

Website Vulnerabilities Revealed

Jeremiah Grossman
WhiteHat Security founder & CTO



Jeremiah Grossman

WhiteHat Security Founder & CTO

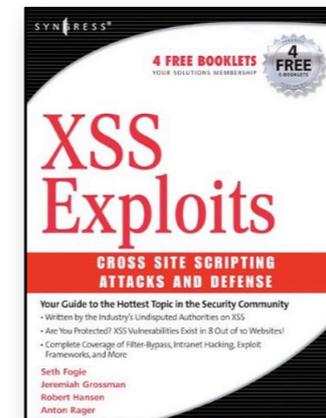
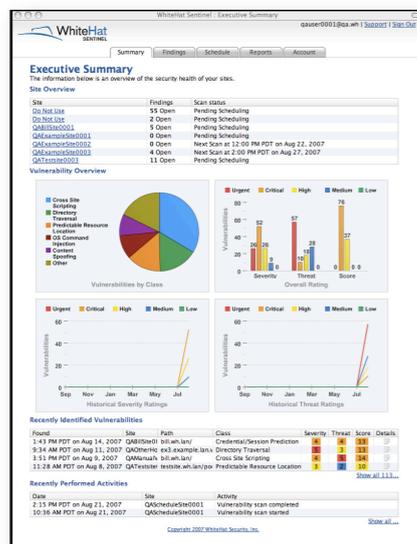
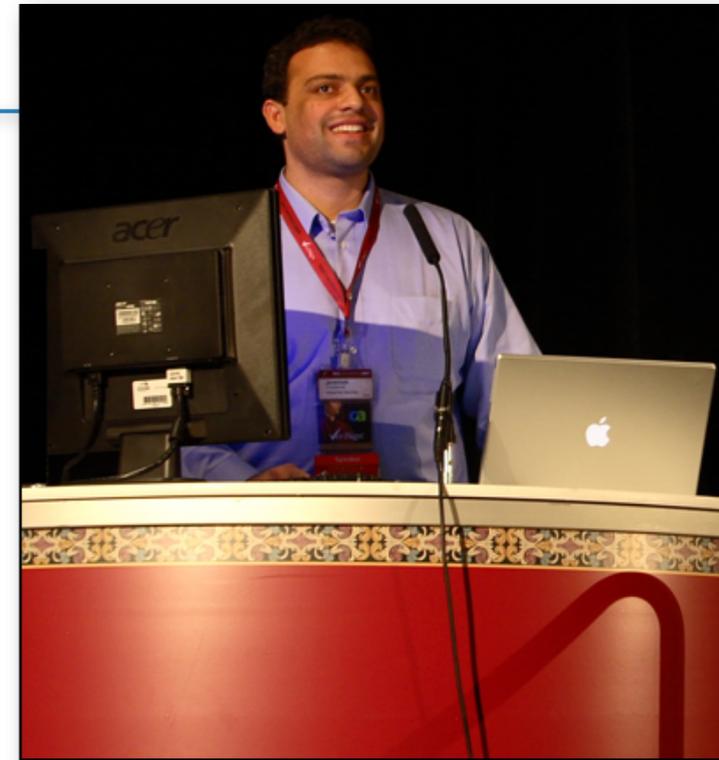
Technology R&D and industry evangelist
(InfoWorld's CTO Top 25 for 2007)

Frequent international conference speaker

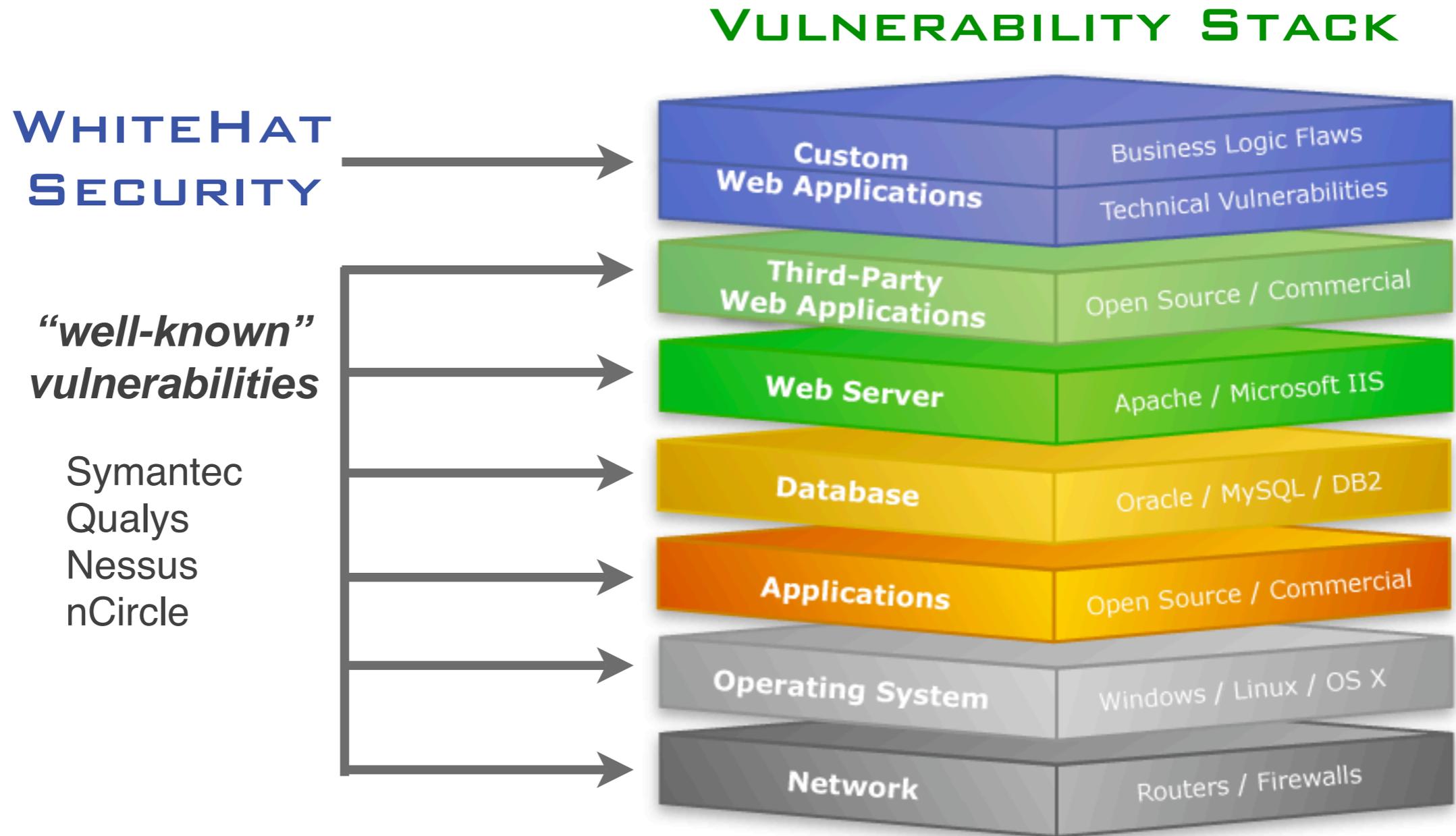
Co-founder of the Web Application Security Consortium

Co-author: *Cross-Site Scripting Attacks*

Former Yahoo! information security officer



Custom Web Applications, Custom Vulnerabilities



2006 © Copyrights WhiteHat Security

Data is unique from reports distributed by Symantec, Mitre (CVE), IBM (ISS) X-Force, SANS, and others. These organizations track publicly disclosed vulnerabilities in commercial and open source software products, which may contain Web application flaws as well. WhiteHat Security's data is different because it focuses solely on previously unknown vulnerabilities in custom web applications, code unique to that organization, on real-world websites

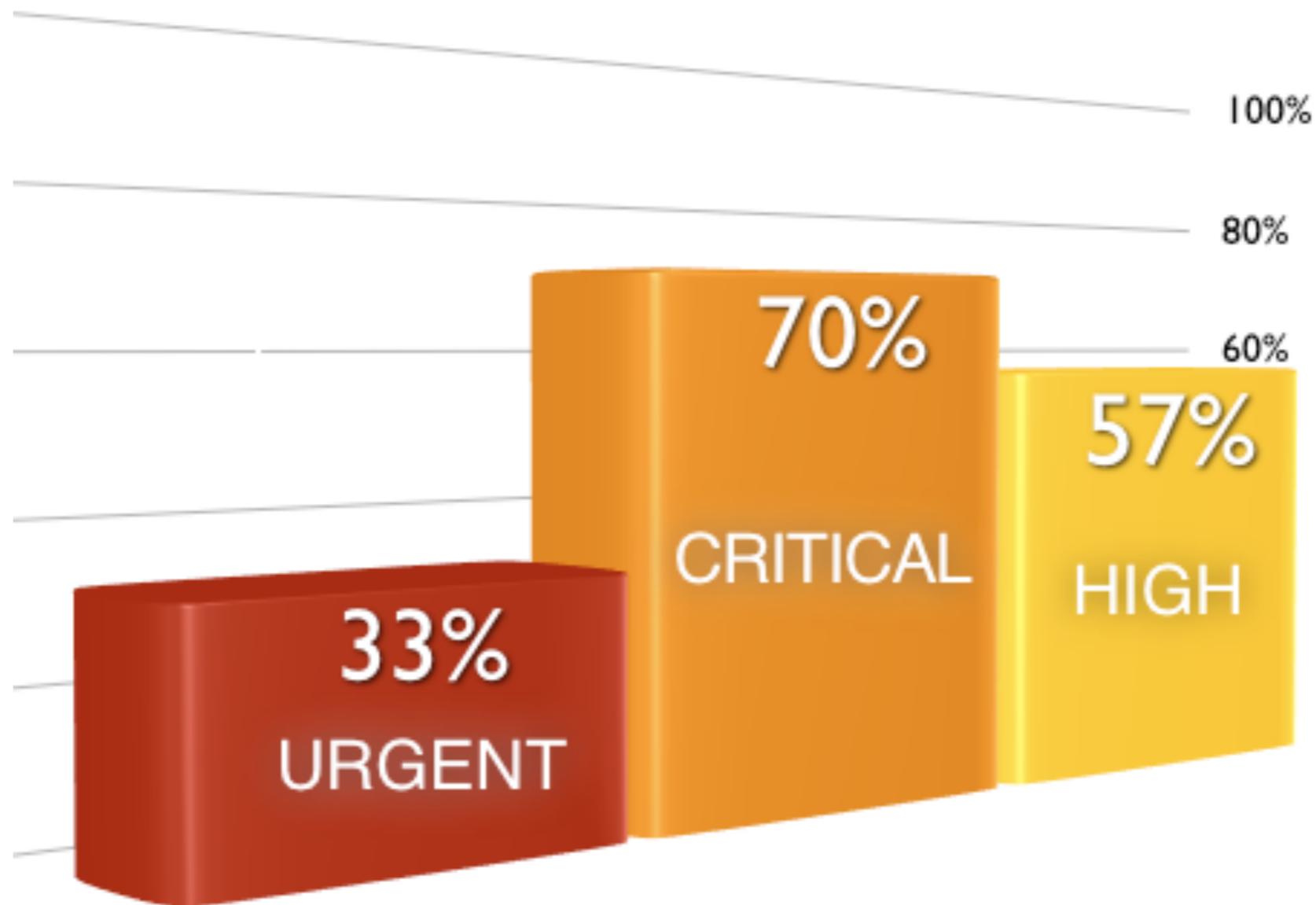
Global Scale

9 OUT OF 10 WEBSITES HAVE SERIOUS VULNERABILITIES

- Obtained between January 1, 2006 and February 22, 2008
- Classified according to the WASC Threat Classification
- Over 600 public-facing and pre-production websites
- Vast majority of websites are assessed weekly for vulnerabilities
- Currently 4,488 unresolved vulnerabilities
- Nine out of ten websites have at least one significant vulnerability
- Average of 7 vulnerabilities per website

But how bad is it really?

LIKELIHOOD THAT A WEBSITE HAS A VULNERABILITY, BY SEVERITY



Websites with Urgent, Critical, or High severity issues technically would not pass PCI compliance

NEWS BLOGS SOFTWARE SECURITY HARDWARE

LINUX JOURNAL
 Find out why Houston is the next big thing in open source and startups

Home Topics Newsletter Community Resources Forums Shop Magazine

Home

Hackers Take Down Pennsylvania Government
 January 10th, 2008 by Justin Ryan

NETCRAFT
 Every Rack Is Private
 10GigE Cisco Network
 Public & Private Networks

SOFTLAY
 do it faster. do it better. do it right.

Webserver Search
 What's that site running?...

Netcraft Services
 News
 Subscribe to Netcraft News

Washington Post > Technology > Special Reports > Privacy

TechNews.com

40 Million Credit Card Numbers Hacked
 Data Breached at Processing Center

By Jonathan Krim and Michael Barbaro
 Washington Post Staff Writers
 Saturday, June 18, 2005; Page A01

QUICK QUOTES

Enter Symbol go
 Tables | Portfolio | Index

MOST VIEWED ARTICLES

Technology On the Site
 Updated 2:03 p.m. ET

- Intel has a chip, but where are the MIDs?
- Rep. Barton Seeks Probe In Theft of Computer
- Intel Unveils New Classmate PCs

More than 40 million credit card numbers belonging to U.S. consumers were accessed by a computer hacker and are at risk of being used for fraud, MasterCard International Inc. said yesterday.

In the largest security breach of its kind, MasterCard officials said all credit card brands were affected, including 13.9 million cards bearing the MasterCard label. A spokeswoman for Visa USA Inc. confirmed that 22 million of its card numbers may have been breached, while Discover Financial Services Inc. said it did not yet know if its cards were affected.

"I don't think we've seen this scale of database intrusion before. SQL injection attacks are usually on a one-at-a-time basis," said Phil Neray, VP of marketing at Guardium, a Waltham, Mass., firm that makes database protection software.

c|net NEWS.com

Today on CNET | Reviews | News | Downloads | Tips & Tricks | CNET TV | Compare Prices

Business Tech | Cutting Edge | Green Tech | Wireless | Security | Media | Markets | Personal Tech

Samy opens new front in worm war

By Munir Kotadia
 Staff Writer, CNET News.com
 Published: October 17, 2005 11:40 AM PDT

Welcome Google user!

Add News.com to Google
 Add CNET News.com headlines to your Google homepage or Google reader.
 Add to Google

More headlines related to "f":

- Harnessing the power of wind and waves
- Police Blotter: Armed robbers nabbed through text messages
- Microsoft-Yahoo the mother of all clusterbombs
- Week in review: Apple goes into thin 'Air'
- More matching headlines >

The newly discovered Samy worm is one of the first to exploit a cross-site scripting vulnerability, a technique security experts fear could be used to open a new front in attacks.

Tools
 Talkback | Print | E-mail | Share

Reprints & Permissions | RSS

Mixx it
 Other ways to share:
 Yahoo! Buzz
 Digg
 Newsvine
 Reddit
 Facebook

ers to use the PC to spread spam and carry out scams. Typically, it...
 a keystroke logger, which collects and transmits your passwords...
 a you type online.

ogle (GOOG) that fails to carefully handle JavaScript — the coding that activates...
 such as changing the color of a button when someone mouses over it — is a potential...
 tes, says tech security firm WhiteHat Security. Hackers have discovered ways to trick...
 un malicious JavaScripts.

re or two smart guys are attacking a few dozen major websites," says David Dewey,...
 security division. "In the next few weeks I would expect to see copycats attacking...
 bsites."

The Register » Security » Enterprise Security »

RIAA wiped off the net

Hacktivists at work

By John Leyden → More by this author
 Published Monday 21st January 2008 12:25 GMT

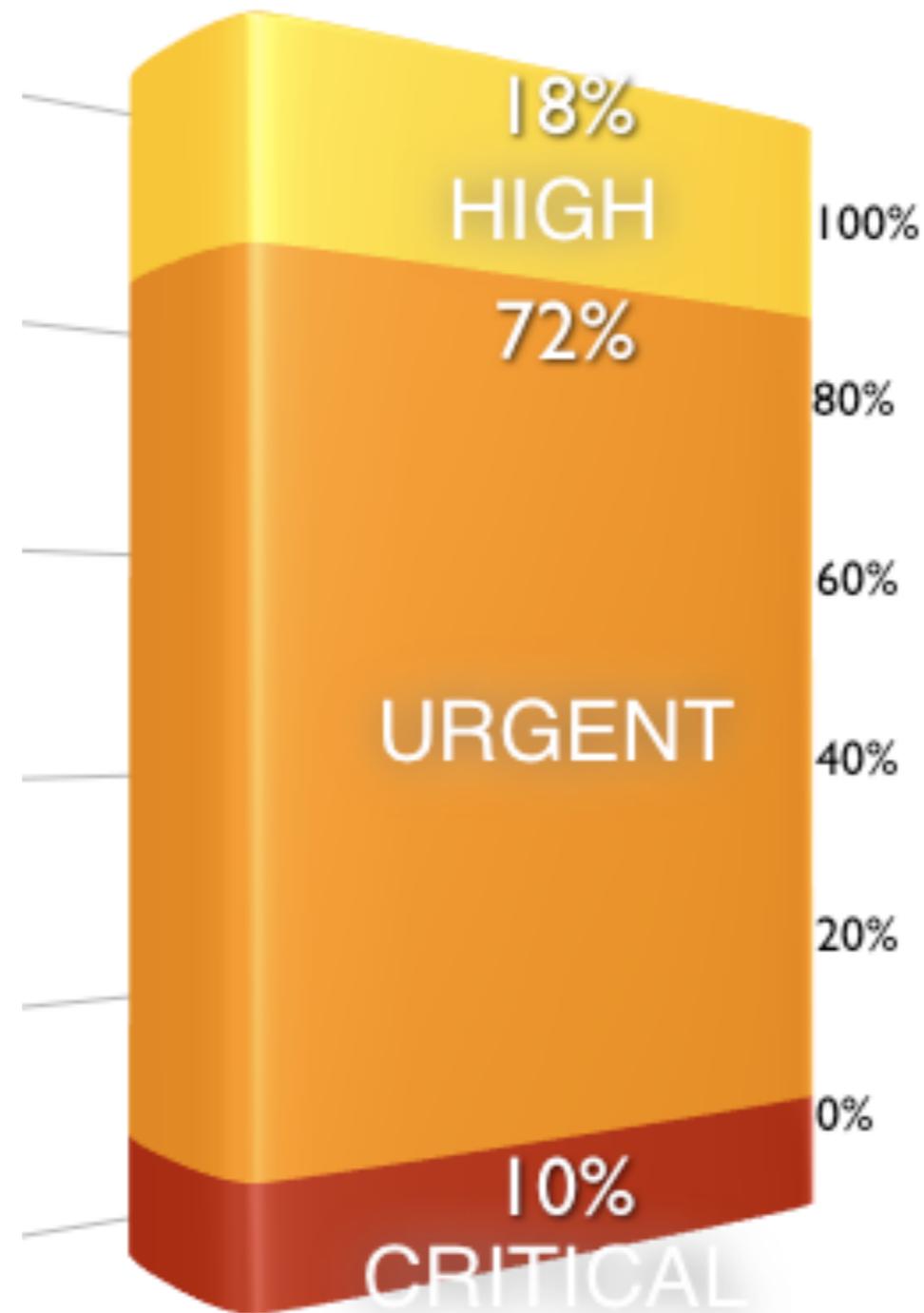
Improve IT Culture and employee satisfaction in your business - Sign up for the latest RegCast here

A lack of security controls allowed hackers to "wipe" the Recording Industry Association of America's (RIAA) website on Sunday.

The existence of an SQL injection attack on the RIAA's site came to light via social network news site Reddit. Soon after hackers were making merry, turning the site into a blank slate, among other things.

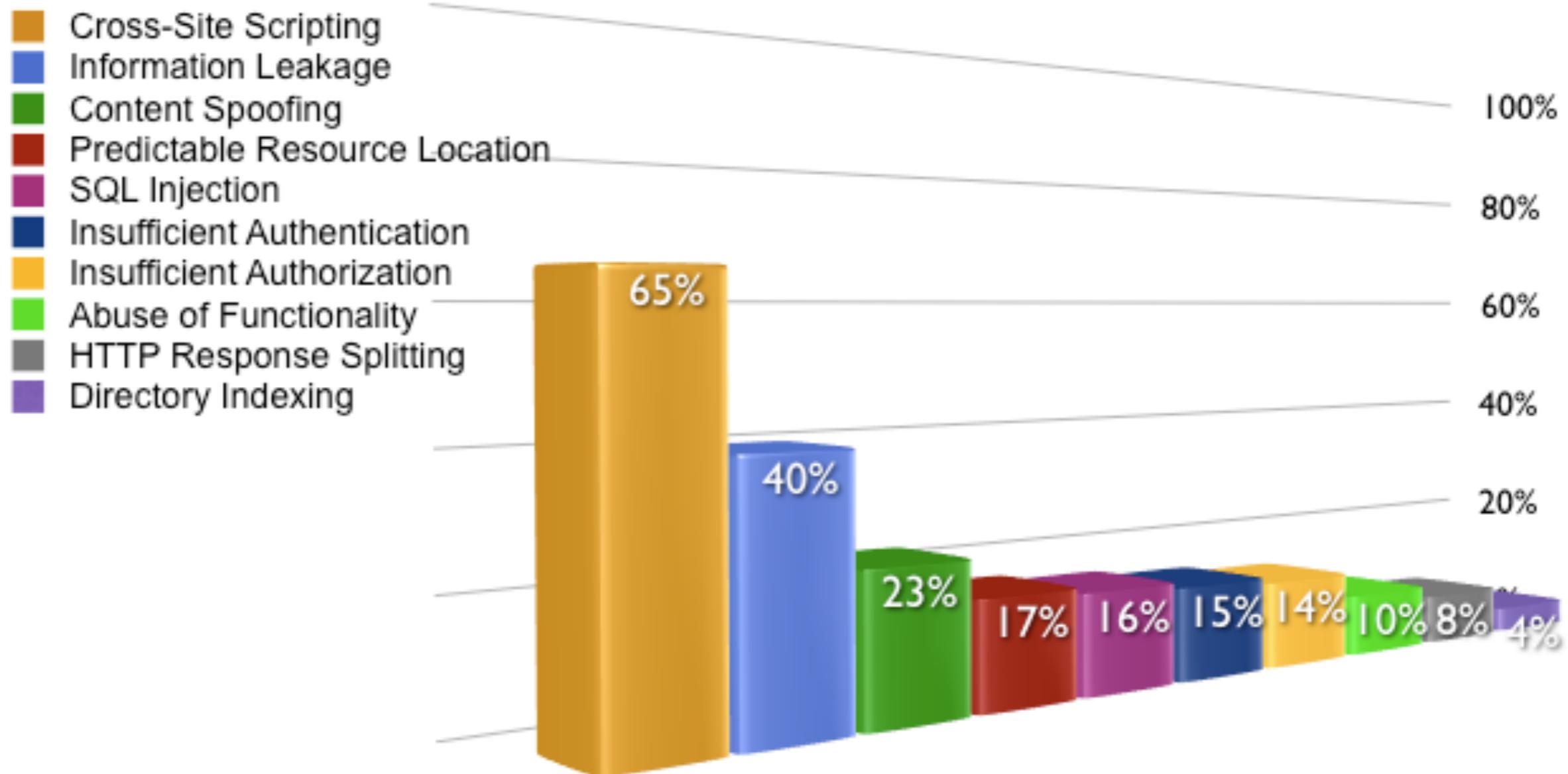
Another way to look at the badness

PERCENTAGE OF VULNERABILITIES RANKED BY SEVERITY

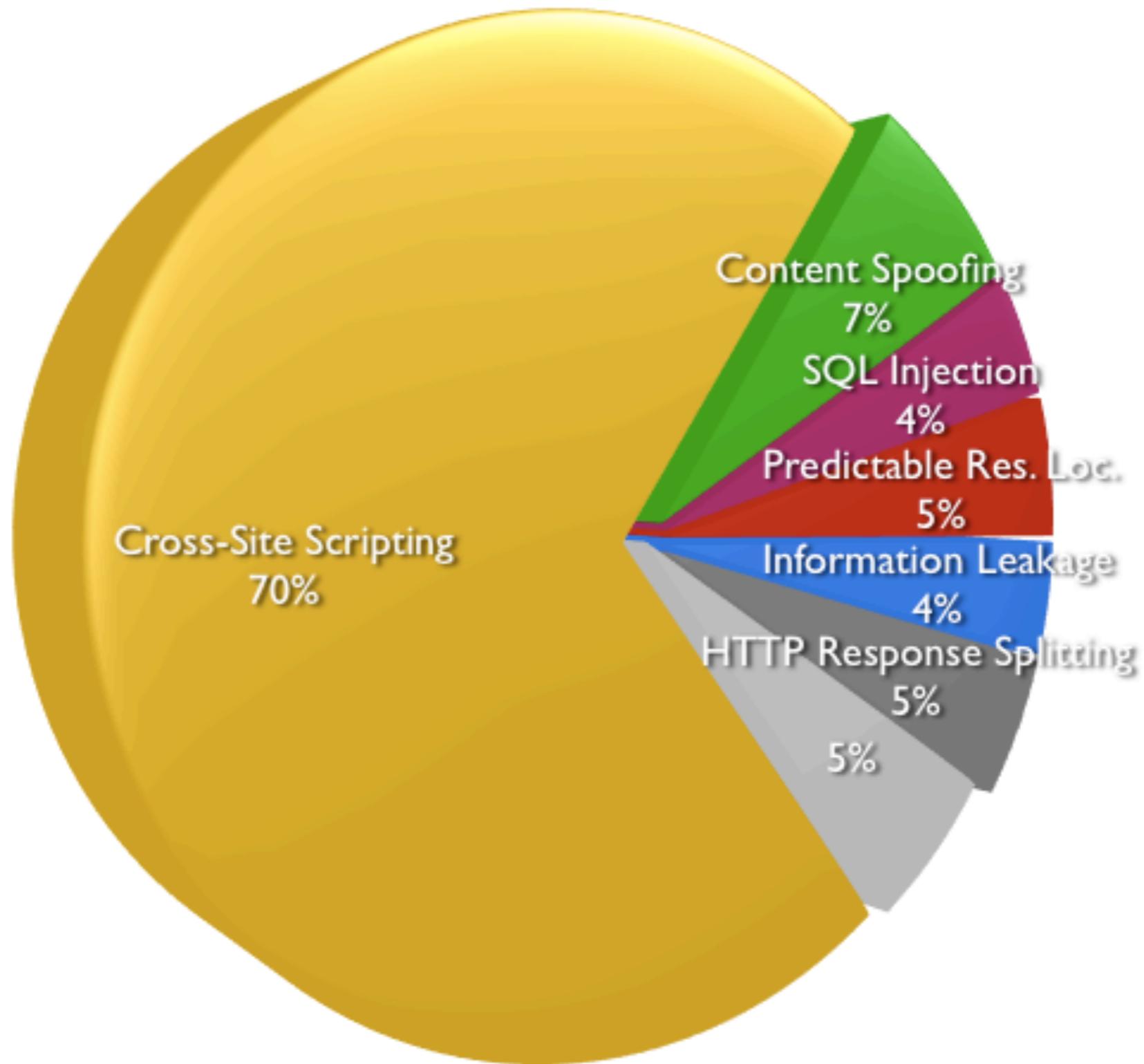


WhiteHat Security: Top 10

LIKELIHOOD THAT A WEBSITE HAS A VULNERABILITY, BY CLASS

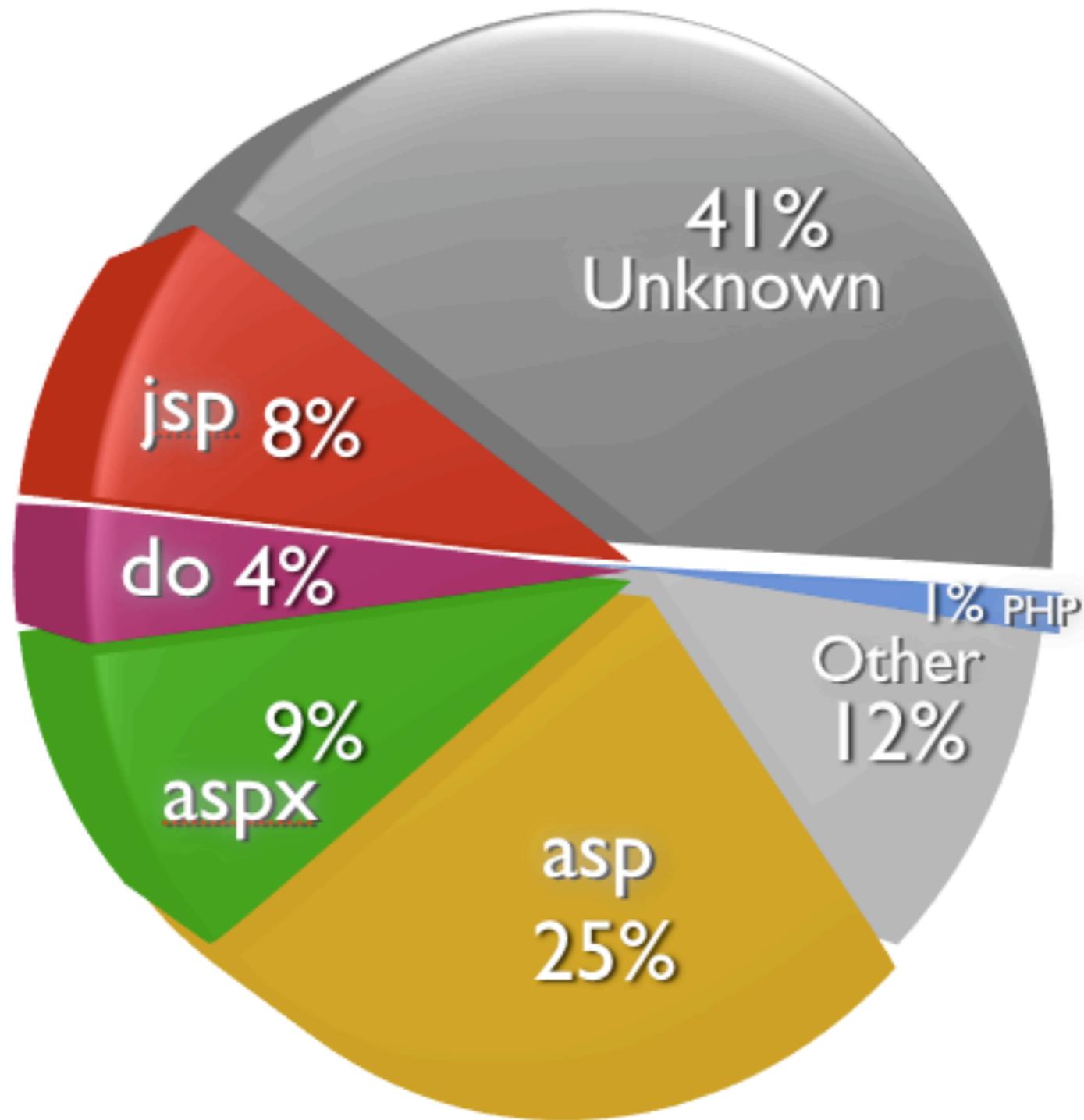


Overall vulnerability population



Technology Breakdown

FILE EXTENSIONS



What's not there

Obviously we're not going to find buffer overflows or format string issues in custom web applications

We're also not looking for the well-known php issues and the like

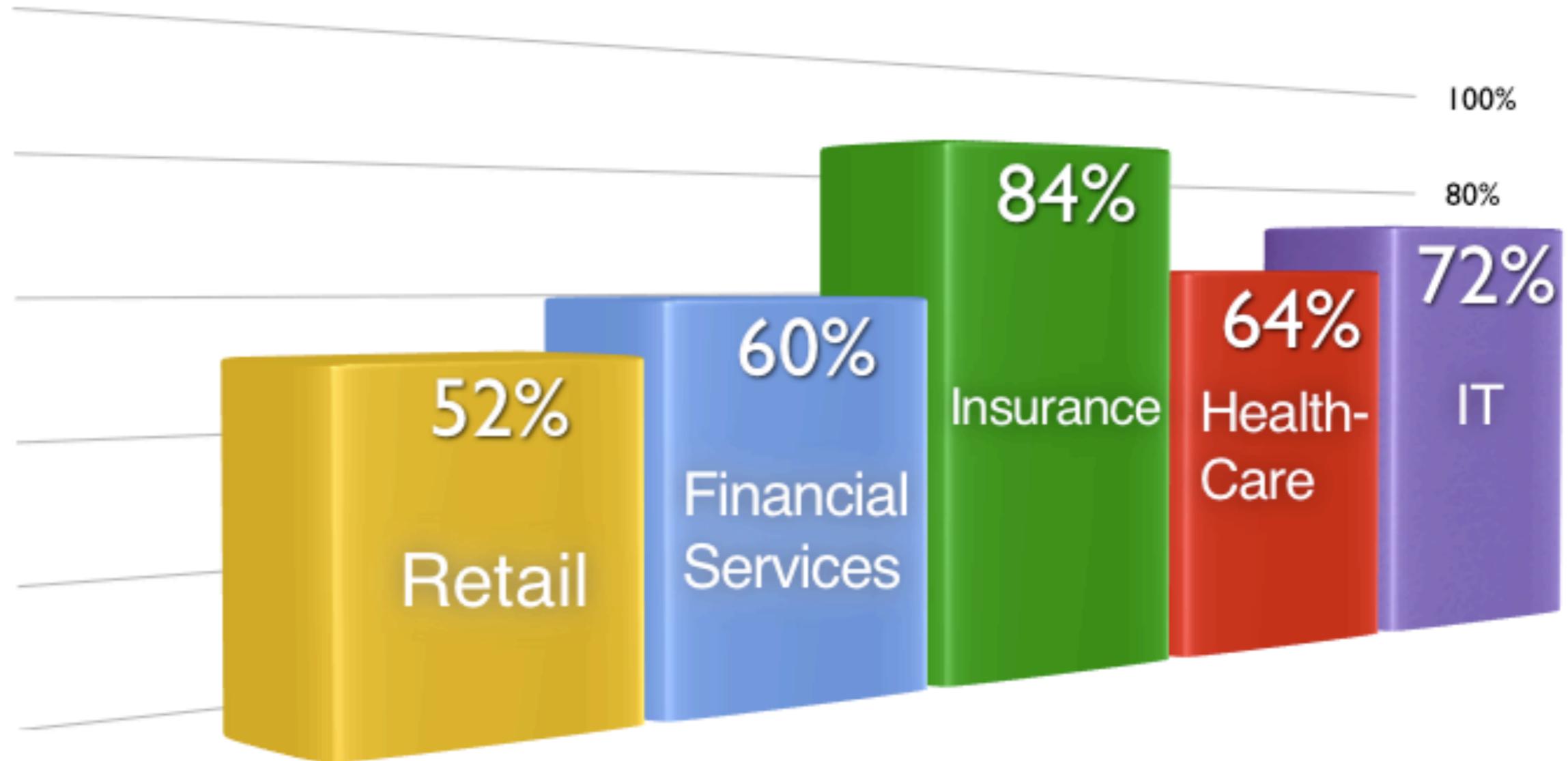
Cross-Site Request Forgery remains **VERY DIFFICULT** to scan for and we only report the most egregious cases identified by hand

We keep finding new and cool ways of performing XSS filter-evasions

HTTP Response Splitting pushed XPath Injection off the list

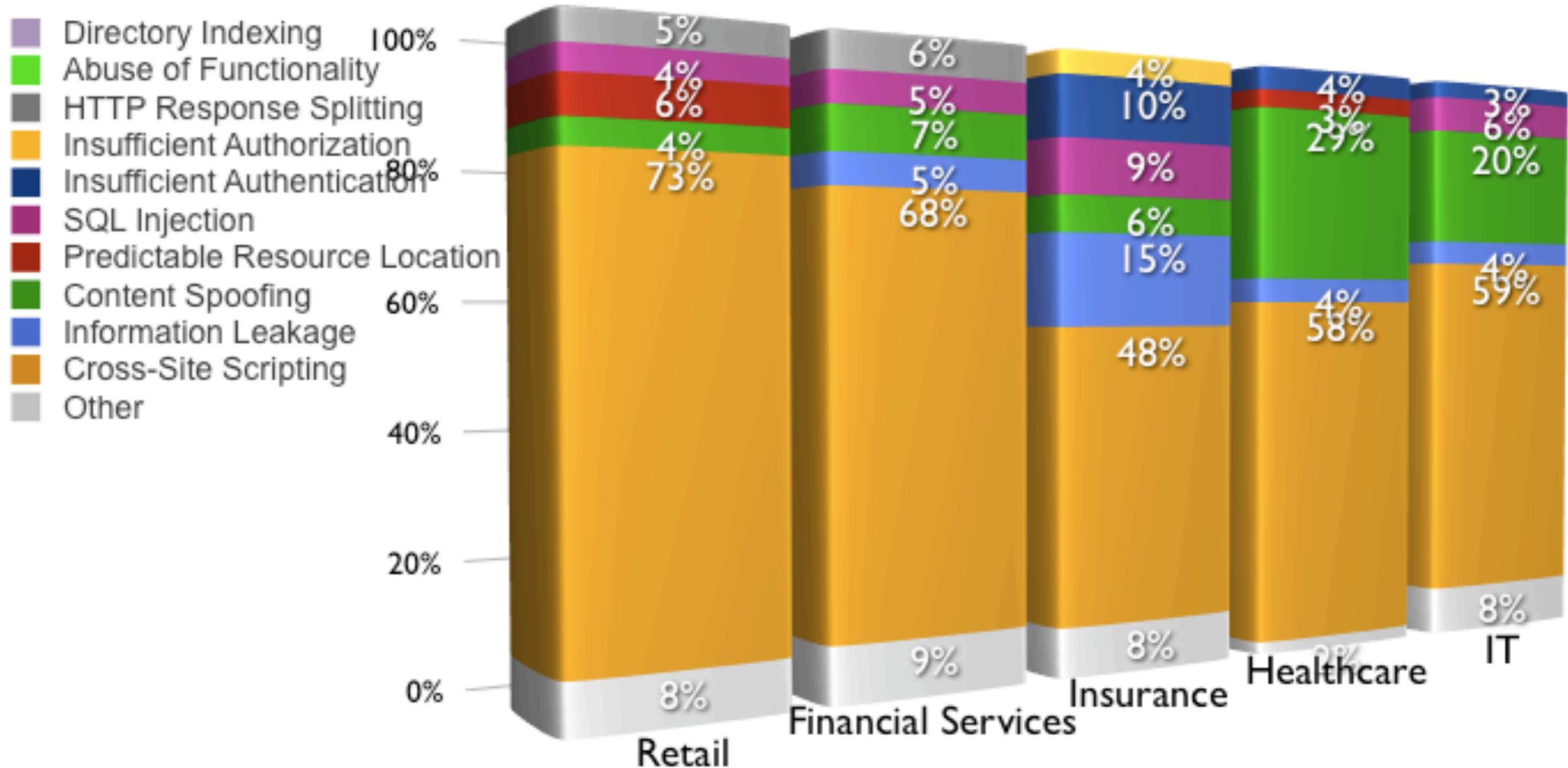
Industry Verticals

PERCENTAGE OF WEBSITES WITH EITHER URGENT, CRITICAL OR HIGH SEVERITY VULNERABILITIES RANKED BY INDUSTRY



Worst of the Worst

PERCENTAGE OF VULNERABILITY CLASSES IN OVERALL POPULATION RANKED BY INDUSTRY

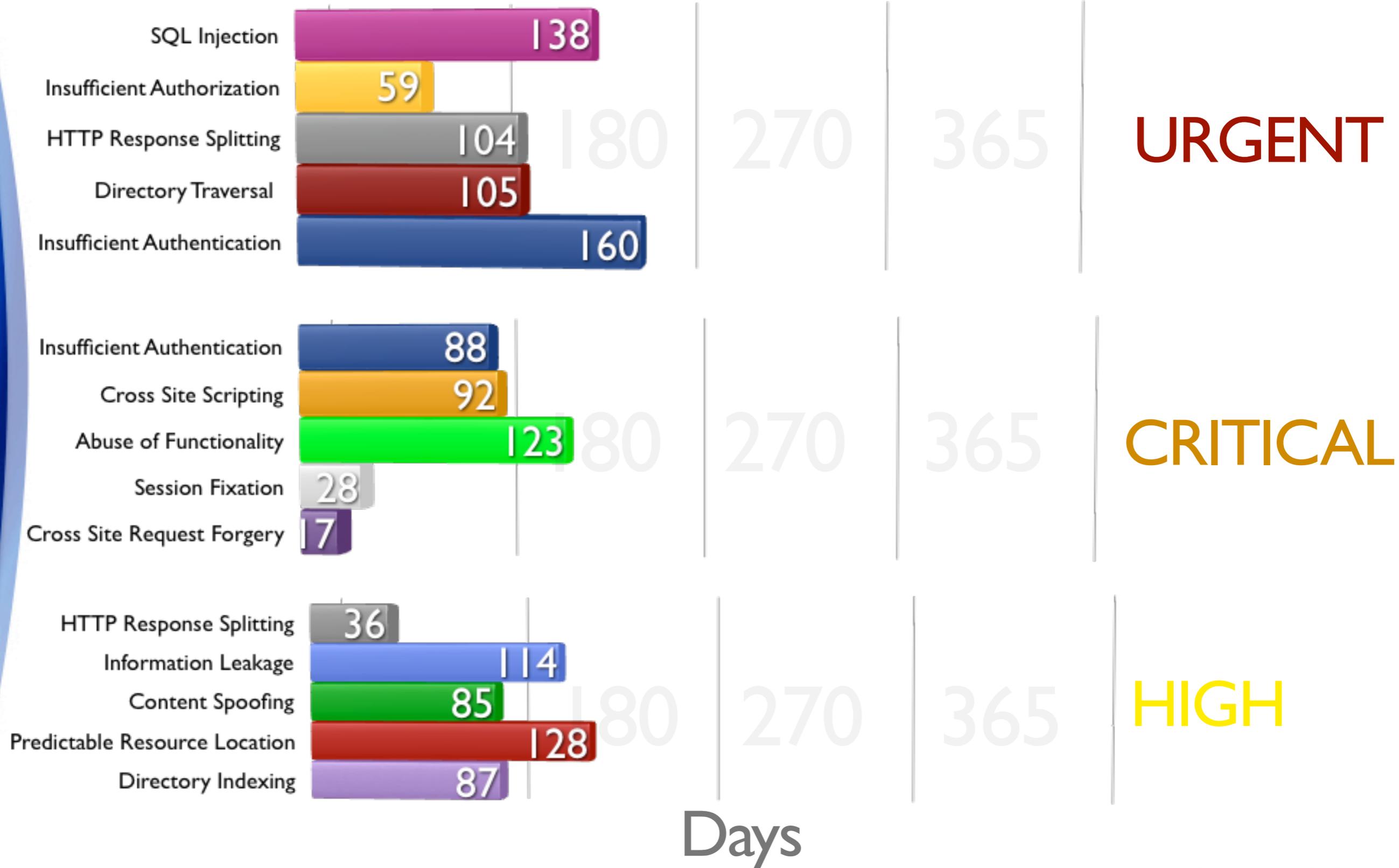


Data input correlation

Average inputs per website: 154

Ratio of vulnerability/inputs: 2.2%

Time to Fix



Lessons Learned

Vertical Comparisons – IT Security is extremely curious about how their security compares to others in their market. When behind the curve, justification for additional resources. When ahead, outside validation and assurance of their security program.

Remediation/Mitigation – IT Security is responsible for website security, but has no control over it (can't patch, no firewalls). The developers don't work for them and have other priorities other than security. This environment causes lengthy time-to-fix cycles.

Possible vs. Probable – Just because a vulnerability is found doesn't mean it'll be exploited. Not all vulnerabilities are created equal, some are easier to take advantage of others, and the bad guys will take the path of least resistance.

Assignment of blame – When an incident occurs exploiting a vulnerability previously reported, its the developers fault. When exploited by a vulnerability not found, its IT Security's fault.

Those that are more "secure" have:

Use of modern development frameworks with security configs turned on (.NET, J2EE, Rails, etc.)

Vulnerability remediation prioritized by severity/threat rating (High: 1 - 7 days, Medium: < 30 days, Low: Next Update)

At least some security involvement in the SDLC (awareness training, threat modeling, QA testing, etc.)

Thank You!

For more information visit: www.whitehatsec.com/

Jeremiah Grossman, founder and CTO
blog: <http://jeremiahgrossman.blogspot.com/>
email: jeremiah@whitehatsec.com

