Website Vulnerabilities Revealed

Jeremiah Grossman
WhiteHat Security founder & CTO

Jeremiah Grossman

WhiteHat Security Founder & CTO

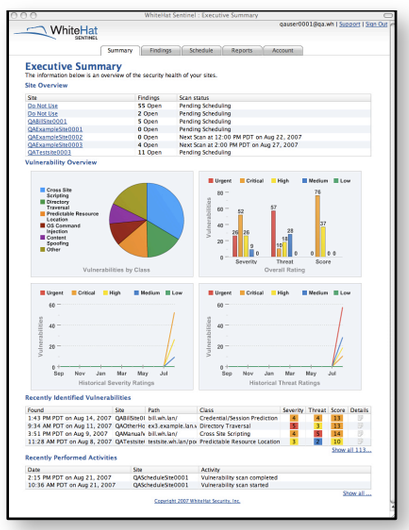
Technology R&D and industry evangelist
(InfoWorld's CTO Top 25 for 2007)

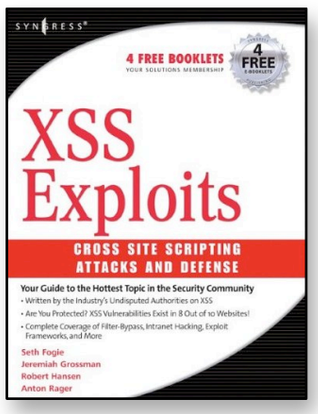
Frequent international conference speaker

Co-founder of the Web Application Security Consortium

Co-author: *Cross-Site Scripting Attacks*

Former Yahoo! information security officer

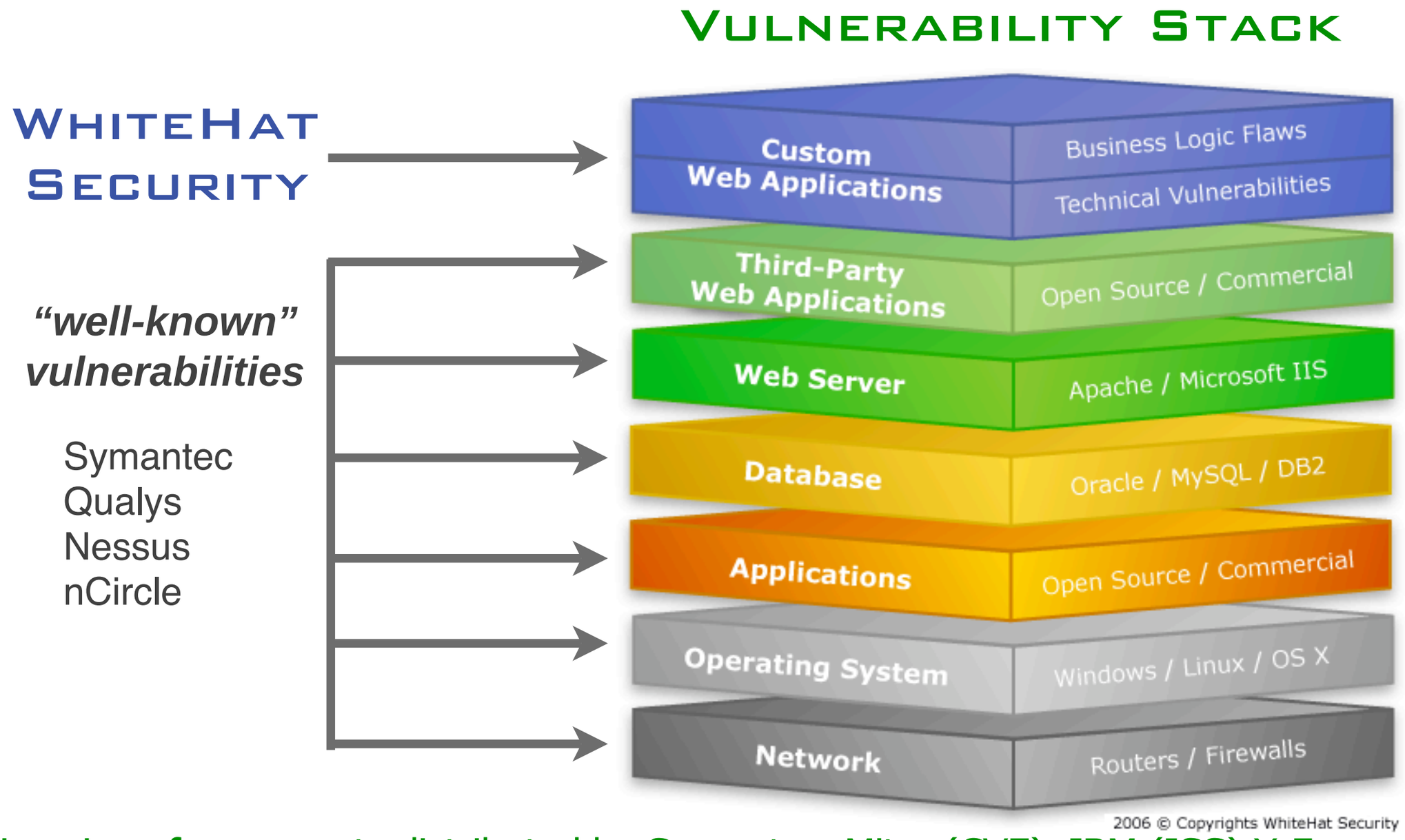




YAHOO!

WhiteHat SECURITY

Custom Web Applications, Custom Vulnerabilities



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

WhiteHat SECURITY

Global Scale

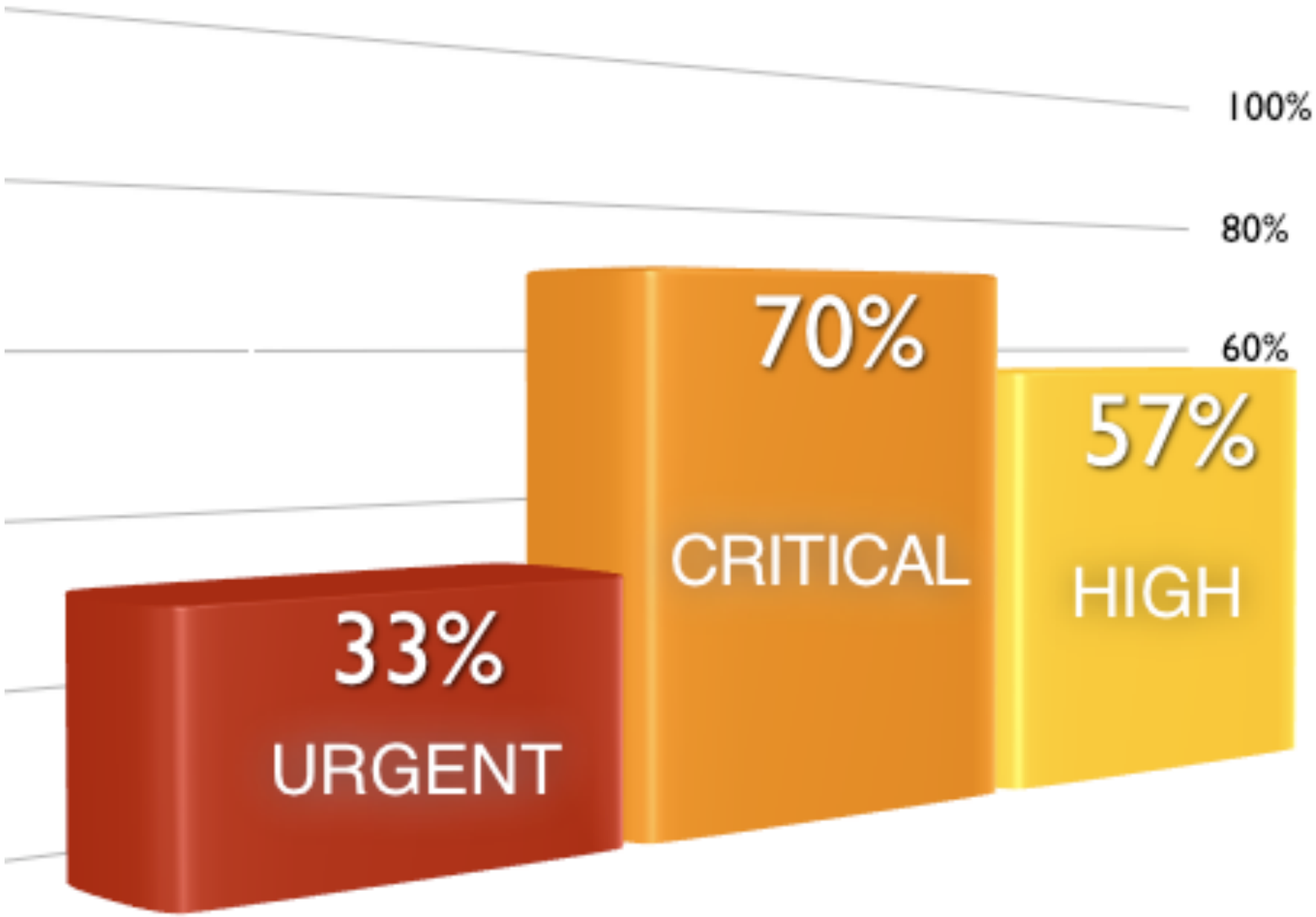
9 out of 10 Websites have serious Vulnerabilities

- 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

WhiteHat SECURITY

But how bad is it really?

Likelihood that a website has a vulnerability, by severity

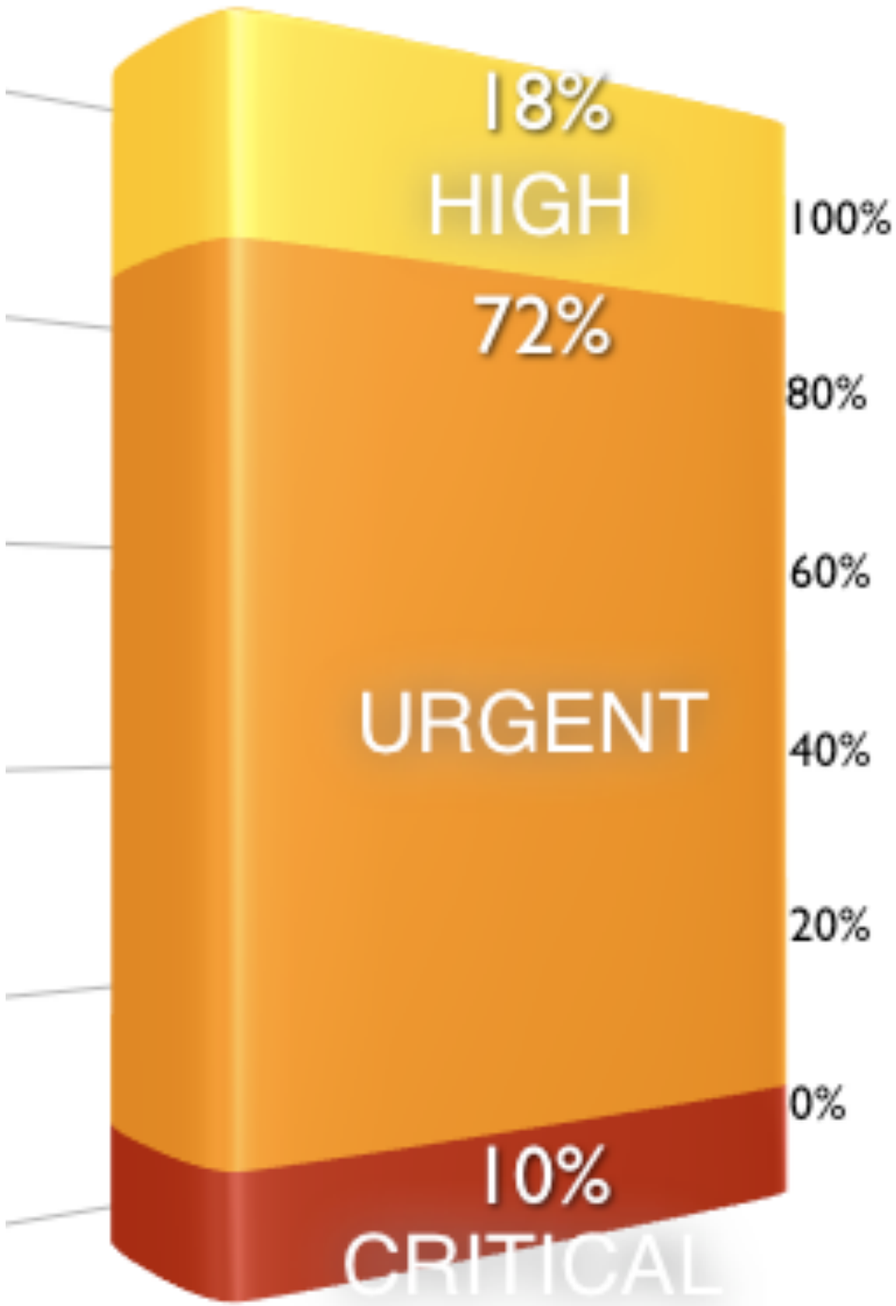


Websites with Urgent, Critical, or High severity issues technically would not pass PCI compliance

WhiteHat SECURITY

Another way to look at the badness

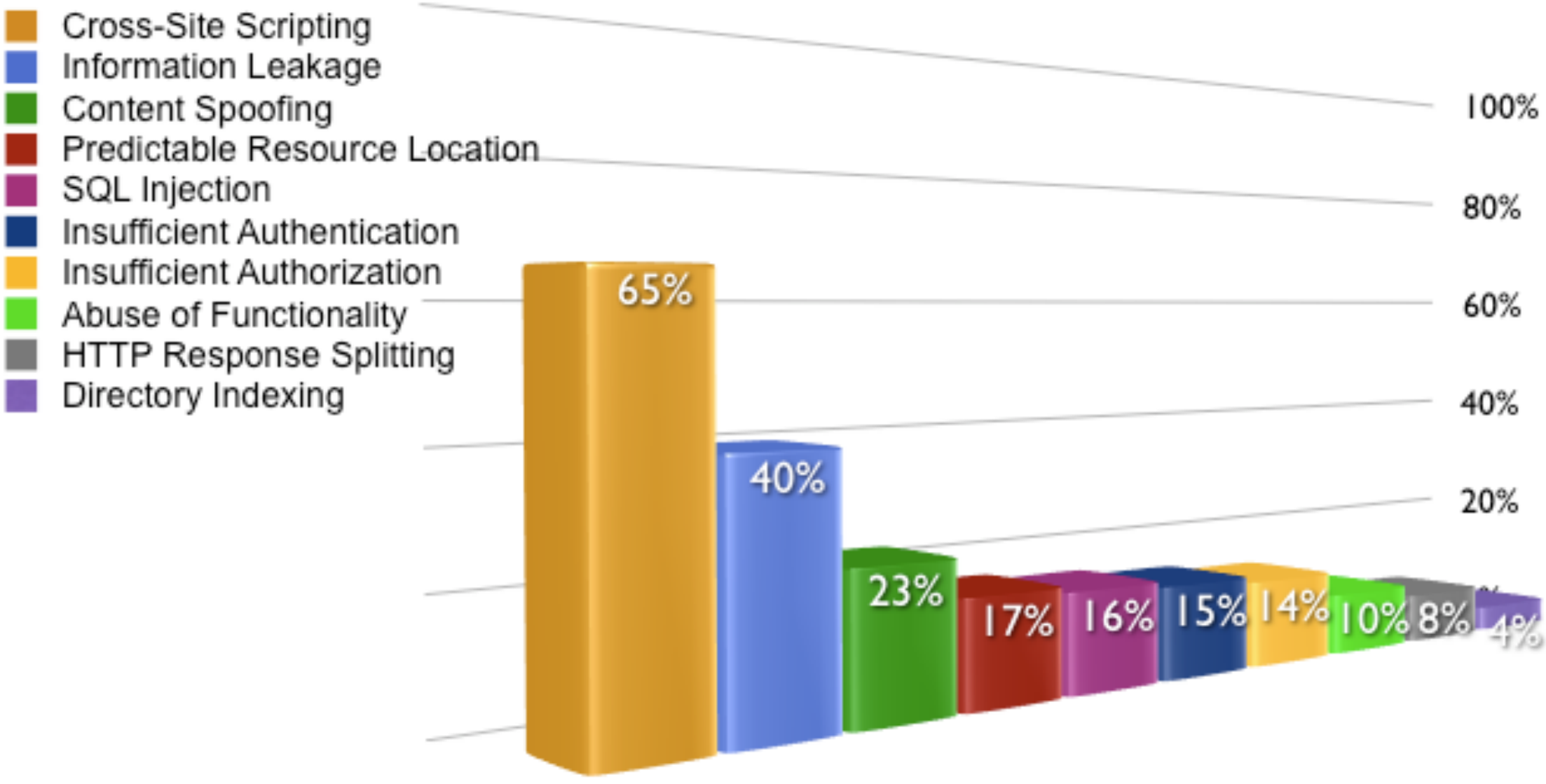
Percentage of vulnerabilities ranked by severity



WhiteHat SECURITY

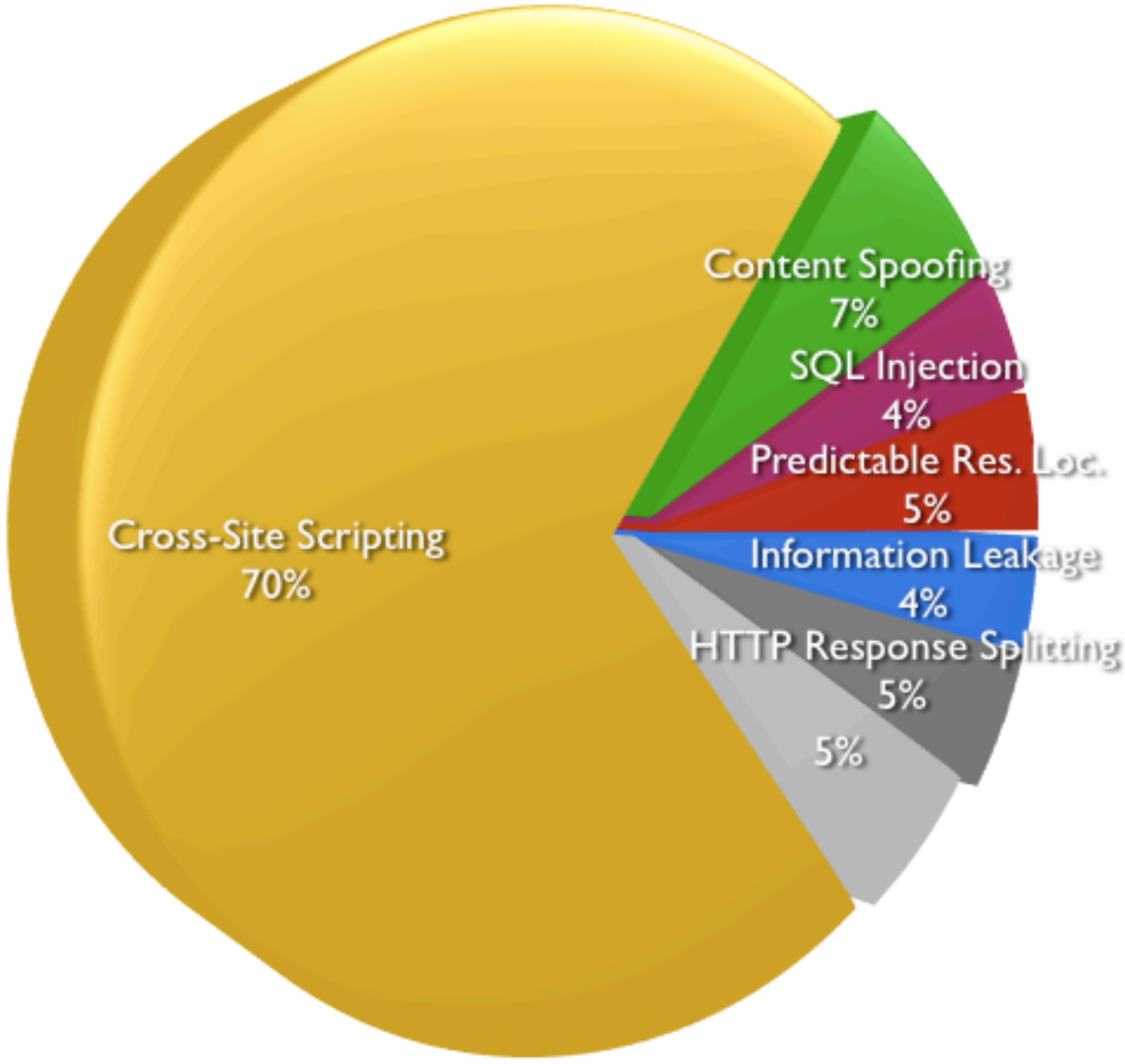
WhiteHat Security: Top 10

Likelihood that a website has a vulnerability, by Class



WhiteHat SECURITY

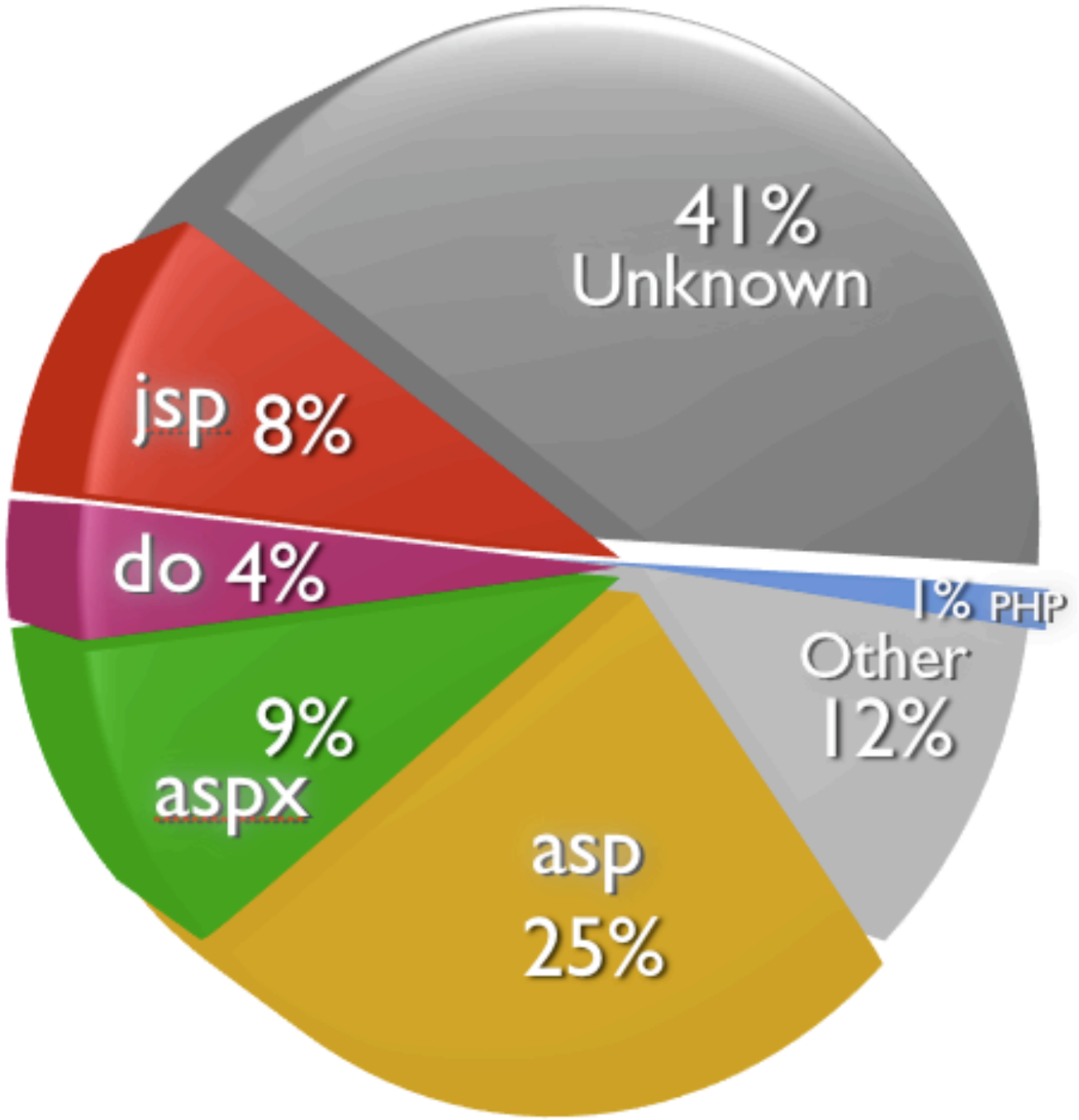
Overall vulnerability population



WhiteHat SECURITY

Technology Breakdown

FILE EXTENSIONS



WhiteHat SECURITY

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

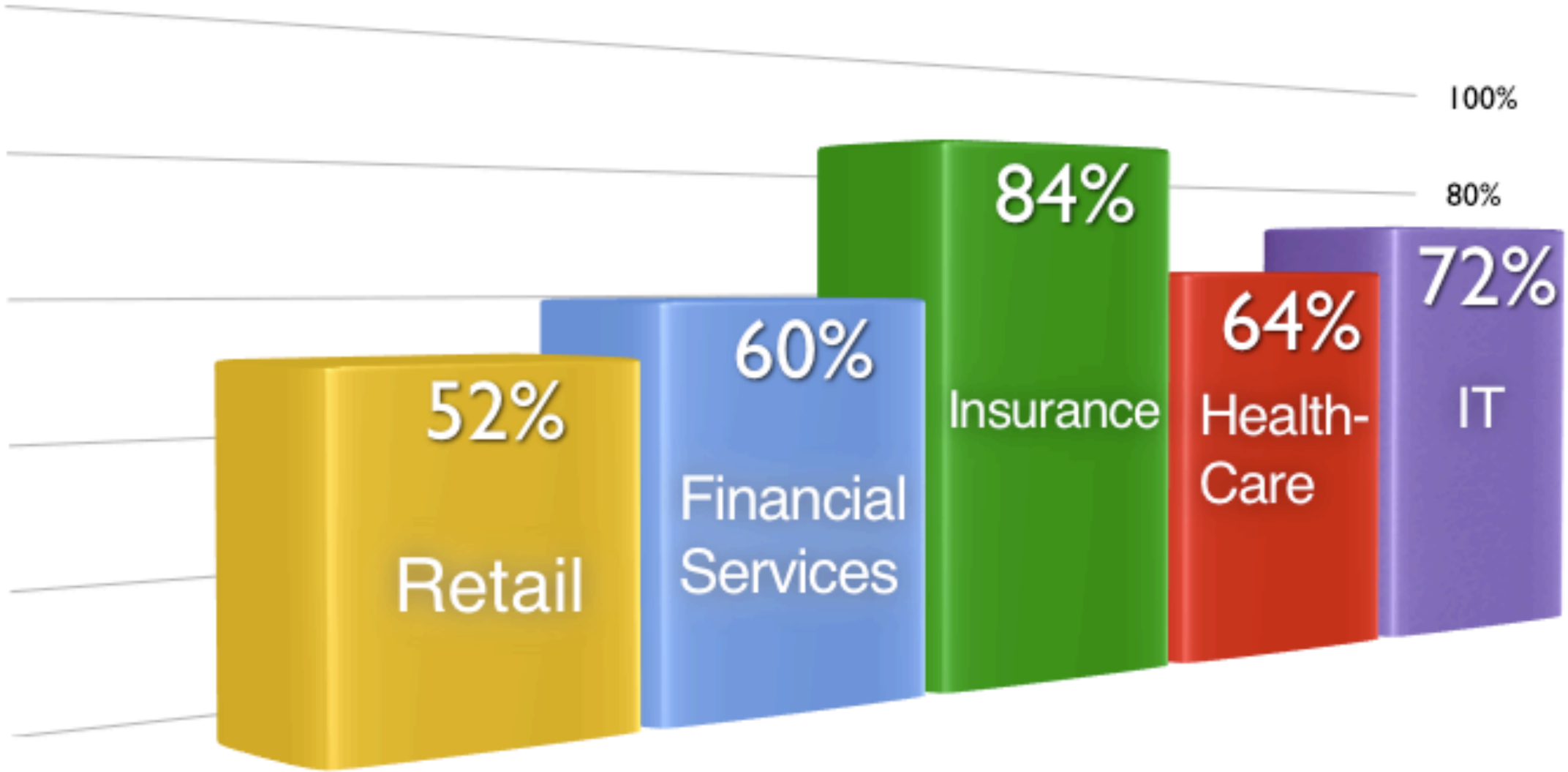
Cross-Site Request Forgery remains VERY DIFFICULT to scan for and we only report the most egregious cases identified by hand

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

HTTP Response Splitting pushed XPath Injection off the list

Industry Verticals

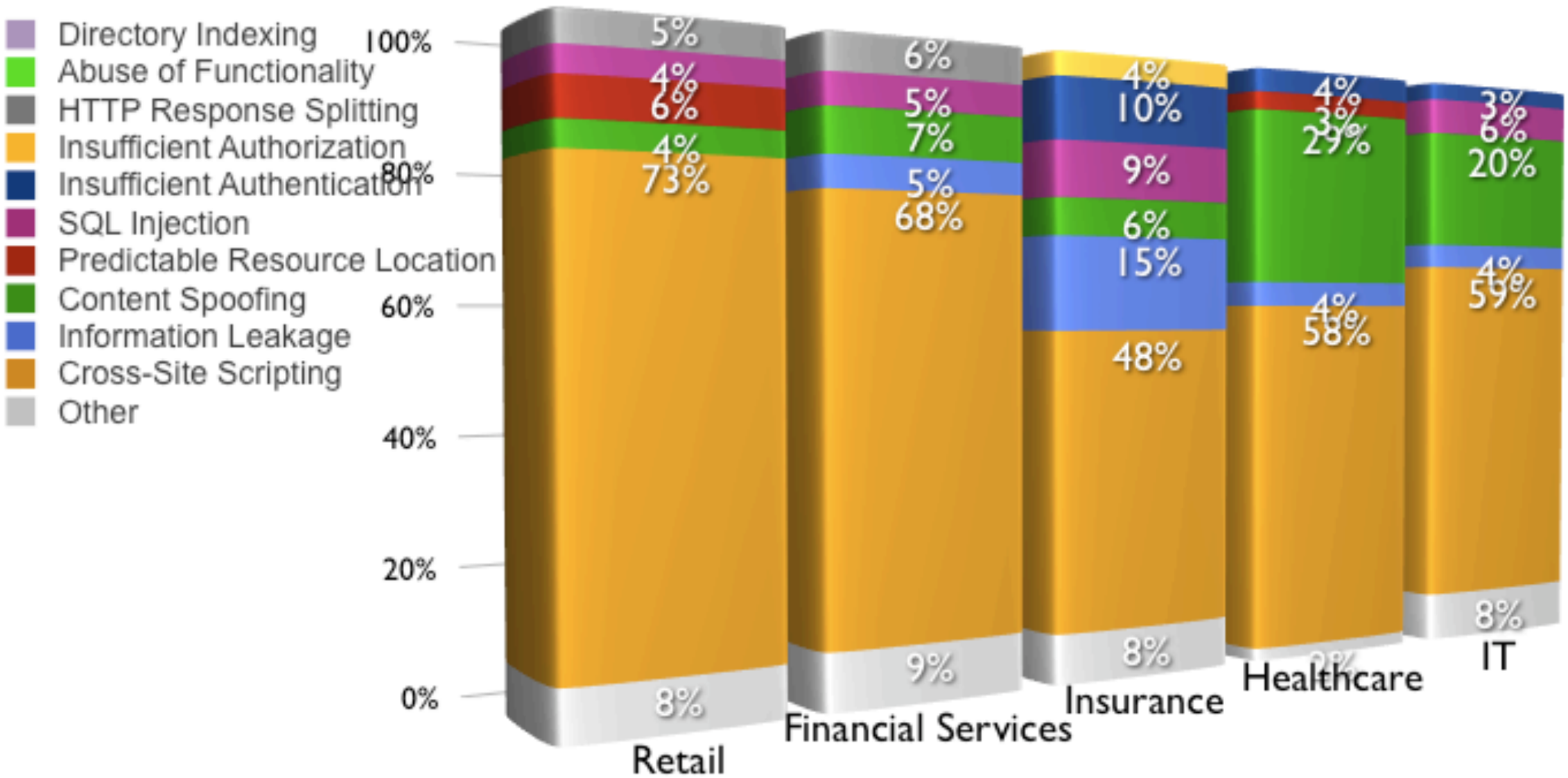
Percentage of websites with either URGENT, CIRTICAL or HIGH severity vulnerabilities ranked by industry



WhiteHat SECURITY

Worst of the Worst

Percentage of vulnerability classes in overall population ranked by industry

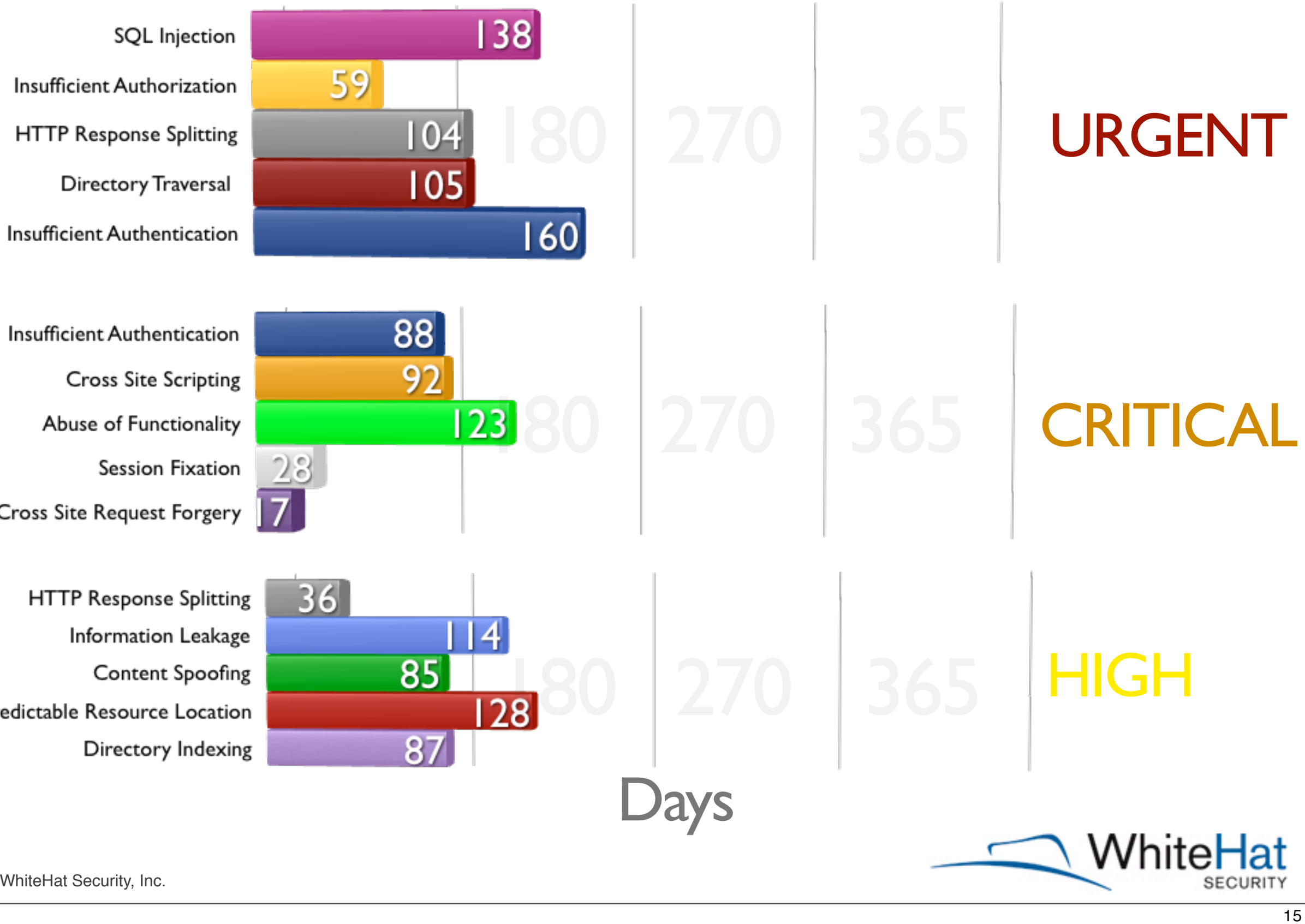


WhiteHat SECURITY

Data input correlation

Average inputs per website:154
Ratio of vulnerability/inputs: 2.2%

Time to Fix



WhiteHat SECURITY

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.

WhiteHat SECURITY

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

WhiteHat SECURITY