CENZIC

CENZIC ENTERPRISE APPLICATION SECURITY

Web Application Security Trends Report
Q3-Q4, 2008

Table of Contents

Contributors

We'd like to thank everyone who contributed to the Q3-Q4 2008 Trends Report.

Project Lead

- Mandeep Khera, Chief Marketing Officer, Cenzic, Inc.

Executive Editor

- Mandeep Khera, Chief Marketing Officer, Cenzic, Inc.

Additional Contributors

- Sameer Dixit, Cenzic ClickToSecure Service
- The Rook Institute
- Kulesa Public Relations

Key Sources

- Cenzic Intelligent Analysis Lab
- Cenzic ClickToSecure Service
- Mitre
- OWASP
- SANS
- Secunia
- Security Tracker
- Symantec
- US-CERT

Executive Summary

With President Obama's stimulus package passed, every one is hoping for a path to economic recovery. With $355M of this package going toward cyber security, let's hope the security of our infrastructure will move toward a stronger future as well. As we had predicted during the first two quarters of 2008, cyber attacks continued through out the second half of 2008 and at a much faster pace, most of them coming through Web applications. Social networking sites like Facebook and Twitter got hit by various Cross-Site Scripting attacks. Millions of users and liberal use of Web 2.0 technologies are making these social networking Web sites prime targets for hackers[1]. Attacks against many financial institutions including one of the largest against Heartland, which affected over 160 institutions continued to prevail throughout the second half of 2008. Many political hacktivism attacks resulted in countries defacing one another's Web sites with the usual suspect countries including India, Pakistan, Israel, Palestine, Russia, Georgia and China. Even security companies like Kraspersky and Symantec were not spared. It's clear that this war is currently being fought on the hackers' terms and they are for the most part winning. Most of the attacks continue to originate from U.S., Brazil, China, and Russia and hackers are getting smarter by the day so in spite of the stronger efforts most of them continue to evade the authorities.

With the economy at its worst in a few decades and unemployment at historically high levels, we are starting to see strong trends toward insider threats. Many employees who have been laid off instill back doors and create holes in the infrastructure before they leave so they can attack when they are out. In fact, some of the insiders are collaborating with the hackers for a mutual financial gain.

Our Q3-Q4 Trends Report once again points out the continued growth of vulnerabilities and growth of attacks through Web applications. The total number of reported vulnerabilities went up to 2835, an increase of over 10 percent from the first half, and the percentage of Web application vulnerabilities went up to a staggering 80 percent.

Of the Web technology vulnerabilities, Web application vulnerabilities comprised about 79 percent, which is slightly lower than the first two quarters of 2008. Plugins and ActiveX vulnerabilities came in at 12 percent, which is much higher than the first half of 2008. Web browsers comprised about 7 percent of Web vulnerabilities which is higher than the previous quarters and Web server comprised 2 percent which is lower than the

[1] Although the correct term for bad hackers is "crackers", we are using the most commonly understood term of "hackers" in this document for the "bad guys".

previous quarters. Of the browser vulnerabilities, Internet Explorer, which had improved in the first half of 2008 got worse with roughly 42 percent of the browser vulnerabilities followed by Firefox at 39 percent.

The top 10 vulnerabilities for the second half of 2008, included the familiar names such as Adobe, Sun, Microsoft, SAP, Mozilla, Apache, and Oracle. Through Cenzic's SaaS offering ClickToSecure, we tested hundreds of applications with thousands of pages and found at least 80 percent applications suffering from severe vulnerabilities. Most Web applications were found to have vulnerabilities related to Information Leaks and Exposures, Cross-Site Scripting, and Session Management.

We are beginning to see a trend of growing awareness around Web application security. The Payment Card Industry (PCI) Section 6.6 initiative is certainly driving a lot of companies especially e-retailers to get compliant. However, the economic crisis is holding a number of organizations back from moving forward with this initiative. What's surprising is that most of these companies are still spending money on network security. With 80 percent to 90 percent of Web applications vulnerable, and with 75 percent of attacks occurring through the Web sites, this budget allocation defies logic. But, lack of awareness and understanding of the issues around application security are partly to blame. Furthermore, most of the regulations around compliance including PCI, Gramm-Leach Bliley Act (GLBA), HIPAA, SB 1385, AB 1950, and others are not enforcing the regulations as strongly as they should. Many organizations don't want to take action unless they have been hacked or audited by one of the regulatory compliance bodies.

But it's not all doom and gloom. In spite of many companies not taking action to secure their Web sites, a lot more, when compared to last year have moved forward with some kind of initiative. Every day we are finding more companies trying to educate themselves on the issues and start an initiative on securing the Web applications. Organizations like OWASP (www.owasp.org), SANS (www.sans.org), and NIST (www.nist.gov) are doing a great job of educating companies on the issues surrounding Web application security.

Even in bad times, and perhaps even more so in bad times, companies have to protect their assets. Web applications are among the top assets with your customer information that need to be protected. Unfortunately, saving a few thousand dollars by not taking care of this will result in proving the adage of being "penny wise and pound foolish" (or "cent wise and dollar foolish").

Mandeep Khera
Chief Marketing Officer, Cenzic

General Observations

Cenzic analyzed reported vulnerability information for Q3 and Q4 2008 (July through December) time period. During this period, Cenzic's CIA Labs identified 2835 vulnerabilities. This is a significant increase over the first half of 2008 for which we had identified 2616 vulnerabilities. Web application vulnerabilities continued to make up the largest percentage of the reported vulnerability volume, even comprising a larger portion of the vulnerability volume than usual. Web technology vulnerabilities comprised roughly 80 percent of the vulnerabilities, up from around 73 percent in Q2 2008 and 70 percent in Q1, 2008. We believe that this trend will continue and we'll see more Web application related vulnerabilities in the coming months as more organizations get exposed to Web application security. Our key findings from the second half of 2008 are listed below:

Key Findings:

- Adobe continued to be plagued by vulnerabilities some of which showed up in our Top 10 list. Others on this list included SAP, Microsoft, Mozilla, Sun, Apache, and Oracle.
- 80 percent of the total reported vulnerabilities affected Web technologies, such as Web servers, applications, Plugins and ActiveX, and Web browsers, which is a significant increase from earlier in the year.
- Of the Web technology vulnerabilities, Web application vulnerabilities comprised about 79 percent, which is slightly lower than the first two quarters of 2008; Plugins and ActiveX vulnerabilities came in at 12 percent which is much higher than the first half of 2008; Web browsers were about 7 percent of the Web vulnerabilities which is much higher than the previous quarters; Web server comprised 2 percent which is lower than the previous quarters.
- Looking at the various classes of vulnerabilities, we found that surprisingly, reported Cross-Site Scripting (XSS) and SQL Injection vulnerabilities went down from previous quarters to 14 percent and 25 percent respectively. In the first two quarters these vulnerabilities hovered around upper 20s and low 30s. Authorization and Authentication vulnerabilities stayed pretty normal at 5 percent of total Web vulnerabilities. Another surprise was an increase in Buffer Overflow vulnerabilities which comprised 10 percent of Web vulnerabilities.
- Of the browser vulnerabilities, Internet Explorer had the highest percentage at 43 percent followed closely by Firefox at 39 percent which is a turnaround from the last two quarters when Firefox had a much higher percentage. This might have something to do with the new IE updates that were released. Safari and Opera continue to report fewer vulnerabilities at 10 percent and 8 percent respectively.
- While the observations listed above focused on published vulnerabilities from commercial and open source applications, our analysis of the Web applications tested by Cenzic as part of the managed service/SaaS showed that Information Leaks, Cross-Site Scripting, and Session Management were dominant with the highest percentage of applications vulnerable in these categories.

Top 10 Vulnerabilities of Q3-Q4 2008

Cenzic classified the following Web application vulnerabilities disclosed during the second half of 2008 as the most severe. These are not necessarily in order.

1. **[CIA-1120-Alert] Microsoft Internet Explorer data binding memory corruption vulnerability**
   Allows remote attackers to execute arbitrary code via a crafted XML document containing nested SPAN elements, as exploited in the wild in December 2008.

   CVE-2008-4844

2. **[CIA-1121-Alert] Adobe Flash Player Multiple Vulnerabilities**
   Remote attackers can read sensitive data from process memory via a crafted PDF file DeclareFunction2 Tag and execute arbitrary code on the victim's machine.

   CVE-2008-5361

3. **[CIA-1122-Alert] Java Runtime Environment (JRE) Buffer Overflow Vulnerabilities**
   Java Runtime Environment (JRE) Buffer Overflow vulnerabilities in processing image files and fonts may allow Applets or Java Web Start Applications to elevate their privileges.

   http://www.us-cert.gov/cas/techalerts/TA08-340A.html

4. **[CIA-1123-Alert] SAP SAPgui ActiveX control code execution vulnerability**
   By convincing a user to view a specially crafted HTML document (e.g. a web page or an HTML email message or attachment), an attacker may be able to execute arbitrary code with the privileges of the user. The attacker could also cause Internet Explorer (or the program using the WebBrowser control) to crash.

   CVE-2008-4387

5. **[CIA-1124-Alert] Adobe Reader and Acrobat Stack-Based Buffer Overflow**
   Allows remote attackers to execute arbitrary code via a PDF file that calls the util.printf JavaScript function with a crafted format string argument.

   CVE-2008-2992

6. **[CIA-1125-Alert] Microsoft Office Snapshot Viewer ActiveX Vulnerability**
   A remote, unauthenticated attacker could execute arbitrary code**.** Systems affected include Microsoft Access Microsoft Office Access 2000, Microsoft Office Access XP, Microsoft Office Access 2003, and Microsoft Office Snapshot Viewer.

   http://www.us-cert.gov/cas/techalerts/TA08-189A.html

7. **[CIA-1126-Alert] Oracle Weblogic Apache connector Buffer Overflow**
   A Buffer Overflow exists in Weblogic Server and Weblogic Express due to the way that the Apache connector plugin handles specially crafted POST requests. A remote, unauthenticated attacker may be able to execute arbitrary code.

   CVE-2008-3257

8. **[CIA-1127-Alert] Mozilla Firefox code execution vulnerability**
   Allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via an image.

   CVE-2008-2811

9. **[CIA-1128-Alert] Apache Tomcat UTF8 Directory Traversal Vulnerability**
   Apache Tomcat contains a vulnerability in the way malformed requests are handled. A remote attacker could gain access to arbitrary files on the server.

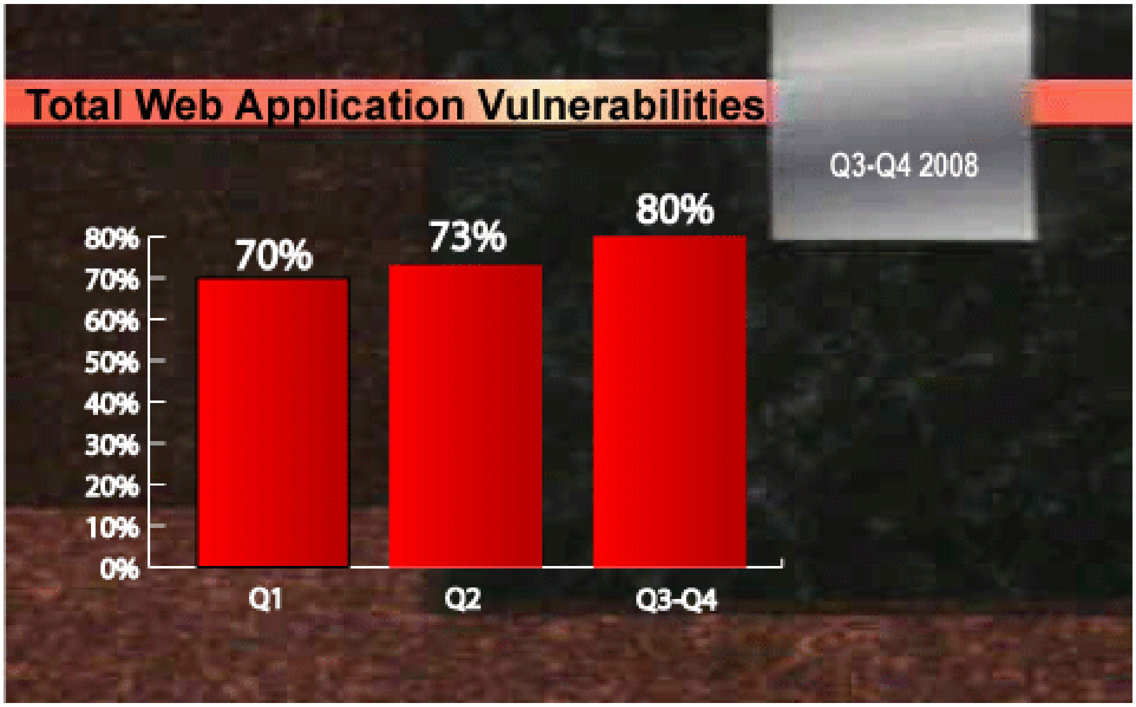
   CVE-2008-2938

10. **[CIA-1129-Alert] Security Vulnerabilities in the Java Runtime Environment may allow Same Origin Policy to be Bypassed**
    Security vulnerabilities in the Java Runtime Environment may allow an untrusted applet that is loaded from a remote system to circumvent network access restrictions and establish socket connections to certain services running on machines other than the one that the applet was downloaded from.

    http://www.us-cert.gov/cas/techalerts/TA08-193A.html

Vulnerabilities in Web Applications

Cenzic analyzed all reported vulnerability information from sources such as NIST, MITRE, SANS, US-CERT, OSVDB, SecurityTracker, as well as other third party databases for Web application security issues reported during the second half of 2008. We looked at specific vulnerabilities associated with Web technologies. Our findings are presented below. Roughly about 80 percent of all vulnerabilities pertained to Web applications and related technologies, which is much higher than the previous quarters. This is the highest percentage we have seen so far and could be an alarming trend. These numbers represent the published vulnerabilities of various commercial off the shelf software as well as open source software.

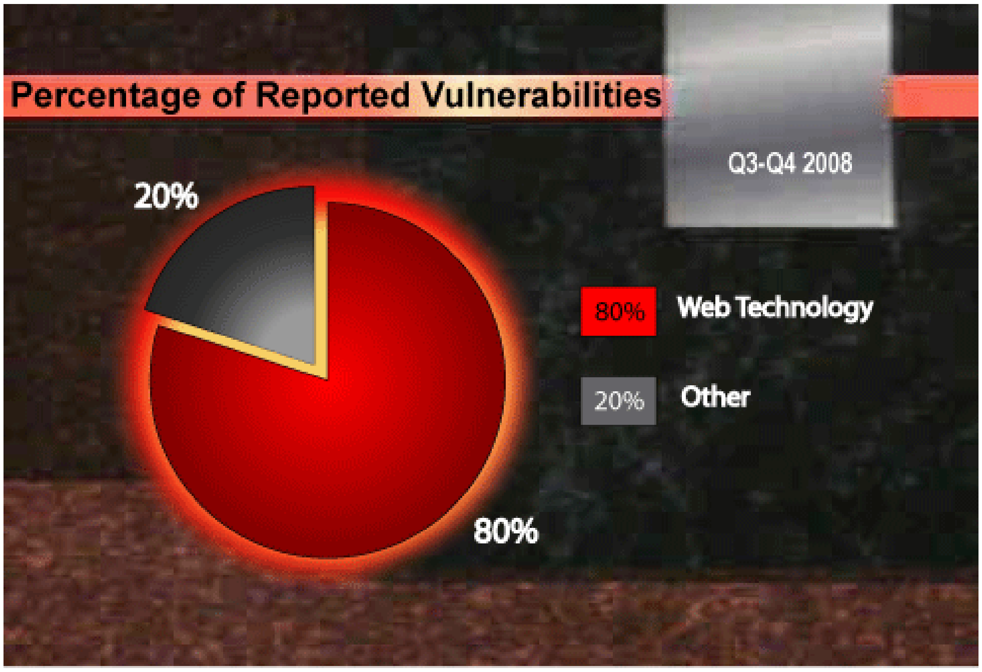


Vulnerability Breakdown for Q3-Q4 2008

The Q3-Q4 reported vulnerability information reveals that 80 percent of the reported vulnerabilities were in Web applications, slightly higher than the Q1 findings. We have analyzed these vulnerabilities based on types and classes with more details below.

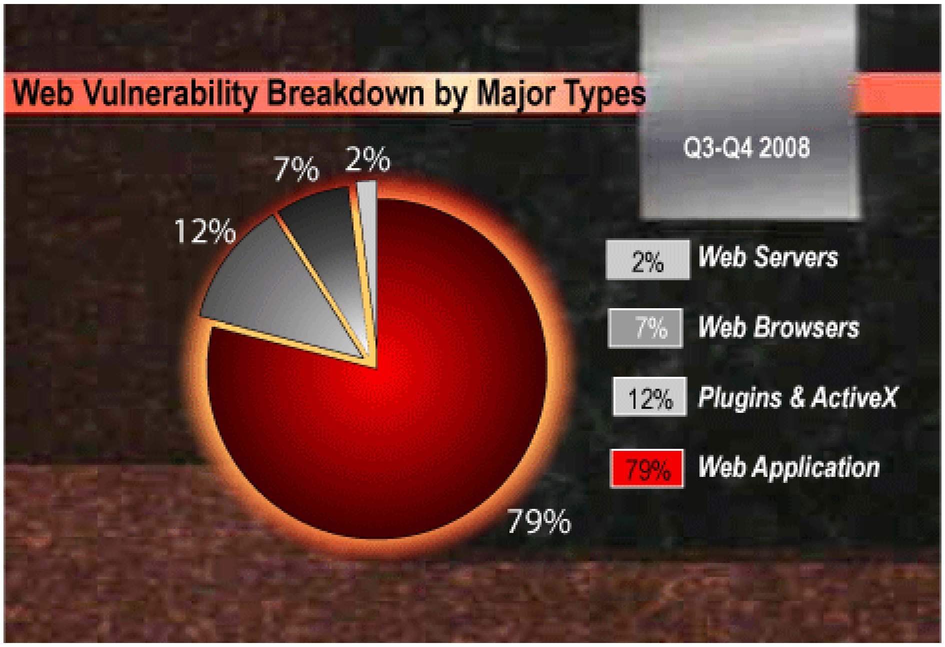
Vulnerability by High-Level Categories

The following chart shows the percentage of Web technology vulnerabilities versus other types of vulnerabilities, such as those within protocols, mail servers, or FTP servers. Much of the emphasis on the part of this research and security community has come to focus on the discovery, and publication of vulnerabilities in Web applications. A couple of years ago, of the total published vulnerabilities, network and infrastructure vulnerabilities formed the majority. However, in the last two years or so, Web application vulnerabilities have dominated as a percentage of the total vulnerabilities. For the second half of 2008, the percentage has climbed to 80 percent, highest so far. This trend can at least partly be attributed to an increased awareness of application security and partly to the fact that network technologies have matured with better security measures.



Vulnerability by Major Type

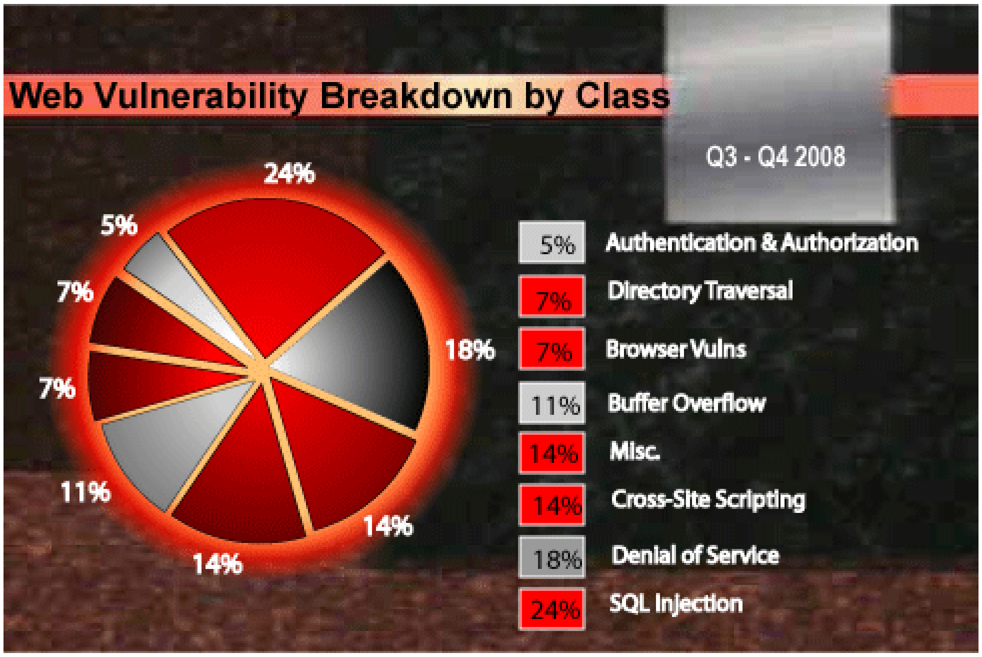
The following detailed view breaks down the Web technology vulnerabilities by major type for Q3-Q4 2008.



The chart above shows the breakdown of overall Web technology vulnerabilities into major categories. Of all the Web related vulnerabilities, 2 percent are in Web servers such as Apache Web server, which is a decline over the first two quarters of 2008. 7 percent relate to Web browsers, which is an increase over the first two quarters which had 3 percent and 4 percent respectively. Plugins and ActiveX vulnerabilities increased to 12 percent. The remaining 79 percent of vulnerabilities affect software written for various Web servers and Web application server technologies. A typical example would be an application written in PHP and released under the GNU open source license. Again, these vulnerability percentages relate only to published or reported vulnerabilities and do not reflect the percentages of vulnerabilities of these categories found “in the wild.”

Vulnerability Reported by Class

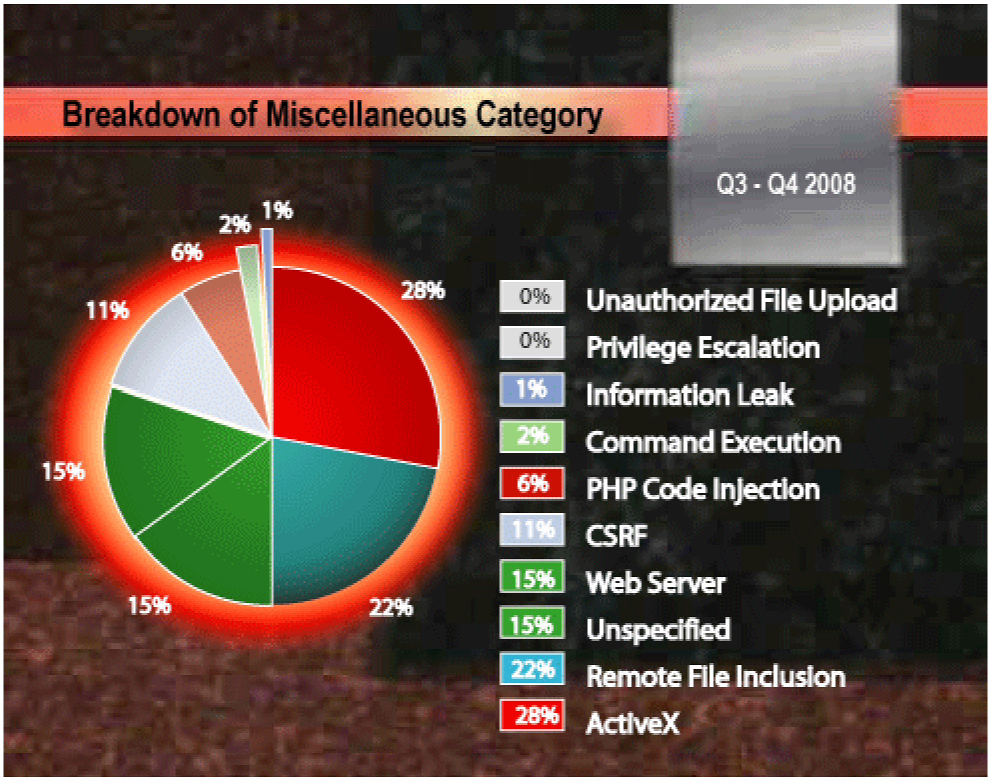
The following data comes from public sources and reflects the percentages of vulnerabilities reported on mailing lists and in security advisories during the second half of 2008 for major Web application security risks.



Although application-layer injection flaws, such as SQL Injection, and Cross-Site Scripting once again dominated in this report's period as the most frequently found and reported vulnerability classes, these percentages were lower than the last two quarters. For example, XSS formed 24 percent in Q1 and 23 percent in Q2 and SQL Injection vulnerabilities formed 27 percent and 34 percent of the total Web vulnerabilities respectively. Directory Traversal comprised 7 percent of the total Web vulnerabilities which was a slight decline from Q2.   Surprisingly, Buffer Overflow was a much bigger percentage this time around at 10 percent. The "Misc" category in the chart above is composed of a mixture of security issues reported in lesser number, such as Cross-Site Request Forgery, Remote File Inclusion, Command Execution, and various less commonly reported vulnerabilities. A breakdown of the Misc category is provided in the next section. Again, these percentages are based on reported vulnerabilities for commercial and open source software. The actual vulnerabilities for all the proprietary or in-house built applications can be totally different as highlighted in the last section of this report under ClickToSecure, Cenzic's managed service/SaaS findings.

Vulnerability Breakdown for Miscellaneous Category

The Misc category comprised 14 percent of all Web application vulnerabilities during the Q3-Q4 period. The chart below gives a detailed breakdown of types of vulnerabilities grouped in this category, and the percentage of the category they comprised. The detailed breakdown of this category for Q3-Q4 2008 is as follows:

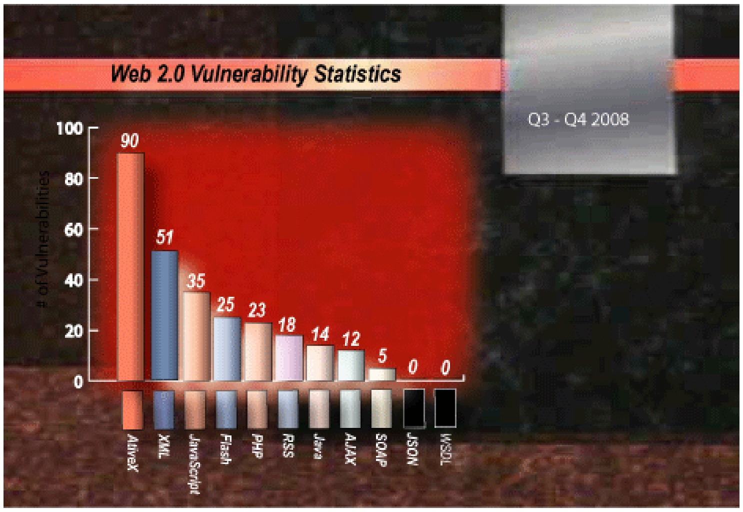


Note: Unauthorized File Upload with 1 vulnerability and Privilege Escalation with 2 vulnerabilities were rounded down to 0%

Web 2.0 Vulnerability Trends

We are starting to see more Web applications utilizing Web 2.0 technologies. We have been tracking the various technology vulnerabilities used in Web 2.0 for the last few quarters. At the core of the trend is increased Web-based access to data processing, particularly on the client-side, that enables Web applications which contain enriched functionality. Web 2.0 technology roughly breaks down into a wide range of technologies and protocols that enable Web architectures greater access to data and functions:

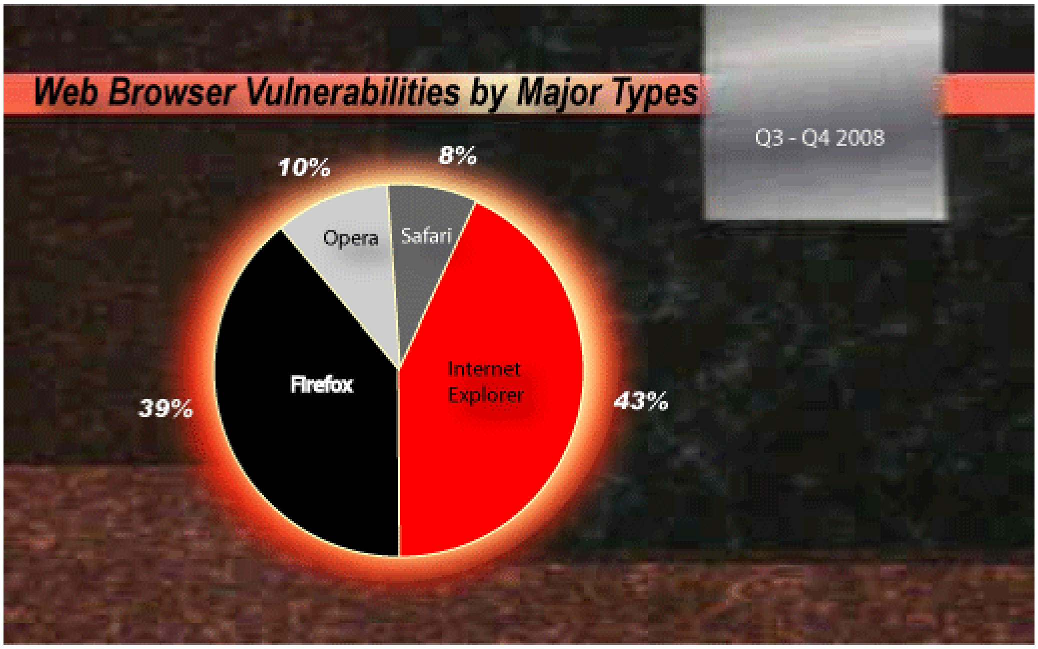
- Asynchronous Javascript and XML (AJAX)
- eXtensible markup language (XML)
- Javascript Object Notation (JSON)
- SOAP and WSDL (Web Services Description Language)
- REST Web APIs
- Javascript, Adobe Flash, Java, ActiveX controls
- Adobe Flex, Microsoft Silverlight
- RSS, RDF, and Atom



Due to increasing awareness of these technologies and more prevalent use in various Web applications, we are starting to see more vulnerabilities spring up as well. During the period of Q3-Q4, 2008, we observed 273 vulnerabilities related to Web 2.0 technologies. This is compared to less than 150 in the first two quarters. About one-third of these vulnerabilities pertained to ActiveX and another one-fifth to XML. The rest were distributed among Javascript, PHP, Flash, Ajax, and others.

Web Browser Vulnerabilities

Vulnerabilities in Web browsers were concentrated among four popular technologies - Internet Explorer, Mozilla Firefox, Opera, and Safari. There was a significant increase in the number of browser vulnerabilities in this time period comprising 7 percent of total Web vulnerabilities. Surprisingly, Internet Explorer, which was doing comparatively better the first two quarters of 2008, got worse during this period with 43 percent of the total browser vulnerabilities. However, Firefox wasn't too far behind with 39 percent. Firefox has continued to have a very high percentage with around 40 percent of the total vulnerabilities for the whole year. Both Opera and Safari browsers continue to show low percentage of vulnerabilities.



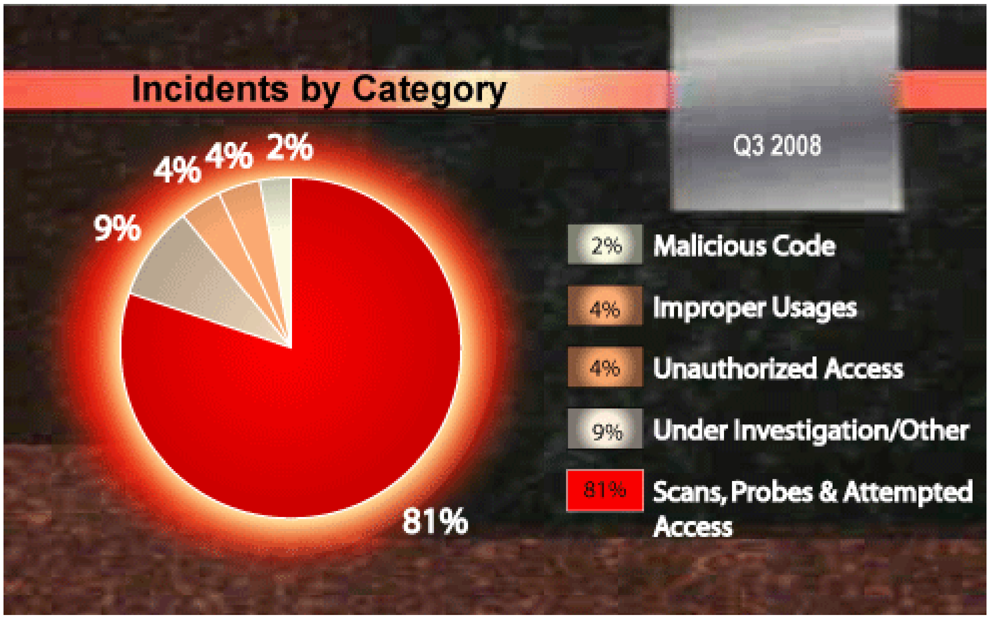
Probe and Attack Data

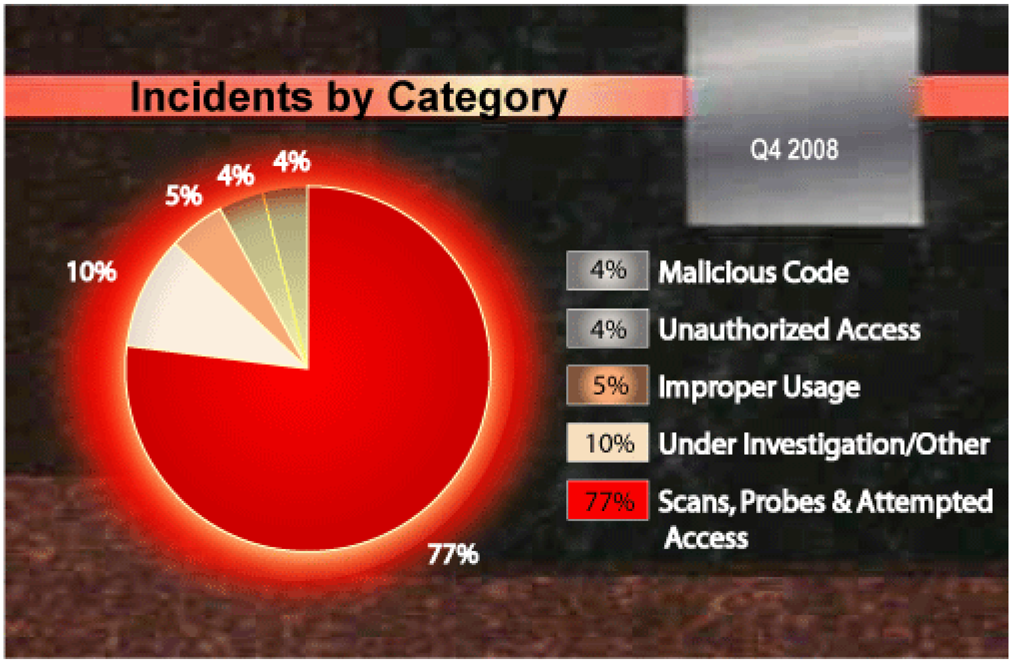
It is difficult to estimate the number of attacks against Web applications from published sources and incident reports because most of the attacks go unreported as companies choose not to report or don't know they have been attacked. Therefore we have chosen to examine data collected by the SANS Internet Storm Center along with data gathered from Dshield.org. The data presented here must be interpreted with the following points in mind:

- Information shared within Dshield and the SANS Internet Storm Center represent the culmination of logs from various security devices, predominantly access control and firewall technologies, with some IPS/IDS compatibility, notably, the Snort Intrusion Detection System.
- The information provided should not be viewed as live attacks against production Web applications. Rather, the data is more likely the result of probing activity detected by IDS/IPS systems and blocked attempts to access Port 80 on networks where that port is "firewalled".
- On machines hosting a Web server, Port 80 is open for use and therefore attacks against Web applications are not as likely to be present in the data as probing activity which is blocked by an access control device.
- The probing and attack data for the first half of 2008 is presented in six graphs and this data is supplemented with security events that may have influenced the probing or attack activity. It is also important to view this data within the context of the CERT-US Incident Reports for Q3 and Q4 2008, since the SANS/Dshield data is transparent to incident or attack type.

Incidents by Category

The US-CERT Quarterly Trends and Analysis for Q3 2008 and Q4 2008 details the category and percentages of security incidents for July to December (based on the most recent report)[2]. It should be noted that US-CERT uses a different fiscal year.

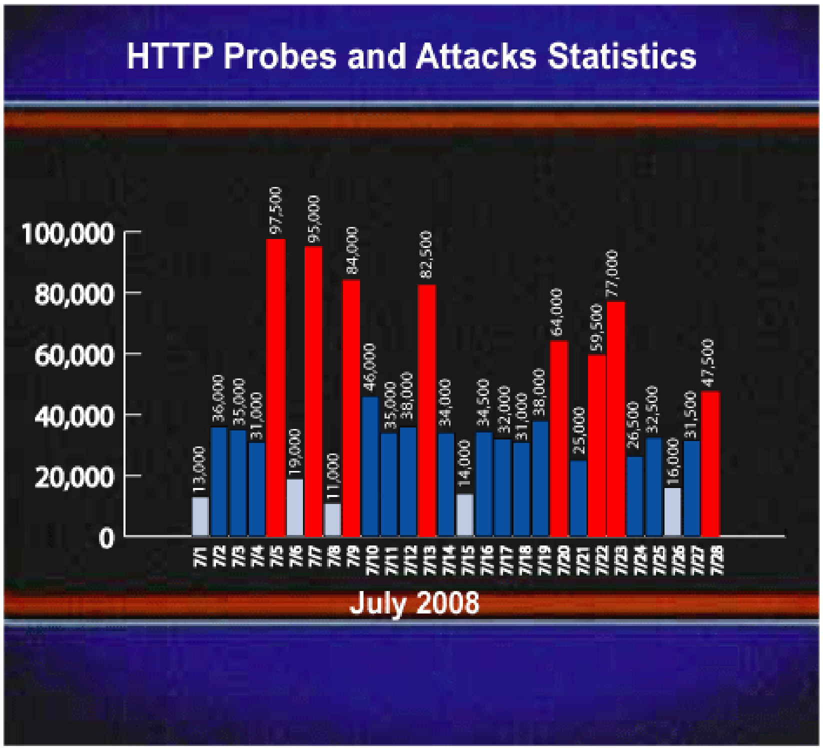




[2] US-CERT Quarterly Trends and Analysis Report Volume 2 No. 4

July 2008 HTTP Probes and Attacks Statistics

Attack activity in July was strongest early in the month, declining gradually in late July. Bursts of attacks close to 100,000 attacks per day occurred a few times in the month.



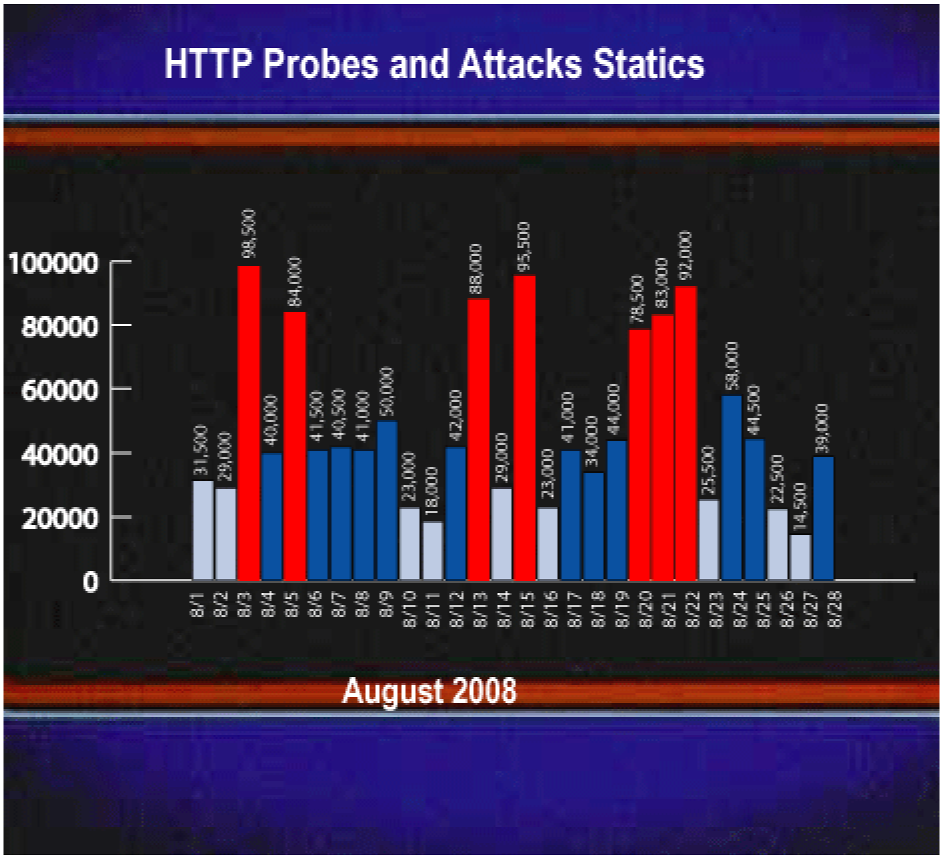
Correlation with Major Vulnerability Data

- 07-07-2008: An unpatched vulnerability in the Microsoft Office Snapshot Viewer ActiveX control is being used in attacks. [3]
- 07-08-2008: Microsoft released updates that address vulnerabilities in Microsoft Windows, Windows Server, Microsoft SQL Server, and Microsoft Outlook Web Access. [2]
- 07-11-2008: Sun released alerts to address multiple vulnerabilities affecting the Sun Java Runtime Environment. The most severe of these vulnerabilities could allow a remote attacker to execute arbitrary code.[2]

[3] http://www.us-cert.gov/cas/techalerts and http://www.dshield.org

August 2008 HTTP Probes and Attacks Statistics

Attacks in August saw a pretty consistent pattern with a few days of over 90,000 attacks and one day close to 100,000.



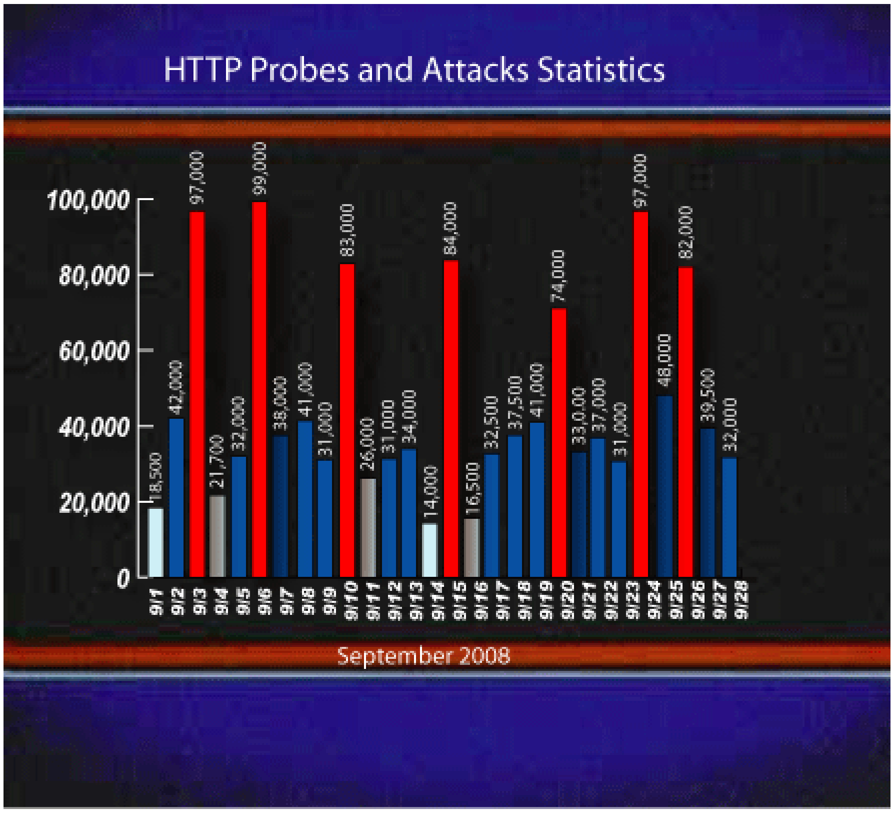
Correlation with Major Vulnerability Data

- 08-12-2008: PHP 5.2.6 released, including fixes for 6 security vulnerabilities[4].

[4] http://www.us-cert.gov/cas/techalerts and http://www.dshield.org

September 2008 HTTP Probes and Attacks Statistics

Attack activity in September was strong throughout the month with frequent bursts to over 100,000 attacks per day.



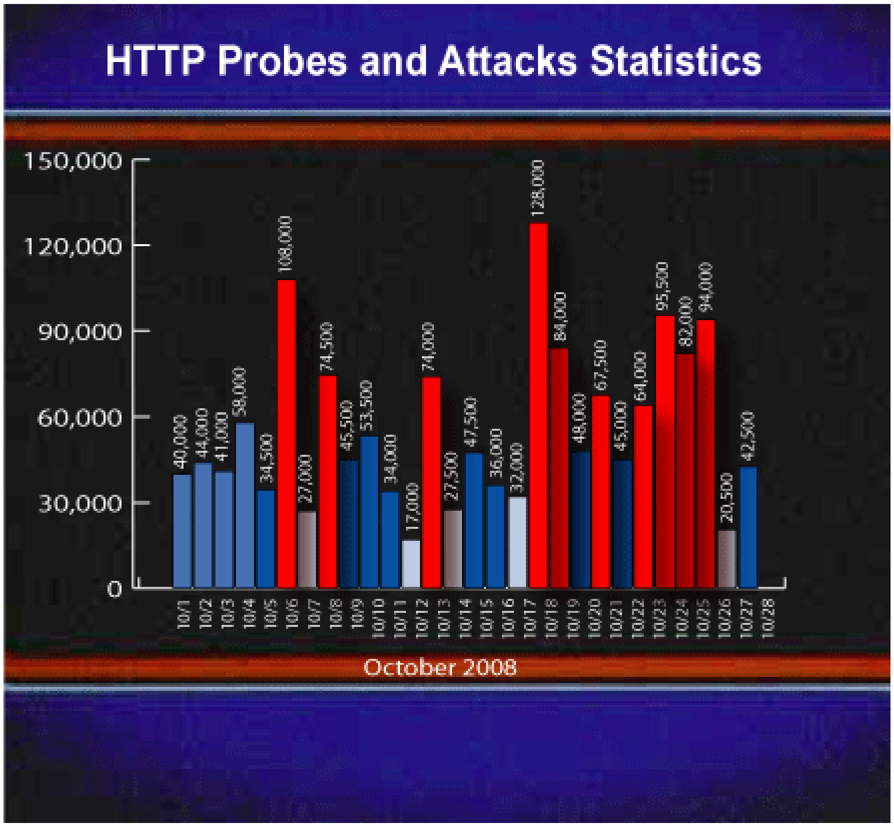
Correlation with Major Vulnerability Data

- 09-09-2008: Microsoft has released updates that address vulnerabilities in Microsoft Windows, Windows Media Encoder, and Microsoft Office. [5]
- 09-16-2008: Apple has released Security Update 2008-006 and Mac OS X version 10.5.5 to correct multiple vulnerabilities affecting Apple Mac OS X and Mac OS X Server. Attackers could exploit these vulnerabilities to execute arbitrary code, gain access to sensitive information, or cause a denial of service. [4]

[5] http://www.us-cert.gov/cas/techalerts and http://www.dshield.org

October 2008 HTTP Probes and Attacks Statistics

Attack activity in September was relatively low except for a couple of major bursts over 100,000 and one of them reaching 130,000 attacks.



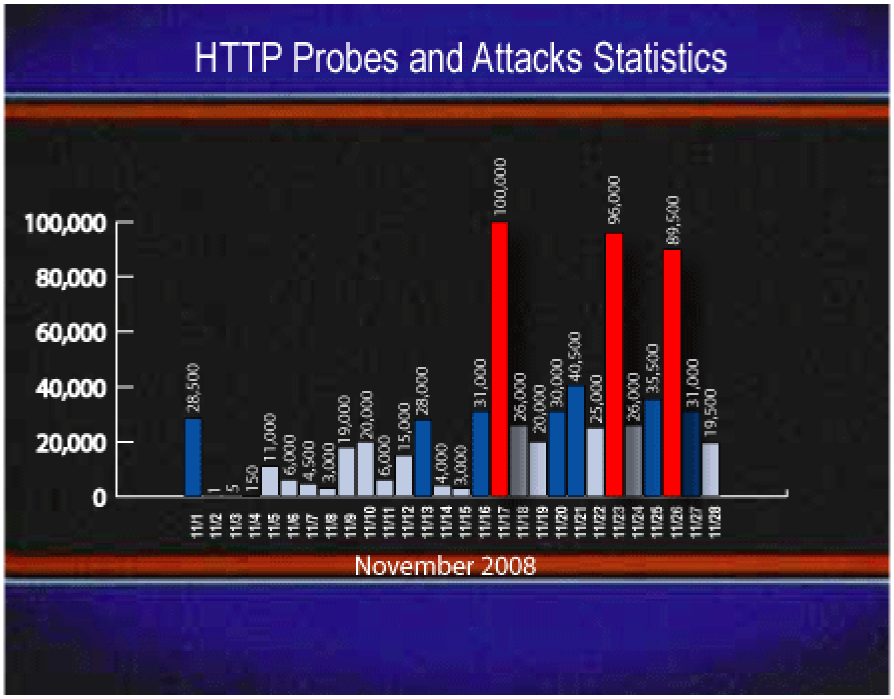
Correlation with Major Vulnerability Data

- 10-14-2008: Microsoft released updates that address vulnerabilities in Microsoft Windows, Internet Explorer, and Microsoft Office. [6]
- 10-23-2008: A vulnerability in the way the Microsoft Windows server service handles RPC requests could allow an unauthenticated, remote attacker to execute arbitrary code with SYSTEM privileges. [5]

[6] http://www.us-cert.gov/cas/techalerts and http://www.dshield.org

November 2008 HTTP Probes and Attacks Statistics

November was an active month for attacks especially toward the latter half of the month with attacks reaching 90,000 numerous times.



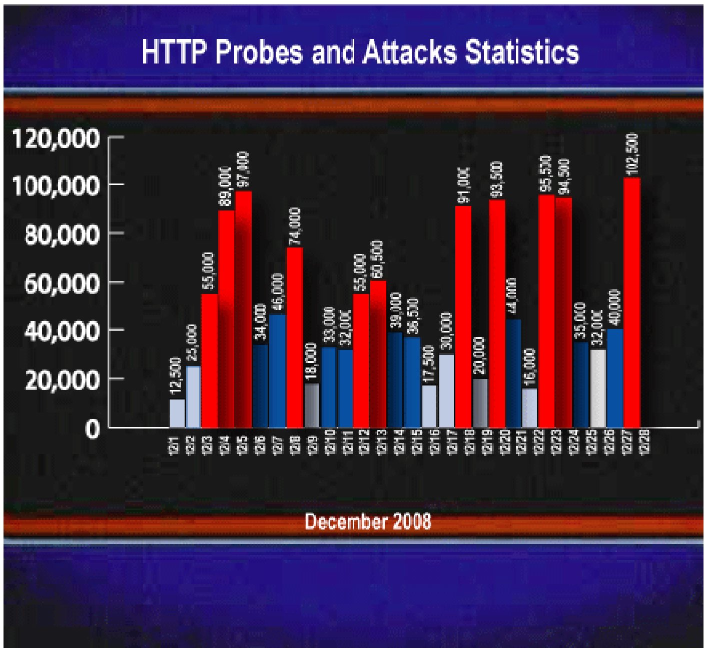
Correlation with Major Vulnerability Data

- 11-04-2008: Adobe has released Security Bulletin APSB08-19 to address multiple vulnerabilities affecting Adobe Reader and Acrobat. The most severe of these vulnerabilities could allow a remote attacker to execute arbitrary code.[7]
- 11-11-2008: Microsoft released updates that address vulnerabilities in Microsoft Windows, Microsoft Office, and Microsoft XML Core Services .[6]
- 11-14-2008: New versions of Firefox, Thunderbird, and SeaMonkey address several vulnerabilities, the most severe of which could allow a remote attacker to execute arbitrary code on an affected system .[6]

[7] http://www.us-cert.gov/cas/techalerts and http://www.dshield.org

December 2008 HTTP Probes and Attacks Statistics

Attack activity in December was pretty consistent with a few spikes reaching close to 100,000 attacks.



Correlation with Major Vulnerability Data

- 012-05-2008: Sun has released alerts to address multiple vulnerabilities affecting the Sun Java Runtime Environment. The most severe of these vulnerabilities could allow a remote attacker to execute arbitrary code. [8]
- 12-09-2008: Microsoft has released updates that address vulnerabilities in Microsoft Windows, Internet Explorer, Word, Excel, SharePoint Server, Visual Basic 6 and related components. [7]
- 12-15-2008: Apple released Security Update 2008-008 and Mac OS X version 10.5.6 to correct multiple vulnerabilities affecting Apple Mac OS X and Mac OS X Server. Attackers could exploit these vulnerabilities to execute arbitrary code, gain access to sensitive information, or cause a denial of service. [7]
- 12-17-2008: Microsoft Internet Explorer contains an invalid pointer vulnerability in its data binding code, which can allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system. Exploit code for this vulnerability is publicly available and is being actively exploited.[7]

[8] http://www.us-cert.gov/cas/techalerts and http://www.dshield.org

Conclusions and Findings from Cenzic ClickToSecure®

Cenzic ClickToSecure is a leading-edge application security assessment and penetration testing managed service (SaaS) that identifies vulnerabilities and provides remediation to allow organizations to stay ahead of hackers. This service leverages the power of the Cenzic Hailstorm software and is also available via a remote assessment or onsite from the customer location. Customers are able to view all their results dynamically on the custom dashboards without additional software or hardware installation. Many companies are using Cenzic's unique hybrid solution where they use the Cenzic's managed service in addition to the on-premise software to allow them the flexibility of increasing their coverage without adding resources.

During the second half of 2008, the Cenzic ClickToSecure service analyzed thousands of Web pages for vulnerabilities. The analyzed applications originated from various business and government sectors. The results of the analysis and key findings are presented below.

Key Findings

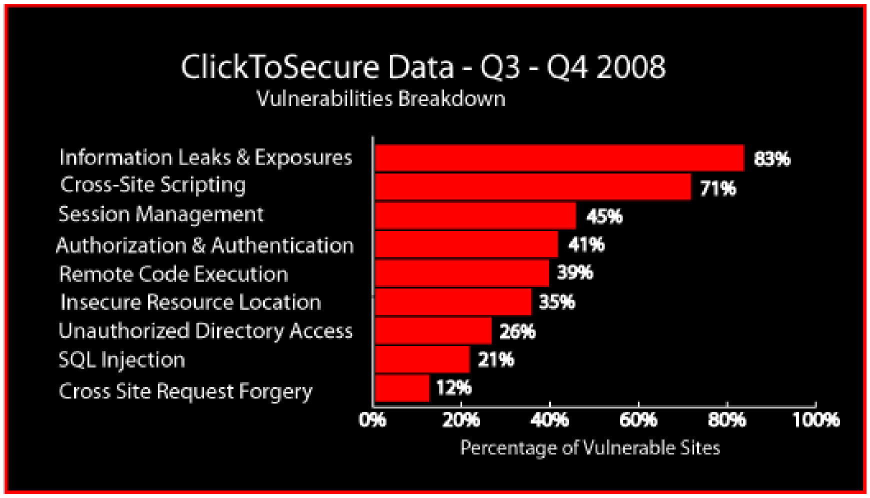
The Q3-Q4 2008 findings are roughly consistent the findings revealed during Q1 2008. Cenzic found that at least 8 out of 10 or 80 percent of the analyzed Web applications had serious vulnerabilities that could potentially lead to the exposure of sensitive or confidential user information during transactions.

Similar to the first two quarters of 2008, Information Leaks and Exposures was the most prevalent vulnerability. In general we observed many types of insecure communications observed were forms that cached sensitive user information, passwords submitted without utilizing SSL for encryption, cases where sensitive information was passed as a URL parameter and hence subject to caching, as well as several instances where the password auto-complete attribute of a Web page exposed user data.

In spite of some highly visible attacks against Facebook, Twitter, and others, Cross-Site Scripting continued to be the second highest vulnerability type discovered by Cenzic ClickToSecure, affecting 7 out of 10 Web applications. Additionally, Session Management, Authorization and Authentication, and Remote Code Execution were very common vulnerabilities found in our testing.

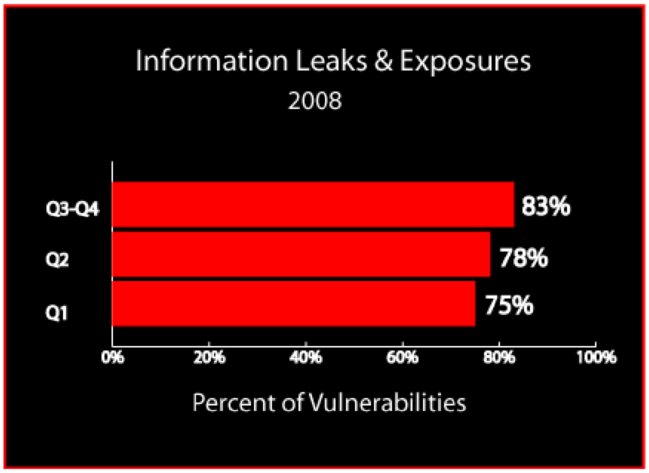
Vulnerabilities Breakdown

Cenzic ClickToSecure found the following percentages of sites with vulnerabilities as belonging to each of the categories below during Q3-Q4 2008. From the data gathered, several vulnerability types were found to be prevalent within the Web applications assessed. The graphs below show the collected Q3-Q4 data for ClickToSecure. The subsections show a comparison between the Q3-Q4 2008 data and previous quarters going back to the first half of 2008.



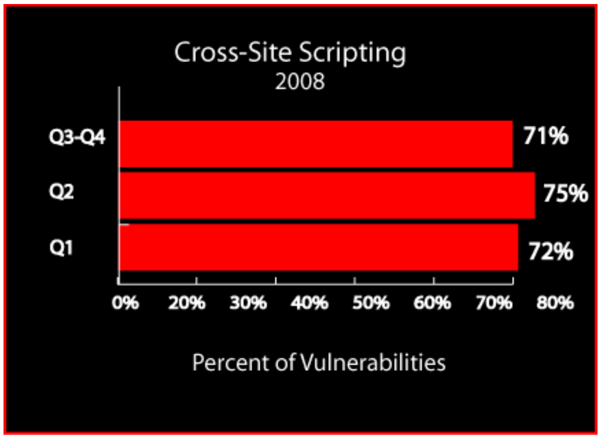
Information Leaks and Exposures (83%)

Transactions during ordinary use of a Web application can reveal sensitive information belonging to other users. It may also be possible to generate application errors by supplying various malformed character sequences, which can contain sensitive information. HTML comments are another example of an information leak, as these comments may assist an attacker in gathering information about the application or its architecture.



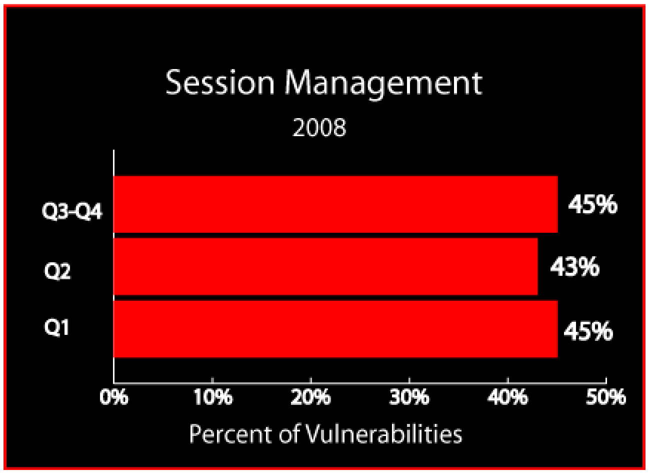
Cross-Site Scripting (71%)

Cross-Site Scripting attacks allow a remote attacker to corrupt the integrity of an application's code by inserting malicious scripts into the application itself, often directly into the database. Cross-Site Scripting attacks may allow an attacker to steal users' session cookies, spoof content, or redirect users to malicious Web sites that exploit Web browser security issues.



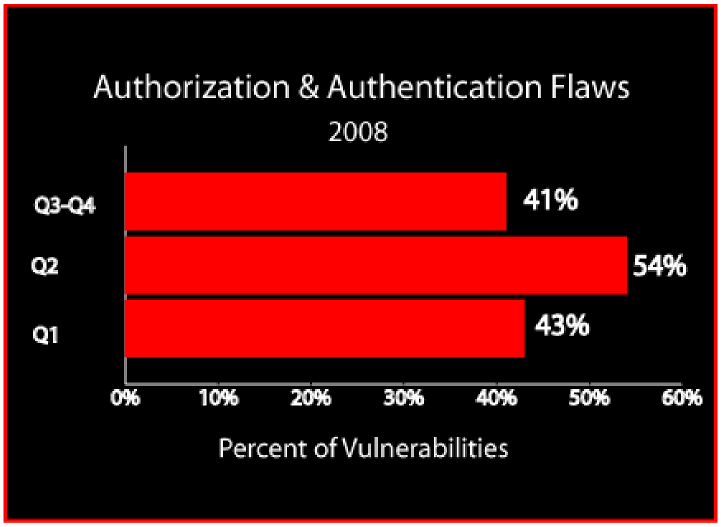
Session Management (45%)

Web applications manage user sessions for the purpose of tracking a user's state and position within a Web application. Vulnerabilities in session management can allow an attacker to take over a user's session by guessing a valid session ID or session token, or by reusing session IDs cached by intermediate logging devices or HTTP server logs. One vulnerability type that facilitates session hijacking occurs when a Web application fails to properly tear down a user's session. The vulnerability results in a user's session ID being valid for a period of time after they have logged out, allowing anyone who has captured this token or observed the session ID in a log file, to reuse it to access the application with the privileges of the user associated with the unexpired session token.



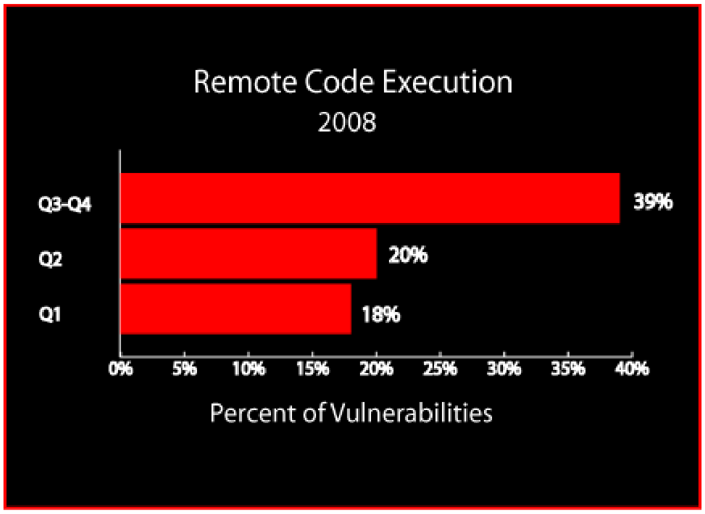
Authorization and Authentication Flaws (41%)

Insufficient authentication occurs when a vulnerability in a Web application allows a user to log in without supplying the correct credentials, such as through the use of a known attack method or by exploiting design flaws. One example of such a condition is a poorly implemented authentication scheme that reveals valid usernames and passwords via brute force methods. Authorization flaws may allow a user to gain access to resources within an application, which should be restricted based on the user's role within the application.



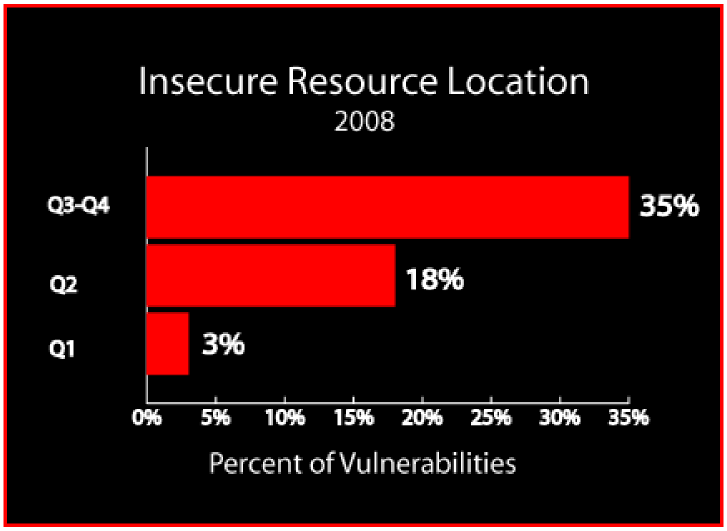
Remote Code Execution (39%)

Buffer Overflows, Integer Overflows, and Format String attacks can give an attacker immediate control over a Web application and its host operating system. In some cases these vulnerabilities may allow an attacker to cause a denial-of-service by crashing the vulnerable Web application.



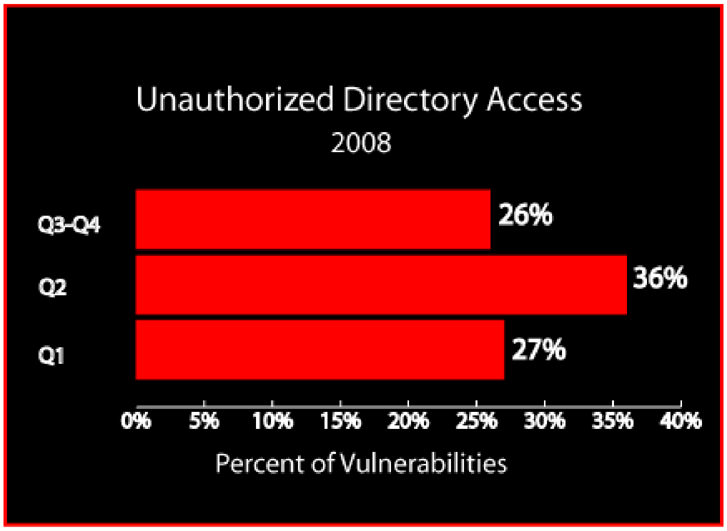
Insecure Resource Location (35%)

Sensitive files or other information may be stored in insecure directories or otherwise exposed to the Internet. Information stored in spreadsheet files, text files, or word documents may be exposed in insecure directories on a Web site. For example, the default configuration of some e-commerce applications stores transaction information, including credit card data in insecure directories.



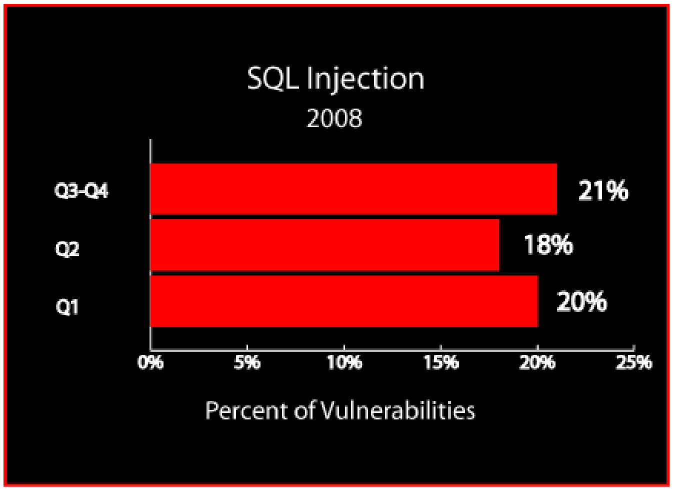
Unauthorized Directory Access (26%)

Insecure permissions on directories can allow an attacker to access areas of a Web site or Web application that should otherwise be protected. In other cases it is possible to directly browse the contents of a directory and enumerate all of the resources it contains. These types of vulnerabilities help an attacker gather information and plan further attacks against a server.



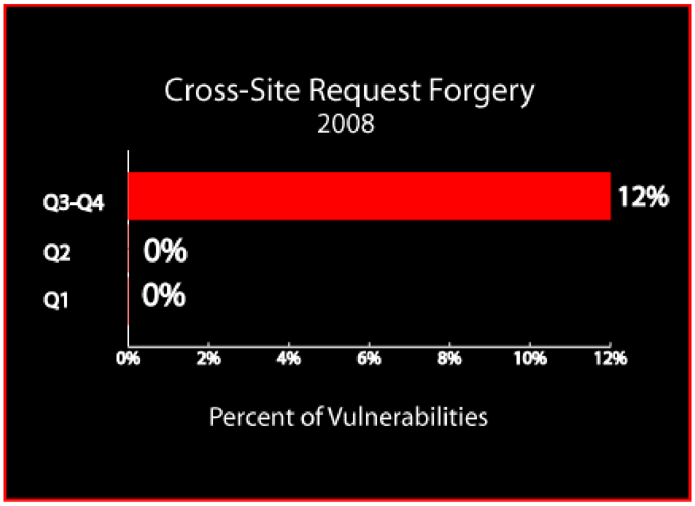
SQL Injection Attacks (21%)

SQL Injection attacks allow an attacker to execute commands on the underlying database of a Web application, gaining access to database contents. In some cases an attacker can use SQL Injection techniques to backdoor the Web application or execute operating system commands.



Cross-Site Request Forgery (12%)

Cross-Site Request Forgery (CSRF) is an attack that tricks the victim into loading a page that contains a malicious request. It is malicious in the sense that it inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf, like change the victim's profile, send an email to third party on his behalf, or purchase something. It exploits the trust a Web site has for the user. This is the first time we are reporting CSRF vulnerabilities as these are starting to become more common so there is no trending data for first half of 2008.



About Cenzic

Winner of numerous 2008 awards including SC Magazine's Best Buy (**http://www.scmagazineus.com/Application-vulnerability-assessment-tools/GroupTest/123/**), and Information Security Magazine's A grade (**http://cenzic.com/downloads/infosec-200901-arc5.7.pdf**), Cenzic is a provider of software and SaaS/Managed Service solutions for Web application security. Cenzic's innovative technology goes beyond signature-based tools to find more "real" vulnerabilities. Cenzic is the only company to provide continuous testing for all Web applications across the SDLC, including ones in production through virtualization. With the most robust attack library, comprehensive reports, and compliance guidance to regulations like PCI, GLBA, HIPAA, OWASP, SANS, and others, Cenzic products have become the favorite choice of large and small corporations, and government agencies.

Cenzic Technology

Cenzic's patented technology goes beyond a signature-based approach by emulating a true hacker with a patent pending Stateful Assessment™ approach that maintains the state of the application while attacking the application at the browser level. This approach allows Cenzic to find all critical vulnerabilities including application logic tests like Session Hijacking, Strong Passwords, Privacy Policy validation, etc. as well as all the core vulnerabilities including XSS, Buffer Overflow and SQL Disclosure. Furthermore, only Cenzic can test for vulnerabilities across all types of applications including commercial and proprietary applications, Web infrastructure and across all stages of a Web application throughout the Software Development Lifecycle (SDLC).

For people who need to manage their risk across multiple applications, we offer a dynamic and intelligent dashboard that allows you to easily and quickly learn how many applications you have, which of those applications have been tested and where the most pressing application vulnerabilities/risks lie. This in turn enables you to prioritize the fixes, allocate resources and input a process into your software development lifecycle for future application development. Role-based deployment and integration to LDAP allows enterprises to deploy the product across all functions with appropriate privileges.

Cenzic's Products

Cenzic's product suite ranges from a software offering (Cenzic Hailstorm® Enterprise ARC™) to its software as service (SaaS) product (Click-to-Secure®) so you can choose which solution best fits your needs. With a Cenzic solution, companies can rely on the most innovative and accurate application security in the industry.

For further information or comments about this report, send an email to **appsectrends@cenzic.com**. For more information on Cenzic, send an email to **request@cenzic.com** or call 1-866-4-CENZIC (866-423-6942).