DOES WEB 2.0 NEED WEB SECURITY 2.0?

RSACONFERENCE2010

SECURITY DECODED

Mike Shema
Qualys, Inc.

Session ID: SPO1-203
Session Classification: Advanced

OVERVIEW

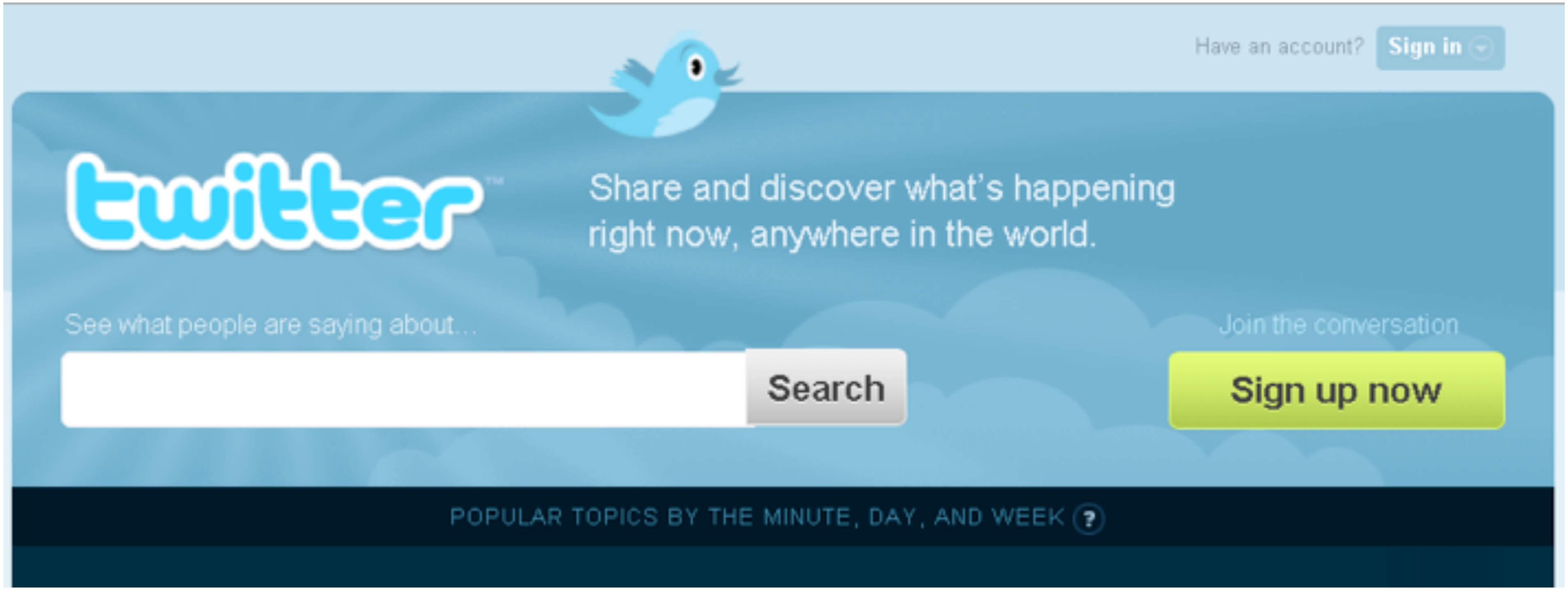
- Is there a definition for Web 2.0 that's useful for discussing security?
- What aspects of attacks have evolved that require new defenses?
- Where do new security controls need to be applied?
- How can next generation security be applied now?

DEFINITION IN SEARCH OF A MEANING

- …an amalgam of business models, profitability, various adjectives for economy, and users.
  - "2.0"– a label seemingly applied to everything without explaining anything.
  - Security may be influenced by business models, but vulnerabilities are not.

- More technical definitions tend to describe particular manifestations of HTML4, CSS, and JavaScript.

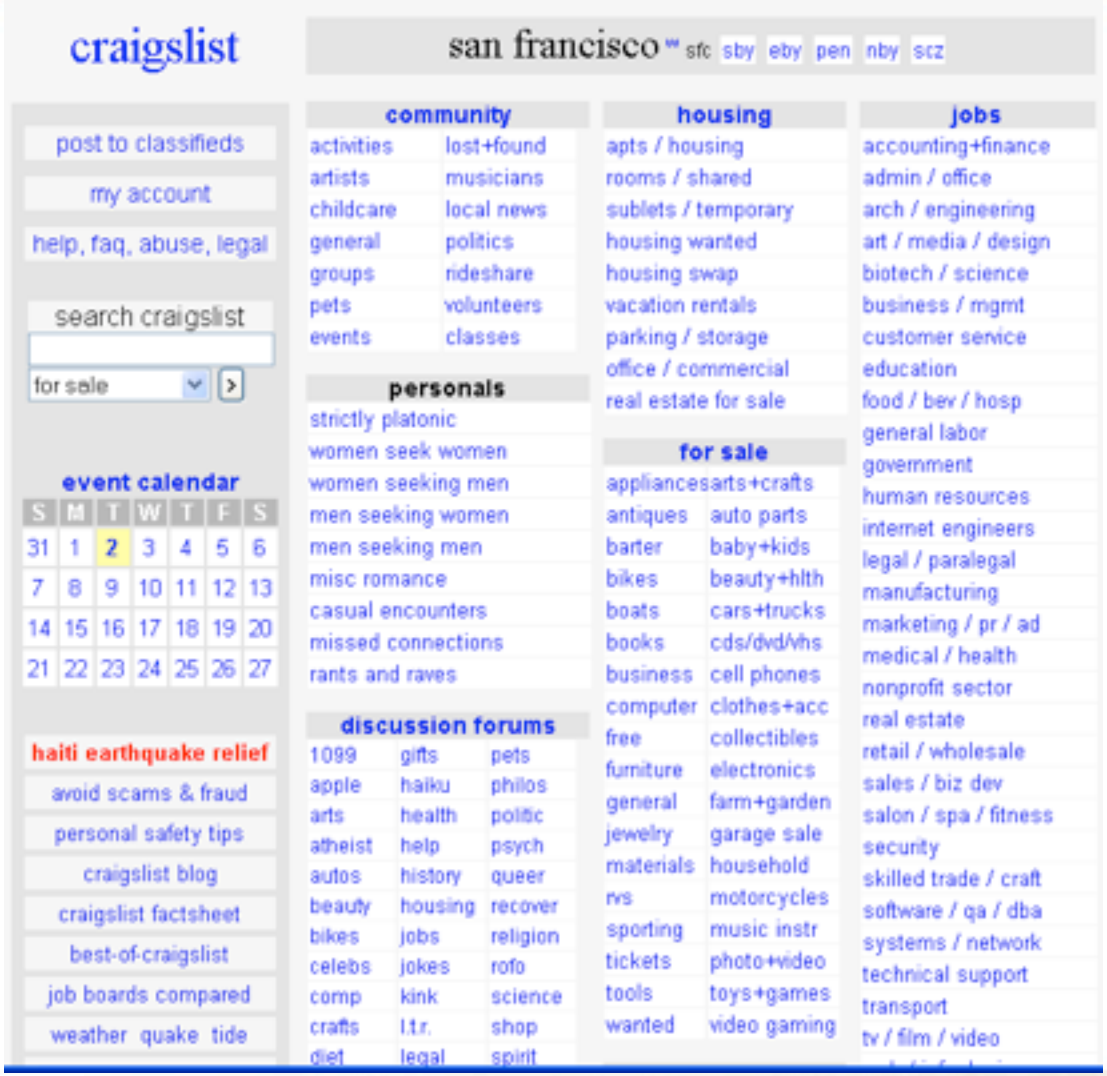
WEB 2.0?



Share and discover what's happening right now, anywhere in the world.

Have an account?
Sign in
twitter
See what people are saying about...
Search
Join the conversation
Sign up now
POPULAR TOPICS BY THE MINUTE, DAY, AND WEEK ?

NOT WEB 2.0?



craigslist

san francisco w sfc sby eby pen nby scz

post to classifieds

my account

help, faq, abuse, legal

search craigslist

for sale >

event calendar

S	M	T	W	T	F	S
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27

haiti earthquake relief

avoid scams & fraud

personal safety tips

craigslist blog

craigslist factsheet

best-of-craigslist

job boards compared

weather quake tide

community

activities	lost+found
artists	musicians
childcare	local news
general	politics
groups	rideshare
pets	volunteers
events	classes

personals

strictly platonic
women seek women
women seeking men
men seeking women
men seeking men
misc romance
casual encounters
missed connections
rants and raves

discussion forums

1099	gifts	pets
apple	haiku	philos
arts	health	politic
atheist	help	psych
autos	history	queer
beauty	housing	recover
bikes	jobs	religion
celebs	jokes	rofo
comp	kink	science
crafts	l.t.r.	shop
diet	legal	spirit

housing

apts / housing
rooms / shared
sublets / temporary
housing wanted
housing swap
vacation rentals
parking / storage
office / commercial
real estate for sale

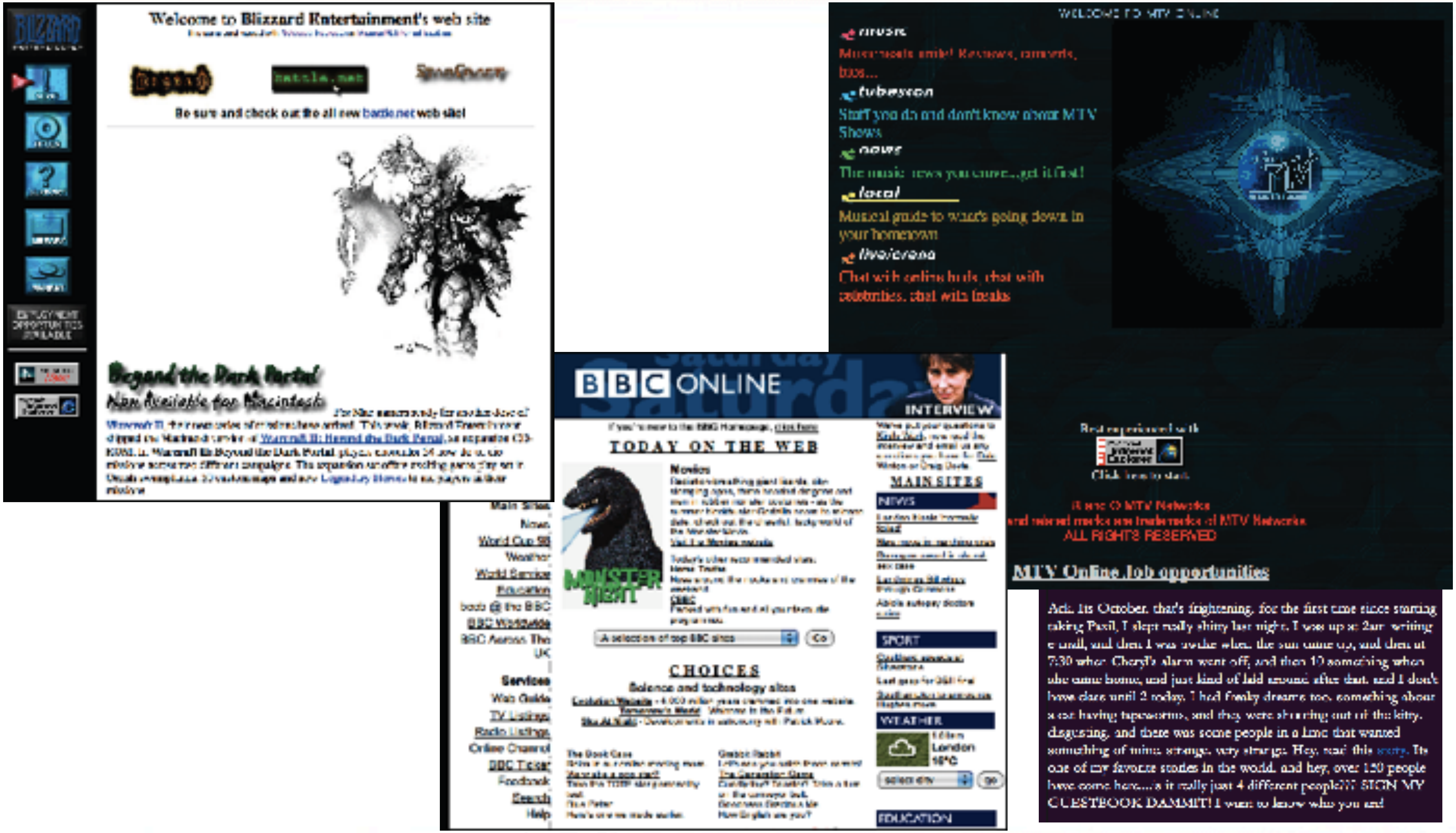
for sale

appliances	arts+crafts
antiques	auto parts
barter	baby+kids
bikes	beauty+hlth
boats	cars+trucks
books	cds/dvd/vhs
business	cell phones
computer	clothes+acc
free	collectibles
furniture	electronics
general	farm+garden
jewelry	garage sale
materials	household
rvs	motorcycles
sporting	music instr
tickets	photo+video
tools	toys+games
wanted	video gaming

jobs

accounting+finance
admin / office
arch / engineering
art / media / design
biotech / science
business / mgmt
customer service
education
food / bev / hosp
general labor
government
human resources
internet engineers
legal / paralegal
manufacturing
marketing / pr / ad
medical / health
nonprofit sector
real estate
retail / wholesale
sales / biz dev
salon / spa / fitness
security
skilled trade / craft
software / qa / dba
systems / network
technical support
transport
tv / film / video

1998: GAMES, NEWS, & ROCK 'N' ROLL



Welcome to Blizzard Entertainment's web site

Be sure and check out the all new battle.net web site!

Beyond the Dark Portal

Now Available for Macintosh

[illegible] Warcraft II [illegible] Warcraft II: Beyond the Dark Portal [illegible] Warcraft II: Beyond the Dark Portal [illegible] Legendary Heroes [illegible] missions

BBC ONLINE

INTERVIEW

If you're new to the BBC Homepage, click here

TODAY ON THE WEB

Movies

MONSTER NIGHT

A selection of top BBC sites

CHOICES

Science and technology sites

MAIN SITES

NEWS

SPORT

WEATHER

London 18°C

EDUCATION

Main Sites
News
World Cup 98
Weather
World Service
Education
books @ the BBC
BBC Worldwide
BBC Across The UK

Services
Web Guide
TV Listings
Radio Listings
Online Channel
BBC Ticket
Feedback
Search
Help

WELCOME TO MTV ONLINE

music
Music news smile! Reviews, concerts, bios...

tubescan
Stuff you do and don't know about MTV Shows

news
The music news you crave...get it first!

local
Musical guide to what's going down in your hometown

livearena
Chat with online hosts, chat with celebrities, chat with freaks

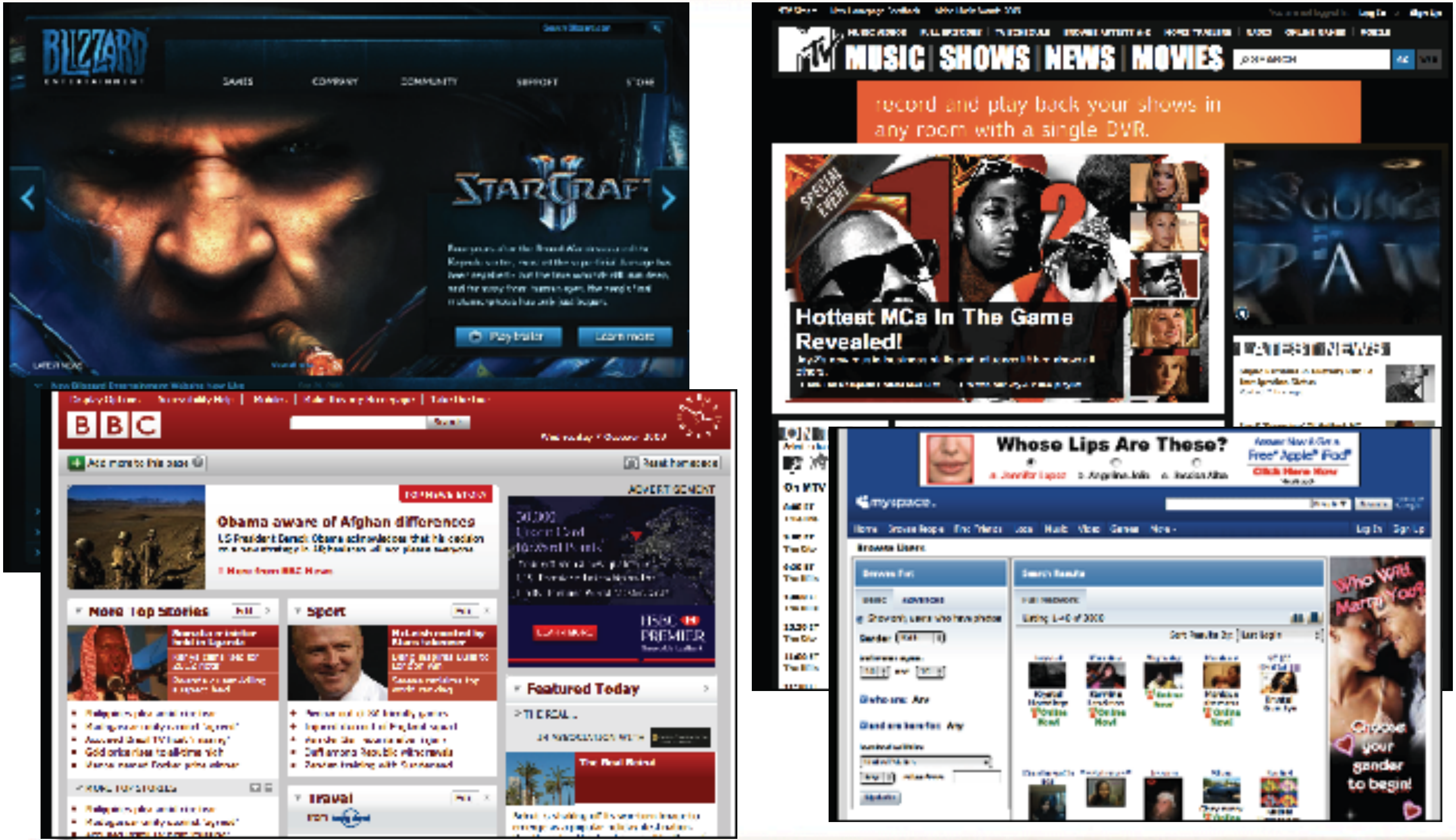
Best experienced with
Click here to start.

® and © MTV Networks
and related marks are trademarks of MTV Networks.
ALL RIGHTS RESERVED

MTV Online Job opportunities

Ack. Its October. that's frightening. for the first time since starting taking Paxil, I slept really shitty last night. I was up at 2am writing e-mail, and then I was awake when the sun came up, and then at 7:30 when Cheryl's alarm went off, and then 10 something when she came home, and just kind of laid around after that. and I don't have class until 2 today. I had freaky dreams too. something about a cat having tapeworms, and they were shooting out of the kitty. disgusting. and there was some people in a line that wanted something of mine. strange. very strange. Hey, read this story. Its one of my favorite stories in the world. and hey, over 150 people have come here....is it really just 4 different people??? SIGN MY GUESTBOOK DAMMIT! I want to know who you are

2009: NOW WITH PICTURES! (AND AD BANNERS)



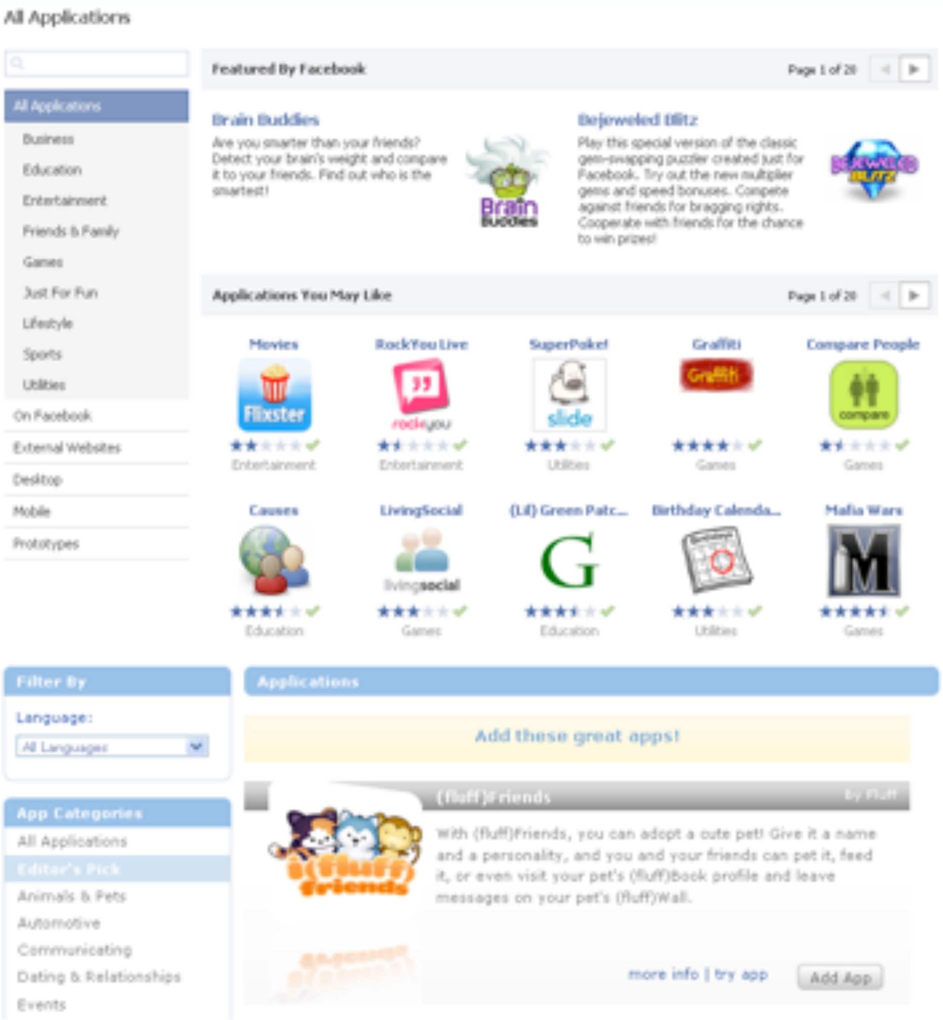
THE NETWORK IS FINALLY THE COMPUTER (AGAIN)

“Beta version 0.10 of Mosaic, NCSA's X/Motif-based networked information systems browser, including full source code and binaries … is now at ftp.ncsa.uiuc.edu...”

-- Marc Andreessen, comp.infosystems.gopher, March 1993

“I WILL WORK HARDER!”*

- Web sites pushing the browser to more closely model desktop application behavior.
- Web sites commingling more dynamic content from third parties, including JavaScript.



All Applications

All Applications
Business
Education
Entertainment
Friends & Family
Games
Just For Fun
Lifestyle
Sports
Utilities
On Facebook
External Websites
Desktop
Mobile
Prototypes

Featured By Facebook — Page 1 of 28

Brain Buddies
Are you smarter than your friends? Detect your brain's weight and compare it to your friends. Find out who is the smartest!

Bejeweled Blitz
Play this special version of the classic gem-swapping puzzler created just for Facebook. Try out the new multiplier gems and speed bonuses. Compete against friends for bragging rights. Cooperate with friends for the chance to win prizes!

Applications You May Like — Page 1 of 28

Movies	RockYou Live	SuperPoke!	Graffiti	Compare People
Entertainment	Entertainment	Utilities	Games	Games

Causes	LivingSocial	(Lil) Green Patc...	Birthday Calenda...	Mafia Wars
Education	Games	Education	Utilities	Games

Filter By
Language:
All Languages

App Categories
All Applications
Editor's Pick
Animals & Pets
Automotive
Communicating
Dating & Relationships
Events

Applications

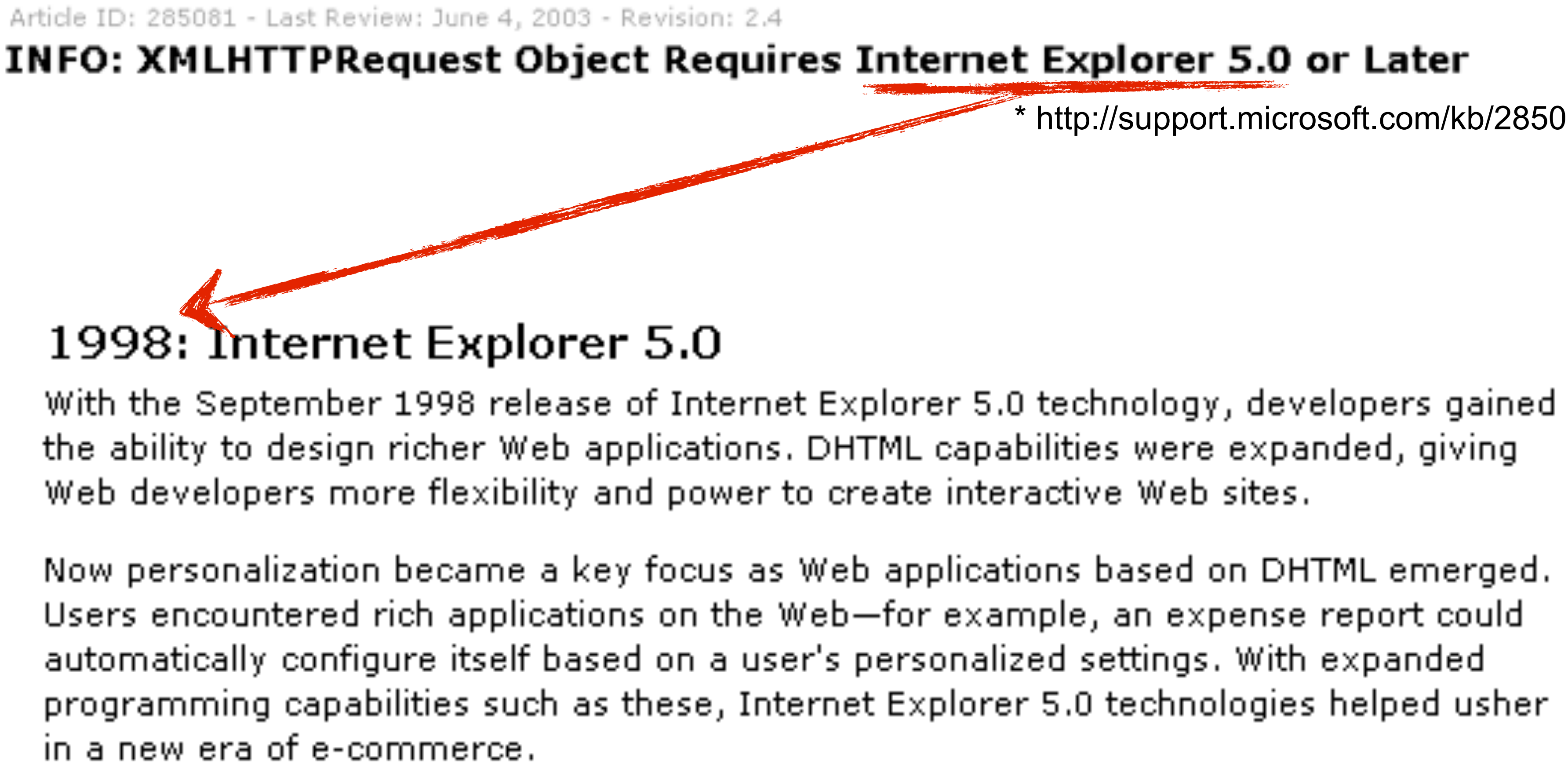
Add these great apps!

(fluff)Friends — by Fluff
With (fluff)Friends, you can adopt a cute pet! Give it a name and a personality, and you and your friends can pet it, feed it, or even visit your pet's (fluff)Book profile and leave messages on your pet's (fluff)Wall.

more info | try app — Add App

*Boxer, from *Animal Farm* by George Orwell

TOMORROW’S WEB WITH YESTERDAY’S TECH



Article ID: 285081 - Last Review: June 4, 2003 - Revision: 2.4

INFO: XMLHTTPRequest Object Requires Internet Explorer 5.0 or Later

1998: Internet Explorer 5.0

With the September 1998 release of Internet Explorer 5.0 technology, developers gained the ability to design richer Web applications. DHTML capabilities were expanded, giving Web developers more flexibility and power to create interactive Web sites.

Now personalization became a key focus as Web applications based on DHTML emerged. Users encountered rich applications on the Web—for example, an expense report could automatically configure itself based on a user's personalized settings. With expanded programming capabilities such as these, Internet Explorer 5.0 technologies helped usher in a new era of e-commerce.

* http://support.microsoft.com/kb/285081

* http://www.microsoft.com/windows/WinHistoryIE.mspx

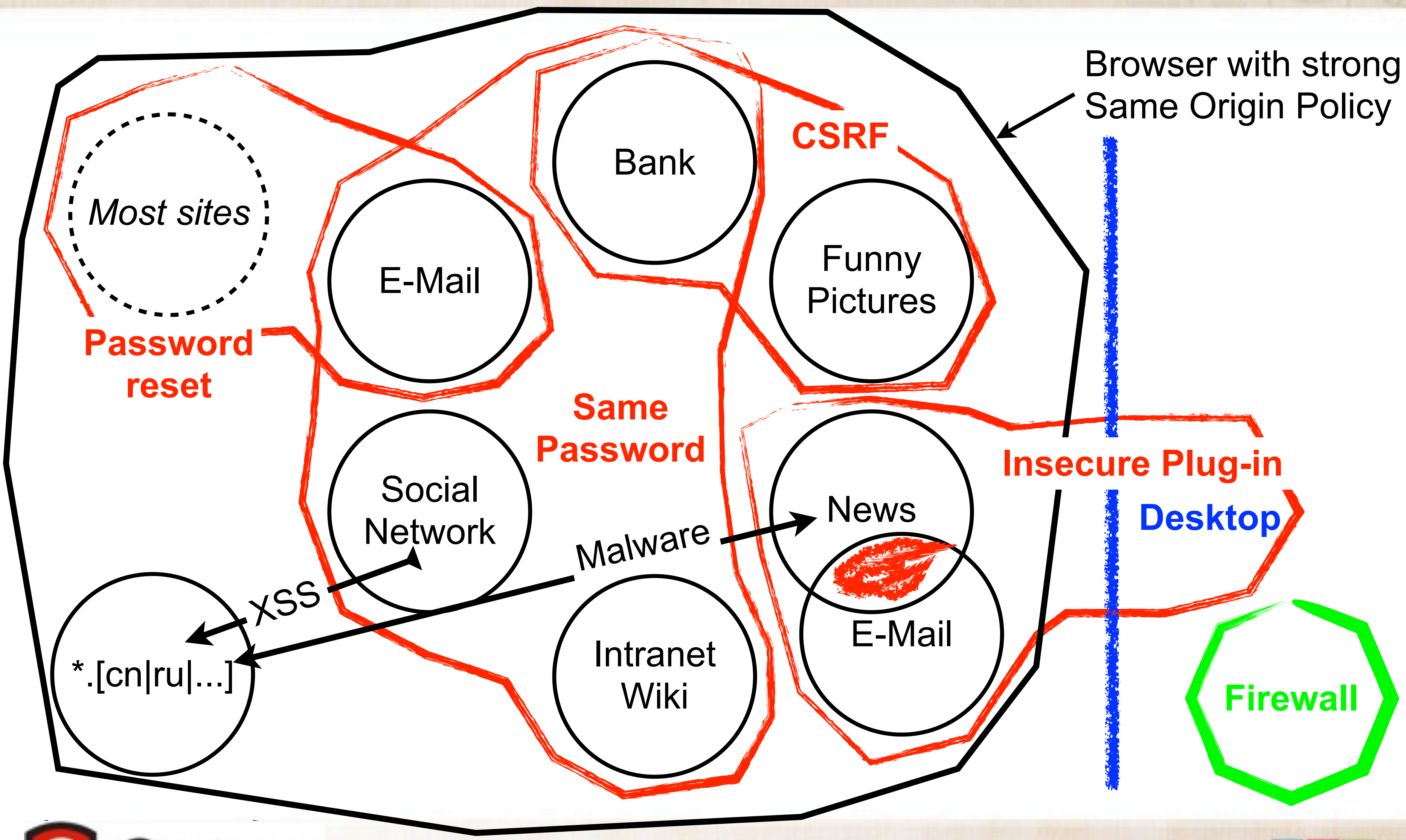
BROWSER COMPUTING & INFO SECURITY

- The browser becomes the network boundary.
  - One-hop distance from web site to desktop.
  - The browser can couple a secure web site with an insecure one.
  - Cross-site request forgery, clickjacking, drive-by downloads.
- Targeting information in the browser doesn't need a buffer overflow or administrator access to the desktop.

“TRIPLE DOG DARE” SECURITY METRIC

- How much do you trust your browser?
  - http://bit.ly/wszWO
  - http://bit.ly/A6Ca
  - http://bit.ly/lSxst
  - http://bit.ly/z18Rv
  - http://bit.ly/OApJX
  - http://bit.ly/2z3MBj
- XSS, CSRF, clickjacking, SQL injection, malware, insecure plug-ins, oh my

DIAGRAM OF ULTIMATE DOOM



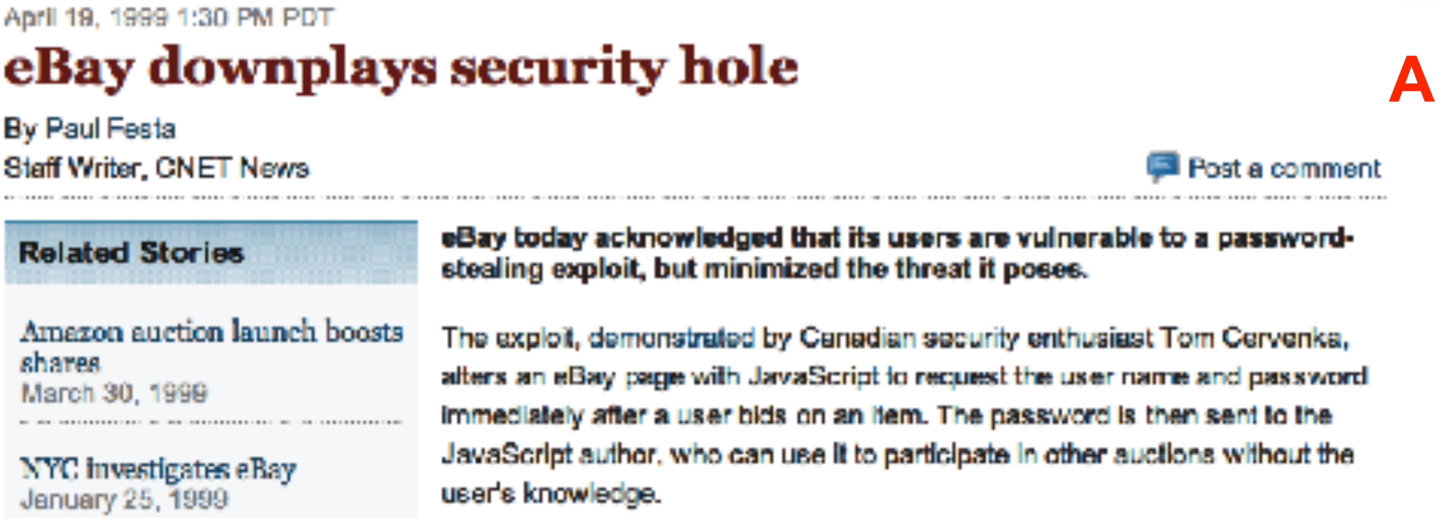
BROWSER COMPUTING & WEB SECURITY

- High degree of interactivity -- more states to track for authentication & authorization.
- User-generated content -- more injection vectors for JavaScript and malicious code.
- Aggregated content -- stressing the Same Origin Policy.
- Advertising banners -- delivery vectors for malware and scams.
- Immense scale -- more motivation to attack one site to affect millions of users.

THE VULNERABILITY REMAINS THE SAME

- Web application vulnerabilities largely unchanged over the past decade.
- Better nomenclature and documentation
  - OWASP & WASC, threats vs. weaknesses
- The sophistication of exploits has increased.
  - https://labs.portcullis.co.uk/application/xss-tunnelling/xss-tunnel/
  - http://xss-proxy.sourceforge.net/
- Still rely on weak identification of the user (passwords) and of the browser (cookies).

THE VULNERABILITY REMAINS THE SAME



April 19, 1999 1:30 PM PDT

eBay downplays security hole

By Paul Festa
Staff Writer, CNET News

Post a comment

Related Stories

Amazon auction launch boosts shares
March 30, 1999

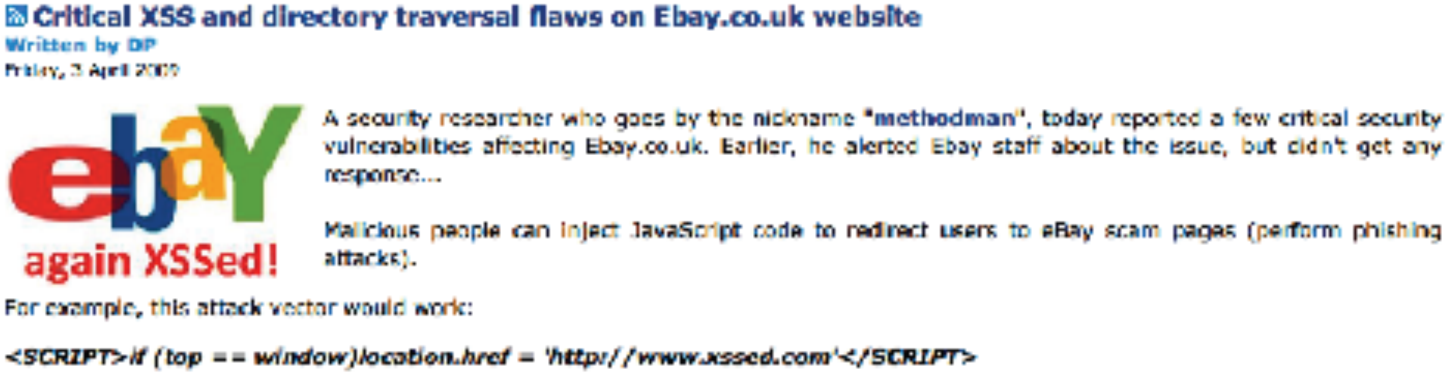
NYC investigates eBay
January 25, 1999

eBay today acknowledged that its users are vulnerable to a password-stealing exploit, but minimized the threat it poses.

The exploit, demonstrated by Canadian security enthusiast Tom Cervenka, alters an eBay page with JavaScript to request the user name and password immediately after a user bids on an item. The password is then sent to the JavaScript author, who can use it to participate in other auctions without the user's knowledge.

April 19, 1999

April 3, 2009



Critical XSS and directory traversal flaws on Ebay.co.uk website

Written by DP
Friday, 3 April 2009

A security researcher who goes by the nickname "**methodman**", today reported a few critical security vulnerabilities affecting Ebay.co.uk. Earlier, he alerted Ebay staff about the issue, but didn't get any response...

Malicious people can inject JavaScript code to redirect users to eBay scam pages (perform phishing attacks).

For example, this attack vector would work:

```
<SCRIPT>if (top == window)location.href = 'http://www.xssed.com'</SCRIPT>
```

EXPLOITS SCALING FOR PROFIT

- Simple attacks work.
- HTML & JavaScript offer an almost universal execution environment
  - Regardless of operating system, patch level, anti-virus, host-based firewall, etc.
  - Plus SSL for outbound, encrypted communications
- Popular sites present a target-rich environment, piggybacking the assumption of trust.
  - Sites more often infected with a single iframe or script tag rather than defaced.

THE IMPACT OF SCALE ON SECURITY

- Given Enough Eyeballs Theories
  - …all bugs are shallow. (Eric Raymond)
  - …all bugs are exploitable.
  - …all web sites are profitable.
- Shema’s Witches’ Brew Conjecture
  - Eyeballs and bugs are profitable.

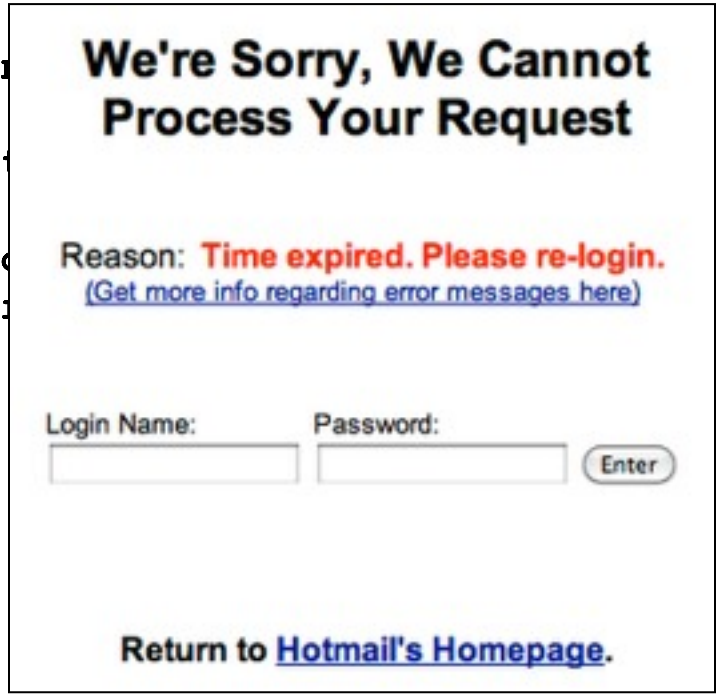
EXPLOITS COMBINING MULTIPLE SITES

- Protecting your users from other web sites.
  - Cross-site request forgery
  - Clickjacking
- Protecting your users from your own site.
  - Mash-ups and mini apps -- placing JavaScript from minimally vetted sources inside the browser's Same Origin Policy.
  - Malicious Facebook apps (http://securitylabs.websense.com/content/Blogs/3563.aspx)
- Isolating advertising banners.

HACKING THE ~~MODERN~~ 1998 SAAS

- Target a HotMail account with an e-mail that contains a malicious image tag, <img src="…">

```
javascript:errurl='http://www.because-we-ca
users/anon/hotmail/getmsg.htm';
nomenulinks=top.submenu.document.links.leng
for(i=0;i<nomenulinks-1;i++) {
    top.submenu.document.links[i].target='w
    top.submenu.document.links[i].href=erru
}
noworklinks=top.work.document.links.length;
for(i = 0; i < noworklinks - 1; i++) {
    top.work.document.links[i].target='work
    top.work.document.links[i].href=errurl;
}
```



We're Sorry, We Cannot Process Your Request

Reason: Time expired. Please re-login.
(Get more info regarding error messages here)

Return to Hotmail's Homepage.

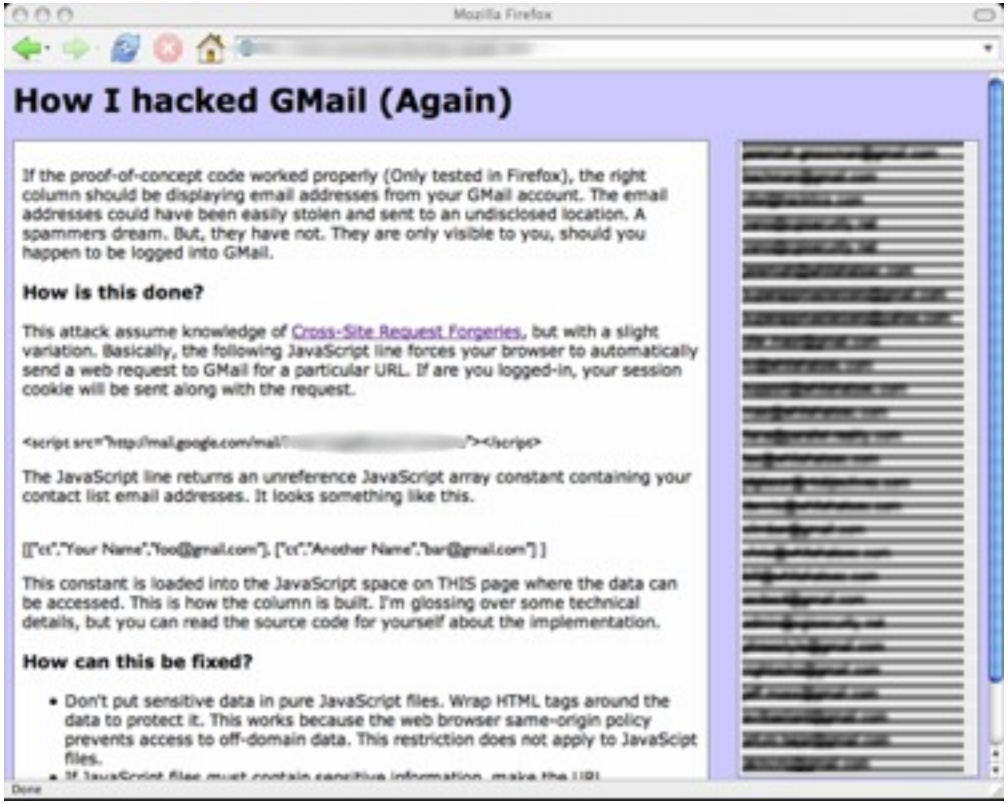
* http://tinyurl.com/yjwyqke

HACKING THE MODERN SAAS

- Target a GMail account with a web site that enumerates an authenticated user’s contact list.

```
function Array() {
...
getNext = function(x) {
obj[ind++] setter = getNext;

if(x) {
var str = x.toString();
if ((str != 'ct') &&
    (typeof x != 'object') &&
    (str.match(/@/))) {
var row = table.insertRow(-1);
var td = row.insertCell(-1);
td.innerHTML = str;
}
```



How I hacked GMail (Again)

If the proof-of-concept code worked properly (Only tested in Firefox), the right column should be displaying email addresses from your GMail account. The email addresses could have been easily stolen and sent to an undisclosed location. A spammers dream. But, they have not. They are only visible to you, should you happen to be logged into GMail.

How is this done?

This attack assume knowledge of Cross-Site Request Forgeries, but with a slight variation. Basically, the following JavaScript line forces your browser to automatically send a web request to GMail for a particular URL. If are you logged-in, your session cookie will be sent along with the request.

```
<script src="http://mail.google.com/mail/[redacted]"></script>
```

The JavaScript line returns an unreference JavaScript array constant containing your contact list email addresses. It looks something like this.

```
[["ct","Your Name","foo@gmail.com"], ["ct","Another Name","bar@gmail.com"] ]
```

This constant is loaded into the JavaScript space on THIS page where the data can be accessed. This is how the column is built. I'm glossing over some technical details, but you can read the source code for yourself about the implementation.

How can this be fixed?

- Don't put sensitive data in pure JavaScript files. Wrap HTML tags around the data to protect it. This works because the web browser same-origin policy prevents access to off-domain data. This restriction does not apply to JavaScipt files.
- If JavaScript files must contain sensitive information, make the URL

[redacted]

* http://jeremiahgrossman.blogspot.com/2006/01/advanced-web-attack-techniques-using.html

MODERN MOTIVATIONS

- ~~Information wants to be free~~
- Users want free information
  - News, music, movies, personal data
- Freedom wants information
- Vulnerability markets
- Hacking as a Service
  - Denial of service
  - Spam
  - Malware
  - Anti-virus signature testing
  - Password cracking

据当地法律法规和政策，部分搜索结果未予显示。

Goo

1 2

DEPLOYING SECURE SITES

- Multiple dangers of hosting user-generated content.
- Securing the JavaScript environment for the site’s own code.
- Securing the JavaScript environment for hosting code from unknown or minimally vetted sources.
- Protecting your users from other sites’ insecurity.

USING FRAMEWORKS TO INCREASE SECURITY

- Code reuse. Don’t repeat yourself.
- Better than reinventing the wheel
  - ...along with reinventing vulnerabilities.
- Centralized functions, securely written.
  - SQL prepared statements vs. string concatenation
- Not guaranteed to be well-written.
  - Quality should rise to the top.

DOCUMENTATION GOES STALE

- MSDN from February 2007: * http://bit.ly/ddoHd8

  Since JSON is merely a subset of JavaScript literals, it can be parsed into an in-memory representation using the eval(expr) function... Consequently, the following single line of code is all that is needed to turn JSON text into a native representation:

  ```
  var value = eval( "(" + jsonText + ")" );
  ```

- New attacks emerge (e.g. GMail CSRF) that lead to improved coding practices
  - Choose to stay up to date with secure programming techniques
  - Choose to maintain secure patch levels for a framework

USING FRAMEWORKS FOR THE RIGHT REASON

- CSRF countermeasures
- More secure JSON parsing
- Native browser JSON parsing
- More secure rendering of user-supplied data (XSS countermeasures)
- JavaScript security & sandboxing
  - Google Caja
  - Facebook FBJS
  - ADsafe

ARE YOU BEING SERVED?

- The challenges to building a secure web application haven't fundamentally changed.
  - More threats looking for financial gain
  - More client-side complexity
  - More types of applications (and more user data!)
- What about relying on web applications for more secure business processes?
  - Software as a Service
  - Platform as a Service
  - Infrastructure as a Service

MOVING TO SERVICE-BASED APPLICATIONS

- Focus on information over infrastructure
- Fast deployment, easy termination
- Immediate scale and reach
- The cloud doesn't solve security, it changes risks vs. reward.
  - Auditing
  - Authentication
  - Data retention
  - Data separation
  - Privacy

LONG-STANDING SECURITY AREAS

- Vulnerabilities without borders
- Everyone has access to the application, even if they don’t have explicit access to your data.
- DDoS remains a concern
- CSRF and phishing will always attack users
- Poor passwords

EMERGING SECURITY AREAS

- Virtualized hosts
  - Security researchers looking into the impact of virtualization on PRNG entropy sources -- affects cryptographic primitives.
  - Probing the hypervisor for bugs.
- Looking ahead to privacy and legal concerns.
- Ensuring subpoenas don’t overreach access to commingled data.
- U.S. Stored Communications Act

OVERCOMING FEARS

- Data can’t leave my network
  - Some good reasons: compliance and legal
  - Uncertainty (is the data being protected or merely contained?)

- Okay, then how is my data being secured?
  - Encrypted channels
  - Encrypted storage
  - Secure backup
  - Secure deletion

USING SERVICES TO ELEVATE SECURITY

- Securing the network
  - Patch management
  - Vulnerability scanning
  - VPNs
- Securing the users
  - E-mail with virus scanning, etc.
  - Proxies with malware prevention, e.g. web reputation
- Securing the business
  - PCI compliance
  - Web app scanners
  - Source code & binary scanners

USING SERVICES PROVIDES BENEFITS..

- Reduce cost of infrastructure management
- Simple deployment and scalability
- On demand resources
- Potential portability of data from one service to another

...WHILE RELINQUISHING SOME CONTROL

- Strong authentication mechanisms, including password reset
- Auditing user activity
- Service level agreements
- Potentially weak support for portability of data

HTML5 – THE REAL 2.0

- HTML5 draft features creeping into browsers now.
- In-browser database will push more valuable information into the application.
- Relaxed rules for cross-domain requests increase the potential attack surface for malicious JavaScript.
- Improving some inherent security problems with JavaScript -- ECMAScript Harmony.

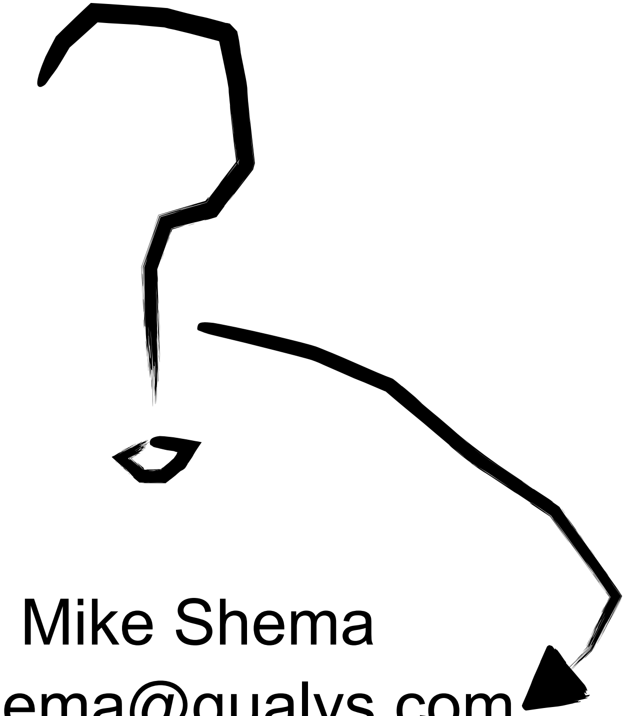
SUMMARY

- The web browser is the network border.
- Vulnerabilities have (mostly) remained the same, but threats have increased and attacks have become more sophisticated.
- Moving to the cloud (“* as a service”) has several implications for data security and control.
- Must understand what is being moved to the cloud -- is it infrastructure, development platform, application?

APPLY

- Address the basic problems first: XSS and SQL injection.
- Use open source libraries to avoid client-side security mistakes.
- Cloud-based applications provide ease of use at the cost of borderless access.
- Cloud-based computing solves some security problems, but creates others -- understand how deployment will affect the security context.

THANK YOU



Mike Shema
mshema@qualys.com