Website Vulnerability Statistics

Trends and Business Effects

Jeremiah Grossman
Founder & Chief Technology Officer

WhiteHat SECURITY

WhiteHat Security - Website Risk Management

- WhiteHat Sentinel Service
  - Unlimited website vulnerability assessment
- SaaS-based, annual subscription model
  - Combination of proprietary scanning technology and expert operations team
- 200+ enterprise customers
  - 1000's of assessments performed annually from start-ups to Fortune 500

WhiteHat Sentinel **PREMIUM EDITION**

WhiteHat Sentinel **STANDARD EDITION**

WhiteHat Sentinel **BASELINE EDITION**

Sentinel PE - Configured assessment delivery including comprehensive manual testing for business logic issues. For high-risk websites with sensitive data and performs critical business functions.

Sentinel SE - Configured assessment delivery with verified vulnerability reporting – designed for medium risk websites with complex functionality requiring extensive configuration.

Sentinel BE - Self-service, automated assessment delivery with verified vulnerability reporting – designed for smaller, less complex, lower risk websites.

WhiteHat SECURITY

WASC 24 (+2)* 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*

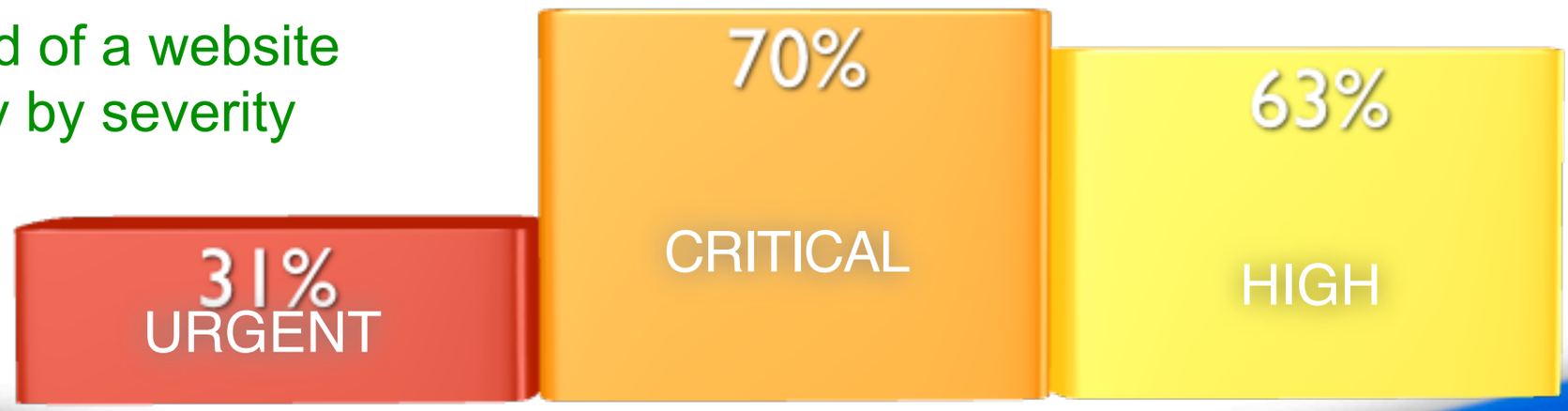
Data Set

- Collection duration: **January 1, 2006 to March 31, 2009**
- Total websites: **1,031**
- Identified vulnerabilities (custom web applications): **17,888**
- Assessment frequency: **~Weekly**
- Vulnerability classes: **WASC Threat Classification**
- Severity naming convention: **PCI-DSS**

Key Findings

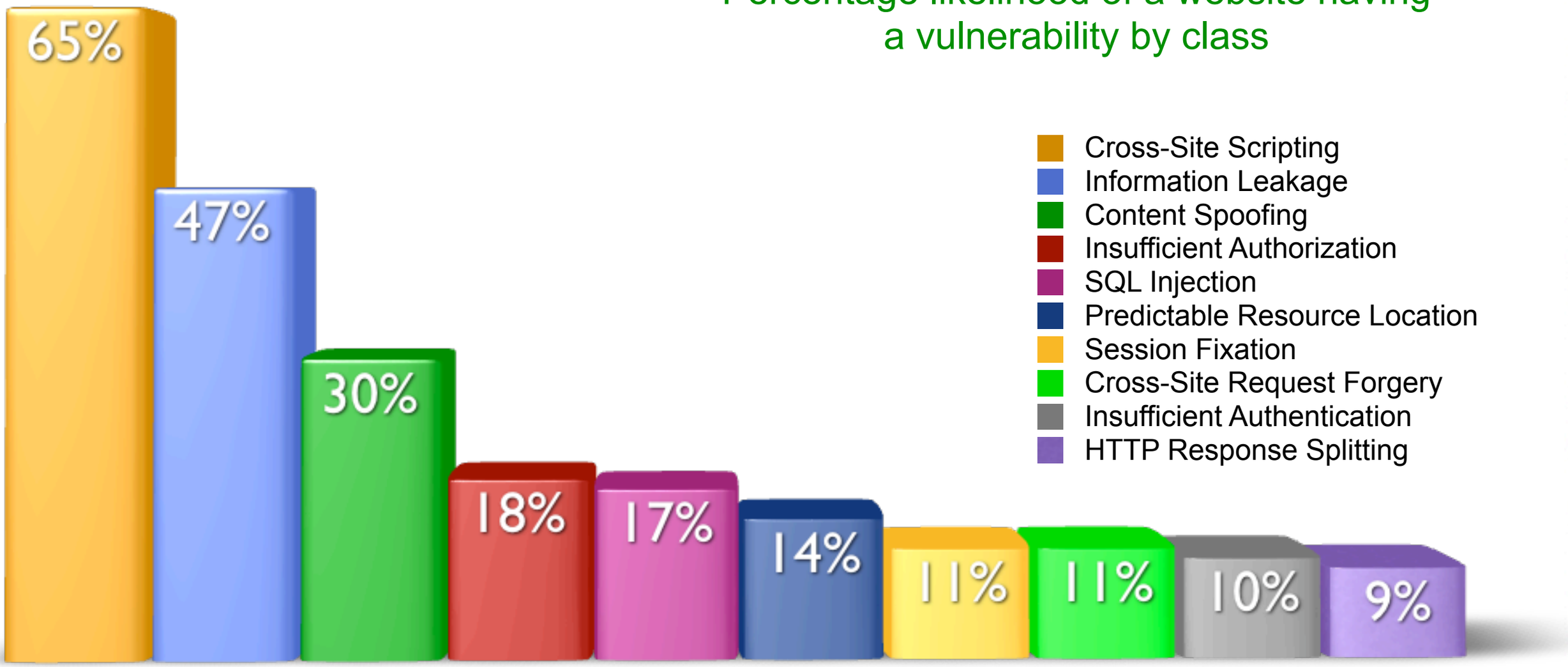
- Unresolved vulnerabilities: **7,157** (60% resolution rate)
- Websites *having had* at least one HIGH, CRITICAL, or URGENT issue: **82%**
- Lifetime average number of vulnerabilities per website: **17**
- Websites currently with at least one HIGH, CRITICAL, or URGENT issue: **63%**
- Current average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

Percentage likelihood of a website having a vulnerability by severity



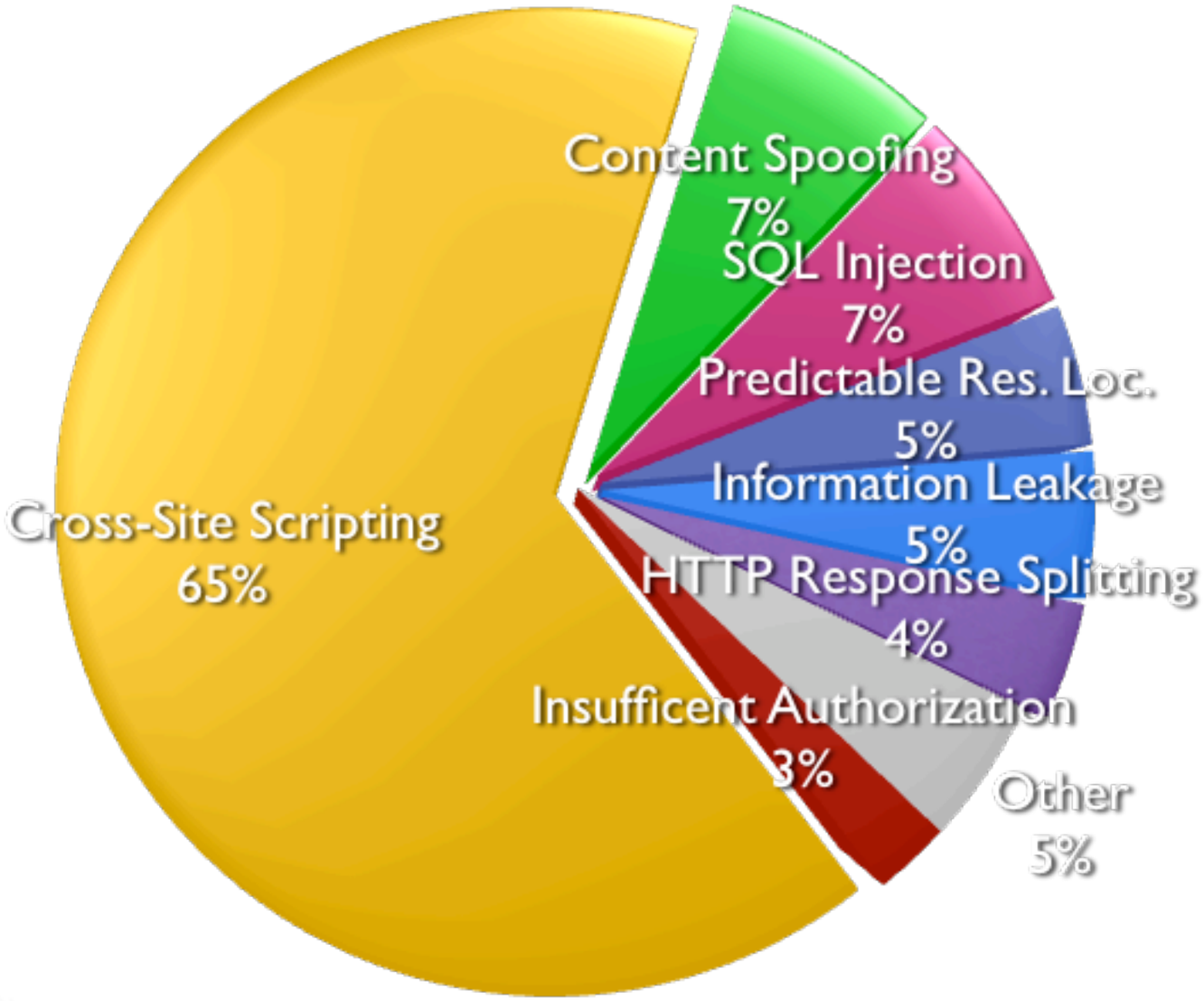
WhiteHat SECURITY

WhiteHat Security Top Ten



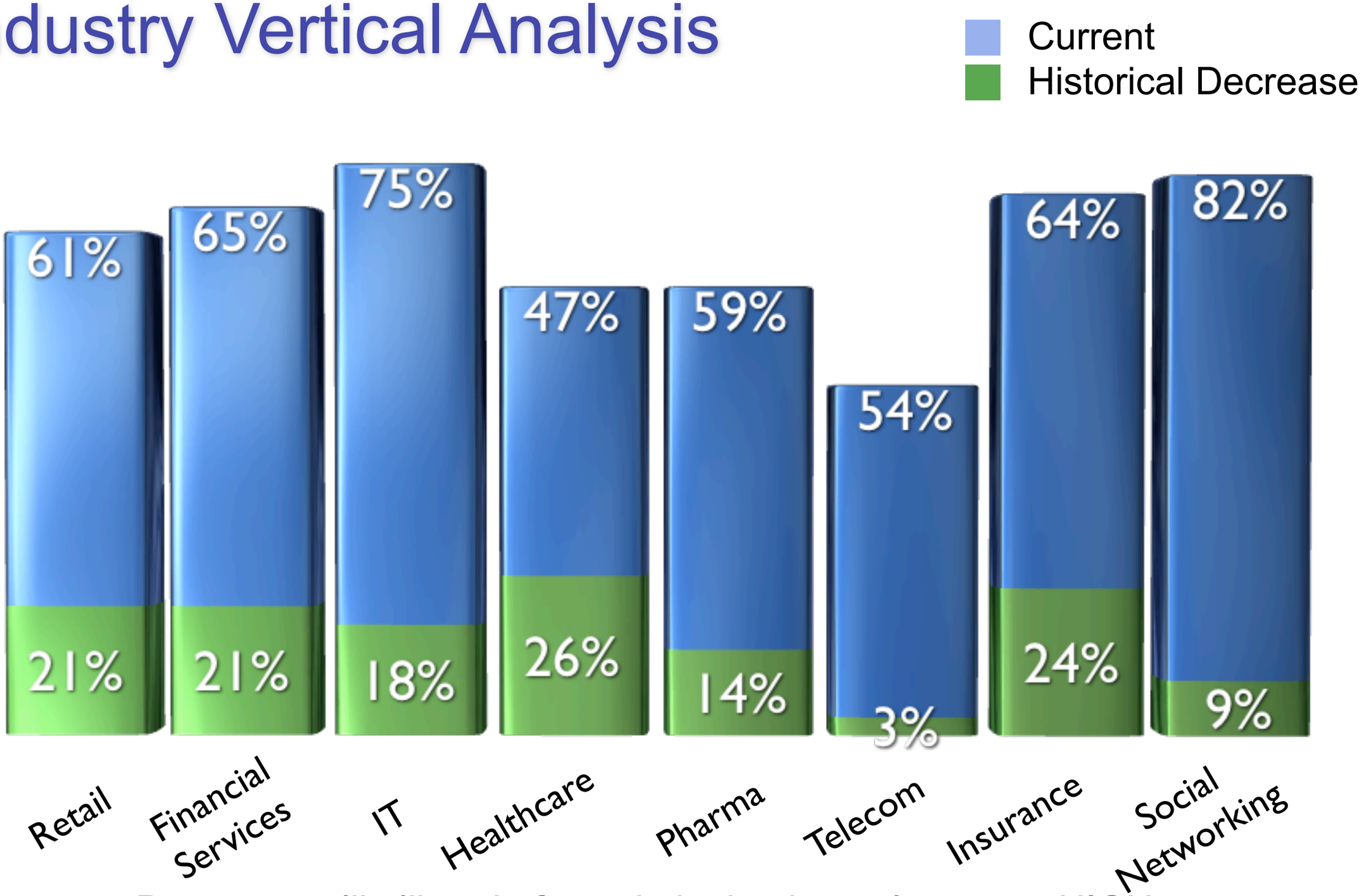
- Average number of inputs per website: **227**
- Average ratio of vulnerability count / number of inputs: **2.58%**

Overall Vulnerability Population



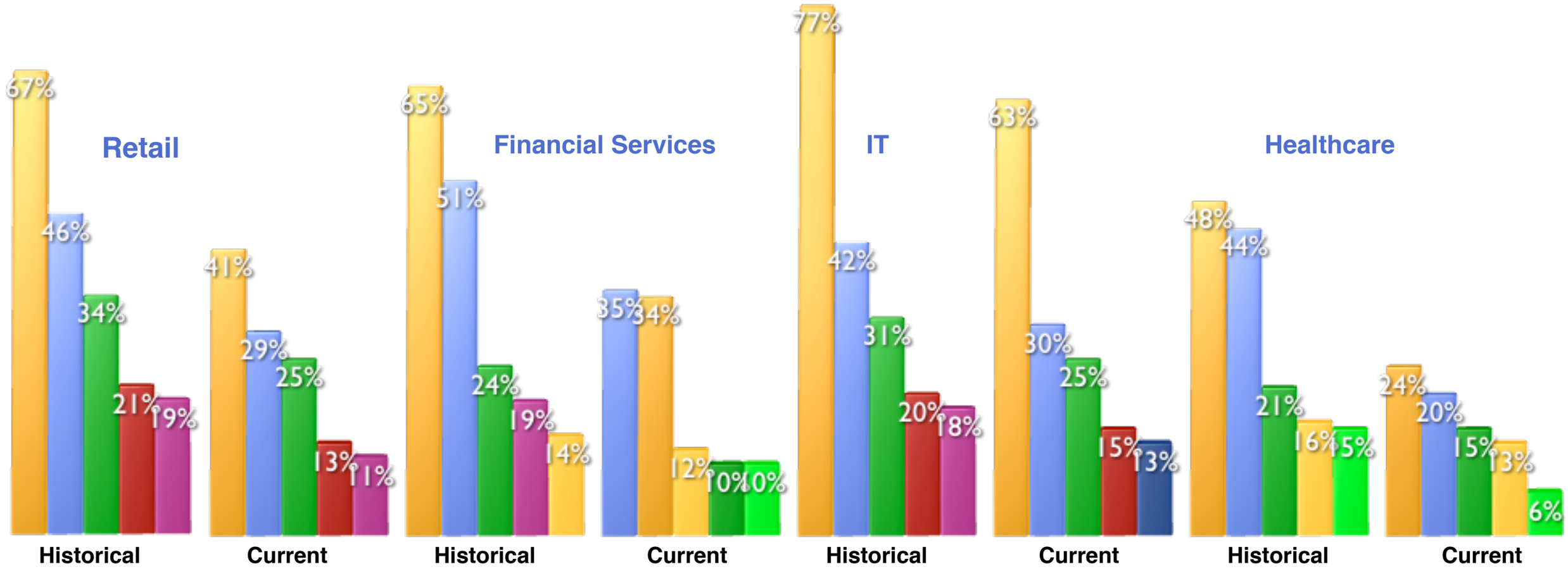
URL Extension	% of websites	% of vulnerabilities
unknown	59%	40%
asp	24%	25%
aspx	23%	9%
xml	10%	2%
jsp	9%	8%
do	7%	3%
php	6%	3%
html	4%	2%
old	4%	1%
dll	4%	1%
cfm	3%	4%

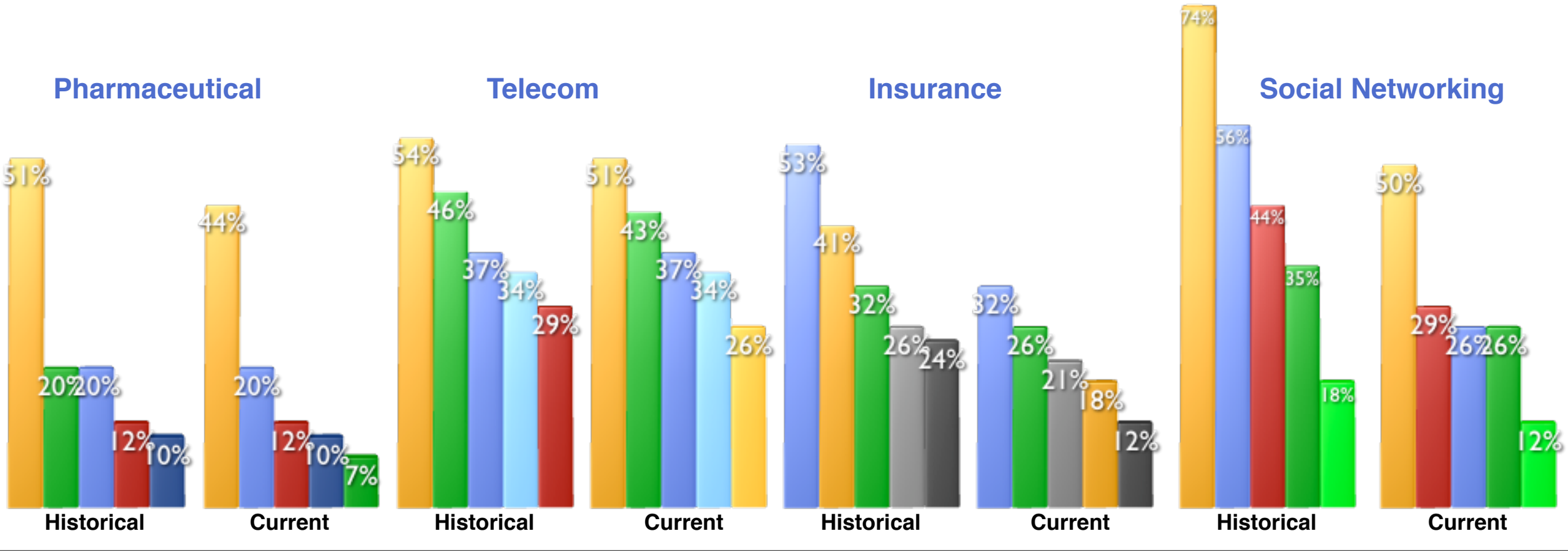
Industry Vertical Analysis



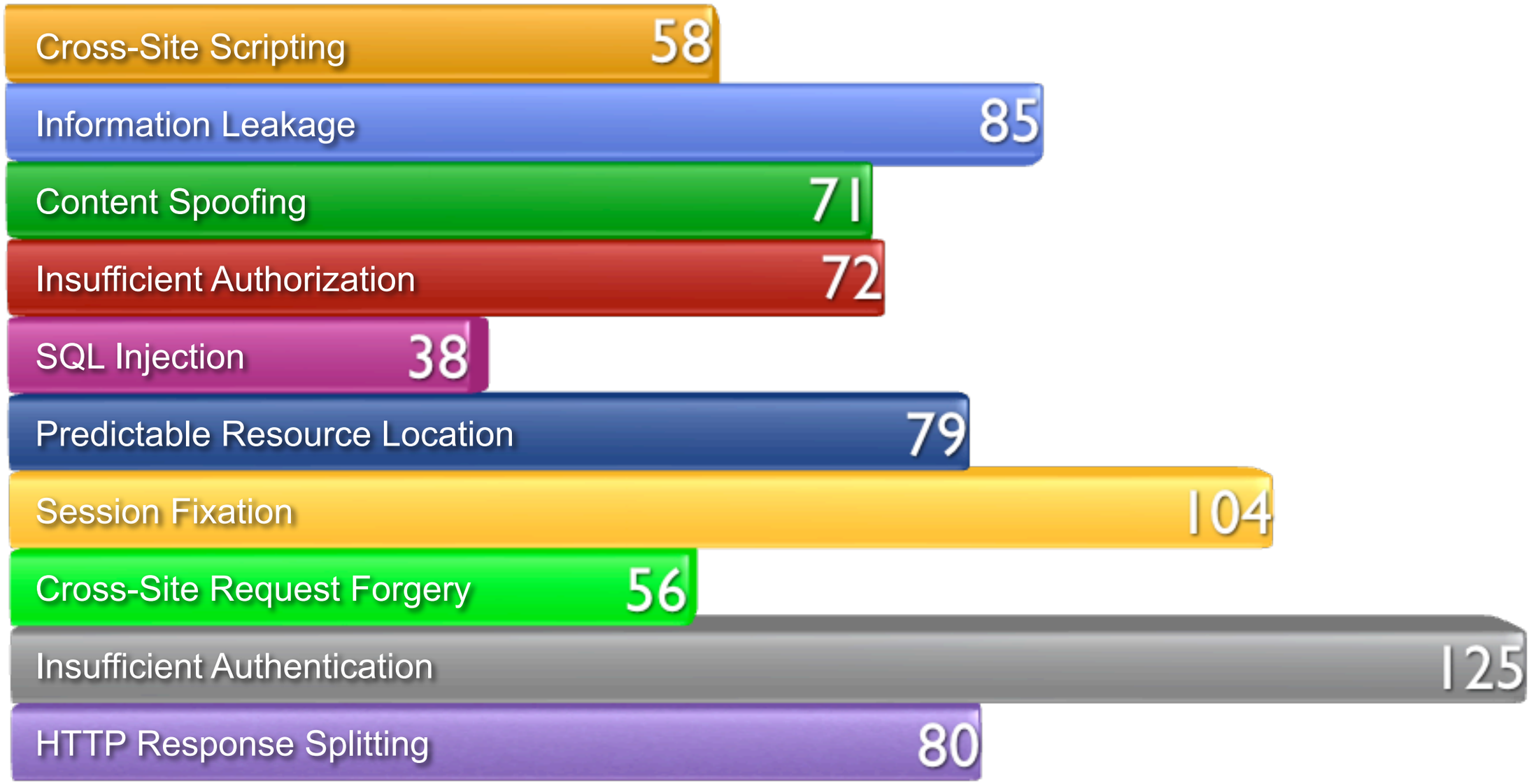
Percentage likelihood of a website having at least one HIGH, CRITICAL, or URGENT issue by industry vertical

Top 5 vulnerabilities by industry vertical. Percentage likelihood of a website having at least one HIGH, CRITICAL, or URGENT issue by class





Time-to-Fix (Days) - WhiteHat Top Ten

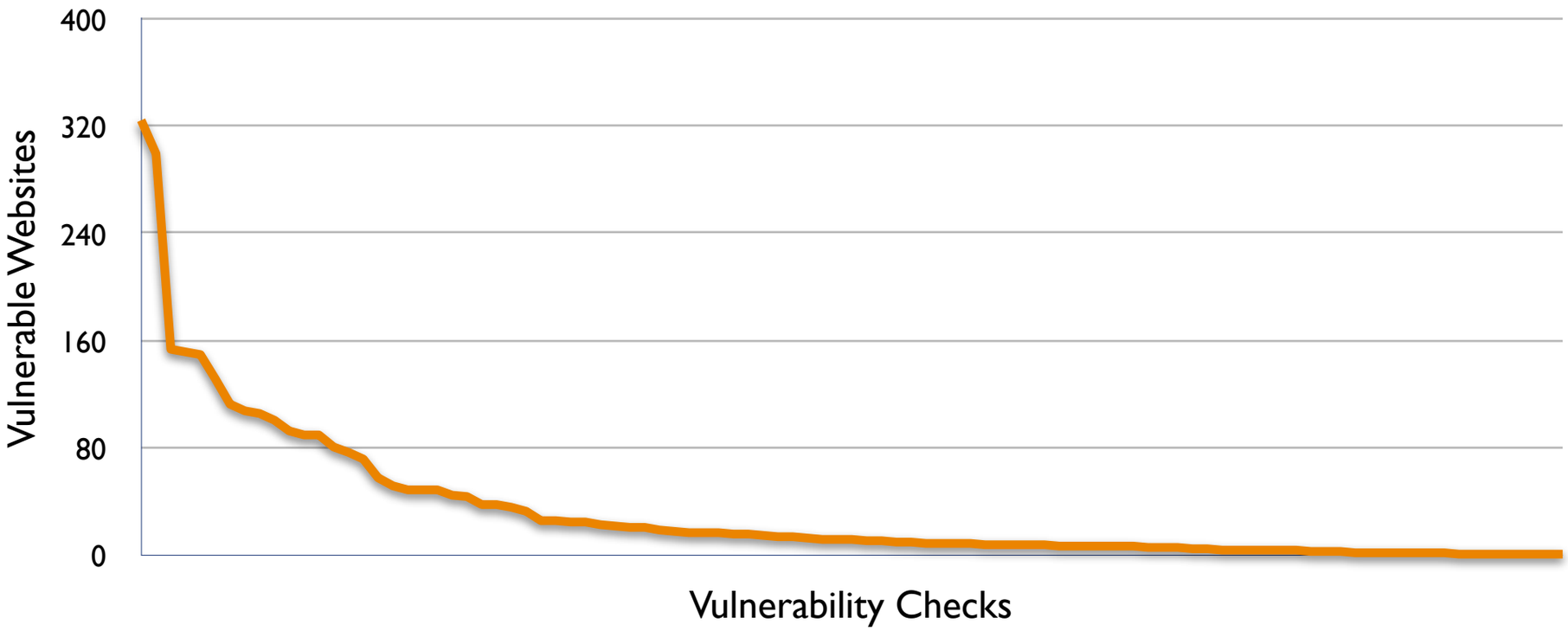


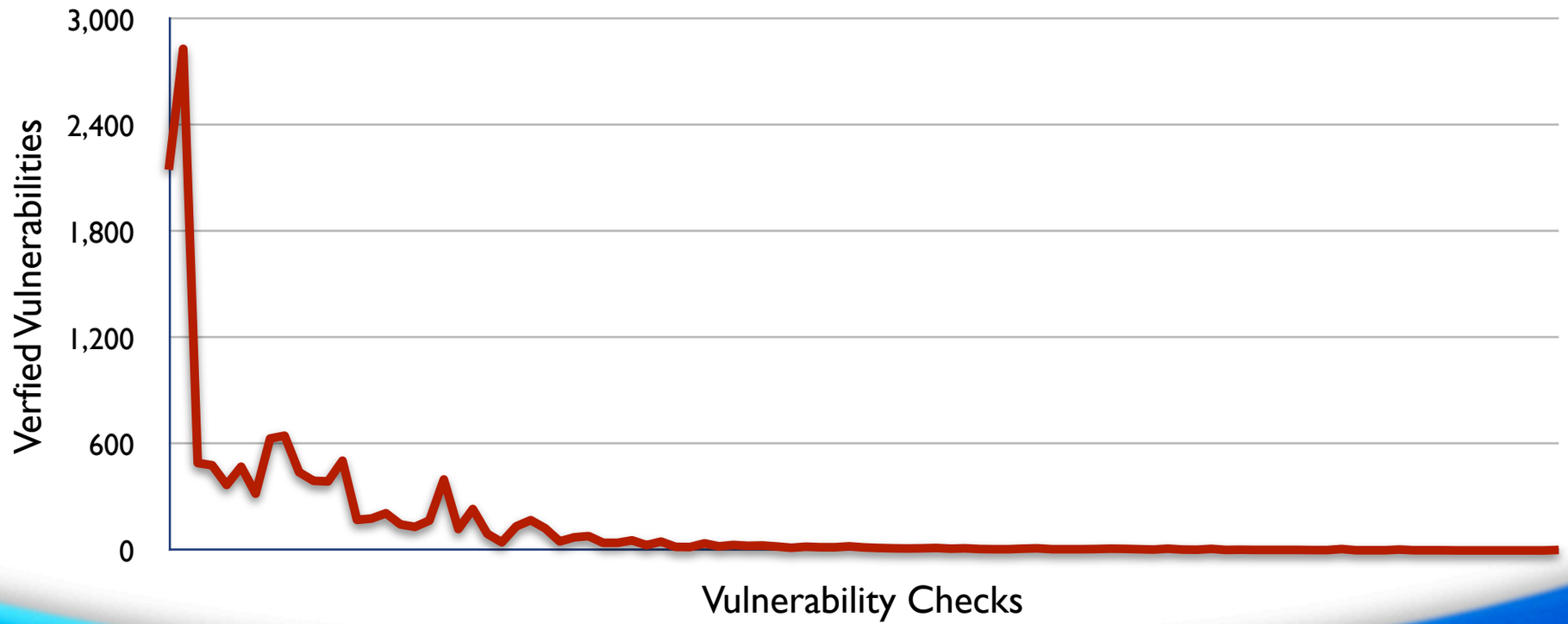
Best-case scenario: Not all vulnerabilities have been fixed...

Resolution rate - Top 5 by Severity

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

The Long Tail of Website Vulnerability Testing





Thank You!

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

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