WhiteHat Website Security Statistic Report

Winter 2011, 11th Edition – Measuring Website Security: Windows of Exposure

11th edition

Spend enough time in the realm of website security and inevitably you learn two very important lessons:

> ***Lesson 1 – Software will always have bugs and by extension, security vulnerabilities. Therefore, a practical goal for a secure software development lifecycle (SDLC) should be to reduce, not necessarily eliminate, the number of vulnerabilities introduced and the severity of those that remain[1].***
>
> ***Lesson 2 – Exploitation of just one website vulnerability is enough to significantly disrupt online business, cause data loss, shake customer confidence, and more. Therefore, the earlier vulnerabilities are identified and the faster they are remediated the shorter the window of opportunity for an attacker to maliciously exploit them.***

Collectively this tells us that the security posture of a website should not only be measured by the number of vulnerabilities, but also must consider remediation rates and time-to-fix metrics. Experience in website security also teaches:

Vulnerabilities do not exploit themselves. Someone or something, an attacker (or "threat"), uses an attack vector to exploit a vulnerability in a website, bypass a control, and cause a technical or business impact. Some attackers are sentient, and others are autonomous. Different attackers have different capabilities and goals in mind. Consequently, to protect websites against a particular threat, security professionals must understand its methods and have the proper security controls in place.

Some organizations are targets of opportunity, others targets of choice. Targets of opportunity are victimized when their security posture is weaker than the average organization and the data they possess can be converted easily into liquid currency. Targets of opportunity possess some form of unique and valuable information that is particularly attractive to an attacker. Organizations are well-advised to determine if they likely represent a target of opportunity, of choice, or both, because it will them help establish a "secure enough" bar.

If an organization is a target of opportunity, the goal of being at or above average regarding website vulnerability numbers among your peers is reasonable. If a target of choice, then the adversary is one who will spend whatever time is necessary looking for gaps in the defenses to exploit. In this case, an organization must elevate its website security posture to a point where an attacker's efforts are detectable, preventable, and in case of compromise, survivable.

These lessons make it clear that an effective website risk management program involves critical thought and planning that extends beyond arbitrarily trying to identify and fix vulnerabilities on an ad hoc basis. Website security is about understanding the threat, appropriately mapping the threat to the business assets and tolerance for risk, limiting the Window of Exposure, and improving organizational responsiveness. Achieving this level of website security readiness and the ability to justify the resource investment requires data. Data about your organization, its progress, and the relative security posture compared to similar companies.

"When you can measure what you are speaking about, and express it in numbers, you know something about it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts advanced to the stage of science."
- Lord Kelvin

The WhiteHat Website Security Statistics Report provides a one-of-a-kind perspective on the state of website security and the issues that organizations must address to safely conduct business online. WhiteHat has been publishing the report, which highlights the top vulnerabilities, tracks vertical market trends and identifies new attack techniques, since 2006.

The WhiteHat Security report presents a statistical picture of current website vulnerabilities among the more than 3,000 websites under management, accompanied by WhiteHat expert analysis and recommendations. WhiteHat's report is the only one in the industry to focus solely on previously unknown vulnerabilities in custom Web applications, code unique to an organization, within real-world websites.

In previous reports WhiteHat Security has published statistics on which classes of vulnerabilities are the most prevalent, measured their remediation rates, analyzed time-to-fix, investigated the impact of programming languages, and sorted our numbers by industry and organization size. While this information was incredibly revealing and valuable, this report will go one step further back into the SDLC to better understand how many and how often vulnerabilities are introduced. For some organizations, the problem area may simply be the volume of vulnerabilities introduced. For other organizations, the primary challenge is obtaining the resources to fix the vulnerabilities that are identified. For others, the greatest need is to accelerate the vulnerability resolution process. Each of these issues directly impacts an organization's Window of Exposure.

This, WhiteHat Security's 11th Website Security Statistics Report, presents a statistical picture gleaned from over five years of vulnerability assessment results taken from over 3,000 websites across 400 organizations under WhiteHat Sentinel management. This represents the largest, most complete, and unique dataset of its kind. WhiteHat Security makes this report available specifically for organizations that aim to start or significantly improve their website security programs, prevent breaches, and data loss.

Key Findings

Most websites were exposed to at least one serious* vulnerability every day of 2010, or nearly so (9–12 months of the year). Only 16% of websites were vulnerable less than 30 days of the year overall.

71% of Education, 58% of Social Networking, and 51% of Retail websites were exposed to a serious* vulnerability every day of 2010.

51% of Banking, 22% of Financial Services, and 19% of Healthcare websites were exposed to a serious* vulnerability less than 30 days of 2010.

During 2010, the average website had 230 serious* vulnerabilities.

Banking, Healthcare, and Healthcare performed the best out of all the industries with an average of 30, 33, and 35 serious* vulnerabilities respectively per website during 2010.

Retail, Financial Services, and Telecommunications, whose websites had the most reported issues, averaged 404, 266, and 215 serious* vulnerabilities respectively per site.

In 2010, 64% of websites had at least one Information Leakage vulnerability, which overtook Cross-Site Scripting as the most prevalent vulnerability by a few tenths of a percent.

Cross-Site Request Forgery (CSRF) continues to climb to 24% of websites, but not because they're becoming more vulnerable, instead a steady improvement of Sentinel combined with customer demand to report these issues.

SQL Injection vulnerabilities, despite large numbers of them being found and fixed during 2010, still occurred in 14% of websites.

On the average, 50% of organizations require 116 days or less to remediate their serious* vulnerabilities. The Banking industry is the fastest with 50% of the issues resolved in 13 days. The slowest is Telecommunications with 50% of serious vulnerabilities resolved in 205 days.

There has been a roughly 5% improvement in the percentage of reported vulnerabilities that have been resolved (Remediation Rate) during each of the last three years (2008, 2009, 2010), which is currently 53%.

** Serious Vulnerabilities: Those vulnerabilities with a HIGH, CRITICAL, or URGENT severity as defined by PCI-DSS naming conventions. Exploitation could lead to breach or data loss.*

Web security is a moving target and enterprises need timely information about the latest attack trends, how they can best defend their websites, and gain visibility into their vulnerability lifecycle. Through its Software-as-a-Service (SaaS) offering, WhiteHat Sentinel, WhiteHat Security is uniquely positioned to deliver the knowledge and solutions that organizations need to protect their brands, attain PCI compliance and avert costly breaches.

The WhiteHat Website Security Statistics Report provides a one-of-a-kind perspective on the state of website security and the issues that organizations must address to safely conduct business online. WhiteHat has been publishing the report, which highlights the top vulnerabilities, tracks vertical market trends and identifies new attack techniques, since 2006.

The WhiteHat Security report presents a statistical picture of current website vulnerabilities among the more than 3,000 websites under management, accompanied by WhiteHat expert analysis and recommendations. WhiteHat's report is the only one in the industry to focus solely on unknown vulnerabilities in custom Web applications, code unique to an organization, within real-world websites.

Industry	Number of Vulnerabilities	Std. Dev	Remediation Rate	Std. Dev	Window of Exposure (Days)
Overall	230	1652	53%	40%	233
Banking	30	54	71%	41%	74
Education	80	144	40%	36%	164
Financial Services	266	1935	41%	40%	184
Healthcare	33	87	48%	40%	133
Insurance	80	204	46%	37%	236
IT	111	313	50%	40%	221
Manufacturing	35	111	47%	40%	123
Retail	404	2275	66%	36%	328
Social Networking	71	116	47%	34%	159
Telecommunications	215	437	63%	40%	260

Figure 1. 2010 at a Glance – Sorted by Industry
The average number of serious vulnerabilities per website, the percentage of reported vulnerabilities that have been resolved (Remediation Rate), and average the number of days a website is exposed to at least one serious vulnerability (Window of Exposure).*

Key Performance Indicator (KPI): Window of Exposure

Window of Exposure is an organizational KPI that measures the number of days a website has at least one serious vulnerability over a given period of time. For example, let's consider two identical websites, SiteA and SiteB. SiteA had 12 serious vulnerabilities identified during the last year and 200 of those days it had at least one of those issues publicly exposed. SiteB also had 12 serious vulnerabilities in the same time span, but only 20 days when they were open to exploitation. From this we can say that during the last year SiteB, despite having exactly the same number of vulnerabilities, had a substantially better security posture than SiteA as measured by the Window of Exposure.

Window of Exposure is an insightful way to measure an organization's current and historical website security posture. Websites are an ongoing business concern and security must be assured all the time, not just at a point in time. Window of Exposure is a useful combination of the vulnerability prevalence, the time it takes to fix vulnerabilities, and the percentage of them that are remediated. Any one of these metrics, or a combination thereof, may be the area that has the greatest impact on a given organization's Window of Exposure outcome. The question is, where exactly should resources be invested.

It is revealing to see how various industries perform in the area of Window of Exposure. Figure 2 (on the following page) demonstrates 2010 performance.

By examining the data it becomes soberingly clear just how large the Window of Exposure is across nearly all industries, even after the organization is well-aware of the risks. Most websites were exposed to at least one serious vulnerability every day of 2010 as highlighted in red, or nearly so (9–12 months of the year) as represented in orange. Except for the Banking sector, no industry performed well. 71% of education, 58% of social networking, and 51% of retail websites were vulnerable to a significant issue every day of the year. Not a single Telecommunications website was found free of serious vulnerabilities fewer than 30 days of the year.

Fortunately it's not all bad news. There were a noticeable percentage of websites in green that performed very well. 51% of Banking, 22% of Financial Services, and 19% of Healthcare websites were vulnerable less than 30 days of 2010. 16% of websites across all industries had a Window of Exposure of less than 30 days of the year overall. This shows us that while vulnerabilities can and will happen to essentially everyone, progress, even exceptional performance and significantly reduced risk, is clearly possible when an organization focuses on it. From our experience the difference comes down to how an organization allocates its resources.

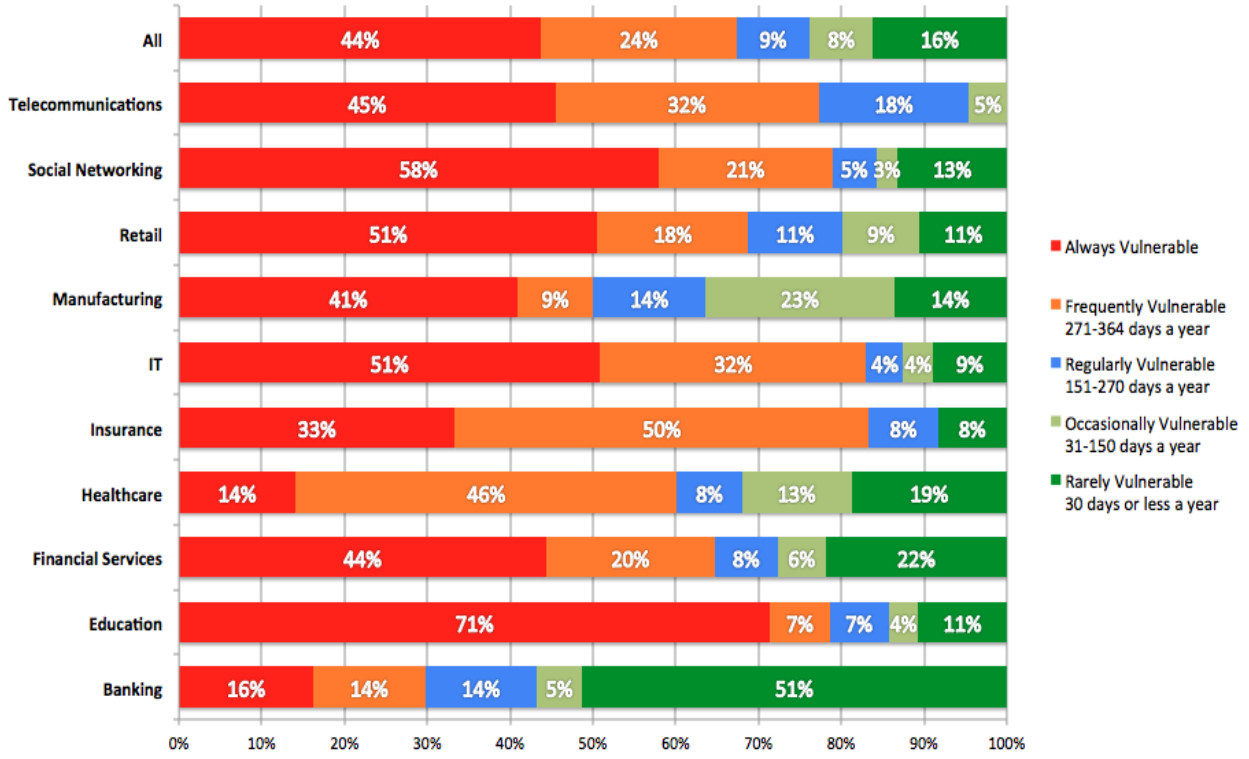

Figure 2. Window of Exposure by Industry (2010)

For example, if a development team is consistently introducing large volumes of new vulnerabilities, it would be advisable to start by focusing on reducing the number of issues first (stop the bleeding). This may be achieved through an executive level mandate, better security controls in the development framework, awareness training, and security testing during QA.

On the other hand if the development team is generating comparably few vulnerabilities, but the issues remain remotely exploitable for long periods of time, then the greatest emphasis should be on improving the remediation processes. As a matter of policy, organizations may consider implementing remediation time mandates according to vulnerability severity. Window of Exposure data is a critical factor in making these strategic decisions.

Vulnerability Prevalence

When approaching information security, it is important not to lose sight of the distinction between what is possible and what is probable. In website security, it is true that a single vulnerability represents a means for an attacker to exploit a system, but not all (vulnerabilities or attackers) are created equal. For example, SQL Injection tends to be exploited far more often than other vulnerability classes that are more common. We also know that attacks are getting more targeted and consequently having numerous serious (Urgent, Critical, or High severity) issues, whatever they be, makes it that much easier for an attacker to achieve a successful compromise. Therefore, it is best to minimize vulnerabilities to the maximum extent possible to increase software security assurance.

During 2010, the average website had 230 serious vulnerabilities reported (see Figure 3 on the following page). For those familiar with our previous research, this number may seem like a dramatic increase, but websites have not suddenly become much more vulnerable. Rather, WhiteHat responded to community feedback and revised our tracking to increase clarity of the results. Vulnerabilities are now counted by unique Web application and class of attack. If three of the five parameters of a single Web application (/foo/webapp.cgi) are vulnerable to SQL Injection, this is counted as 3 vulnerabilities (e.g. attack vectors) and not 1 as they were before. Secondly, if a single parameter can be exploited in more than one way, each of those are counted as well. This is done because a vulnerability in each parameter may actually lead to a different problem in a different part of the code.

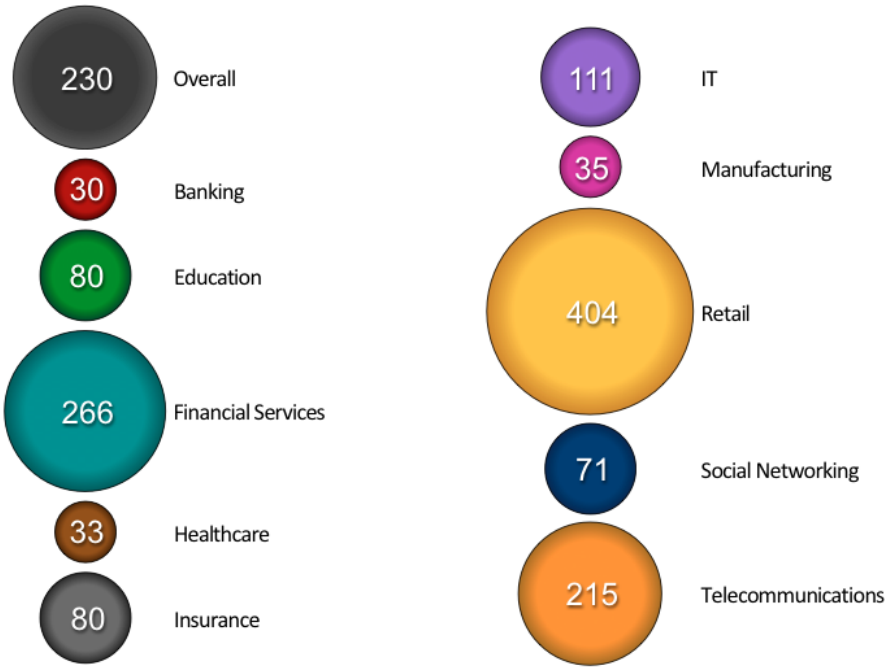

Figure 3. Average Number of Serious Vulnerabilities during 2010 – Sorted by Industry

Initially, the number of issues is quite stunning, until the number of variables is taken into account. Consider all the discrete Web applications that make up a website, the many input parameters, the many ways each parameter may be exploited by several dozen classes of attack, multiply that over a year with frequent code updates and the breadth of the problem becomes clear. Then the number does not appear unreasonable. For many security professionals, the overall number is not that important, but rather how one company compares to others in its industry vertical.

While no industry approached anywhere near zero for an annual average, Banking, Healthcare, and Manufacturing performed the best out of all the industries with 30, 33, and 35 serious vulnerabilities respectively per website during 2010 for a rough average of 2.5 or so vulnerabilities per month. On the opposite end of the spectrum, Retail, Financial Services, and Telecommunications, whose websites had the most reported issues measured 404, 266, and 215 serious vulnerabilities per site – or between 18 and 34 per month.

It is difficult to know why certain industries perform better than others. Factors may include the types of data stored, financial data is certainly appealing to cyber criminals; and the industry regulation placed upon them to protect it. One could reason that the "more secure" websites would typically have large volumes of payment card data, identity information, and access to financial transactions. This then requires them to have a more advanced website security program in place.

That logic explains the relatively low numbers in Banking and Healthcare, but not necessarily why Manufacturing did well. It could be the typical Manufacturing website has less functionality than most Social Networking websites, which average twice the number of vulnerabilities, as well as Banking and Healthcare. It also doesn't explain why Financial Services and Retail performed more poorly than the overall average. It could be that these industries' websites have more application functionality (attack surface) whose code changes more often, which naturally contributes to an increased number of vulnerabilities.

We could compensate for this "unfairness" by adjusting for relative attack surface, but this is not how the bad guys operate. As Lesson #2 above states, the bad guys only need one exploit to win and they aren't at all concerned about the operational considerations of the business. If this is how many vulnerabilities an average website has, so be it.

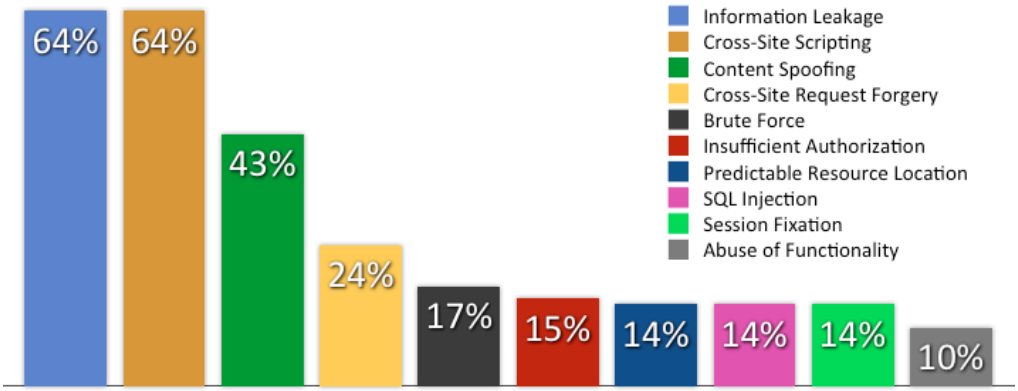

Figure 4. Overall Top Ten Vulnerability Classes of 2010
(Percentage likelihood that at least one vulnerability will appear in a website)

WhiteHat Security Top Ten (2010)

Now that we have some insight into the average total number of serious* vulnerabilities across industry verticals, next look at the distribution across the classes. In Figure 4 the most prevalent classes of vulnerabilities are calculated based upon their percentage likelihood of being found within any given website. This approach minimizes data skewing in websites that are either highly secure or extremely risk-prone.

In 2010, 64% of websites had at least one Information Leakage vulnerability, which overtook the notorious Cross-Site Scripting as the most prevalent issue by a few tenths of a percent. This was a long time coming as increased awareness of Cross-Site Scripting has steadily reduced its numbers, below that of Information Leakage, which is a very positive sign.

Information Leakage is generally a catchall term that describes a vulnerability in which a website reveals sensitive data, such as technical details of the Web application, environment, or user-specific data. Sensitive data may be used by an attacker to exploit the system, its hosting network, or users. Common examples are a failure to scrub out HTML/Script comments containing sensitive information (database passwords), improper application or server configurations, or differences in page responses for valid versus invalid data.

As predicted, Cross-Site Request Forgery (CSRF) continues to climb the rankings at 24% of websites, not because websites are becoming more vulnerable to it. Instead, a steady improvement in WhiteHat Sentinel identification combined with customer demand to report them accounts for the rise. CSRF attacks involve forcing a victim's Web browser, typically while authenticated, to send an HTTP request to a target website without their knowledge to perform an unintended action as the victim. This action could be a bank wire transfer, email spam, add a friend, and so on. Practically speaking, just about every feature on every website has the potential of being vulnerable to CSRF unless very specific safeguards are put in place.

Only a few years back, CSRF was widely disregarded as not a "real vulnerability" and considered an artifact of "the way the Web was designed to work." Over time malicious hacker activity leveraging CSRF has forcibly changed this perception and more website owners are asking them to be reported so they may be fixed.

Brute Force, moving up to the fifth spot at 17% of websites, follows a similar path to CSRF. The bulk of these Brute Force vulnerabilities occur when a website login field reveals which entry of the username / password combination is incorrect. Due to spammers mining for valid email addresses (usernames) on a variety of websites, specifically social networks, enterprises have an increased awareness and appreciation for the issue. They have subsequently elevated the demand for testing and reporting of this particular type of "Brute Force" attack.

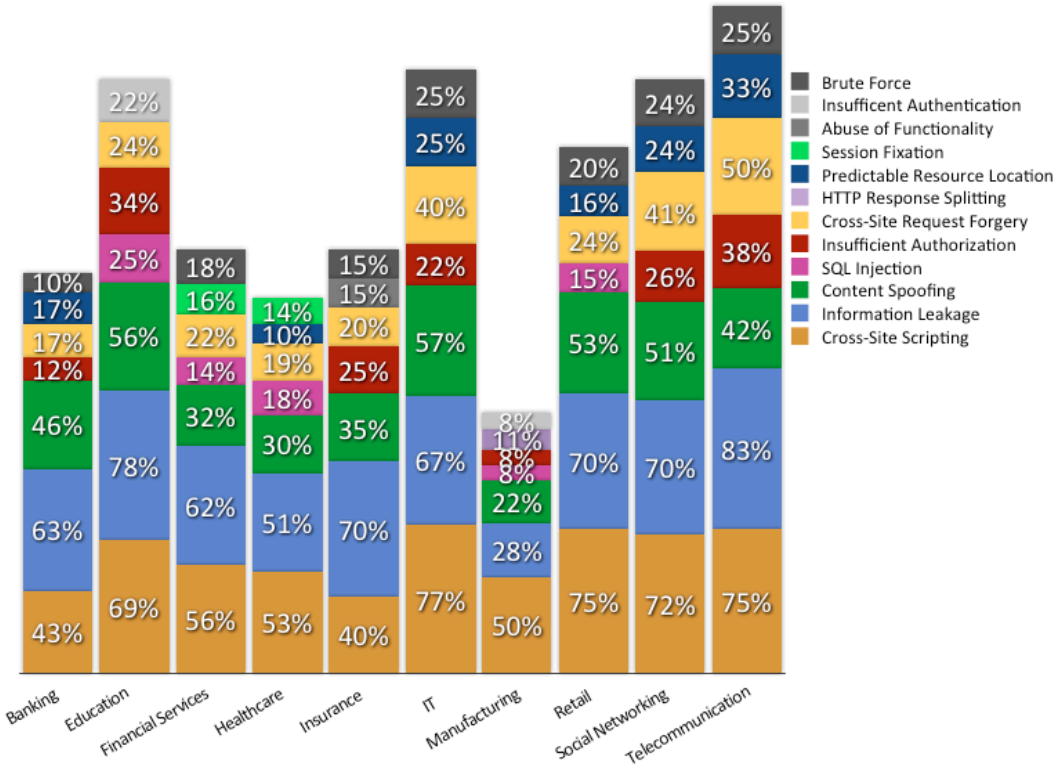

Figure 5. Top Seven Vulnerability Classes of 2010 – Separated by Industry
(Percentage likelihood that at least one vulnerability will appear in a website)

Another interesting way to view the vulnerability classes is sorting by industry (Figure 5). At first glance it seems that every industry suffers from the same sorts of issues. The difference is in degree, rather than kind, but upon close inspection there are some notable exceptions. Chief among them is that Banking, Insurance, IT, Social Networking, and Telecommunications websites do not have SQL Injection listed in their top seven vulnerabilities and there a few possible explanations for this.

The Industry could have made overall progress in significantly reducing SQL Injection, clearly the case in Banking since it is below 10%. Another explanation could simply be that SQL Injection is just as prevalent across industries as the overall average, but it just happens that several other vulnerability classes are more common. Whatever the case may be, it is again important to point out that while tracking prevalence is important, so too is keeping an eye on threat landscape and tracking which issues are most likely to be exploited. They are often not the same.

Time-to-Fix and Remediation Rates

Once website vulnerabilities are identified, verified, and reported to customers by WhiteHat Sentinel, a certain amount of time transpires before the issue is resolved and confirmed as such. As no remedy can be instantaneous, it is important to measure the amount of time, or time-to-fix, required to resolve certain issues. Resolution could take the form of a software update, configuration change, Web application firewall rule, etc. Open vulnerabilities represent a window of opportunity for malicious hackers to exploit the website.

Custom Web application vulnerabilities cannot generally be resolved by deploying a patch from a third-party vendor. The IT security team must work with the organization's internal development team to update the code. As a result a negotiation must take place, a resource tradeoff. The organization must decide to either allocate resources to producing a revenue-generating feature or use those resources to remediate an issue that may or may not be exploited. This is not always an easy or clear-cut risk management decision as reflected in the data below (Figure 6 & 7), data that illuminates striking differences when organized by industry.

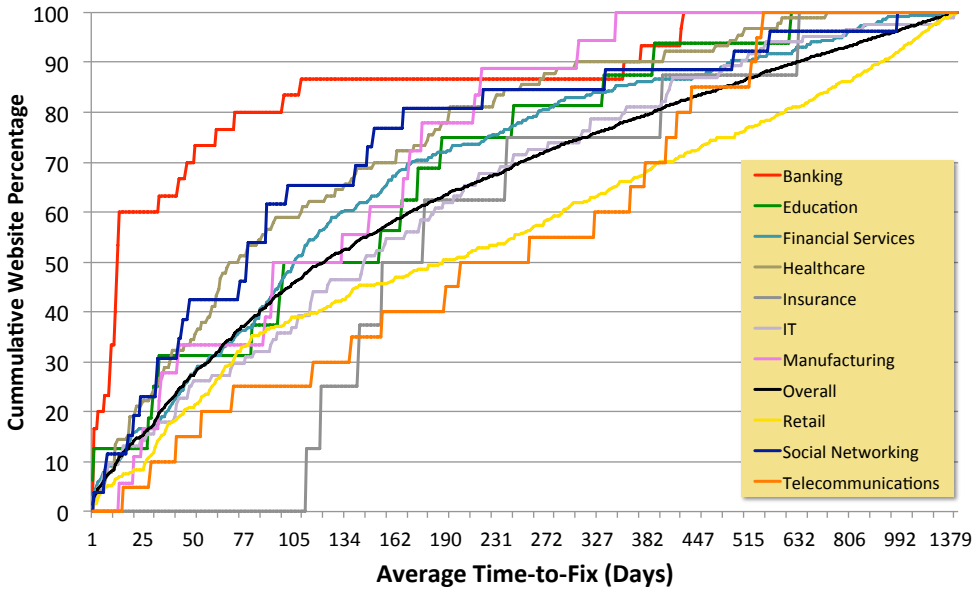

Figure 6. Aggregate Average Time-to-Fix (Days) – Sorted by Industry

Factors influencing the data:

Should a vulnerability be resolved, it could take up to seven days before it is retested and confirmed closed by WhiteHat Security's Threat Research Center, depending upon the customer's preferred assessment schedule. A customer can also proactively use the auto-retest function to get real-time confirmation of a fix.

Not all vulnerabilities identified within this period have been resolved, which means the time-to-fix measurements are likely to grow as resolution rates increase.

By arranging the time-to-fix data in a cumulative format we get a sense of the time required to remediate vulnerabilities in a given percentage of an industry's websites. From Figure 6 we can see that number is 116 days. For example, on average 50% of organizations require 116 days or less to remediate their serious* vulnerabilities. The Banking industry is the fastest, remediating 50% of serious issues in under 13 days. The slowest is Telecommunications, which significantly underperforms the overall average, taking 205 days to remediate serious* vulnerabilities on 50% of the websites.

This data helps answer a common question, "How fast should our organization be fixing our vulnerabilities?" From a risk management perspective, if the organization is a target of opportunity, perhaps a goal of being at or above average is good enough. If however the organization is a target of choice, either ASAP or being among the fastest is more appropriate

Even if serious* vulnerabilities are identified, verified, and explained it does not necessarily mean they are fixed, quickly or at all. As such it is important to analyze the resolution rates of organizations that do get their vulnerabilities fixed, or not, and in what volumes (Figure 7). Some organizations target the easier issues first to demonstrate their progress in vulnerability reduction. Others prioritize the high severity issues to reduce overall risk. Most industries in 2010 fixed roughly half of their outstanding reported issues. What we can also clearly see is a positive historical trend line. A roughly 5% improvement in the percentage of reported vulnerabilities that have been resolved during each of the last three years (2008, 2009, 2010), currently 53%.

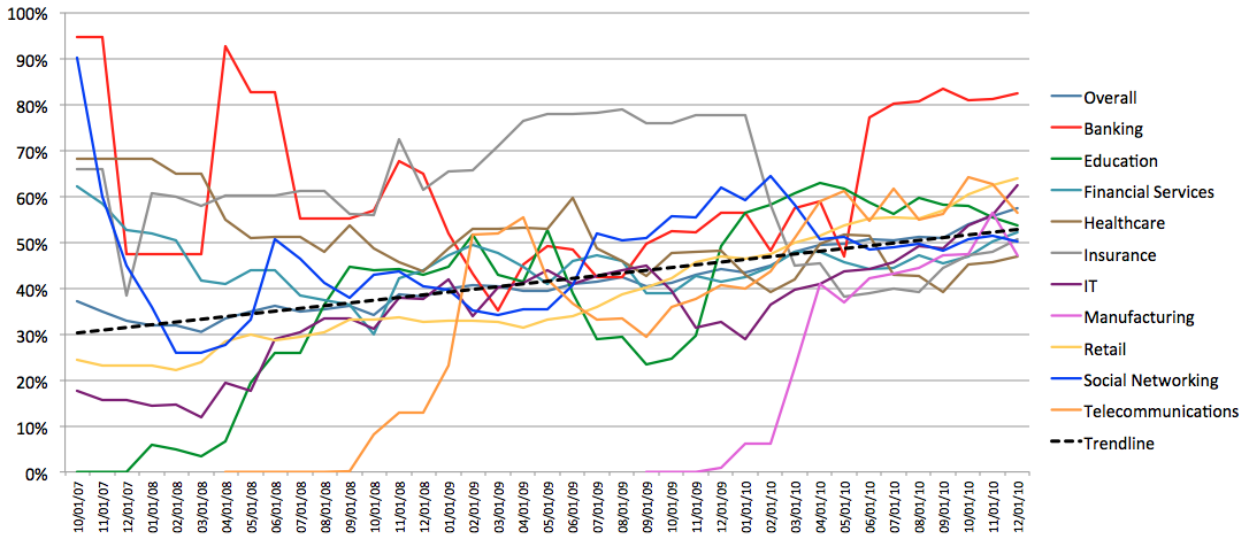

Figure 7. Historical trend of the percentage of reported vulnerabilities that have been resolved – Sorted by Industry

Factors inhibiting organizations from remediating vulnerabilities:

- *No one at the organization understands or is responsible for maintaining the code.*
- *No one at the organization knows about, understands, or respects the vulnerability.*
- *Feature enhancements are prioritized ahead of security fixes.*
- *Lack of budget to fix the issues.*
- *Affected code is owned by an unresponsive third-party vendor.*
- *Website will be decommissioned or replaced "soon." To note, we have experienced deprecated websites under the Sentinel Service still in active use for over two years.*
- *Risk of exploitation is accepted.*
- *Solution conflicts with business use case.*
- *Compliance does not require fixing the issue.*

Recommendations

- *For those organizations that wish to start or improve their website security programs, and prevent breach and data loss, following are recommendations from WhiteHat Security:*
- *Do the Basics*
- *Locate all websites you are responsible for, what they do, document the data they possess, who is responsible for them, and any other helpful metadata.*
- *Rank each website according to its value to the organization as some facilitate financial transactions, others generate advertising revenue, and more still contain distribute marketing materials.*
- *Next decide if each website, or the organization in general, is more likely to be a target of opportunity or choice as not all adversaries have the same technical capability, motivation, or end-goal. Some adversaries are sentient, others are fully automated, unauthenticated, and self-propagating, such as worms and viruses.*

From this point you should have a reasonable understanding of which assets are in need of protection and the security posture the business desires to attain. To get from point A to point B there needs to be a gap analysis, best measured through a website vulnerability assessment / penetration test. The testing methodology must meet or exceed the technical capabilities of the adversary the organization would like to repel.

Identifying vulnerabilities is one byproduct of the exercise. Any identified vulnerabilities may be "fixed" with an application code change, a virtual patch using a Web Application Firewall, system configuration update or other action. Or, an organization may need to decommission the website or roll back the code. The testing should also give the organization more visibility into what types of issues they have, where they are being introduced, how many, by what business unit at a strategic and a tactical level and how to improve.

Alignment of Interests

It is common for business stakeholders and development teams to resist the recommendations made by security teams. They'll fight for the status quo, or against anything that might increase their workload and does not directly lead to additional revenue or market-share. Unless security is seen as a business enabler. There are two ways that organizations have overcome these obstacles and brought the interests of all parties into alignment towards security.

The first is to select a small set of reasonable security metrics to begin tracking over time to measure where the organization can improve. WhiteHat Security recommends measuring Window of Exposure, but counting the number of serious* vulnerabilities or the percentage of developers who have passed security awareness training are also good suggestions. When enough data is gathered, organized by business unit, the results can be periodically published internally for the stakeholders to see. The groups who rise to the top will be proud to see their performance recognized and sets an example for coworkers to follow. Those who fall behind will feel a sense of per pressure to do the things necessary to keep pace keep up with their peers

The second tip is finding a way to justify making security investments by using "security" as a competitive advantage to increase sales rather than a cost of doing business for loss avoidance. For example instead of saying, "If we spend $X on Y, we'll reduce risk of loss of $A by B%," say "If we spend $X on Y, it will attract more customers, which has an estimated financial upside of $C." To get there security managers are encouraged to interact with the sales and marketing departments to understand how often "security" is seen as part of the customer's buying criteria. If often, this is an excellent opportunity to align security with business goal.

Addendum: Data Collection and Report Methodology

Data Overview

- *Data collected from January 1, 2006 to February 16, 2011*
- *3,000+ websites*
- *400+ organizations (Start-ups to Fortune-ranked)*
- *~500,000 verified custom Web application vulnerabilities (non-CVE)*
- *Majority of websites assessed multiple times per month*
- *Vulnerabilities classified according to WASC Threat Classification*[2]
- *Severity naming convention aligns with PCI-DSS*[3]

Note: The websites WhiteHat Sentinel assesses likely represent the most "important" and "secure" websites on the Web, owned by organization that are very serious about their security.

Data Collection and Measurement Methodology

Built as a Software-as-a-Service (SaaS) technology platform, WhiteHat Sentinel combines proprietary scanning technology with s analysis by security experts in its Threat Research Center, to enable customers to identify, prioritize, manage and remediate website vulnerabilities. WhiteHat Sentinel focuses solely on previously unknown vulnerabilities in custom Web applications– code unique to an organization (Figure 8). Every vulnerability discovered by any WhiteHat Sentinel Service is verified for accuracy and prioritized by severity and threat.

In order for organizations to take appropriate action, each website vulnerability must be independently evaluated for business criticality. For example, not all Cross-Site Scripting or SQL Injection vulnerabilities are equal, making it necessary to consider its true "severity" for an individual organization. Using the Payment Card Industry Data Security Standard[4] (PCI-DSS) severity system (Urgent, Critical, High, Medium, Low) as a baseline, WhiteHat Security rates vulnerability severity by the potential business impact if the issue were to be exploited and does not rely solely on default scanner settings.

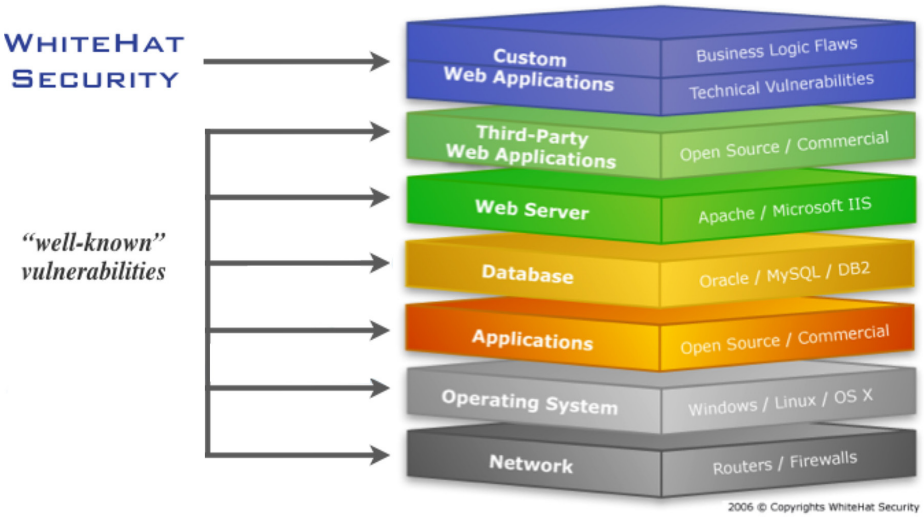

Figure 8. Software / Vulnerability Stack

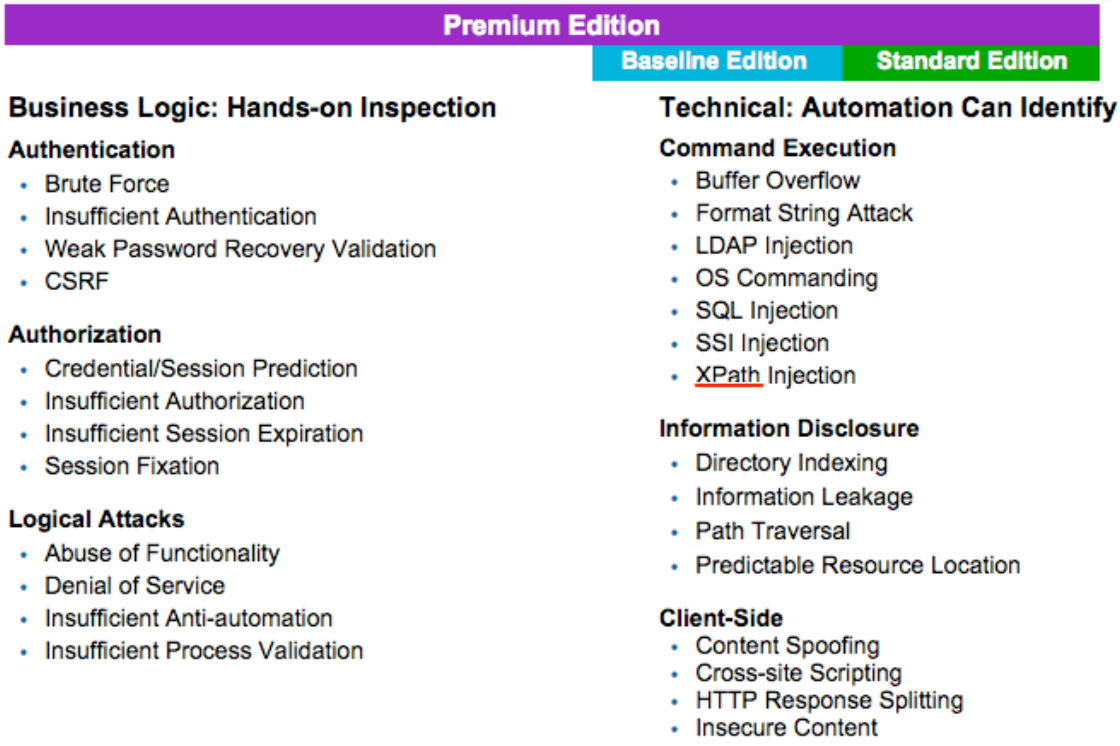

Figure 9. WhiteHat Sentinel Vulnerability Coverage

WhiteHat Sentinel offers four different levels of service (Premium, Standard, Baseline, and PreLaunch) to match the level of security assurance required by the organization[5]. Additionally, WhiteHat Sentinel exceeds PCI 6.6 and 11.3.2 requirements for Web application scanning[6].

Scanning Technology

Production Safe (PE, SE, BE): Non-invasive testing with less performance impact than a single user.

False-positives: Every vulnerability is verified for accuracy by WhiteHat Security's Threat Research Center.

Web 2.0 Support: JavaScript, Flash, AJAX, Java Applets, and ActiveX are handled seamlessly.

Authenticated Scans: Patented automated login and session-state management for complete website coverage.

Business Logic: customized tests analyze every form, business process, and authentication / authorization component.

Factors Influencing the Data:

Websites range from highly complex and interactive with large attack surfaces to static brochureware. Brochureware websites, because of a generally limited attack surface, tend to have a limited number of "custom" Web application vulnerabilities.

Vulnerabilities are counted by unique Web application and class of attack. If three of the five parameters of a single Web application (/foo/webapp.cgi) are vulnerable to SQL Injection, this is counted as 3 individual vulnerabilities (e.g. attack vectors). Secondly, if a single parameter can be exploited in more than one way, each of those are counted as well.

"Best practice" findings are not included in the report. For example, if a website mixes SSL content with non-SSL on the same Web page, while this may be considered a policy violation, it must be taken on a case-by-case basis. Only issues that can be directly and remotely exploitable that lead to data loss are included.

Vulnerability assessment processes are incremental and ongoing, the frequency of which is customer-driven and as such should not automatically be considered "complete." The vast majority of WhiteHat Sentinel customers have their sites assessed multiple times per month.

New attack techniques are constantly being researched to uncover previously unknown vulnerabilities, including in previously tested and unchanged code. Likewise assessments may be conducted in different forms of authenticated state (i.e. user, admin, etc.). As such it is best to view this report as a best-case scenario and there are always more vulnerabilities to be found.

Websites may be covered by different WhiteHat Sentinel service levels (Premium (PE), Standard (SE), Baseline (BE), PreLaunch (PL)) offering varying degrees of testing criteria, but all include verification. PE covers all technical vulnerabilities and business logic flaws identified by the WASC Threat Classification v1 (and some beyond). SE focuses primarily on the technical vulnerabilities. BE bundles critical technical security checks into a production-safe, fully-automated service. The bulk of websites under management are under the PE offering.

References

1 Michael Howard – http://blogs.msdn.com/b/sdl/archive/2009/10/15/ms09-050-smbv2-and-the-sdl.aspx

2 WASC Threat Classification – http://projects.webappsec.org/Threat-Classification

3 PCI Data Security Standard (PCI DSS) – https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

4 PCI Data Security Standard – https://www.pcisecuritystandards.org/

5 WhiteHat Sentinel Selection Guidelines – http://www.whitehatsec.com/home/services/selection.html

6 Achieving PCI Compliance with WhiteHat Sentinel – http://www.whitehatsec.com/home/services/pci.html

The WhiteHat Sentinel Service

WhiteHat Sentinel is the most accurate, complete and cost-effective website vulnerability management solution available. It delivers the flexibility, simplicity and manageability that organizations need to take control of website security and prevent Web attacks. WhiteHat Sentinel is built on a Software-as-a-Service (SaaS) platform designed from the ground up to scale massively, support the largest enterprises and offer the most compelling business efficiencies, lowering your overall cost of ownership.

Unlike traditional website scanning software or consultants, WhiteHat Sentinel is the only solution to combine highly advanced proprietary scanning technology with custom testing by the Threat Research Center (TRC), a team of website security experts who act as a critical and integral component of the WhiteHat Sentinel website vulnerability management service.

Scalable

WhiteHat Sentinel was built to scale and assess hundreds, even thousands of the largest and most complex websites simultaneously. This scalability of both the methodology and the technology enables WhiteHat to streamline the process of website security. WhiteHat Sentinel was built specifically to run in both QA/development and production environments to ensure maximum coverage with no performance impact.

- *Designed to scale and assess the largest and most complex websites simultaneously*
- *3,000+ websites under management*

Accurate

Every vulnerability discovered by WhiteHat Sentinel is verified for accuracy (by the TRC) and prioritized, virtually eliminating false positives and radically simplifying remediation. So, even with limited resources, the remediation process will be sped up by seeing only real, actionable vulnerabilities.

- *The WhiteHat Sentinel remediation process identifies only real vulnerabilities, so you get more accurate results faster than other security solution can provide*

Predictable Costs – Unlimited Assessments

All the costs involved in building a scalable infrastructure and technology are built into the WhiteHat Sentinel Service. So, a company does not have to bear the burden of an upfront investment in hardware, software and personnel.

- *No headcount required – scanner configuration and management run by WhiteHat's Threat Research Center (TRC)*
- *No hardware or scanning software to install*

About WhiteHat Security, Inc.
Headquartered in Santa Clara, California, WhiteHat Security is the leading provider of website risk management solutions that protect critical data, ensure compliance and narrow the window of risk. WhiteHat Sentinel, the company's flagship product family, is the most accurate, complete and cost-effective website vulnerability management solution available. It delivers the visibility, flexibility, and control that organizations need to prevent Web attacks. Furthermore, WhiteHat Sentinel enables automated mitigation of website vulnerabilities via integration with Web application firewalls. To learn more about WhiteHat Security, please visit our website at www.whitehatsec.com.

WhiteHat SECURITY
WhiteHat Security, Inc. | 3003 Bunker Hill Lane | Santa Clara, CA 95054
408.343.8300 | www.whitehatsec.com

030311