

Enabling Un-trusted Mashups

c70n3r@gmail.com



SECURITYBYTE

CONFERENCE & WORKSHOPS

2011

Talk Outline

- Definition
- Web Mashups
- Mashup Vulnerabilities
- Secure Mashup Principles & Technologies
- Solution: Today and Tomorrow

What is a Mashup?

- An experience delivered by combining properties of more than one sources



Web Mashup: Types

- An app that combines services from multiple origins to create new experiences
- Mostly based on DHTML. Also, the focus of this talk.
- Mashup Approaches:
 - Client-side: Browser retrieves and aggregates as per the provided template
 - Server-side: Backend aggregation then serving pre-composed mashup to the browser
 - Hybrid: Leverages benefits of approaches above

Note: From here on we refer web mashups as mashups

Web Mashup: The Business Case

- Ads were and will remain to be the backbone of Internet business model
 - User behavioral targeting, social and interactive ads are set to revolutionize further
- Social plugins and 3rd party widgets help drive engagement and rich user experience
- Need to grow. Getting viral. Enter app platforms. The ultimate manifestation of user generated content in mashups – FB, YAP, iGoogle

Web Mashup: The Technology Case

- Traditional tech stack provides little or no control over the embedded service
- Intrinsically insecure model
- Ads do go bad. Widgets do get compromised.
- But we have a legal agreement?
 - Yes, that's just a partial reactive solution.
 - What about 3rd part developer? Does the agreement going to stop him sitting in *&^%\$(!, %\$@#),.....

Web Mashup: Client-side with Ads and Social Plugins

in.movies.yahoo.com/blogs/movieplayer/dil-toh-baccha-hai-ji-173834884.html

Hi, **Bishan** | Sign Out | Help

YAHOO! MOVIES
INDIA

Search

HOME TRAILERS & CLIPS NEWS & GOSSIP PH

TRENDING NOW Anna Hazare Jan Lokpal Bill Yahoo! Movieplex IRCTC Live Scores Movie reviews EPL n

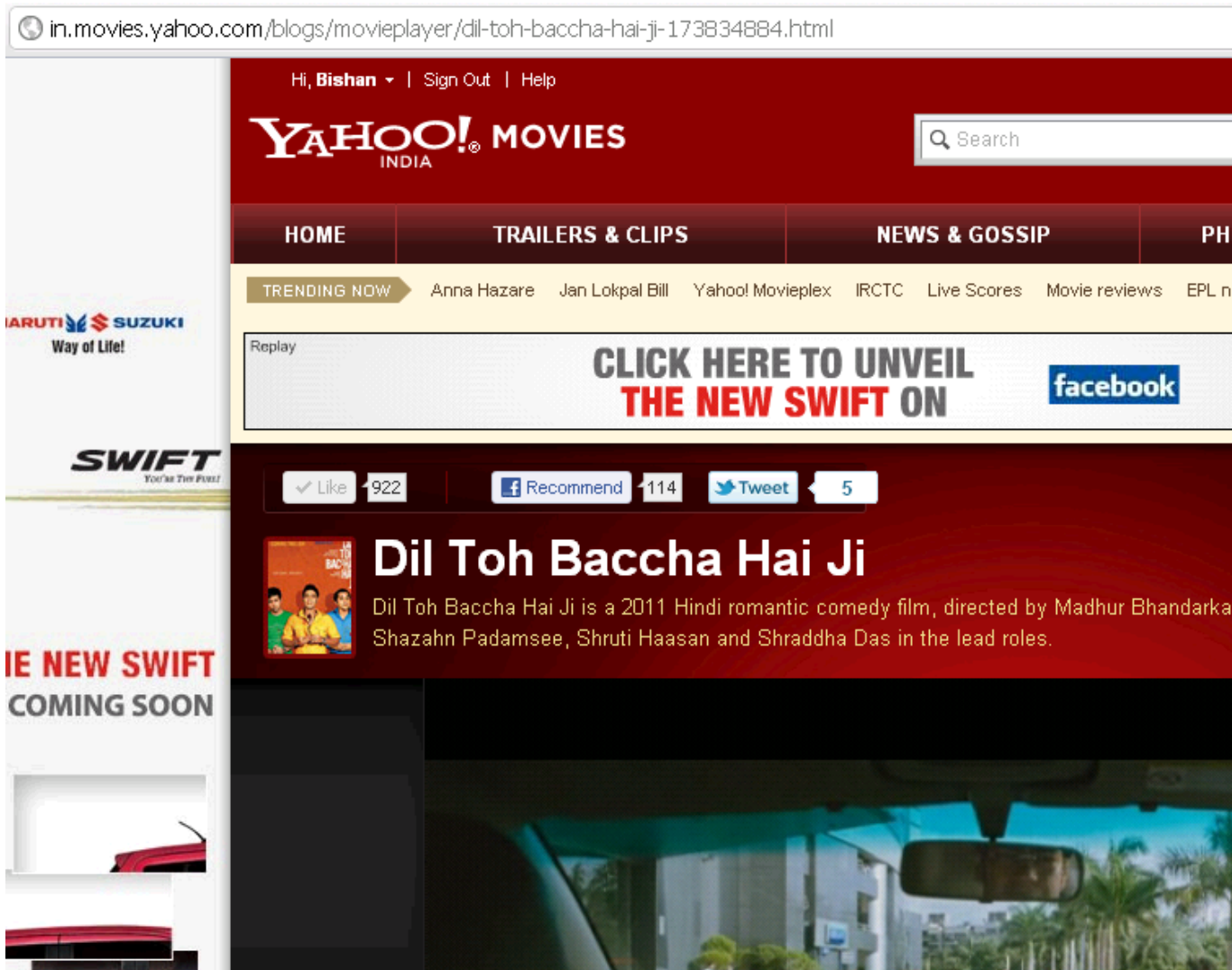
Replay

**CLICK HERE TO UNVEIL
THE NEW SWIFT ON** **facebook**

Like 922 Recommend 114 Tweet 5

Dil Toh Baccha Hai Ji

Dil Toh Baccha Hai Ji is a 2011 Hindi romantic comedy film, directed by Madhur Bhandarkar. Shazahn Padamsee, Shruti Haasan and Shraddha Das in the lead roles.



SECURITYBYTE

CONFERENCE & WORKSHOPS

2011

Web Mashup: Client-side with 3rd Party developers

The screenshot shows a web browser displaying a Facebook page for "Levi's Store - SoHo". A Bing map is overlaid on the page, showing the location of the store in New York, NY. The map includes a red location pin and the text "Levi's Store - SoHo Shopping & Retail New York, NY". Below the map are buttons for "Like", "Get Directions", and "Edit".

On the right side of the page, there is a section titled "HELP US REACH 100,000 PLEDGES" with a large digital counter showing "030308" and the text "GLOBAL PLEDGES". Below this is a paragraph: "With your help, we can raise awareness of a global crisis and **bring clean water to up to 8,000 people—for life.** All we need is 100,000 pledges to make it happen."

At the bottom of the page, there is a section titled "MORE ABOUT WATER.ORG" with the text: "Did you know that nearly 1 billion people don't have access to safe, clean water? Water.org does, and they're doing something about it. So can you. Join us as we partner with Water.org to assist people around the globe in obtaining sustainable water and sanitation systems. Pledge your support today and help create a world where every person can have access to this basic human right."

The browser's developer console is open, showing the HTML structure of the page. The selected element is an `<iframe>` tag with the following attributes: `width="100%" scrolling="no" height="1880px" frameborder="0" style="border:none" src="http://scg-levis-go-forth.herokuapp.com/en"`.

Web Mashups: Hybrid with 3rd party developers & providers

The screenshot shows a web browser window with the address bar displaying "my.yahoo.com". The page is a mashup of several services:

- Personal Assistant:** Includes widgets for Mail, Weather, Horoscope, Calendar, Stocks, and EU Score.
- Advertisement:** A banner for "make my trip" with the text "Fly from Tourism to B'lore at lowest airfares" and a "Book now!" button.
- Stock Portfolios:** A table showing stock quotes for DJIA, NYA, S&P 500, and YHOO.
- EU Scoreboard:** A message stating "Your scoreboard is empty. Please add a sport or team."
- Weather:** A widget showing "21°C Mostly Cloudy" for Bangalore, India.
- Mashable:** A news section with a trending story titled "What Does Steve Jobs' Retirement Mean for the Future of Apple? [VIDEO]" and a "LATEST NEWS" section.
- LinkedIn:** A section for "Mafia Wars, by Zynga" with a "PLAY NOW" button and a description: "Create a powerful empire in Mafia Wars, the biggest crime game in the world. Build, manage, and arm your empire to take control."
- TotalBeauty.com:** A section for "Beauty tips and how-tos" with a link to "Detox: Diets: My Three-Day 'Fruit Rush'".

Web Mashup: The Tech Stack

- **Server-side:** No standard solutions. Mostly custom implementations, proxies and hacks
- **Client-side:** The more popular mashup. Leverages browser SOP (Same Origin Policy).
 - Two solutions: Scripts and iframes
 - Script based
 - Offers NO separation but provides FULL interaction
 - Interaction not authenticated, nor can confidentiality or integrity be ensured
 - Iframe based
 - FULL separation between cross origins
 - NO separation within the same origin
 - NO provision for interaction between components

Mashup Vulnerabilities: iframe based

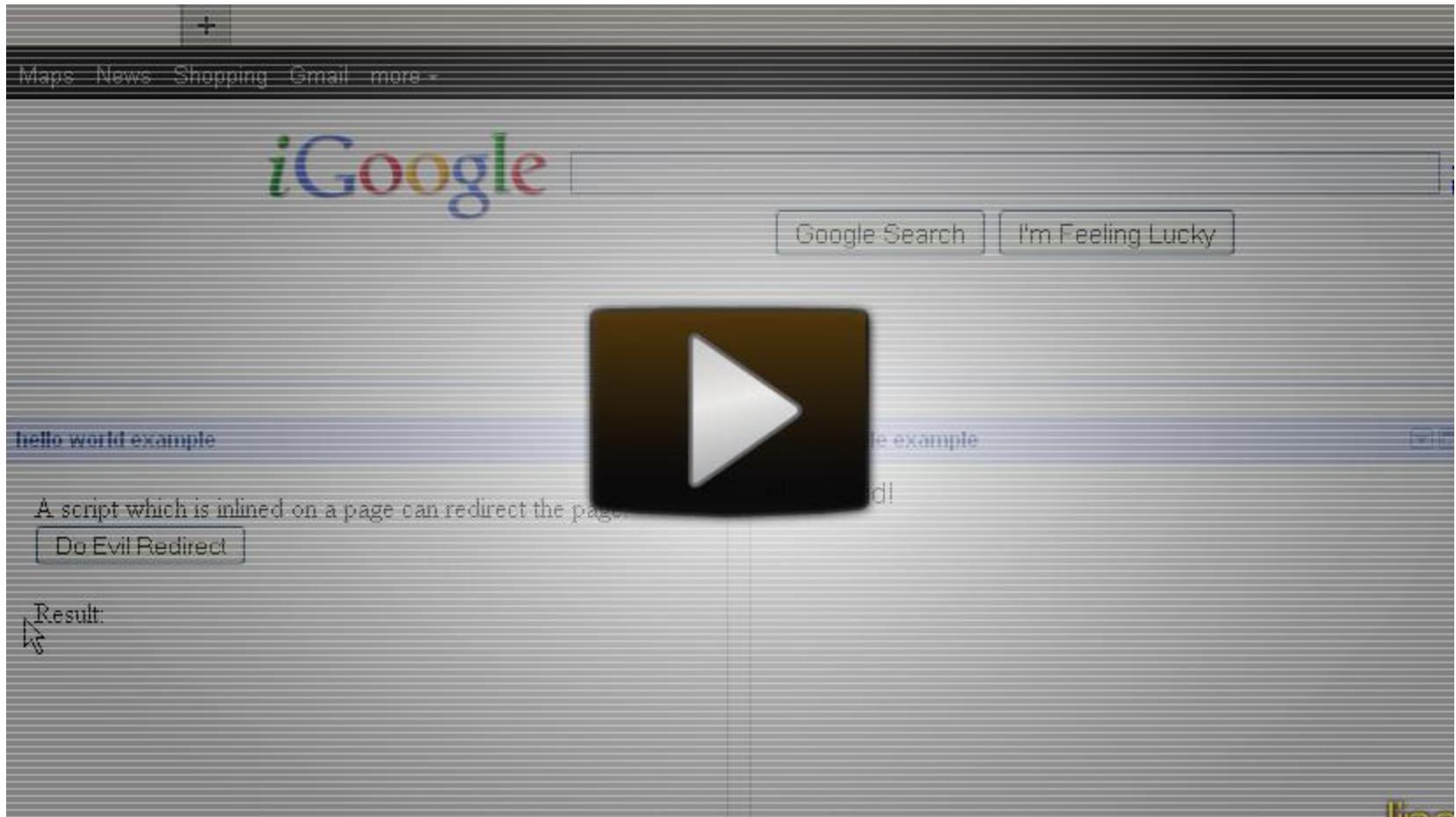
- **Malicious Redirection**
 - `top.location = http://s0m3phishing.com`
- **Fake / Malicious UI**
 - `<form method=...>`, `window.open()`
- **Drive-by Downloads/Malware**
 - `Content-Disposition: attachment`
- **Denial of Service (DoS) and Noise**
 - Infinite `alert()` and `while` loops
- **History Sniffing/Mining**
 - `getComputedStyle()`
- **Referrer Leak**
 - `Referrer: http://<ip>/r.html?a=secret&b=private`
- **LAN Scanning**
 - ``

Mashup Vulnerabilities: Script based

- Steal Username, Password and other secret data by calling, intercepting or spoofing DOM events like `onsubmit`
- Steal cookies via `document.cookie`
- Malicious GET and POST via `xhr.open`
- Abuse features like `autocomplete`
- **All iframe vulnerabilities**
- And, many more.....

Redirection Attack: FB iframe tab

Redirection Attack: igooglegadgets



Fake Login

facebook.com/pages/History_iframe/236914123018065?sk=app_203221333070867

The screenshot shows a Facebook page for a user named 'History_iframe'. The page layout includes a top navigation bar with the Facebook logo and a search bar. Below the navigation bar, there is a section for 'Link Your Page to Your Twitter Account' with a 'Click here' link. The main content area features the page name 'History_iframe' followed by 'login' and a 'Like' button. Below this, there is a 'Facebook Login' form with fields for 'Email' and 'Password', a 'Keep me logged in' checkbox, and 'Log In' and 'Sign up for Facebook' buttons. A 'Forgot your password?' link is also present. The left sidebar contains a navigation menu with options like 'Get Started', 'Wall', 'Info', 'Photos', 'History', 'infinite', 'alerts', and 'login' (which is highlighted). Below the menu, there is a '0 like this' section and links for 'Add to My Page's Favorites', 'Subscribe via RSS', and 'Share'. At the bottom of the page, there is a language selection menu with options for English (US), বাংলা, हिन्दी, ਪੰਜਾਬੀ, தமிழ், తెలుగు, and മലയാളം.

facebook

Search

Link Your Page to Your Twitter Account
You can now export your Facebook Page updates to Twitter. [Click here](#) to enable this feature.

History_iframe ▶ login Like

Community · Edit Info

Facebook Login

Email:

Password:

Keep me logged in

Log In or Sign up for Facebook

[Forgot your password?](#)

0 like this

Add to My Page's Favorites
Subscribe via RSS
Share

English (US) বাংলা हिन्दी ਪੰਜਾਬੀ தமிழ் తెలుగు മലയാളം Es

SECURITYBYTE

CONFERENCE & WORKSHOPS

2011

Fake Login Pop-up

Drive-by Downloads

The screenshot shows the XP Antivirus 2008 interface. The main status area displays a 'Protection level: low' with a progress bar indicating the level. Below this, a 'Recommendation' section suggests to 'Update antivirus'. The status of various protection features is listed as follows:

Protection Feature	Status
Virus Protection	NOT FOUND
Spyware Protection	NOT FOUND
General Security	NOT FOUND
Automatic Updating	NOT FOUND

At the bottom of the status area, there are two main action buttons: 'Scan Now' (with the subtext 'Check your computer for viruses and other threats') and 'Update Now' (with the subtext 'Download the latest protection to help keep your PC safe').

Registration information at the bottom right shows: 'Last scan: 22.07.2008 12:27:05', 'Total scans: 1', 'Registration e-mail: Unregistered', and 'Registration code:'. A yellow banner at the bottom left of the window reads: 'Get full real-time protection with XP Antivirus 2008'.

Drive-by Downloads

69.50.201.152



Warning: Something's Not Right Here!

69.50.201.152 contains malware. Your computer might catch a virus if you visit this site.

Google has found malicious software may be installed onto your computer if you proceed. If you've visited this site in the past or you trust this site, it's possible that it has just recently been compromised by a hacker. You should not proceed, and perhaps try again tomorrow or go somewhere else.

We have already notified 69.50.201.152 that we found malware on the site. For more about the problems found on 69.50.201.152, visit the Google [Safe Browsing diagnostic page](#).

[Go back](#)

If you understand that visiting this site may harm your computer, [proceed anyway](#).

Help improve detection of malware by sending additional data to Google about sites on which you see this warning. This data will be handled in accordance with the [Safe Browsing privacy policies](#).

SECURITYBYTE

CONFERENCE & WORKSHOPS

2011

DoS / Noise

SECURITYBYTE

CONFERENCE & WORKSHOPS

2011

DoS / Noise

SECURITYBYTE

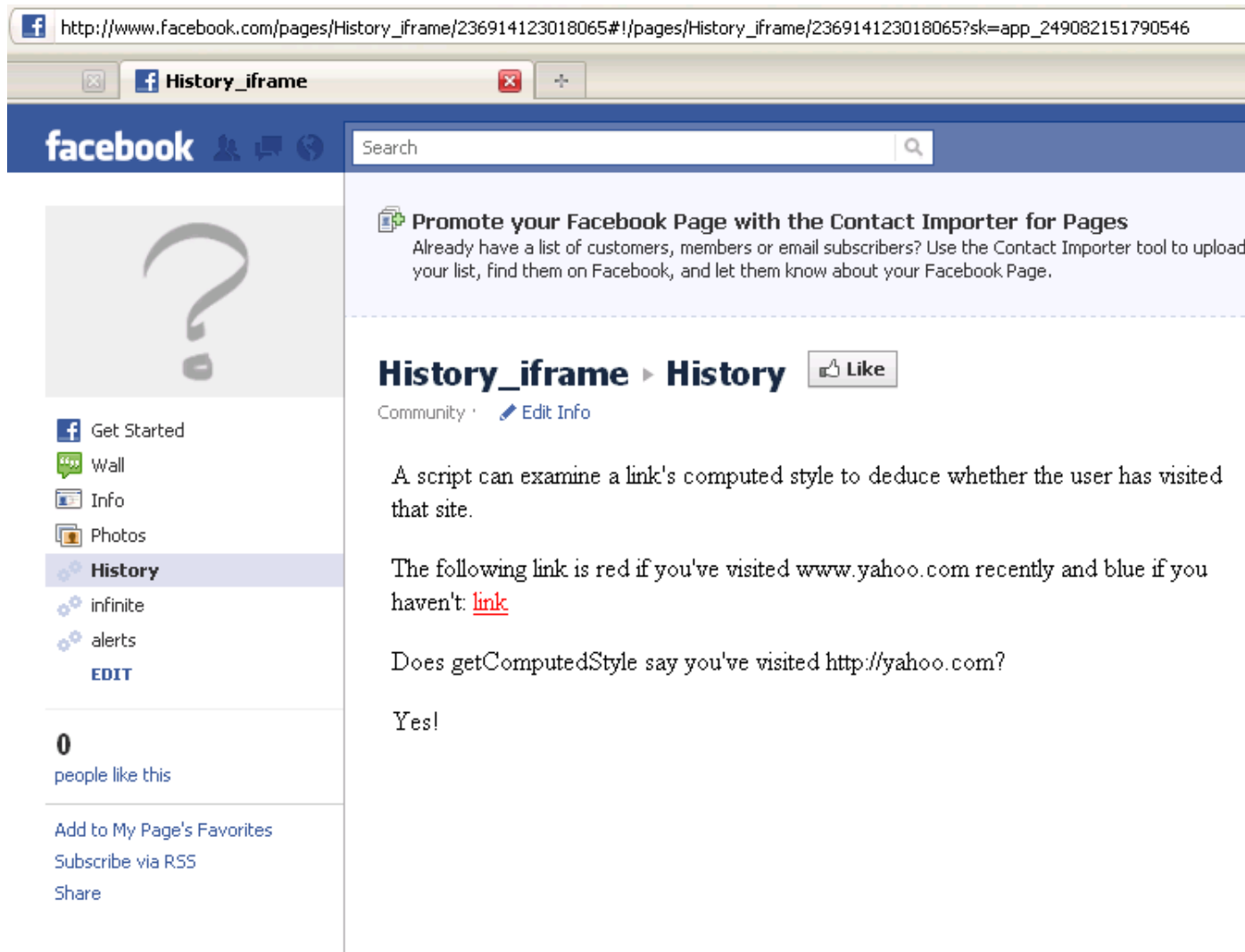
CONFERENCE & WORKSHOPS

2011

DoS / Noise

The screenshot shows a web browser window displaying a Facebook page. The address bar shows the URL: `www.facebook.com/pages/history_iframe/236914123018065?sk=app_198487210214052`. The page title is "History_iframe (1)". A search bar and navigation links (Home, Profile, Find Friends, Account) are visible at the top. A large dialog box titled "Page(s) Unresponsive" is overlaid on the page. The dialog contains the text: "The following page(s) have become unresponsive. You can wait for them to become responsive or kill them." Below this text is a list of unresponsive pages, showing "History_iframe (1)". At the bottom of the dialog are two buttons: "Kill pages" and "Wait". The background page shows a large question mark icon, a sidebar with navigation options (Wall, Info, Photos, History, infinite), and a main content area with a "Create a Page" button, a "See All" link, and several sponsored advertisements for Rinku Desai, Cool Nike Merchandise, and spicybids.com. The status bar at the bottom of the browser shows "Waiting for route13.in..."

History Sniffing/Mining



The screenshot shows a browser window with the address bar containing the URL: `http://www.facebook.com/pages/History_iframe/236914123018065#!/pages/History_iframe/236914123018065?sk=app_249082151790546`. The browser tab is titled "History_iframe". The Facebook interface shows the page name "History_iframe" and a search bar. A navigation menu on the left includes "Get Started", "Wall", "Info", "Photos", "History" (selected), "infinite", and "alerts". Below the menu, it says "0 people like this" and provides options to "Add to My Page's Favorites", "Subscribe via RSS", and "Share".

Promote your Facebook Page with the Contact Importer for Pages
Already have a list of customers, members or email subscribers? Use the Contact Importer tool to upload your list, find them on Facebook, and let them know about your Facebook Page.

History_iframe ▸ History

Community · [Edit Info](#) Like

A script can examine a link's computed style to deduce whether the user has visited that site.

The following link is red if you've visited `www.yahoo.com` recently and blue if you haven't: [link](#)

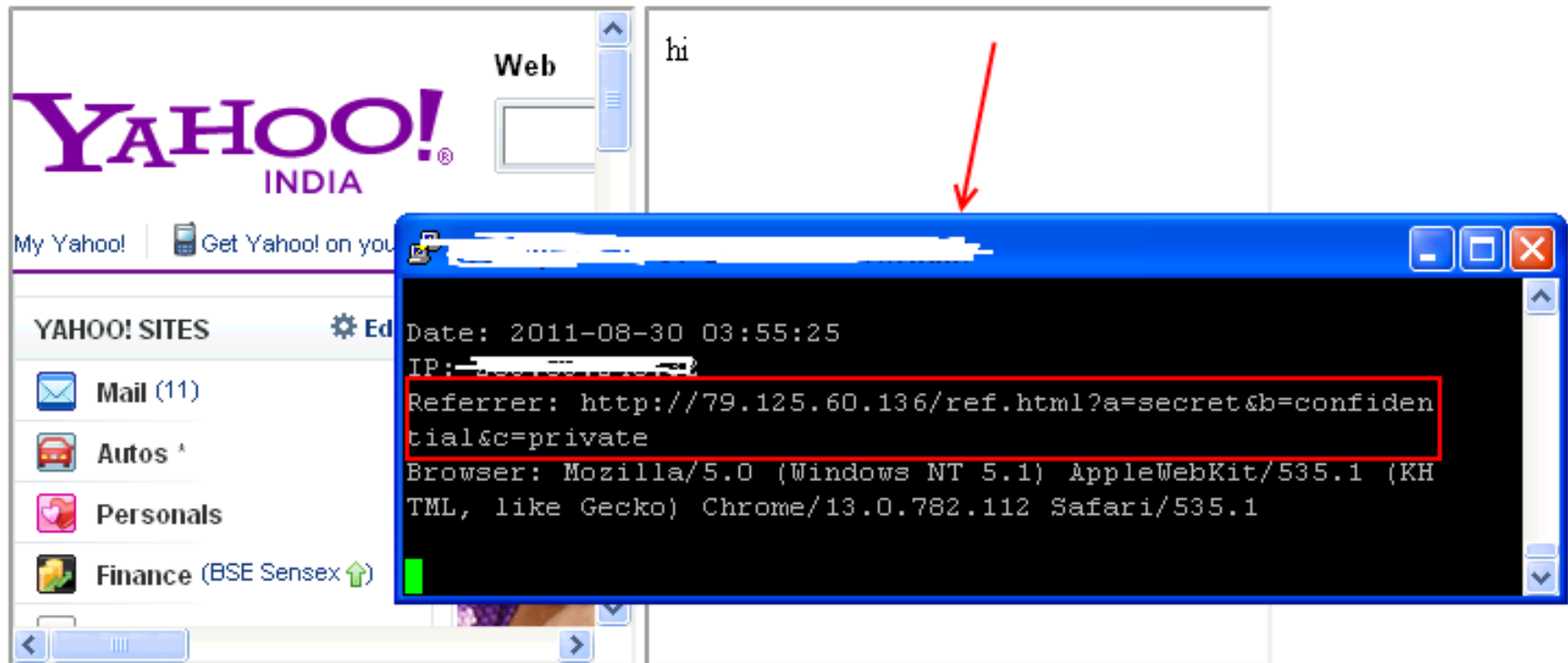
Does `getComputedStyle` say you've visited `http://yahoo.com`?

Yes!

Referrer Leak

← → ↻ 79.125.60.136/ref.html?a=secret&b=confidential&c=private

iframe referrer mis-use



The screenshot shows a web browser window displaying the Yahoo! India homepage. The address bar shows the URL `79.125.60.136/ref.html?a=secret&b=confidential&c=private`. A red arrow points to a console window that is open, displaying the following information:

```
Date: 2011-08-30 03:55:25  
IP: [redacted]  
Referrer: http://79.125.60.136/ref.html?a=secret&b=confiden  
tial&c=private  
Browser: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/535.1 (KH  
TML, like Gecko) Chrome/13.0.782.112 Safari/535.1
```

The referrer URL is highlighted with a red box, indicating that the browser is leaking the sensitive information from the parent page to the child page.

Secure Mashup Principles

- Integrator responsible to enforce intended separation and interaction
- **Separation** – Deter interference and malicious behavior of rogue components
- **Interaction** – Enable secure cross-document messaging

Secure Mashup Principles: Client-side Developments

▪ **Separation: Iframe sandbox**

- When set, enables new restrictions on any content hosted by the iframe
- By default, the content is treated as being from a unique origin, forms and scripts are disabled, links are prevented from targeting other browsing contexts, and plugins are disabled

▪ **Interaction: postMessage**

- Secure & improved replacement of Fragment Identifier Messaging (FIM)
- Provides controlled and safe cross-document messaging between iframes
- Enables authentication, other than confidentiality and integrity that FIM provided too
- Authentication achieved by browser validating the destination when sending a message and the recipients ability to validate sender on message receive.

▪ **Content Security Policy (CSP)**

- Primarily designed to defend against XSS, as a side-effect, enables better mashups
- Provides better granularity over authority of components by restricting their capabilities that make certain attacks possible
 - `eval()`, `setTimeout()`, `javascript:`, `new Function()`, `onclick()` and the likes are restricted

Secure Mashup Principles: iframe Sandbox

Secure Mashup Principles: iframe Sandbox

Pros

- Simplicity and low learning curve
- Incremental features lead to better adoption within devs
- Better adoption by browser vendors being part of HTML5 std
- Completely backward compatible
- Minimal hooks needed on existing code base
- Excellent support on mobile browsers

Cons

- **Not production ready!**
 - No support in older browsers (IE6 must die!)
 - Not a replacement but complement to existing defenses
 - Supported only in Chrome. FF proposes through CSP but yet to be implemented. No support in IE

Secure Mashup Principles: postMessage

Secure Mashup Principles: postMessage

Pros

- Nearly production ready
 - Supported by all major browsers (FF, Chrome, and IE8+ covers 85% browser market share)
- Simplicity and low learning curve
- Better adoption by browser vendors being part of HTML5 std
- Excellent support on mobile browsers

Cons

- No support in older browsers

Secure Mashup Principles: CSP

Pros

- Good granular control over authority of components
- Simplicity and low learning curve

Cons

- **Not production ready!**
 - No support in older browsers
 - A Mozilla standard supported only by FF4+. Chrome is next. No word on IE
 - Moving spec. Needs more scrutiny

Secure Mashup Principles: Server-side Developments

- **Interaction** delegated to browser SOP
- **Separation** introduced by implementing object capability model i.e. an object cannot be created if there is no reference to it
 - Achieved by restricting JavaScript (JS) to a subset and providing run-time control over specific operations, such as DOM access.
- Popular implementations include – Caja, FBJS, AdSafe and Web Sandbox
- Caja better adopted and supported (YAP, iGoogle, Orkut) compared to others

Secure Mashup Principles: Caja

Secure Mashup Principles: Caja

Pros

- **Production ready**
- Excellent granular control over authority of components
- Excellent protection against most of the DHTML mashup attacks

Cons

- High learning curve for developers
 - Compiling and debugging challenges
 - the line numbers don't correspond to line numbers in your source code.
- Not a standard
- Limited adoption over the years
- Limited support for JS libraries
- Limited protection against JS DoS conditions
- Quirky support on old browsers (Again, IE6 must die!)
- Performance hit at compilation and run-time due to virtualization

Secure Mashup Principles: Caja Virtualization

developer.yahoo.com/yap/guide/caja-support.html#how-does-caja-work

- Rewrites references to `this` to prevent access to the real global scope
- Replaces most JavaScript code with semantically similar code that has runtime checks for security
- Rejects some JavaScript code early, such as `with(obj){...}`.

Here's an example transformation. This JavaScript source code:

```
view plain print ?
1. size = 3;
2. function arf(geo, out) {
3.     var s4 = geo.compute(4 * size);
4.     var s5 = geo.compute(5 * size);
5.     out.value = (s4+s5)/2;
6.     return this;
7. };
```

is cajoled into something like this:

```
view plain print ?
1. $v.so('arf', (function () {
2.     function arf$_caller($dis, geo, out) {
3.         var s4 = $v.cm(geo, 'compute', [ 4 * $v.ro('size') ]);
4.         var s5 = $v.cm(geo, 'compute', [ 5 * $v.ro('size') ]);
5.         $v.s(out, 'value', (s4+s5)/2);
6.         return $dis;
7.     }
8.     ___markFuncOnly(arf$_caller, 'arf$_caller');
9.     return $v.dis(___primFreeze(arf$_caller), 'arf');
10. }) ());
11. $v.so('size', 3);
```

Secure Mashup Principles: Caja – JS DoS Attack

Solution: Today

3rd Party Partners

- Keep doing what you are doing to **sanitize at the server-side**
- **Iframe** Ads, Widgets and other content. Avoid scripting
- Keep signing/updating legal and security **agreements**

3rd Party Developers

- Your choice!
 - Minimal policing, low learning, high portability (iframe) leads to high growth and viral networks
 - Policing (Caja, FBJS), high learning curve, low portability - low growth

Solution: Tomorrow

3rd Party Partners

- One day. Some day. Once those are dead and buried. Yes, you can leave it to them - Sandbox, postMessage, CSP.
- Some would still need exceptions
 - Iframe Ads, Widgets and other content. Avoid scripting
- Keep signing/updating legal and security agreements

3rd Party Developers

- Iframe sandbox + postMessage + CSP + <?>

References

Web Links

- Yahoo! YAP <http://developer.yahoo.com/yap/guide/yap-overview.html>
- FB IFrame Tabs <http://developers.facebook.com/blog/post/462>
- WebSand Project <https://www.websand.eu/deliverables/index.html>
- WHATWG Blog <http://blog.whatwg.org/whats-next-in-html-episode-2-sandbox>
- iFrame Sandbox <http://www.whatwg.org/specs/web-apps/current-work/multipage/the-iframe-element.html#attr-iframe-sandbox>
- postMessage <https://developer.mozilla.org/en/DOM/window.postMessage>
- HTML5 Demos <http://html5demos.com/>
- Mozilla CSP <http://people.mozilla.com/~bsterne/content-security-policy>
- Google Caja <http://code.google.com/p/google-caja/>
- Caja Playground <http://caja.appspot.com/>
- Caja DoS <http://code.google.com/p/google-caja/issues/detail?id=1406&sort=-id>
- Microsoft Web Sandbox <http://www.websandbox.org/>
- Gadget Hijacking <http://seclab.stanford.edu/websec/frames/post-message.pdf>
- Browser Security Features <http://www.browserscope.org/?category=security&v=1>
- Browser Market Share <http://www.netmarketshare.com/browser-market-share.aspx?spider=1&qprid=0&qpcustomd=0>

Creative Commons Image Attribution

- Slide 1 <http://www.flickr.com/photos/donkeyhotey/5679642883/sizes/o/in/photostream/>
- Slide 3
 - http://www.flickr.com/photos/jesse_sneed/2383953694/
 - <http://www.flickr.com/photos/31856336@N03/4848321266/>
 - <http://www.flickr.com/photos/umpcportal/4147481868/>