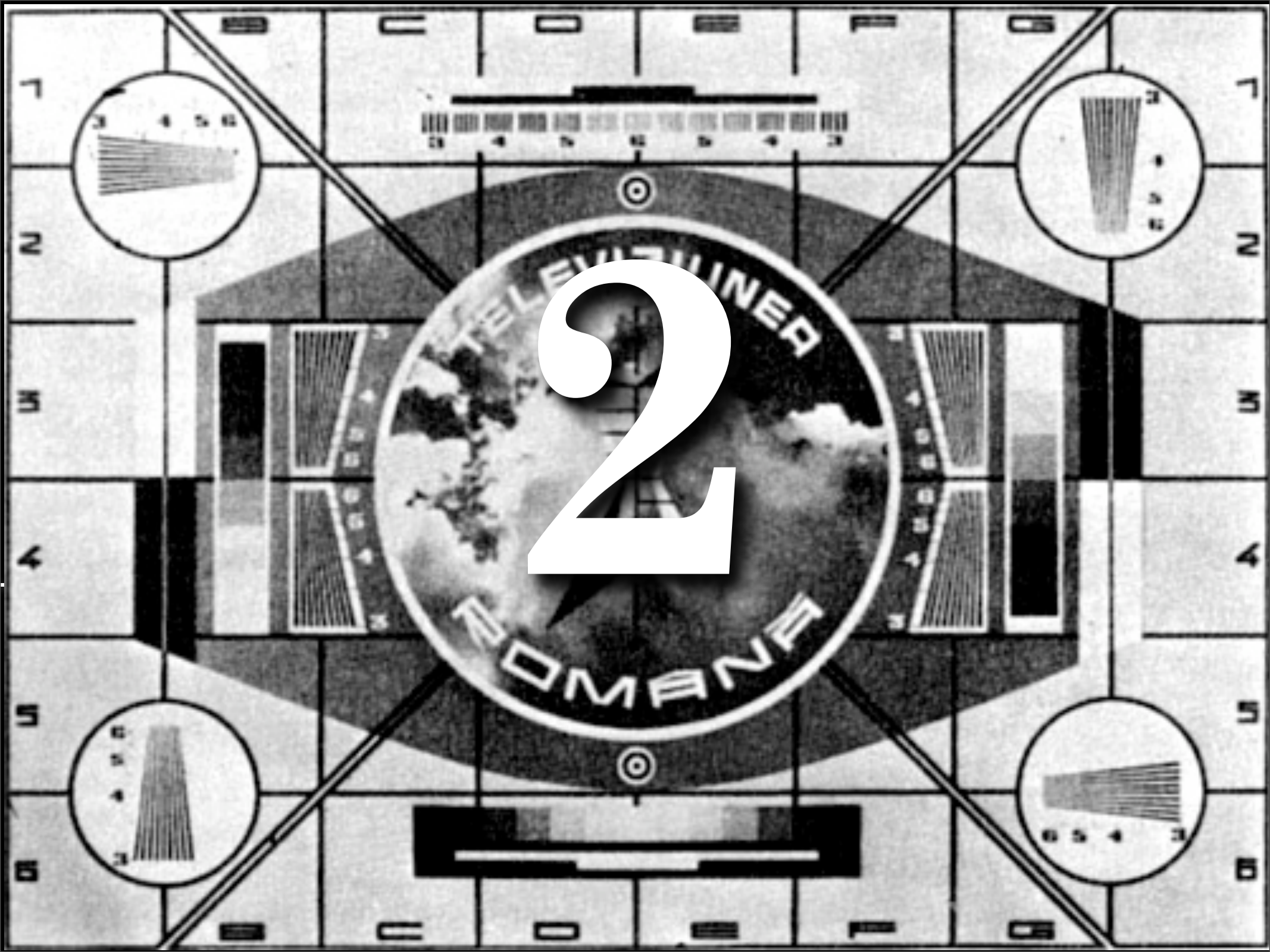


1



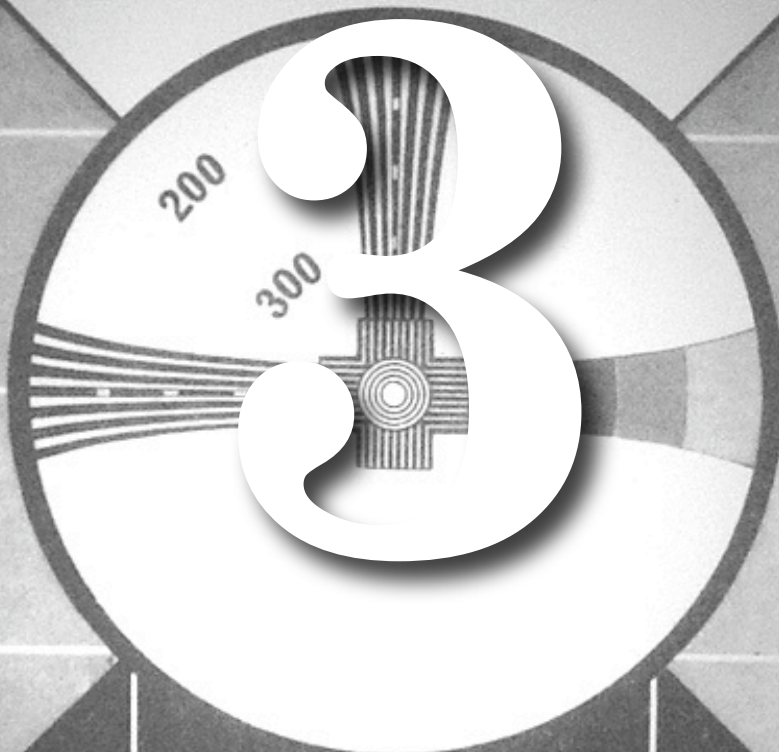
2

TELEVISIONER

ROMANIAN

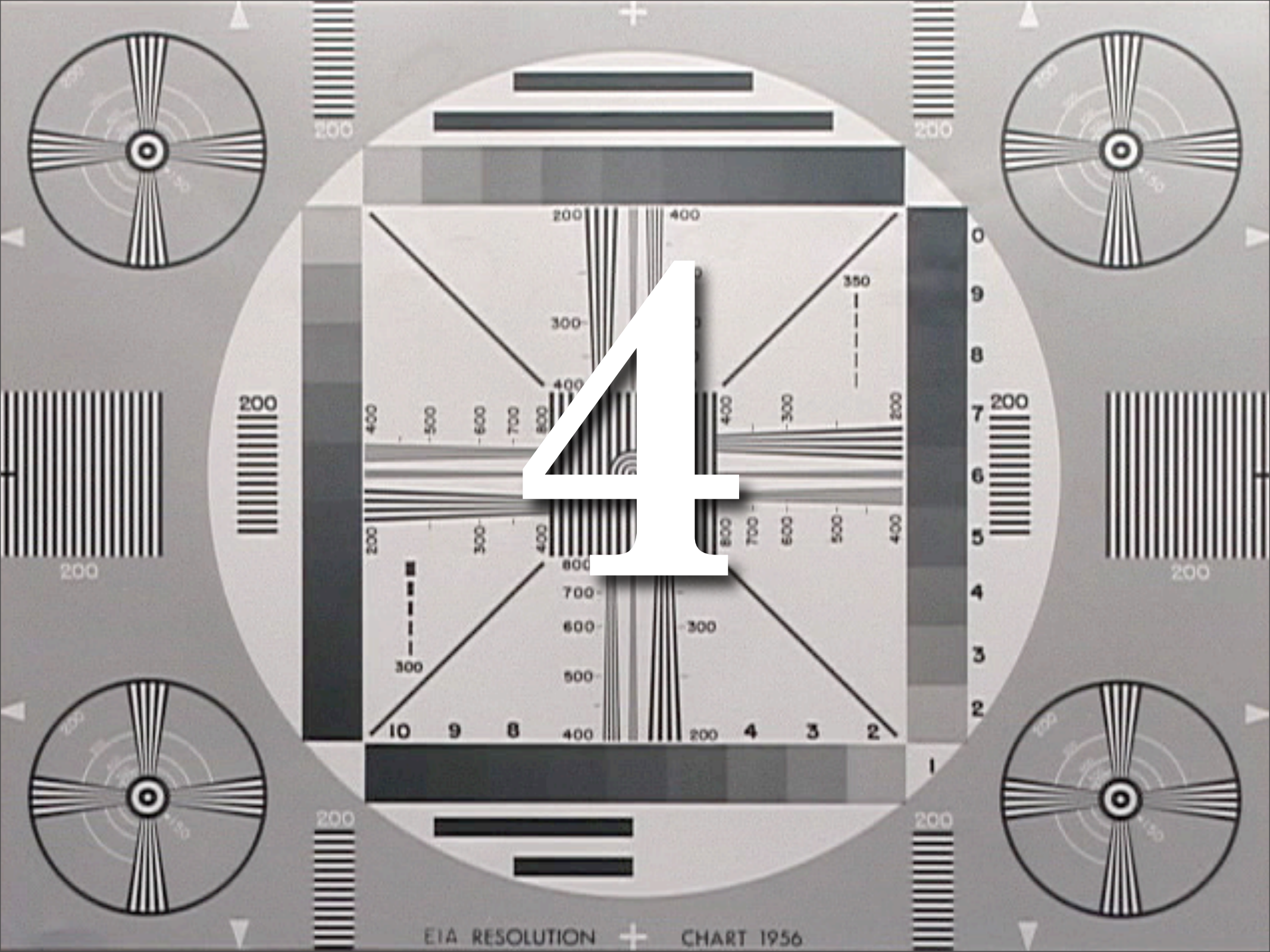


**CBC**



**RADIO - CANADA**





4

# Satan Is On My Friends List

Attacking Social Networks

---

# We're in your Extended Network!

## ★ Nathan Hamiel

- ★ Senior Consultant @ Idea InfoSec
- ★ Associate Professor at UAT
- ★ Facebook, LinkedIn, MySpace, Twitter

## ★ Shawn Moyer

- ★ Hacking for dollars @ FishNet Security
- ★ BH speaker, multipurpose windbag
- ★ LinkedIn, Twitter, kinda-sorta Facebook

[ Please pay us to come break your web apps. kthxbye. ]

# And so is ....

**satan**



Male  
69 years old  
CONNECTICUT  
United States

Last  
Login:03/07/2008

View My: [Pics](#) | [Videos](#)

[Contacting satan](#)

**satan is in your extended network**

**satan's Latest Blog Entry** [[Subscribe to this Blog](#)]

[[View All Blog Entries](#)]

**satan's Blurbs**

**About me:**

**Who I'd like to meet:**

**satan's Friend Space (Top 7)**

# Intro / Disclaimer

***No animals, bloggers, journalists*** or camwhores were harmed during these demonstrations. While actual SocNet sites and users were involved, all payloads were benign and only resulted in wounded pride and possibly high blood pressure.

***We are not experts*** and should not be trusted in any way. Always ask your doctor before changing prescriptions or viewing LiveJournal session captures.

***MySpace contains*** the most feature-complete OpenSocial implementation. Many of the issues discussed here are on their platform.

The rest of you guys suck too, srsly. We mean it.



# So, WTF is this about?

## ★ Our obsession with SocNets, mostly.

- ★ Impromptu threat modeling over  $\{\text{drinks}\}$ .
- ★ Various (harmless) sorties on SocNet sites.
- ★ SocEng experiments and silliness.

## ★ But... Are you dropping 0day?

- ★ No, at least we don't think so...
- ★ "Featurebilities". Design flaws. Architecture FAIL.
- ★ They put it there... On purpose! Srsly!
- ★ Still, lots of soft, squishy attack surface.

# Roadmap and Nickel Tour

## ★ SocNets as attack platform

- ★ Millions of users^H^H^H^Htargets
- ★ Business model: Ads, user-generated content

## ★ Vuln Mashups 2.0

- ★ Promiscuous and pervasive trust
- ★ SocEng + vulns = attacker ROI

## ★ Dance, monkey, dance!

- ★ Demos-of-shame, captures, bugs
- ★ Things we wish we could un-see

# Roadmap and Nickel Tour

## ★ App threats (OpenSocial, FB)

- ★ Attacking clients with apps
- ★ Attacking apps with apps
- ★ SocNet as lightweight Botnet.

## ★ CSRF-palooza

- ★ Innocuous functions and escalation
- ★ Broken token + breaking the membrane

## ★ External content. Bad. Discuss.

- ★ Markup, attributes, blacklisting. Fail.



# Don't Taze Us, Bro...

- ★ Please don't hate, Chris.
- ★ You seem very cool. :)
- ★ Still, this is a lot of fail, in one handy package.



# External Content = Fuxor

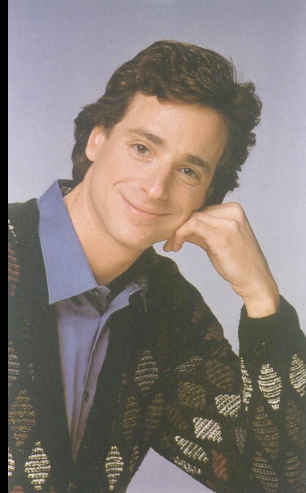
## ★ Link to crap offsite = epic fail

- ★ IMG tag CSRF
- ★ CSS Jscript hijacking, click fraud, SocNet as botnet
- ★ Hello, SocNets. Plz fix. kthxbye.
- ★ MySpace, Hi5, LiveJournal, many others.

## ★ Request Conversions (SSRF)

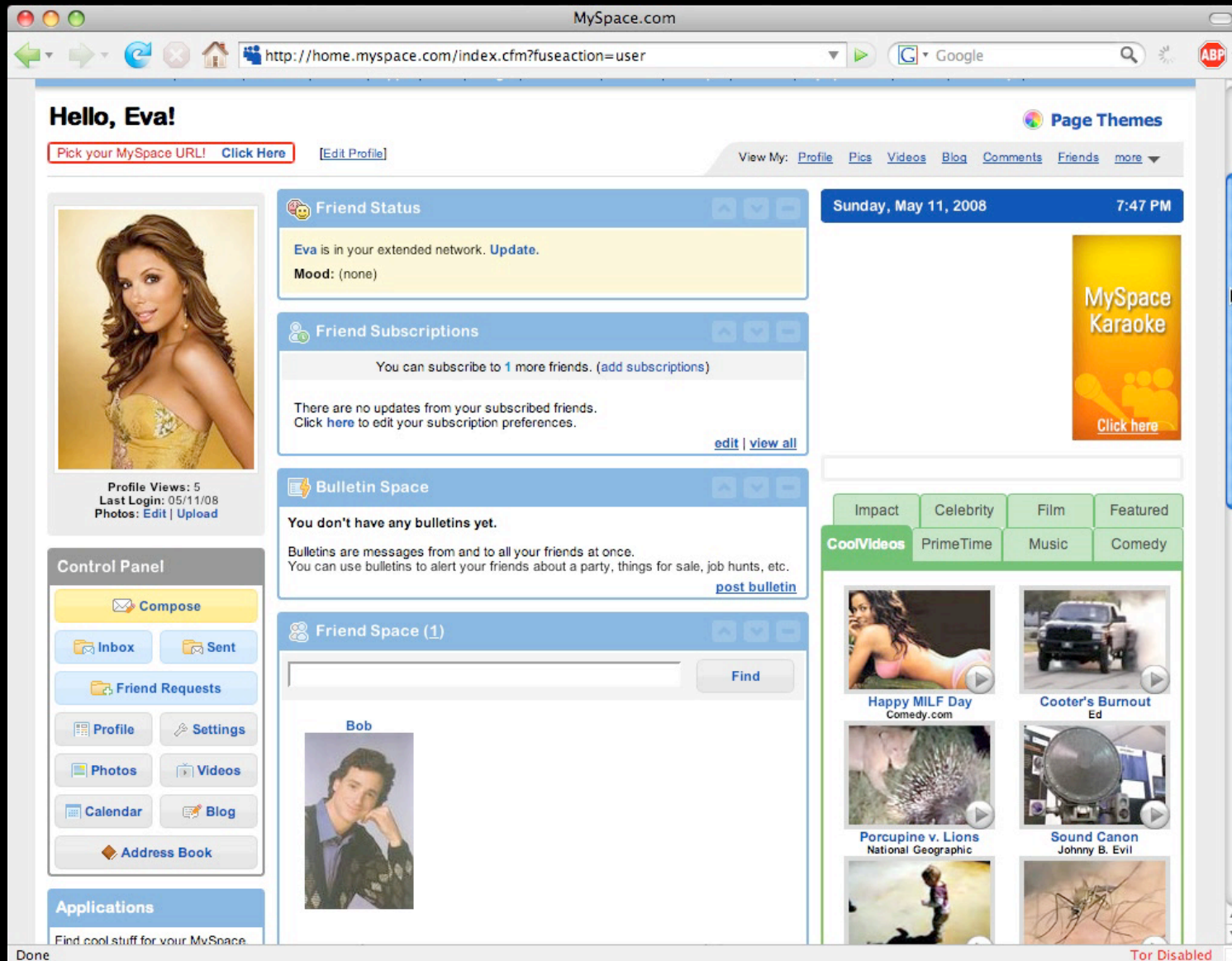
- ★ POST to GET
- ★ Sometimes enforced / validated differently based on method
- ★ Viewstate MAC, params, auth components
- ★ We don't need XMLHTTP kung fu for GET-based CSRF

# Meet Alice, Bob, and Eva





# External content -> CSRF

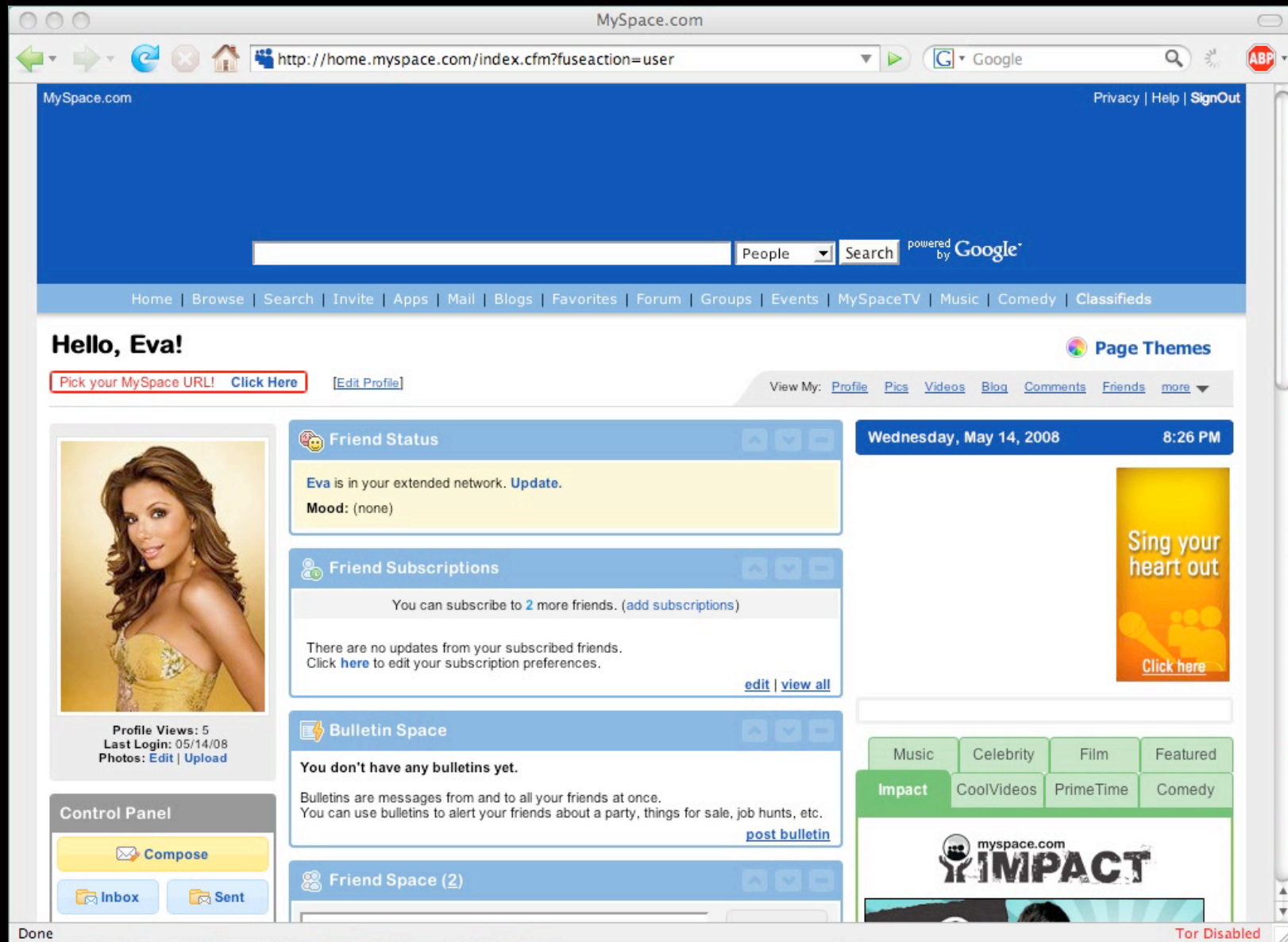


★ MySpace add hack

# Innocuous Functions

- ★ Most sites protect functions that appear valuable
  - ★ Account changes, messaging, profile admin
  - ★ Computationally expensive, overhead
  - ★ Tokenized against CSRF (varying entropy... Brutable?)
- ★ Things that don't appear valuable
  - ★ Logging out
  - ★ Blocking communication
  - ★ Friend adds, apparently
  - ★ Lots of other stuff

# MySpace DoS (Irritation)



★ MySpace DoS



# No JavaScript, No Problem

★ There may be other ways ;)

★ ``


★ `<meta http-equiv="refresh" content="0;url=http://domain.com/whatever">`

★ `<iframe src="http://domain.com/whatever"></iframe>`


# Logic Attacks on SocNets

- ★ Attacks don't always have to be so straight forward
- ★ Extremely difficult to identify through automated testing.
- ★ AdultFriendFinder privilege escalation
  - ★ It's a SocNet, right? We think so!
  - ★ Allows for the viewing of paid for content

# Elite AFF pwnage. Ph33r.

 **My Mood: Naughty**  
Looking for hot playmates!

[Add to Favorite Photos](#) | [See Larger Photo](#)



**Standard Member**  
Online Now!

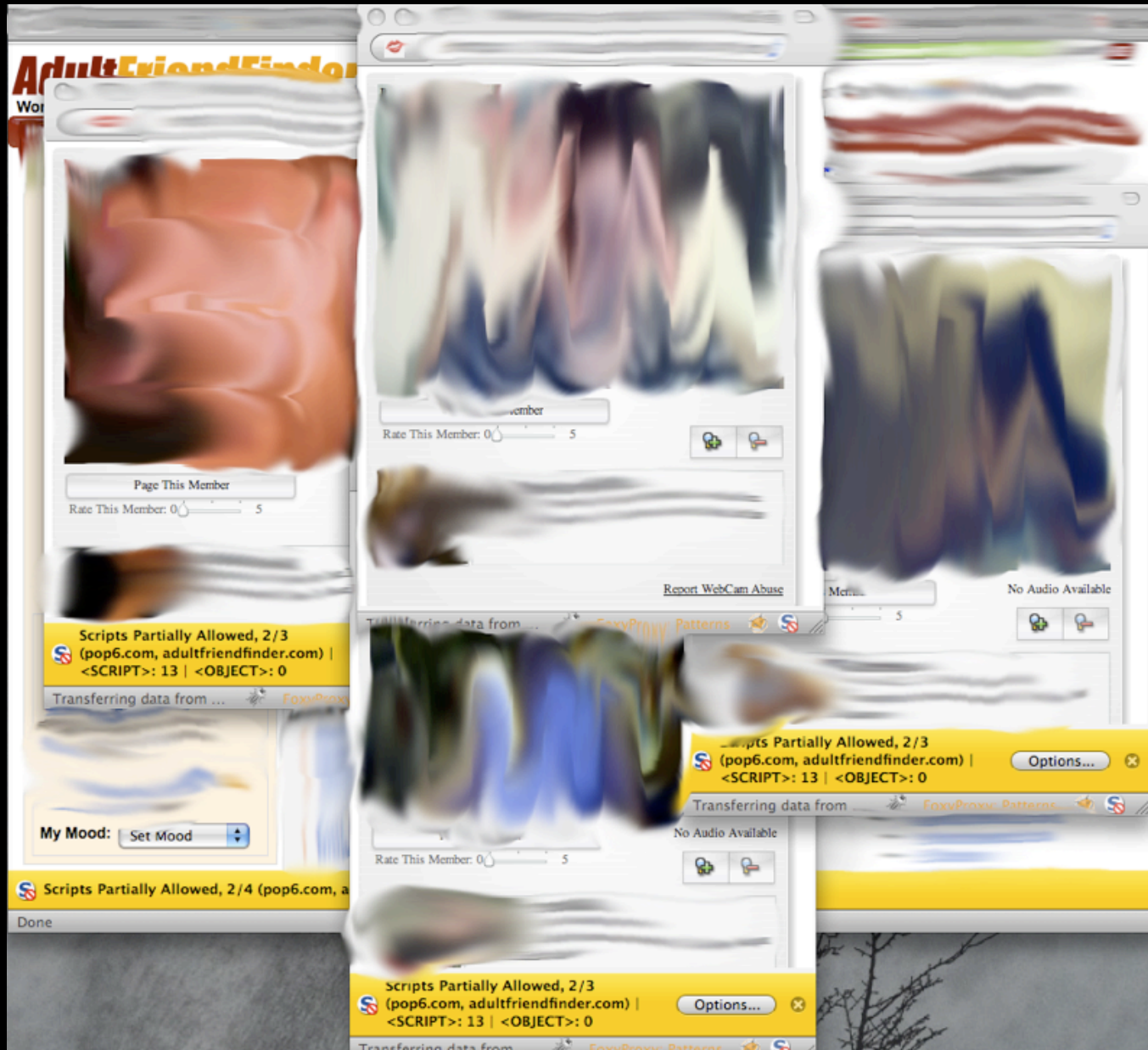
**Kudos: 0** [Give kudos](#)

**year old Couple (man and woman)** in **year old Couple (man and woman)**

**Looking For:** Men, Women, Couples (man and woman), Groups, Couples (2 women), Couples (2 men) or TS/TV/TG for 1-on-1 sex, Bondage & Discipline, Cross-Dressing, Discreet Relationship, Erotic Chat or Email, Exhibitionism/Voyeurism, Group sex (3 or more!), Misc. Fetishes, Other "Alternative" Activities or Sadism & Masochism

Profile for **year old Couple (man and woman)**

# We did you a favor, we promise.



# Pwning Kevin Bacon

## ★ SocNet attacks = SocEng++

- ★ Much of this is about blended threats.
- ★ The social and technical are always linked.

## ★ This is why this stuff was so fun!

- ★ Generally, we PoC the technical or social.
- ★ Why "weaponize the obvious"? [ @dakami ]
- ★ The combination of the two get ugly FAST.



# Profiling and OpSec

- ★ It's on a public site, you eee-diot!
  - ★ We think ID theft via SocNet is hype
  - ★ You shared it, so ASSUME IT'S PUBLIC
  - ★ If you give your CC to FB, you deserve to fail

# Profiling and OpSec

- ★ It's on a public site, you eee-diot!
  - ★ We think ID theft via SocNet is hype
  - ★ You shared it, so ASSUME IT'S PUBLIC
  - ★ If you give your CC to FB, you deserve to fail

# Some SocEng sorties

★ SocEng = low line noise, high hit rate

★ Great ROI for a targeted attack.

★ Diamond-tipped spearphishing. =))

★ Build a plausible profile

★ Public sources, company data

★ Get “respectable” # of connections

★ And then what, pray tell?

★ We just built friends / connections

★ Real attack: mail / msg custom payload

# The Marcus Experiment



Marcus was concerned about SocNets. He agreed to help us out.

# The Marcus Experiment

## ★ Profiling was pretty trivial

- ★ Press releases, bios, articles
- ★ Took us about 3 hours to build

## ★ But, wait... How to build connections?

- ★ Need quick legitimacy (friends, groups)
- ★ Meet the linkwhores! =)



# The Marcus Experiment

The screenshot shows a web browser window with the following details:

- Browser Title Bar:** "invites accepted" OR "open networker" OR "accepts all invites" OR lion OR toplinked.com OR mylink500 +site:linkedin.com +security +cissp +inurl:/in/ -inu
- Address Bar:** <http://www.google.com/search?hl=en&client=firefox-a&rls=com.ubuntu%3Aen-US%3Aunofficial&q=invites+accepte>
- Search Bar:** "invites accepted" OR "open networker" OR "accepts all invites" OR lion OR toplinked.com
- Search Results:** Web Results 1 - 10 of about 835 from linkedin.com for "invites accepted" OR "open networker" OR "accepts all invites" OR lion OR toplinked.com OR mylink500 +security +cissp +inurl:/in/ -inurl:updates
- Results:**
  - Thomas Kearns, CISSP [LION] TopLinked.com - LinkedIn**  
View Thomas Kearns, CISSP [LION] TopLinked.com's professional profile on LinkedIn. ... Certified Information Systems Security Professionals (CISSP) member ...  
[www.linkedin.com/in/kearns](http://www.linkedin.com/in/kearns) - 38k - [Cached](#) - [Similar pages](#) - [Note this](#)
  - Ian Philpot, CISSP - LinkedIn**  
Certified Information Systems Security Professionals (CISSP) member ... Information Security Community member; TopLinked.com member TopLinked.com member ...  
[www.linkedin.com/pub/4/374/1A8](http://www.linkedin.com/pub/4/374/1A8) - 24k - [Cached](#) - [Similar pages](#) - [Note this](#)
  - Patrick Hanley, MBA, CISSP, PMP - LinkedIn**  
Patrick Hanley, MBA, CISSP, PMP. Expert Information Assurance Professional, 3100+ connections, LinkedIn LION, MyLink500.com, Patrick.L.Hanley@gmail.com ...  
[www.linkedin.com/in/hanleyp](http://www.linkedin.com/in/hanleyp) - 16k - [Cached](#) - [Similar pages](#) - [Note this](#)
  - Karl Wabst - CIPP, [LION] - LinkedIn**  
View Karl Wabst - CIPP, [LION]'s professional profile on LinkedIn. ... Certified Information Systems Security Professionals (CISSP) member; Executive Suite ...  
[www.linkedin.com/in/karlwabst](http://www.linkedin.com/in/karlwabst) - 31k - [Cached](#) - [Similar pages](#) - [Note this](#)
  - Francesco Camilucci - LinkedIn**  
CISSP, AAC, PMI, LION, plusonenetwork.com, TopLinked.com, TEN, PMI Information Systems SIG, DUBAI, UAE | Dubai, IT Recruiters, Mainframe Security Gurus ...  
[www.linkedin.com/in/fcamilucci](http://www.linkedin.com/in/fcamilucci) - 54k - [Cached](#) - [Similar pages](#) - [Note this](#)
  - Patricia Moulder TopLinked.com - LinkedIn**  
View Patricia Moulder TopLinked.com's professional profile on LinkedIn. ... Certified Information Systems Security Professionals (CISSP) member ...  
[www.linkedin.com/in/patriciamoulder](http://www.linkedin.com/in/patriciamoulder) - 22k - [Cached](#) - [Similar pages](#) - [Note this](#)

# The Marcus Experiment

The image shows a screenshot of a LinkedIn profile for Marcus J. Ranum. The profile is set to public and includes a summary, current and past work experience, education, connections, industry, and websites. It also lists groups he shares with and provides contact options like InMail and adding to a network.

**LinkedIn** Account & Settings | Help | Sign Out

People | Jobs | Answers | Companies | Advanced Search People [ ] Search

**Profile** Edit My Profile View My Profile Edit Public Profile Settings

Forward this profile Go back to Home Page

**Marcus J. Ranum** (you)  
Chief Security Officer at Tenable Network Security  
State College, Pennsylvania Area

Send InMail  
Get introduced through a connection  
Add Marcus J. to your network

Profile Q&A

**Current**

- Chief Security Officer at Tenable Network Security

**Past**

- Hired Gun at Ranum Security Consulting
- Chief Technical Officer at Network Flight Recorder
- Chief Scientist at V-One Corporation

see all...

**Education**

- The Johns Hopkins University

**Connections** 51 connections

**Industry** Computer & Network Security

**Websites**

- My Company
- My Website
- My Blog

**Public Profile** <http://www.linkedin.com/in/marcusjranum>

**Summary**

**Groups you share with Marcus J.:**

- ExecuNet Executive Suite member
- CISO: Meaningful Metrics member
- Black Hat member
- ISACA ISACA Professionals member
- Enterprise Security member
- Security Security Leaders Group member

**Home**  
**Groups** My Groups Groups Directory Create a Group  
**Profile** Edit My Profile View My Profile  
**Contacts** Connections Imported Contacts Network Statistics  
**Inbox (5)** Compose Message Messages InMail Introductions Invitations (5) Profiles Q&A Jobs Recommendations

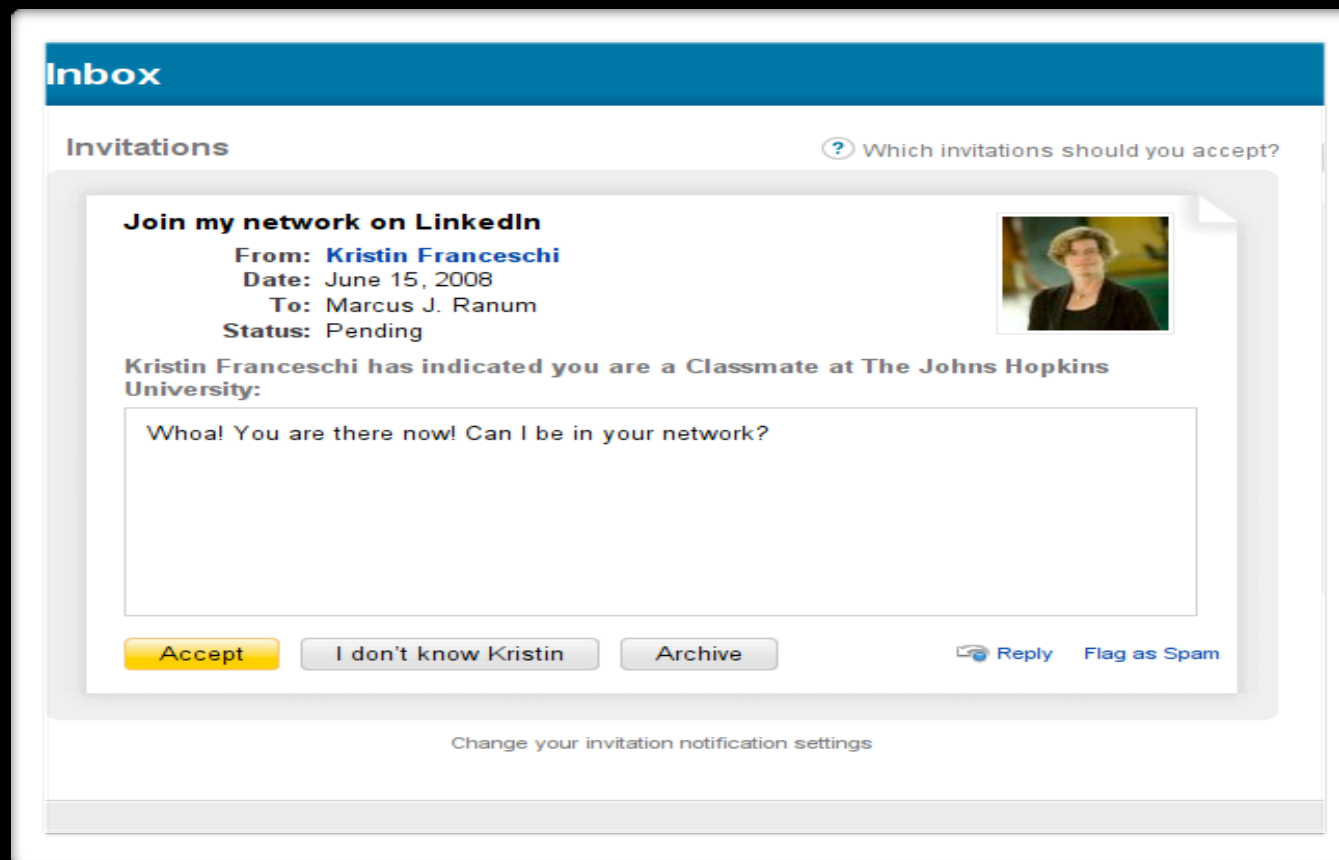
**Add Connections**

**Marcus J. Ranum**  
Chief Security Officer at Tenable Network Security  
What are you working on?


# The Marcus Experiment

## ★ The end result

- ★ 50+ connections in less than 24 hours
- ★ CSOs, bigwigs, CISSPs, feds, ISSA ppl, and my personal favorite...



# DoppelGadi!



**gadi\_evron**

[@GeorgeVHulme](#) It'ss not something I can talk to yet, but yes, it's there.

40 minutes ago from web in reply to [GeorgeVHulme](#)

---

RealPlayer bug again. The botmasters will have a busy weekend. <http://tinyurl.com/5rjegg> about 2 hours ago from web

---

RealPlayer stack overflow from ZDI. Anyone knows this is different than the heap bug? <http://tinyurl.com/85umzp> about 4 hours ago from web

---

Spam King dead in apparent suicide: <http://blogs.zdnet.com/secu...> about 5 hours ago from web

---

First 1M \$ phishing fraud hits inboxes: <http://tinyurl.com/8lkqgh> about 5 hours ago from web

[RSS](#) [Older >](#)

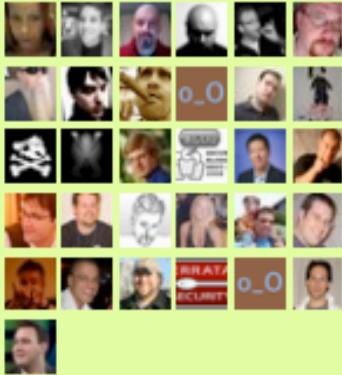
**About**

Name Gadi Evron.  
Location Tel Aviv, Israel  
Web <http://gevron.liv...>  
Bio Security Visionary.

**Stats**

Following	92
Followers	12
Favorites	0
Updates	5

**Following**



# MySpace Apps and OpenSocial

An advertisement for MySpace Apps. The background is a close-up profile of a man wearing gold-rimmed sunglasses and having gold teeth. He is holding a large diamond ring. The text 'myspace Apps' is in the top left. Below it, the text 'Accessorize with Malware' is displayed, with 'Malware' in red. At the bottom left is the URL 'apps.myspace.com'. On the right is a yellow button with a right-pointing arrow and the text 'Check It Out'.

Your bling just bit you in the ass, douchebag.



# User-Installed Nunchaku

## ★ Who needs vulns?

- ★ Convenient APIs, 100% arbitrary code
- ★ OpenSocial: "Write once, Own anywhere."(tm)
- ★ Pick a meme, get installs... Then "go rogue".
- ★ Your own personal botnet, for a few lines of PHP.

## ★ SocNet sites DON'T CARE. Period.

- ★ EULA and separate domain = zero responsibility
- ★ Arbitrary execution on most sites
- ★ Little to no validation (vetting process, # friends)
- ★ Any app can attack another app (same domain)

# Origin Shmorigin

## ★ What about same origin?

- ★ What are you attacking? Site, or user?
- ★ API functions allow you to proxy requests
  - ★ Comes from server, not client though ;)
  - ★ GETs
  - ★ POSTs

## ★ Depends on the attacker and goal.

- ★ Are you targetting the site itself?
- ★ Can still hit many clients via apps
- ★ Useful for propagation: installs, messages, adds
- ★ We can also CSRF via simple GETs w/o XSS

# Pudding and Proof

The screenshot shows a MySpace profile for a user named Nathan. A JavaScript error message is displayed in the center, stating: "The page at http://api.msappspace.com says: name=Pants\_Secret\_Cookie". The profile includes a profile picture of a man with glasses, a bio, and various interaction buttons. A notification box on the right says "Nathan is in on your network." Below this, there are sections for "Nathan's Latest Blog Entry" and "Nathan's Blurbs". The "About me" section describes Nathan as a security professional and professor. The "Who I'd like to meet:" section lists "All of the members of the A-Team." At the bottom right, there is a green hexagonal logo with a circuit-like pattern and the text "Are you down with the Hex?".

MySpace.com - Nathan - 31 - Male - JACKSONVILLE, Florida - www.myspace.com/372734803

http://profile.r

The page at http://api.msappspace.com says:  
name=Pants\_Secret\_Cookie

OK

**myspace.com**  
a place for friends.

Home Mail Profile Fr

**Nathan**

"Maximum Minimalist"

Male  
31 years old  
JACKSONVILLE,  
Florida  
United States

Online Now!

Last  
Login: 7/29/2008

Mood: sneaky  
View My: [Pics](#) | [Videos](#)

**Contacting Nathan**

Send Message	Forward to Friend
Add to Friends	Add to Favorites
IM / Call	Block User
Add to Group	Rank User

**CSRfer**

Coming Soon

**Nathan is in on your network.**

**Nathan's Latest Blog Entry** [[Subscribe to this Blog](#)]

[[View All Blog Entries](#)]

**Nathan's Blurbs**

**About me:**  
I am Nathan. I am a security professional and a professor at a University. I spend most of my time pondering problems of the world and trying to work solutions for them. I have been involved with art and music most of my life as well.

**Who I'd like to meet:**  
All of the members of the A-Team.

Are you down with the Hex?

# OpenSocial GET Request

★ Defaults to GET if method not specified

```
function makeRequest(url) {  
    var params = {};  
    params[gadgets.io.RequestParameters.METHOD] =  
gadgets.io.MethodType.GET;  
    gadgets.io.makeRequest(url, response, params);  
};
```

# OpenSocial POST Request

## ★ OpenSocial POST method

```
function makeRequest(url, postdata) {  
    var params = {};  
    postdata = gadgets.io.encodeValues(postdata);  
    params[gadgets.io.RequestParameters.METHOD] =  
gadgets.io.MethodType.POST;  
    params[gadgets.io.RequestParameters.POST_DATA]= postdata;  
    gadgets.io.makeRequest(url, response, params);  
};
```

```
function response(obj) {  
    alert(obj.text);  
};
```

```
var data = {  
    data1 : "test",  
    data2 : 123456  
};  
makeRequest("http://example.com", data);
```

# More on OpenSocial Requests

★ You can add your own headers

★ Reference for 0.7 OpenSocial

★ <http://code.google.com/apis/opensocial/docs/0.7/reference/>

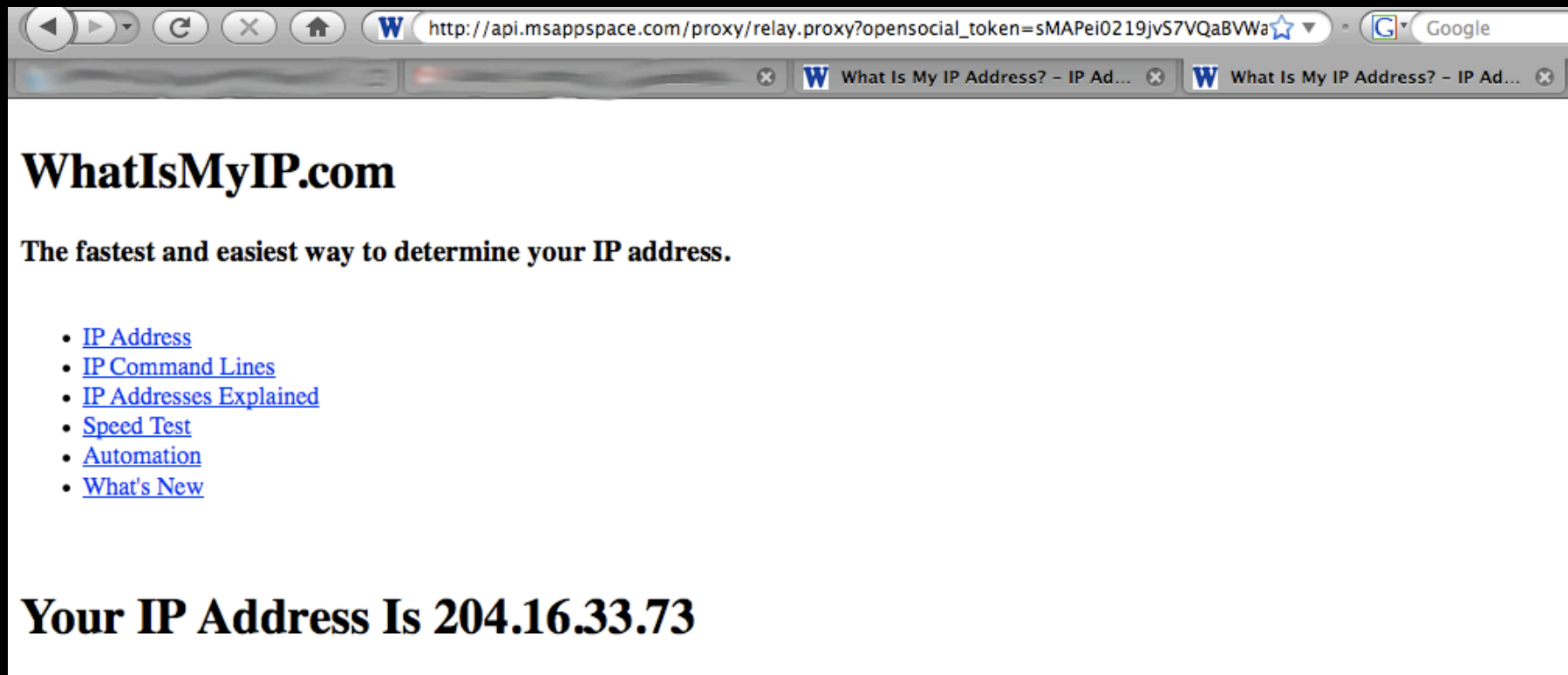
★ Relay.proxy smells like fail.

★ MySpace server makes the request for you, even without an app or dev access.

**[http://api.msappspace.com/proxy/relay.proxy?  
opensocial\\_token=sMApei02I9jvS7VQaBVWaKTsI6cFED5lwyeM  
NNFEIzQgqBRJBhXM8EugjDvqPIFS8uDoTjHfGEYGe74uvFMCQ/  
Uu2mTyxAQaILH3w55n3u8=&opensocial\\_url=http%3A//  
www.hexsec.com](http://api.msappspace.com/proxy/relay.proxy?opensocial_token=sMApei02I9jvS7VQaBVWaKTsI6cFED5lwyeMNNFEIzQgqBRJBhXM8EugjDvqPIFS8uDoTjHfGEYGe74uvFMCQ/Uu2mTyxAQaILH3w55n3u8=&opensocial_url=http%3A//www.hexsec.com)**



# Routing Traffic via MySpace



http://api.msappspace.com/proxy/relay.proxy?opensocial\_token=sMAPEi0219jvS7VQaBVWa

## WhatIsMyIP.com

The fastest and easiest way to determine your IP address.

- [IP Address](#)
- [IP Command Lines](#)
- [IP Addresses Explained](#)
- [Speed Test](#)
- [Automation](#)
- [What's New](#)

**Your IP Address Is 204.16.33.73**

# MySpace Apps Capabilities

- ★ If provided it, an app can get
  - ★ Interests
  - ★ Heros
  - ★ Photo Albums
  - ★ Friends / Connections
- ★ If you provided it to the app, it's probably offsite.
  - ★ Delivers code via the API
  - ★ Deliver off-site code / content via iframe

# SocNet Apps Jujitsu

- ★ Attacking social net is trivial.
- ★ Apps are delivered as:
  - ★ External site though iframe
    - ★ Functionality on Canvas
    - ★ Functionality on Profile
    - ★ Functionality on Home
  - ★ Contained app grabbing external content
    - ★ Functionality in same areas as above
  - ★ Coded by people who shouldn't be writing code
    - ★ Trivial to find out who has what apps installed ;)
    - ★ Let's look at a couple examples.

# Keep It Real

★ Allows for “secret” communication



**MySpace Apps** MySpace Apps | View My Apps

### Keep It Real! Box

 Made by **Marh-The first hood social app developer!**  
2614 active users

Categories: **Communicating / Dating & Relationships**

[Uninstall this Application](#)




This app was not developed by MySpace. [Report this App](#)

#### About Keep It Real! Box

Keep It Real Box lets your friends send you messages secretly. New Game included! Keep it Real!

#### Keep It Real! Box's Friend Space (Top 7)



Keep It Real! Box has 11 friends.

<b>Marh-The first hood social app developer!</b> 	<b>P.Diddy</b> 	<b>TK FLY SOCIETY SK8SITE.COM</b> 	<b>Usher</b> 	<b>TILA TEQUILA</b> 	<b>Ryan Leslie - "Addiction" on iTunes Now!</b> 	<b>Ride Siddy Entertainment</b> 
---	--	--	--	---	--	---

View Keep It Real! Box- Friends: [All](#) | [Online](#) | [New](#) | [Mutual](#)

#### Forum

[Post a New Topic](#) | [View All Topics](#)

Forum Topic	Posts	Last Post	Topic Starter
 <a href="#">re.saul</a>	1	 31/07/2008 3:41 PM by: <b>GUCCI MANE</b>	 31/07/2008 3:39 PM by: <b>GUCCI MANE</b>
 <a href="#">kim</a>	0	 29/07/2008 4:21 PM by:	 29/07/2008 4:21 PM by:

# Keep It Real Own3d

★ The ownage

The screenshot displays the 'Keep It Real! Box' interface. At the top, there is a header with a speech bubble icon and the text 'Keep It Real! Box'. Below this, a central message reads 'Invite Friends To get more Truth:' followed by a button labeled '[Click for recipient]'. A navigation bar contains four buttons: 'Inbox' (highlighted in blue), 'Outbox', 'Friends', and 'Get More Truth!'. The main content area is titled 'INBOX' and features a 'new:' indicator with a speech bubble icon. The inbox contains a list of seven messages, each with a sender name, a timestamp, and the message content.

Sender	Time	Message
Somebody said	Wednesday, 2:43pm	i think u sexy now...
Somebody said	Friday, 8:28pm	Ohh well Im sorry :/...
Somebody said	Thursday, 10:38pm	aww thanks :) I think...
Somebody said	Thursday, 12:38am	aww. Im sorry :/ Well...
Somebody said	Wednesday, 11:24pm	??????...
Somebody said	Wednesday, 8:04pm	Portland Ave ? Thats in...
Somebody said	Wednesday, 1:58pm	Hi...










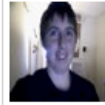







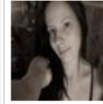


# Sexual Positions Poll

★ Kama Sutra poll

**What is my favorite sex position?** MySpace Apps | View My Apps

Results Compare Search Funbox Invite Friends Cool People Fun Quizzes Settings Create Survey











1% people are like you (148 out of 54810) Male Female All

 brad <input checked="" type="checkbox"/>	 kalie cant take it <input checked="" type="checkbox"/>	 Guardian Angel <input checked="" type="checkbox"/>	 Fuck.Living.Average((F.L. <input checked="" type="checkbox"/>	 starbelly john <input checked="" type="checkbox"/>
 jennifer. <input checked="" type="checkbox"/>	 anthony <input checked="" type="checkbox"/>	 Falling in love with you <input checked="" type="checkbox"/>	 ♥Stephanie♥ <input checked="" type="checkbox"/>	 Jenessa <input checked="" type="checkbox"/>
 Bethannu Has Krebs <input checked="" type="checkbox"/>	 ♥<3Chelsey Rene <input checked="" type="checkbox"/>	 Clyde <input checked="" type="checkbox"/>	 TAKEEYAH...THATS ME! <input checked="" type="checkbox"/>	 SILENT SUICID <input checked="" type="checkbox"/>
 Living Life... <input checked="" type="checkbox"/>	 courtney <input checked="" type="checkbox"/>	 CaT <input checked="" type="checkbox"/>	 Lonzo <input checked="" type="checkbox"/>	 ~ã Chelle Belleã <input checked="" type="checkbox"/>

Next

Select all

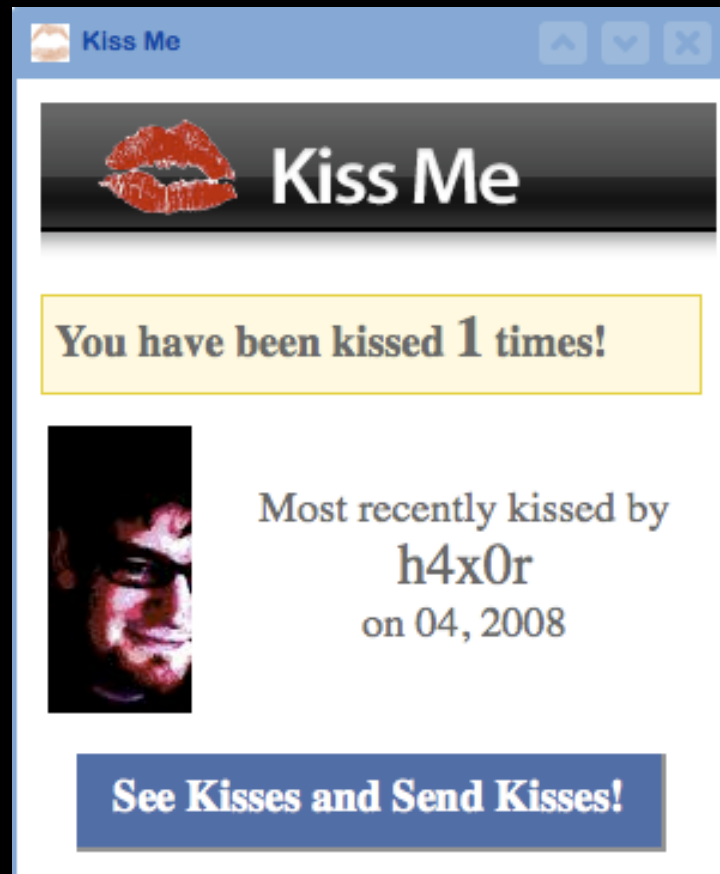
**Just Taken**

-  Which teddy bear are you?  
!~MiSsUnDeRsToOd~! (Im BaD.....N03 DaT)
-  What Kind Of Sex Should You Have?  
\*I Luv Him He kno's who he is\*
-  What brand of car are you?  
Superman
-  What's Your Sexy Fetish?  
amber
-  What Love Type Are You?  
Tina
-  How Do You Kiss?  
ãBrittanyãJohnã4ãEVERã
-  whats rock band are u  
Blake
-  What Love Type Are You?  
Fuzz
-  Are you addicted to porn  
ã@i ♥ mOoKIE pOoKIE bEaR!™ã
-  What is your RPG Class?  
Why so serious???



# Properly Done?

- ★ An self-contained OpenSocial app not an offsite iframe.
- ★ Utilizing signed requests with authtype=SIGNED.
- ★ Request tampering still worked. Why?



# Kiss Me App Ownage

```
api.msappspace.com:80/proxy/relay.proxy?  
opensocial_authtype=SIGNED&opensocial_token=Yn7XsoORUtjDaANU0WRKy/  
Julah6OvUQYG0VrTU7NSFXXweXSLAomgmuGbIegf5XSDwilli29lim+UduxZUBzFnf9S0QlwFTLNi  
+34gg9Is=&opensocial_url=http%3A//kiss-dynamic-lb.myspacegamingapps.com/hugme/sendmessage  
%3Fnetwork%3Dmyspace%26to_user_id%3DREMOVED%26type%3DKISS%26from_user_id  
%3DREMOVED%26from_user_name%3Dcstm_REMOVED%26from_user_profile%3Dhttp%3A//  
a680.ac-images.myspacecdn.com/images01/110/REMOVED.jpg%26nocache%3D1217872981976
```

# Cajoley Caja, Batman!

- ★ Caja is meant to create "safe" JavaScript in OpenSocial
- ★ Tries to un-suckify .js, removing:
  - ★ eval()
  - ★ top.location
  - ★ And many others...
  - ★ Demonstrates the way this problem is typically approached anyway.
- ★ Seems irrelevant if it's opt-in.

# DoSer Function?

- ★ Stupid test MySpace app
  - ★ 7 seconds after viewing, it logs you out
  - ★ Logs anyone out that views your page for 7 seconds
  - ★ Logs you out after viewing for 7 seconds ;)
  - ★ Demonstrates content on canvas, profile, and home



The screenshot shows a MySpace App listing for 'DoSer'. At the top left is the 'MySpace Apps' logo. Below it, the app name 'DoSer' is displayed in bold. To the left of the app details is a small thumbnail image showing two people in a physical confrontation. To the right of the image, the text reads 'Made by Nathan' and '< 100 active users'. Below this, the categories 'Fun Stuff / Dating & Relationships' are listed. At the bottom of the listing, there is an 'About DoSer' section with the text 'A general Kick in the Nuts.'

# Surfs Up!

- ★ Meet CSRFer
  - ★ Demonstrates 3 different ways to do CSRF on MySpace
  - ★ Image tags, iframes, and meta tags, oh my!
  - ★ Demonstrates content on canvas, profile, and home



The screenshot shows the MySpace Apps interface. At the top left is the MySpace logo and the text "MySpace Apps". Below this is the title "CSRFer". To the left of the main content is a small image of an astronaut. To the right, it says "Made by Nathan" and "< 100 active users". Below that, it lists "Categories" as "Communicating / Dating & Relationships". At the bottom left, there is a link "About CSRFer" and the text "Request Nunchuck".



The screenshot shows a window titled "CSRFer" with a blue header bar. Below the header, the text "CSRFer Dev" is displayed. There are three radio button options: "Get More Friends" (which is selected), "Log Out Viewers", and "Block Viewer Comms". At the bottom of the window is a "Save" button.

# Are we hosed? Plz advise.

- ★ Kill external content
- ★ Drastically reduce API functionality
- ★ Threat model your stuff, people
- ★ Props to late adopters. =)
- ★ No opt in security models
- ★ Developers, Developers, Developers
- ★ Profile lifetime bit (member since / training wheels)
- ★ Email verification for corporate socnets
- ★ Create a profile, before someone else does ;)