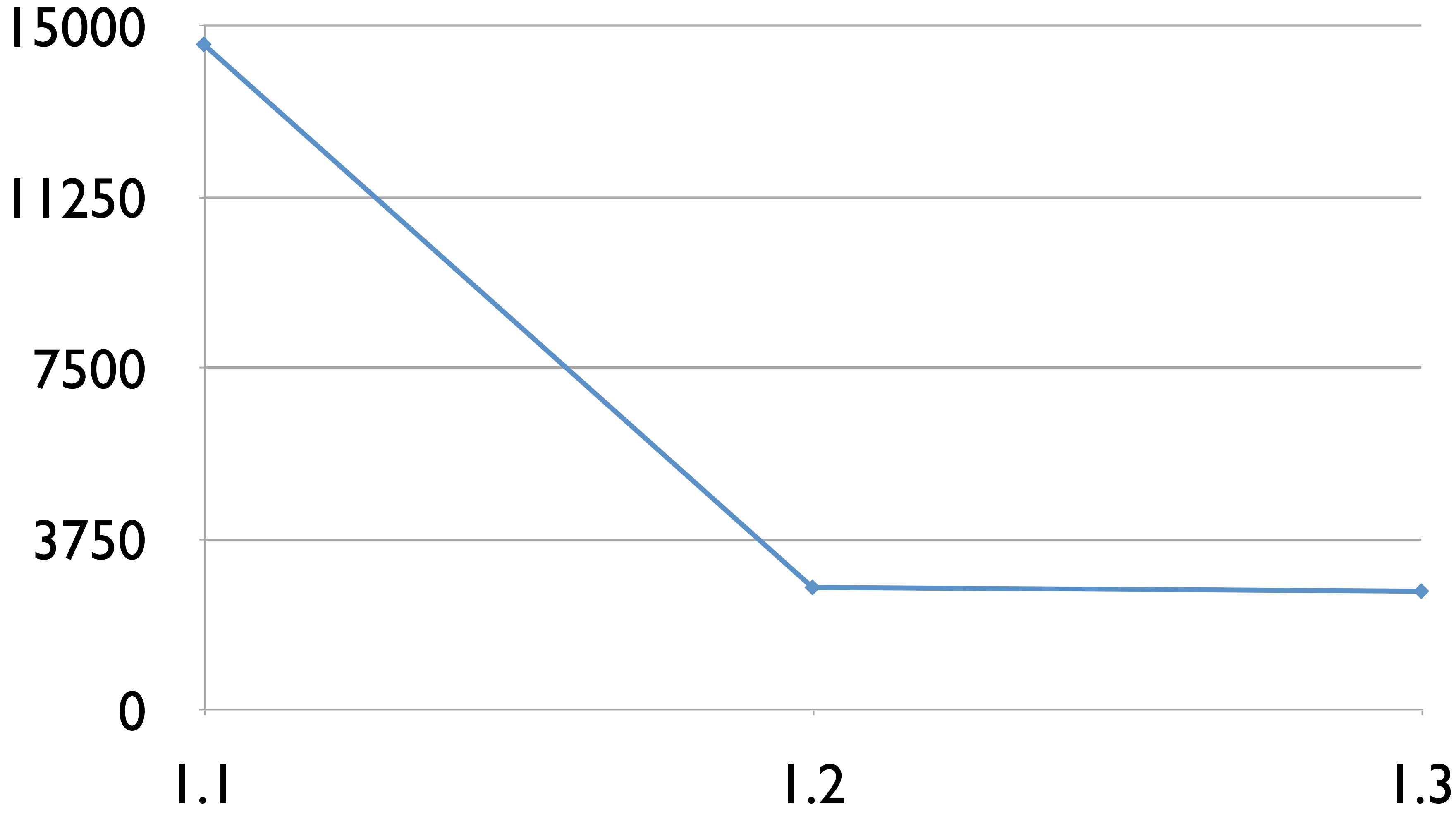
JavaScript Libraries

- Ext JS 1.1.1 to 4.0.7
  - 423 total
- jQuery 1.0.2 to 1.7.2
  - 188648 total
  - 82 with unknown or SCM rev
- Modernizer 1.1 to 2.5.3
  - 4705 total
- MooTools 1.1 to 1.4.5
  - 24808 total
- Prototype 1.3.0 to 1.7.0
  - 6433 total
- YAHOO 2.2.0 to 2.9.0
  - 7938 total
- YUI 3.0.0 to 3.4.1
  - 722 total

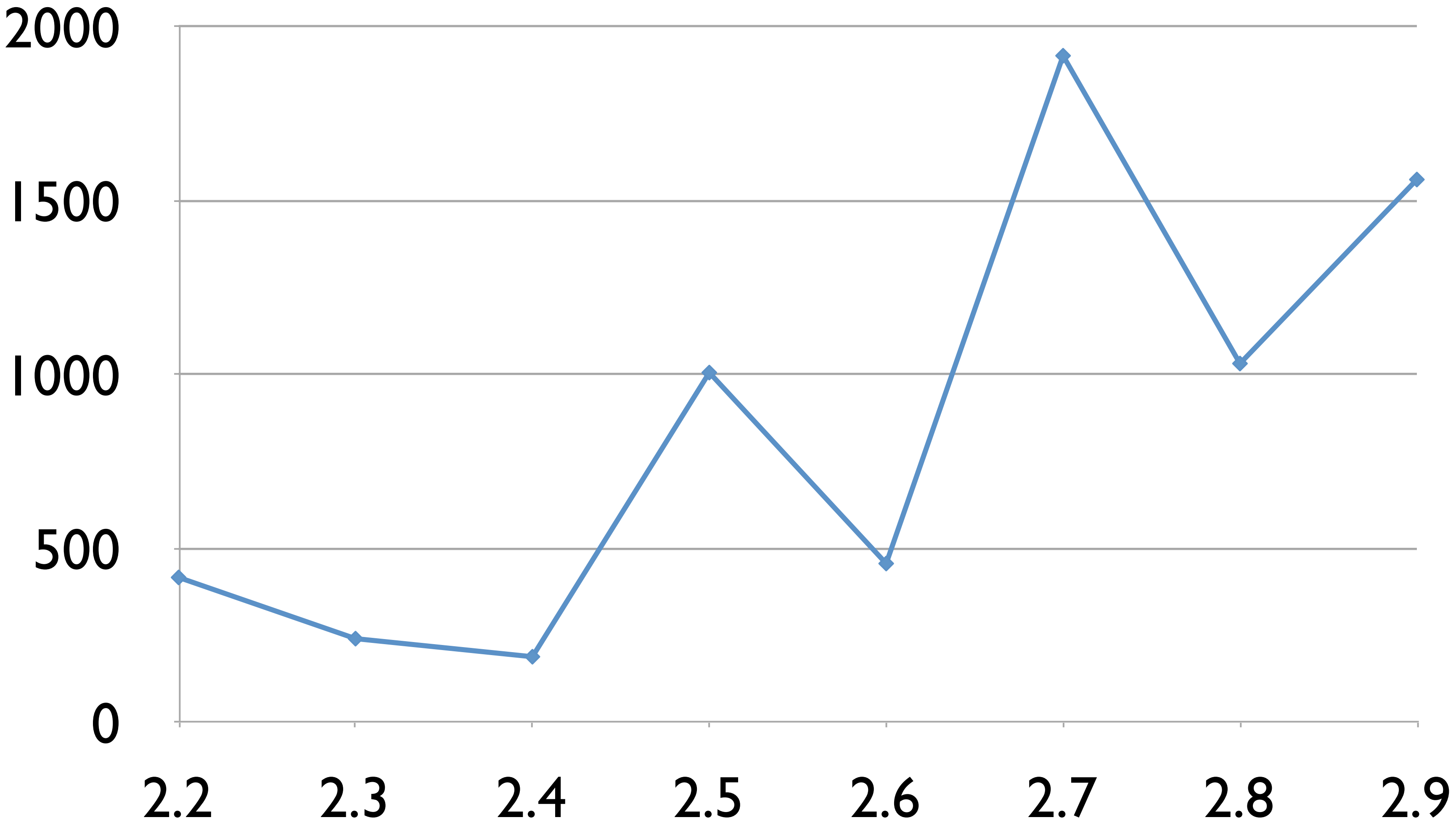
jQuery



MooTools

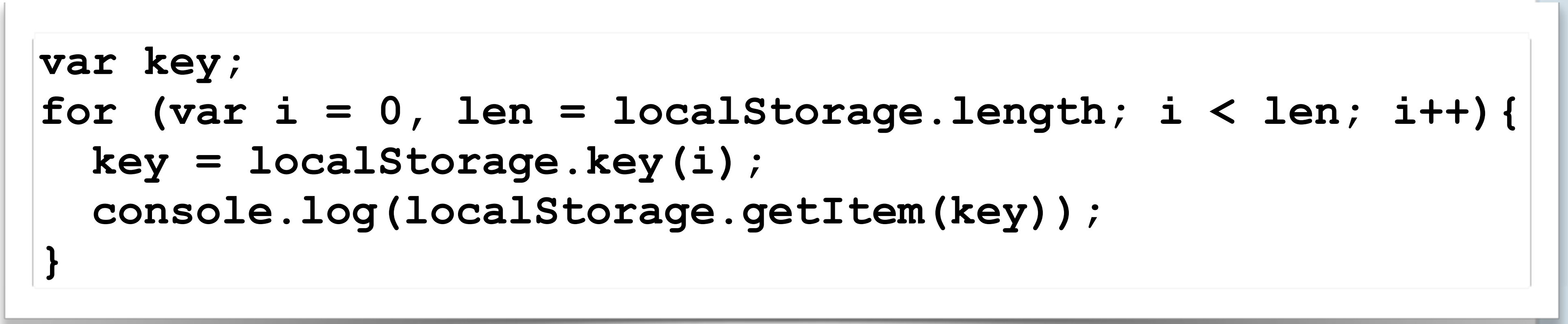


YAHOO



Web Storage API

- Transparent resource
- Privacy extraction, not SQL injection
- Better for cached content than secure storage



```
var key;
for (var i = 0, len = localStorage.length; i < len; i++){
  key = localStorage.key(i);
  console.log(localStorage.getItem(key));
}
```

WebSocket API

- Does not confer authentication & authorization to a protocol layered over WebSockets
- Another vector for launching DoS attacks from the browser

Reinventing Protocol Vulnerabilities

- Prefixed strings
- Identification
- Authorization
- Information leakage
- Replay
- Spoofing
- eval()

```
Alice:Bob:5:Hello
```

```
UUID:UUID:5:Hello
```

```
SessionID:SessionID:5:Hello
```

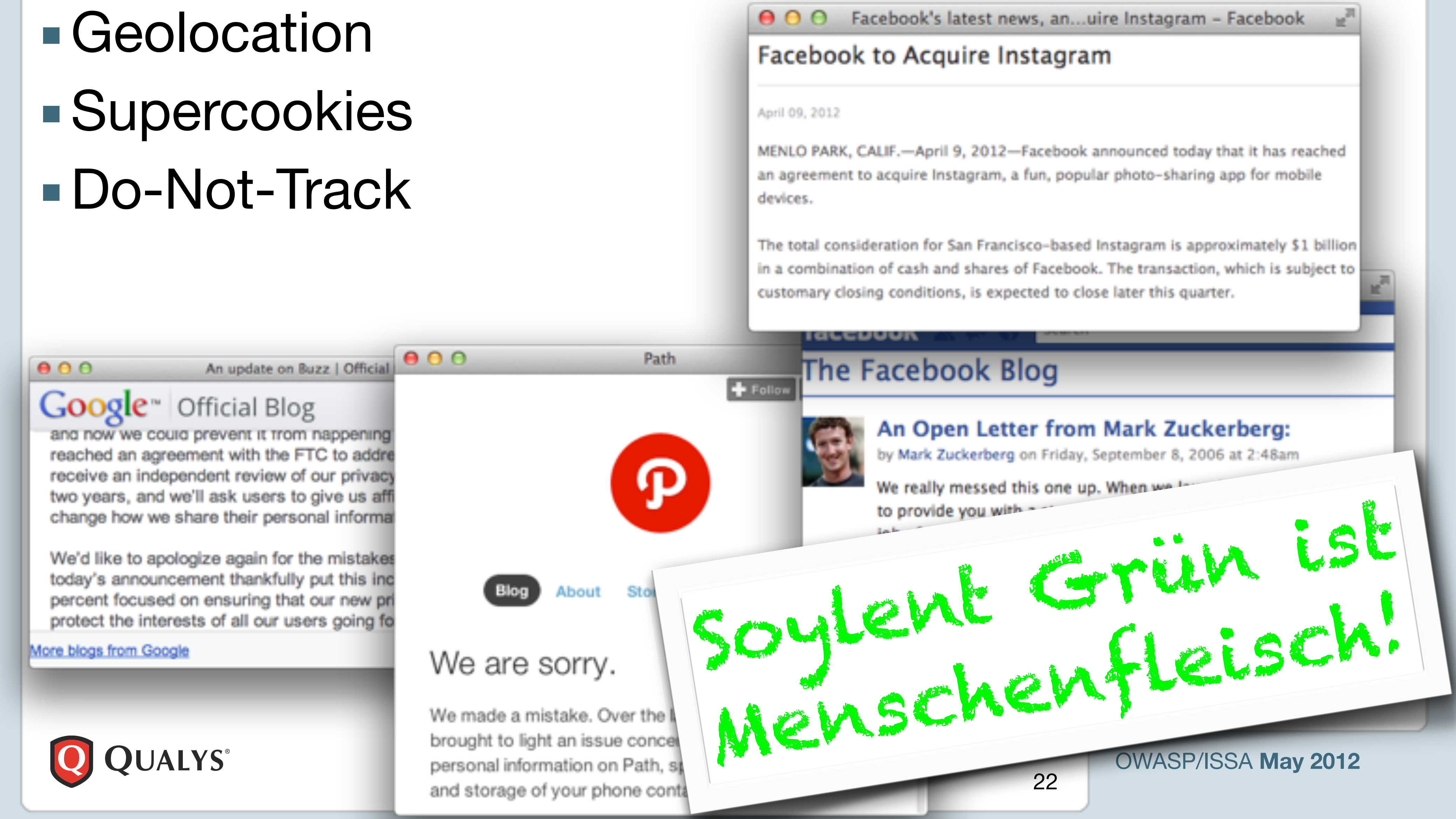
Here Lies Safe Links. Honest.

Mobile: The Re-Animator

- User expectations
  - Who cares about the URL anymore? It’s hardly even visible.
- Embedded browser-like features are not embedded browsers
  - Same Origin Policy enforcement
  - Certification verification
- User tracking

Privacy: 1 Billion Reasons To Care

- Geolocation
- Supercookies
- Do-Not-Track



Facebook to Acquire Instagram

April 09, 2012

MENLO PARK, CALIF.—April 9, 2012—Facebook announced today that it has reached an agreement to acquire Instagram, a fun, popular photo-sharing app for mobile devices.

The total consideration for San Francisco-based Instagram is approximately $1 billion in a combination of cash and shares of Facebook. The transaction, which is subject to customary closing conditions, is expected to close later this quarter.

The Facebook Blog

An Open Letter from Mark Zuckerberg:

by Mark Zuckerberg on Friday, September 8, 2006 at 2:48am

We really messed this one up. When we ... to provide you with ...

Google™ Official Blog

and now we could prevent it from happening reached an agreement with the FTC to addre receive an independent review of our privacy two years, and we'll ask users to give us aff change how we share their personal informa

We'd like to apologize again for the mistakes today's announcement thankfully put this inc percent focused on ensuring that our new pri protect the interests of all our users going fo

More blogs from Google

We are sorry.

We made a mistake. Over the l brought to light an issue conce personal information on Path, sp and storage of your phone conta

Soylent Grün ist Menschenfleisch!

Ongoing Threats & Issues

- Frames
  - Sharing, nesting, moving between Origins
- Cacheing
  - Poison different origins
  - Another way to track UAs?
- Plugins
  - Outside of sandbox, outside of HTML5
  - Worse security than browsers
- Passwords

HTML5 Is Good For You

- Beware of legacy support for and within old browsers
- Abolish plugins
- Deploy headers: X-Frame-Options, HSTS, CSP
- Data security is better

Thank You!

Mike Shema

mshema@qualys.com

[http://deadliestwebattacks.com/]

QUALYS®

Recognizing Positive Security Design

- Acknowledges threats intended to counter, and those it doesn't
- Encrypted transport
- Adherence to Same Origin
- Preflight checks for authorization
- Authentication & authorization grants have short lifetimes
- Requires minimum privilege, minimum data