CENZIC ENTERPRISE APPLICATION SECURITY

Web Application Security Trends Report
Q1-Q2, 2009

Table of Contents

Contributors 3

Executive Summary 4

General Observations 6

Top 10 Vulnerabilities of Q1-Q2 2009 7

Vulnerabilities in Web Applications 10

Vulnerability Breakdown for Q1-Q2 2009 11

Web Browser Vulnerabilities 12

Interesting Web Attacks for First Half of 2009 13

Probe and Attack Data 15

Conclusions and Findings from Cenzic ClickToSecure® 22

Contributors

We'd like to thank everyone who contributed to the Q1-Q2 2009 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 Faul, Inc.
- Erin Swanson, Sr. Director, Product and Strategic Marketing

Key Sources

- Cenzic Intelligent Analysis Lab
- Cenzic ClickToSecure Service
- Mitre
- OWASP
- SANS
- OSVDB
- Symantec
- US-CERT

Executive Summary

What do the Swine flu and hacker attacks have in common? Both are extremely harmful and the Obama administration has recently issued guidelines for protection against both. From Twitter to Facebook, the U.S. Army to Motion Pictures Association, banks to telecom companies, hackers were relentless in the first half of 2009. They exploited all kinds of vulnerabilities including Cross Site Scripting, SQL Injection, Session Management, and ClickJacking. Billions of dollars as well as millions of identities were stolen. What we saw in 2008 only accelerated in 2009 in terms of attacks. The down economy contributed as many former employees, now unemployed are collaborating with hackers to find alternate financial means. Hacking continues to be the only hot career in this economy, with some hackers reportedly making $10K per week tax free.

Our Q1-Q2, 2009 Trends Report once again points out the continued growth of vulnerabilities and increase in attacks through Web applications. The total number of reported vulnerabilities went up to almost 3100, an increase of over 10 percent, and the percentage of Web vulnerabilities continued to be dominate at around 78 percent.

Of the Web vulnerabilities, 90 percent pertained to code in commercial Web applications, while Web browsers comprised about 8 percent and Web servers about 2 percent. Of the browser vulnerabilities, Firefox had 44 percent of the total, but perhaps the biggest surprise was Safari, which formed 35 percent of the browser vulnerabilities. Internet Explorer was third, with 15 percent, and Opera was at 6 percent.

Of the published vulnerabilities in Commercial Off The Shelf (COTS) applications, SQL Injection, and XSS were once again the most common vulnerabilities, which is why, it is no coincidence that most of the attacks in first half exploited these two vulnerabilities. Based on thousands of assessments performed by Cenzic's managed service, nine out 10 applications continue to be vulnerable with Information Leaks, Cross Site Scripting, Authentication Flaws, and Session Management as the most common categories.

The top 10 vulnerabilities for the first half of 2009, included familiar names such as Sun, IBM, SAP, PHP, and Apache.

In terms of progress, a significant number of companies have started testing their Web applications for vulnerabilities. Payment Card Industry (PCI), California AB1950, and other regulations continue to be the driving force behind most of these initiatives. The

Obama administration's continuous outreach and work on this front is also helping educate organizations that cyber security is extremely important to protecting our nation's infrastructure. However, we have a long way to go. Of the 100 million plus Web applications, there are very few that are being secured.

Data breaches can cost more than $500K per breach. According to the Ponemon Institute, the cost of a data breach can be $202 per record. So, even for a small company with 5,000 records, that's over one million dollars. Non-compliance with regulations can put businesses in jeopardy. Hacked sites can scare away consumers and lead them to seek out a competitors' site. And, yet most companies are *not* focusing on securing their Web applications. The main reason continues to be lack of understanding and knowledge. There are many myths around Web security that lead people into a false sense of security. Many IT professionals still believe that having a network firewall, IDS, SSL certificate, etc. will protect them from hackers attacking their Web sites. It's like having locks on your front door but leaving your windows and side doors wide open and hoping that burglars will only try to come through the front door.

Most companies don't realize that information on how to secure your Web applications is easily available. Organizations like OWASP (www.owasp.org) and NIST (www.nist.gov) are doing a great job of educating companies on these issues. Getting a jump start in having your applications tested is very easy with SaaS/managed service solutions.

Government agencies are also launching initiatives to get their Web sites more secure. The Chinese government, per a recent congressional advisory panel, is gearing up Cyberspying efforts against the U.S. We have already seen the use of Cyberwarfare in some cases. Who can forget the North Korean attacks against South Korea and U.S. sites and the frightening suspected attack on the U.S. electrical grid?

Hackers are smart and only getting smarter. They are becoming more organized and well funded by foreign governments or criminal gangs. Attacks will only continue to increase against our Web infrastructure, therefore it is extremely important that all organizations conducting business transactions online, as well as government agencies and education institutions, regardless of their size, start taking these issues a lot more seriously --before it's too late.

Mandeep Khera
Chief Marketing Officer, Cenzic

General Observations

Cenzic analyzed reported vulnerability information for the Q1 and Q2, 2009 (January through June) time period. During this period, Cenzic identified about 3,100 total vulnerabilities. This is an increase of over 10 percent from the second half of 2008 for which we had identified 2835 vulnerabilities. As we have seen over the past few quarters, Web application vulnerabilities continue to make up the largest percentage of the reported vulnerability volume. Web related vulnerabilities comprised roughly 78 percent of all vulnerabilities, down a little from the second half of 2008 but still significantly up from the first half of 2008. We believe that this trend will continue and we will see Web application related vulnerabilities continue to form majority of vulnerabilities. Our key findings from first half of 2009 are listed below:

Key Findings:

- Sun Java, PHP, and Apache continue to be among the Top 10 vendors having the most severe vulnerabilities for the first half of 2009.
- 78 percent of the total reported vulnerabilities affected Web technologies, such as Web servers, applications, Web browsers. Plugins and ActiveX, which is a significant increase from earlier in the year.
- Of the Web vulnerabilities, Web Browser vulnerabilities comprised eight percent of the total vulnerabilities found, and Web servers comprised two percent. Vulnerabilities in the code of commercial Web applications was 90 percent of the total Web related vulnerabilities. Looking at the various classes of vulnerabilities, we found that SQL Injection and Cross Site Scripting (XSS) vulnerabilities continued to dominate with 25 percent and 17 percent respectively. Authorization and Authentication vulnerabilities were higher at about 14 percent of total Web vulnerabilities followed by Directory Traversal at 12 percent.
- Of the browser vulnerabilities, the big surprise was that Firefox at 44 percent had significantly more vulnerabilities than the other browsers. What was also surprising was that Safari vulnerabilities which are usually very low came in at 35 percent, significantly higher than even Internet Explorer which comprised 15 percent of the browser vulnerabilities.
- Based on the vulnerabilities found using Cenzic's managed service, ClickToSecure, Information Leaks, XSS, Authentication and Authorization and Session Management flaws continue to dominate.
- The majority of assessments completed by Cenzic had a high HARM score, highlighting the continuing risk and exposure faced by organizations.

Top 10 Vulnerabilities of Q1-Q2 2009

Cenzic classified the following Web application vulnerabilities disclosed during the first half of 2009 as the most severe. These are not necessarily in any specific order.

1. **phpMyAdmin Configuration File PHP Code Injection Vulnerability**
   An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system; other attacks are also possible.
   CVE-2009-1285

2. **SAP cFolders Cross Site Scripting And HTML Injection Vulnerabilities**
   SAP cFolders are prone to multiple cross-site scripting and HTML-injection vulnerabilities because they fail to sufficiently sanitize user-supplied data. Attacker-supplied HTML or JavaScript code could run in the context of the affected site, potentially allowing the attacker to steal cookie-based authentication credentials and to control how the site is rendered to the user; other attacks are also possible.
   Bugtraq ID – 34658

3. **Sun Java System Access Manager Cross-Domain Controller (CDC) Cross Site Scripting Vulnerability**
   Sun Java System Access Manager is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data.

   An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker steal cookie-based authentication credentials and launch other attacks.
   CVE-2009-2268

4. **Citrix Web Interface Unspecified Cross-Site Scripting Vulnerability**
   Citrix Web Interface is prone to a cross-site scripting vulnerability because the application fails to properly sanitize user-supplied input.

An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may help the attacker steal cookie-based authentication credentials and launch other attacks.
Bugtraq ID – 34761

5. **Sun Java System Web Server Reverse Proxy Plug-in Cross-Site Scripting Vulnerability**
   Sun Java System Web Server is prone to a cross-site scripting vulnerability because the application fails to properly sanitize user-supplied input.

   An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of a site that uses the affected functionality. This may help the attacker steal cookie-based authentication credentials and launch other attacks.
   CVE-2009-1934

6. **Apache Tomcat Form Authentication Existing/Non-Existing Username Enumeration Weakness**
   Apache Tomcat is prone to a username-enumeration weakness because it displays different responses to login attempts, depending on whether or not the username exists.

   Attackers may exploit this weakness to discern valid usernames. This may aid them in brute-force password cracking or other attacks.
   CVE-2009-0580

7. **phpMyAdmin 'setup.php' PHP Code Injection Vulnerability**
   phpMyAdmin is prone to a remote PHP code-injection vulnerability.

   An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system; other attacks are also possible.
   CVE-2009-1151

8. **F5 Networks FirePass SSL VPN 'password' Field Cross-Site Scripting Vulnerability**
   F5 Networks FirePass SSL VPN is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input.

   An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may help the attacker steal cookie-based authentication credentials and launch other attacks.
   CVE-2009-2119

9. **Multiple Symantec Products Log Viewer Multiple Script Injection Vulnerabilities**
   Multiple Symantec products are prone to multiple script-injection vulnerabilities because the applications fail to properly sanitize user-supplied input before using it in dynamically generated content.

   Attacker-supplied script code would run in the context of the affected browser, potentially allowing the attacker to steal cookie-based authentication credentials or to control how the site is rendered to the user. Other attacks are also possible.

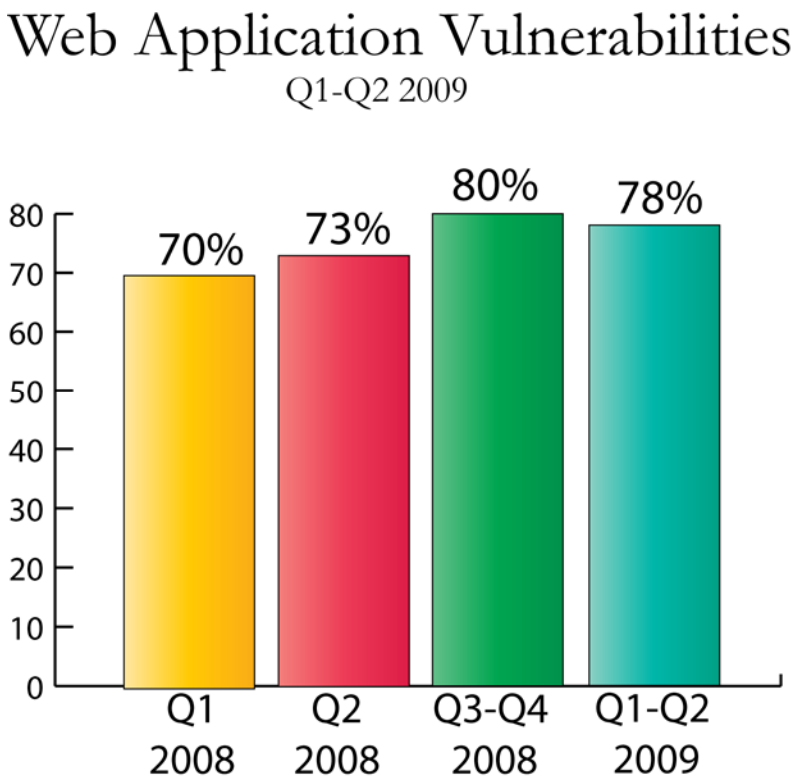
   Attacker-supplied script code would run in the context of the affected browser, potentially allowing the attacker to steal cookie-based authentication credentials or to control how the site is rendered to the user. Other attacks are also possible.
   CVE-2009-1428

10. **IBM Tivoli Identity Manager Multiple Cross Site Scripting Vulnerabilities**
    Tivoli Identity Manager is prone to multiple cross-site scripting vulnerabilities because the application fails to sufficiently sanitize user-supplied data.

    Attacker-supplied HTML or JavaScript code could run in an administrator's browser session in the context of the affected site. This could potentially allow the attacker to steal cookie-based authentication credentials; other attacks are also possible.
    Bugtraq ID – 35566

Vulnerabilities in Web Applications

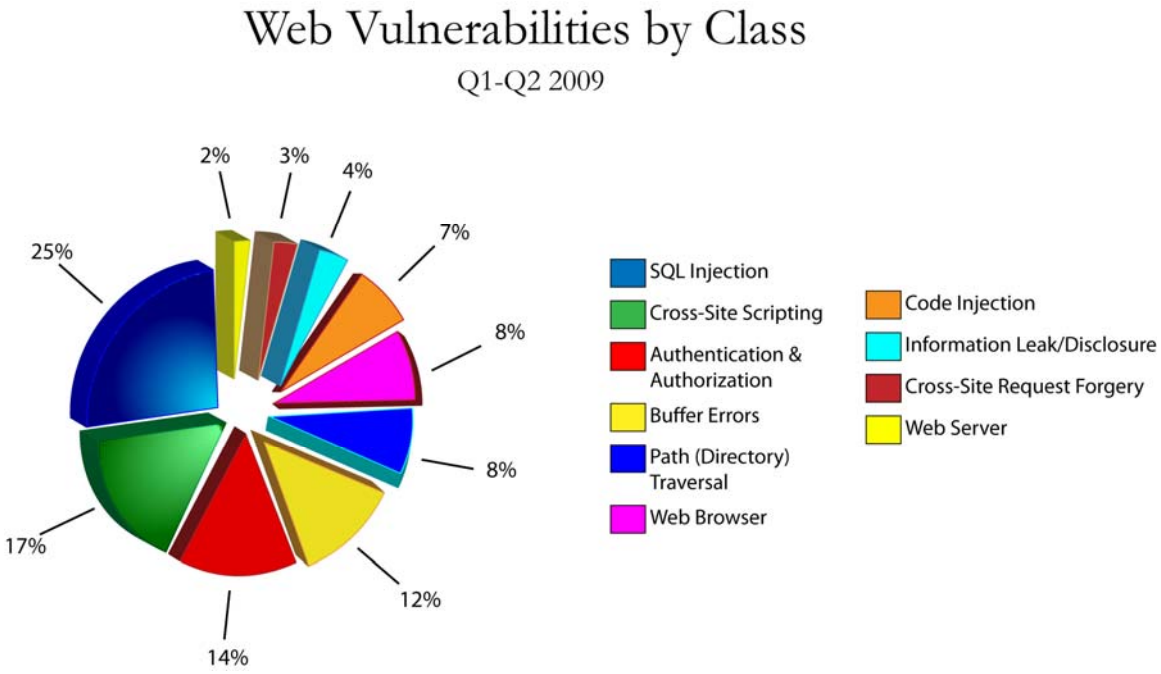
Cenzic analyzed all reported vulnerability information from sources including NIST, MITRE, SANS, US-CERT, OSVDB, as well as other third party databases for Web application security issues reported during the first half of 2009. We looked at specific vulnerabilities associated with Web technologies. Our findings are presented below. Roughly 78 percent of all vulnerabilities pertained to Web applications and related technologies, which is slightly lower than the second half of 2008 but significantly higher than the first part of 2008. These numbers represent the published vulnerabilities of various commercial off the shelf software as well as open source software. There are various types of vulnerabilities that exist in proprietary Web applications whether developed in-house or outsourced to programming firms in India, China, Russia, and other countries.



Vulnerability Breakdown for Q1-Q2 2009

The Q1-Q2 reported vulnerability information reveals that 78 percent of the reported vulnerabilities were in Web applications, slightly lower than the Q3-Q4, 2008 findings. We have analyzed these vulnerabilities based on type and class in more detail below.

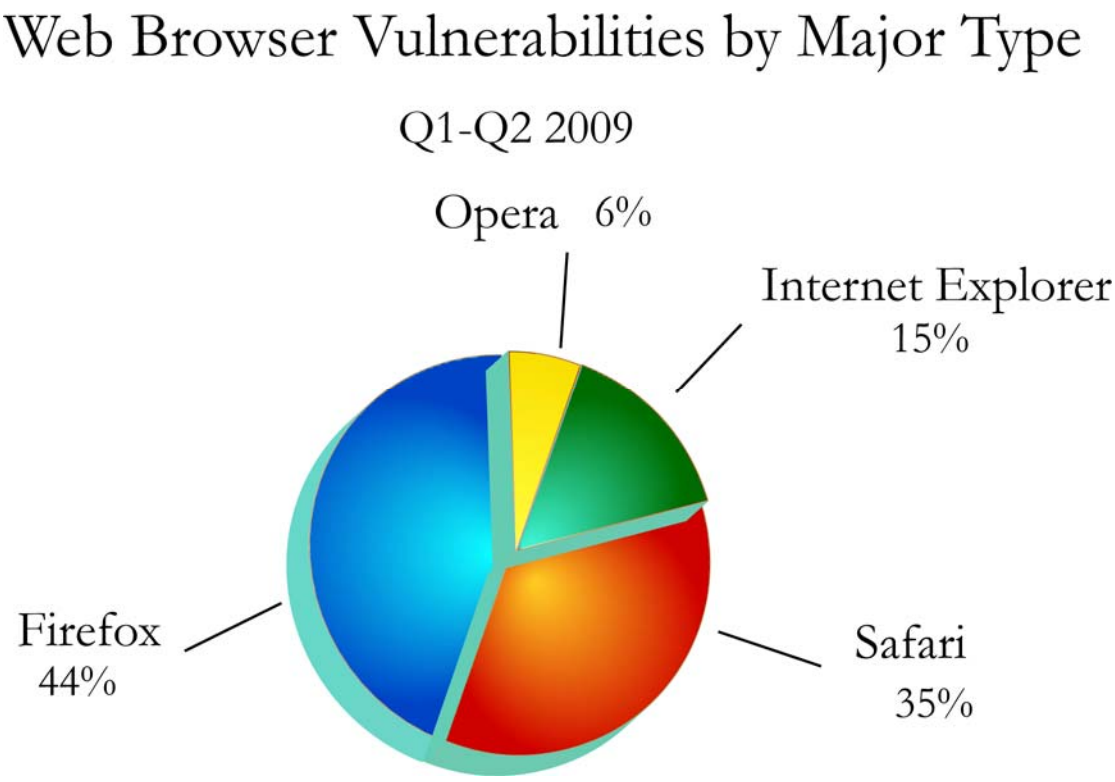
Some critical application-layer injection flaws, such as SQL Injection, and Cross-Site Scripting once again dominated in this report's period as the most frequently found and reported vulnerability classes, and were higher than the second half of 2008. XSS formed 17 percent in this period compared to 14 percent in the last 6 month period, and SQL Injection vulnerabilities formed 25 percent compared to 24 percent in the second half of 2008. Authentication and Authorization related vulnerabilities also jumped, comprising 14 percent of total compared to 5 percent in the previous period.



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.

Web Browser Vulnerabilities

Vulnerabilities in Web browsers were concentrated among four popular technologies - Internet Explorer, Mozilla Firefox, Opera, and Safari. The number of browser vulnerabilities in first half of 2009 comprised about 8 percent of total Web vulnerabilities. Mozilla Firefox had the largest percentage at 44 percent. What was surprising was that the Safari browser had a lot more vulnerabilities at 35 percent this time around mainly due to vulnerabilities reported in iPhone Safari. Internet Explorer was third at 15 percent and Opera with six percent of total browser vulnerabilities.



Interesting Web Attacks for First Half of 2009

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. We believe that for every attack that's reported, there are a hundred more that have gone unnoticed as most companies don't know when they are being hacked. It's evident from some of the highly visible attacks in the last couple of years, that many attacks go unnoticed for months and years before they are caught and even those by accident. Based on reports from SANS, CERT, and other sources, we know that there have been millions of hacking attempts. According to government sources, The Pentagon's computer systems are probed 360 million times a day.

We have listed some of the interesting and visible Web application related attacks from the first half of 2009. These are not in any particular order.

- **UK Communist Website Attacked by Chinese Hackers – June, 2009**
  - Infection by the iFrame-F script. Communist Party's Website infection was invisible to the naked eye. The malicious code was inserted in a file called silverlight.js that served up an iFrame that pointed to a malicious Website in China

- **British Banking and Publishing Sites Hit by XSS – June, 2009**
  - HSBC, and Barclays sites were both hit by major XSS vulnerabilities and The Telegraph site was exposed by a severe SQL injection vulnerability.

- **SQL Injection Exploited in US Army Servers – May, 2009**
  - Exploiting SQL vulnerabilities, Turkish hackers known as "m0sted" caused users to be redirected to a Web page protesting climate change.

- **SQL Injection on Orange France exploited – May, 2009**
  - Uno, the Romanian hacker, exploited a SQL Injection vulnerability in Orange France Web site and accessed 245,000 records.

- **SQL Injection Compromises Thousands of Sites – May, 2009**
  - The attack exploits a SQL injection vulnerability to sneak in malicious javascript onto the front page of Websites. When a user visits one of the compromised sites, the IFRAME silently loads content from the malware-hosting sites. The attack runs through dozens of exploits to attempt to find one to which the user's machine is susceptible. By some accounts, almost 60,000 Web sites were compromised.

- **XSS Vulnerability in Motion Picture Association sites – May, 2009**
  - Vektor, a member of the Team Elite group exploited XSS flaws in MPAA's Web sites to post links from The Pirate Bay. These vulnerabilities allow iFrames from third party servers to be presented to users pretending to come from the site they are visiting.

- **XSS/CSRF Vulnerabilities on Twitter – April, 2009**
  - Mooney Twitter worm (named after Mikeyy Mooney, 17 year old hacker who created StalkDaily.com, a Twitter competitor) was exploited using Cross-Site Scripting and Cross Site Request Forgery vulnerabilities on Twitter.

- **ClickJacking attack on Twitter – February, 2009**
  - Hackers got really creative with this attack by having users click on a link that had an underlying code for installing malware. A ClickJacking vulnerability is exploited by superimposing an invisible iFrame over a genuine link. Users have no idea that they are clicking on the malicious code because they only see the real link.

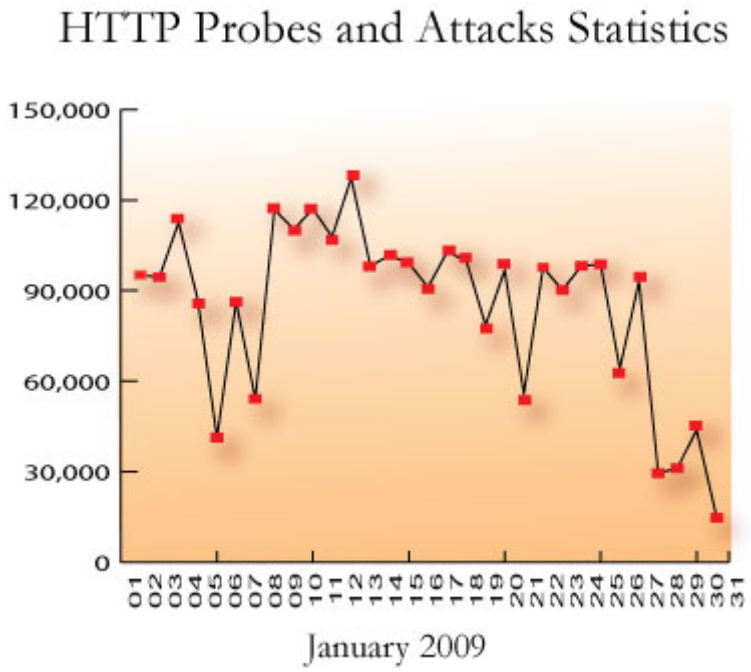
Probe and Attack Data

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 2009 is presented in six graphs and this data is supplemented with security events that may have influenced the probing or attack activity.

January 2009 HTTP Probes and Attacks Statistics

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

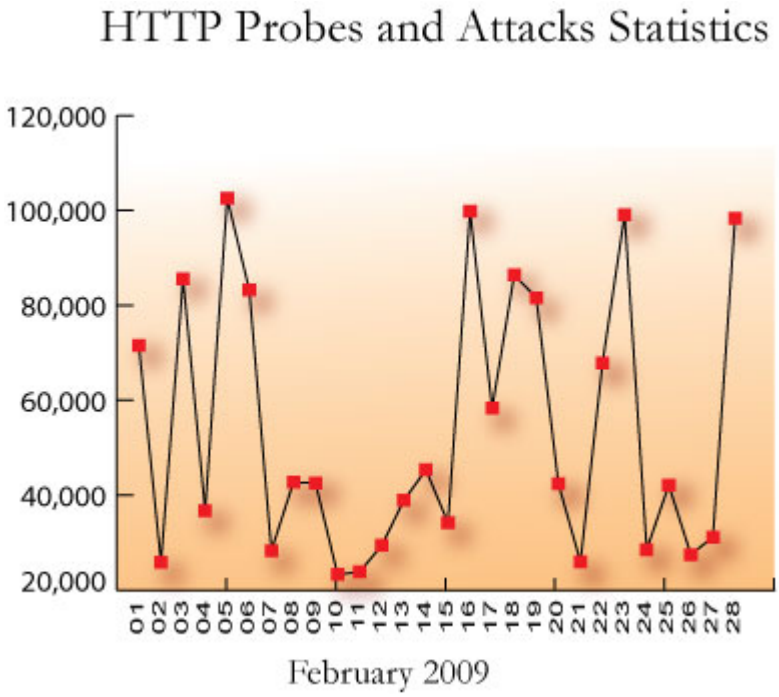


Correlation with Major Vulnerability Data

- 01-13-2009: Microsoft has released updates that address vulnerabilities in Microsoft Windows and Windows Server
- 01-15-2009: Oracle products and components are affected by multiple vulnerabilities. The impacts of these vulnerabilities include remote execution of arbitrary code, information disclosure, and denial of service. [2]
- 01-20-2009: Apple has released QuickTime 7.6 to correct multiple vulnerabilities affecting QuickTime for Mac OS X and Windows. Attackers may be able to exploit these vulnerabilities to execute arbitrary code or cause a denial of service.

February 2009 HTTP Probes and Attacks Statistics

Attack activity in February was the strongest in the beginning and toward the end of the month. Bursts of attacks close to 100,000 attacks per day occurred a handful of times.

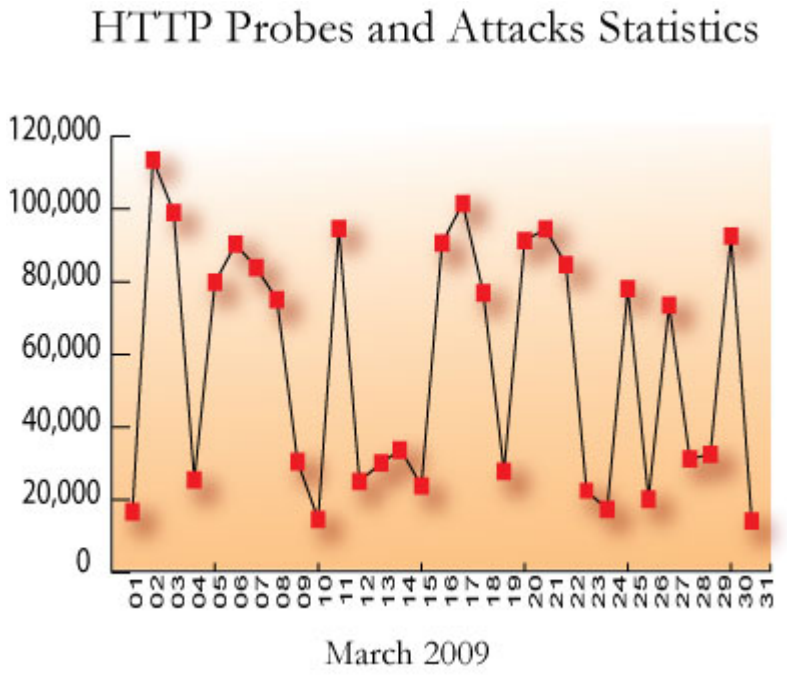


Correlation with Major Vulnerability Data

- 02-13-2009: Microsoft has released updates that address vulnerabilities in Microsoft Windows and Windows Server.
- 02-21-2009: Adobe has released Security Advisory APSA09-01, which describes a buffer overflow vulnerability that occurs when Adobe Reader and Acrobat handle files with specially crafted JBIG2 streams. This vulnerability could allow a remote attacker to execute arbitrary code.

March 2009 HTTP Probes and Attacks Statistics

Attack activity in March was strong throughout the month with many bursts of attacks over 100,000 per day, occurring a handful of times.

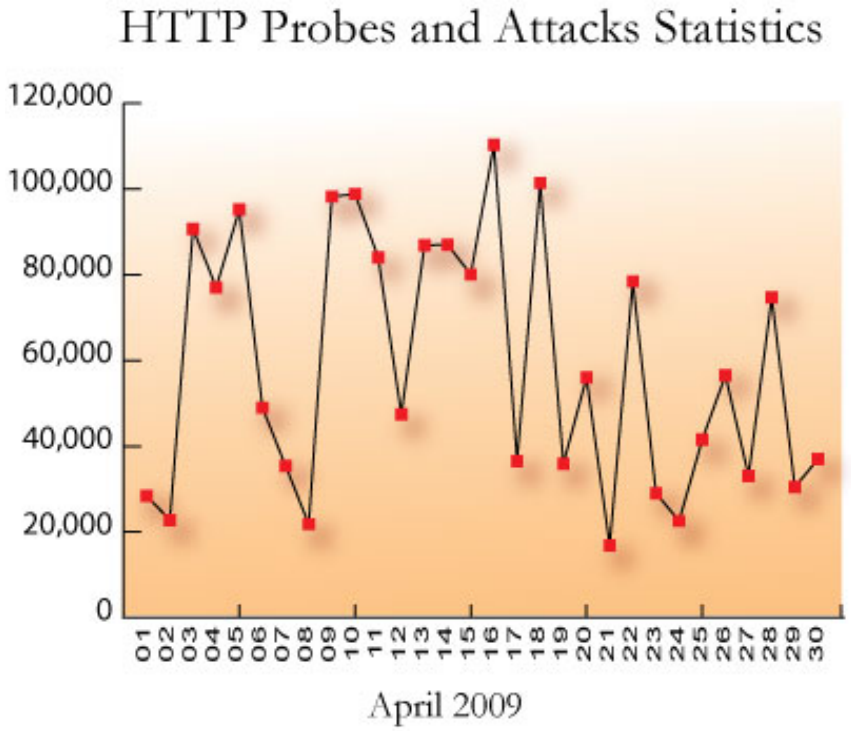


Correlation with Major Vulnerability Data

- 03-10-2009: Microsoft has released updates that address vulnerabilities in Microsoft Windows and Windows Server.
- 03-29-2009: US-CERT is aware of public reports indicating a widespread infection of the Conficker/Downadup worm, which can infect a Microsoft Windows system from a thumb drive, a network share or directly across a corporate network, if the network servers are not patched with the MS08-067 patch from Microsoft.

April 2009 HTTP Probes and Attacks Statistics

Attack activity in April was moderate throughout the month with a few bursts of attacks over 100,000 per day.

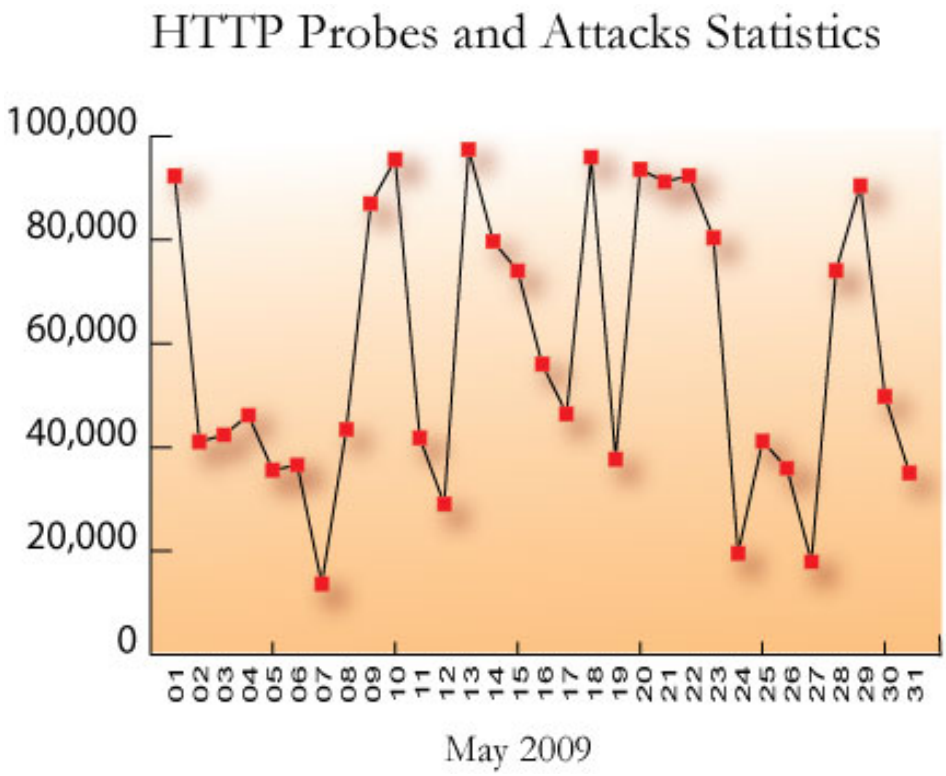


Correlation with Major Vulnerability Data

- 04-14-2009: Microsoft has released updates that address vulnerabilities in Microsoft Windows, Office, Windows Server, and ISA Server.
- 04-15-2009: Oracle products and components are affected by multiple vulnerabilities. The impacts of these vulnerabilities include remote execution of arbitrary code, information disclosure, and denial of service.

May 2009 HTTP Probes and Attacks Statistics

Attack activity in May was moderate throughout the month.

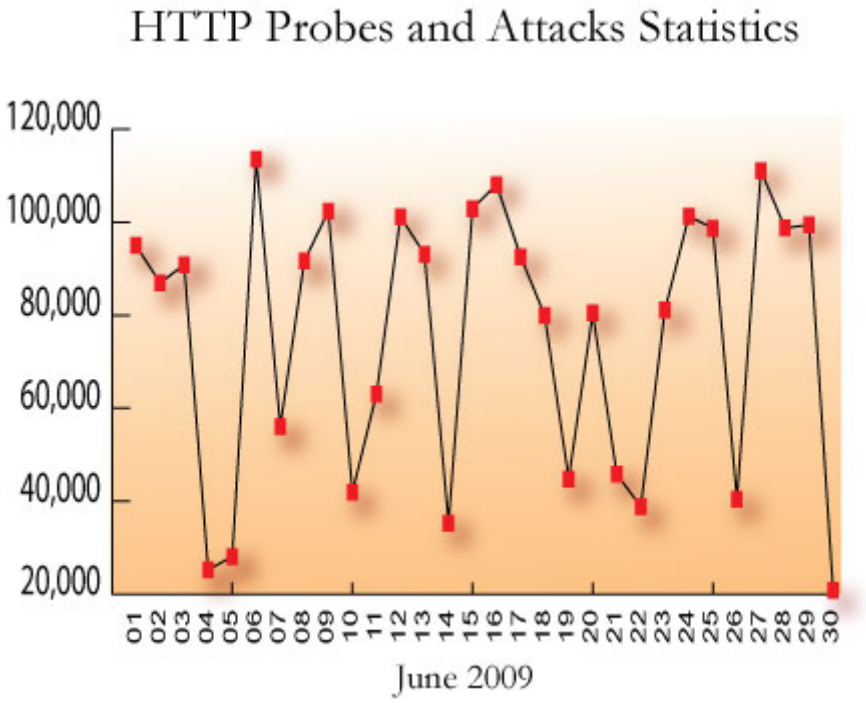


Correlation with Major Vulnerability Data

- 05-12 -2009: Microsoft has released updates that address vulnerabilities in Microsoft PowerPoint.
- 05-13-2009: Apple has released multiple Security Updates, 2009-002 / Mac OS X version 10.5.7 and Safari 3.2.3, to correct multiple vulnerabilities affecting Apple Mac OS X , Mac OS X Server, and the Safari web browser. Attackers could exploit these vulnerabilities to execute arbitrary code, gain access to sensitive information, or cause a denial of service.

June 2009 HTTP Probes and Attacks Statistics

Attack activity in June was strong throughout the month with a few bursts of attacks over 100,000 per day.



Correlation with Major Vulnerability Data

- 06-9-2009: Microsoft has released updates that address vulnerabilities in Microsoft PowerPoint.
- 06-10-2009: Adobe has released Security Bulletin APSB09-07, which describes several buffer overflow vulnerabilities that could allow a remote attacker to execute arbitrary code.

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 managed service in addition to the on-premise software to allow them the flexibility of increasing their coverage without adding resources.

During the first half of 2009, 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 Q1-Q2 2009 findings are consistent the findings revealed for the last couple of years with a few minor differences. Cenzic found that almost nine out of 10 or 90 percent of the analyzed Web applications had serious vulnerabilities that could potentially lead to the exposure of sensitive or confidential user information during transactions.

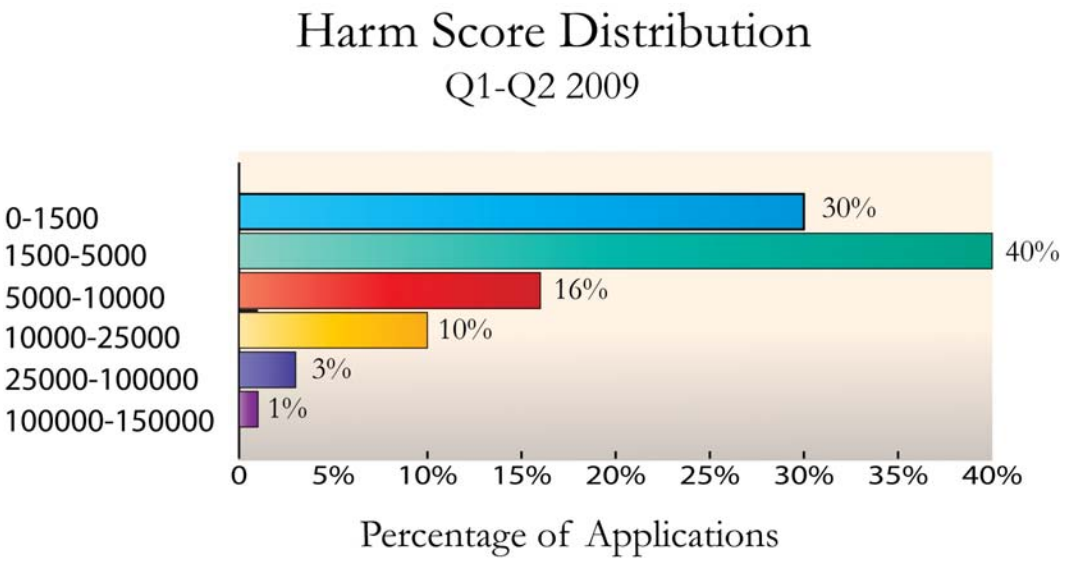
Similar to the previous quarters, Information Leaks and Exposures were the most prevalent vulnerabilities. In general, many types of insecure communications observed were forms that cached sensitive user information, passwords submitted without utilizing SSL for encryption, cases where sensitive information 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 seven out of 10 Web applications. Additionally, Session Management, Authorization and Authentication, and Remote Code Execution were very common vulnerabilities found in our testing.

For the first time in this report, we are also showing the Cenzic HARM score, which is a quantitative score, across all assessments. Most sites have a very high HARM score signifying seriousness of these issues across the board.

HARM Score

HARM stands for Hailstorm Application Risk Metric and is the industry's only quantitative score to identify the severity of vulnerabilities in applications. It takes into account several variables like severity of the vulnerability, probability of getting attacked, and importance of the Web application to the organization. Cenzic's software customers can configure this algorithm to their environment. Normally, a HARM score less than 1500 is considered very good. As is evident from the chart below, most organizations have HARM scores much higher than 1500 and if unfixed can result in major risk exposures for companies. The HARM score allows Cenzic customers to prioritize their remediation efforts.

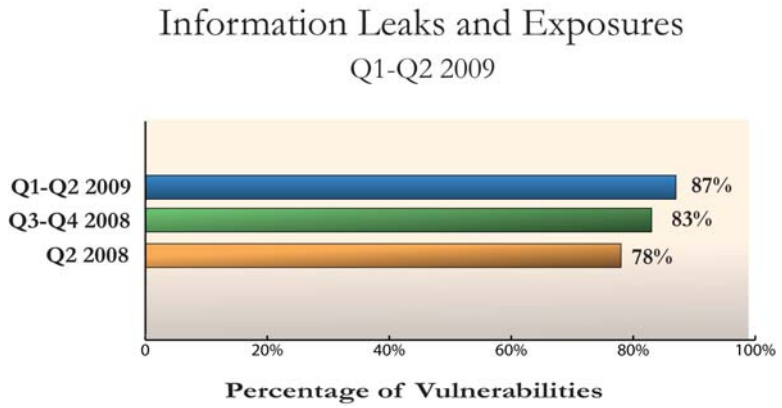


Vulnerabilities Breakdown

Cenzic ClickToSecure found the following percentages of sites with vulnerabilities as belonging to each of the categories below during Q1-Q2 2009. From the data gathered, several vulnerability types were found to be prevalent within the Web applications assessed. The subsections show a comparison between the Q1-Q2 2009 data and previous quarters going back twelve months.

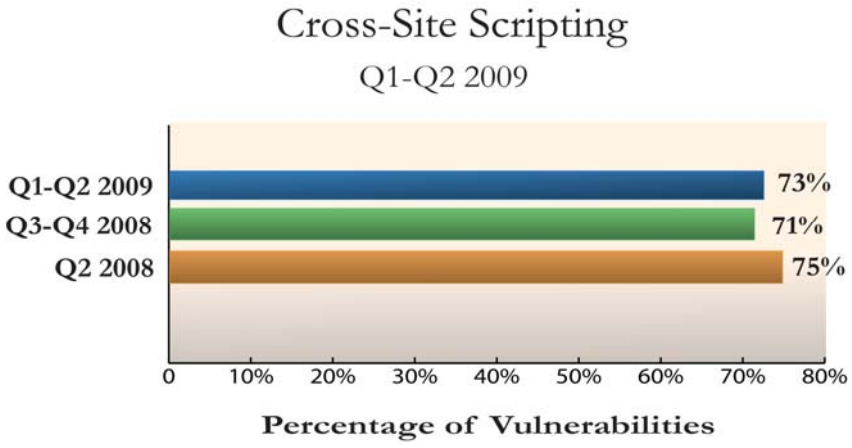
Information Leaks and Exposures (87%)

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. In the first half of 2009, we saw the highest percentage of applications with these vulnerabilities since we have been tracking these numbers.



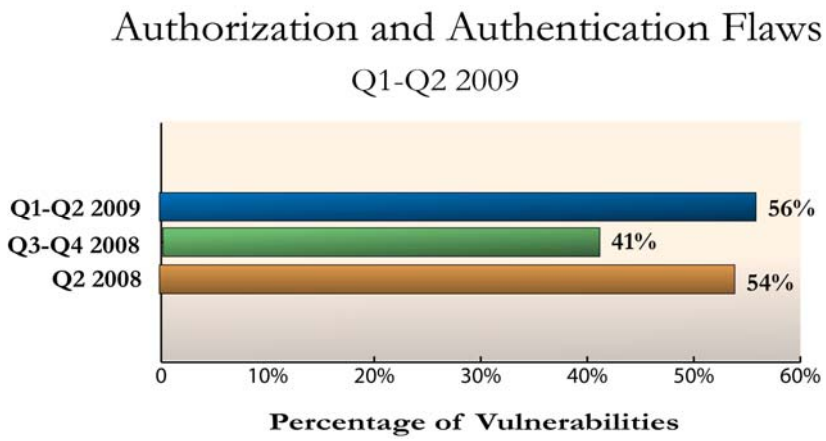
Cross-Site Scripting (73%)

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. In this period, XSS vulnerabilities were pretty close to what we had seen in the previous quarters.



Authorization and Authentication Flaws (56%)

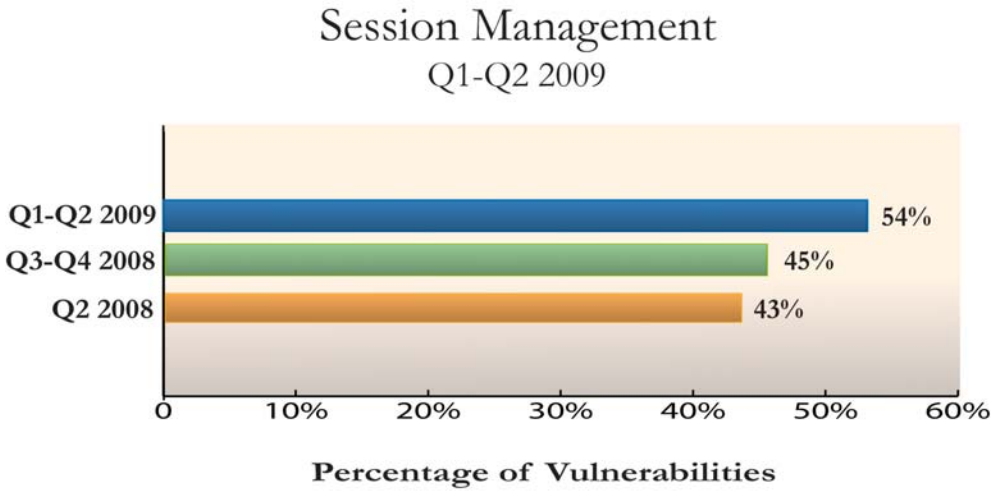
Insufficient authentication occurs when a vulnerability in a Web application allows a user to log in without supplying the correct credentials, such as through the use of a known attack method or by exploiting design flaws. One example of such a condition is a poorly implemented authentication scheme 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. Applications with this vulnerability saw a jump from the previous period.



Session Management (54%)

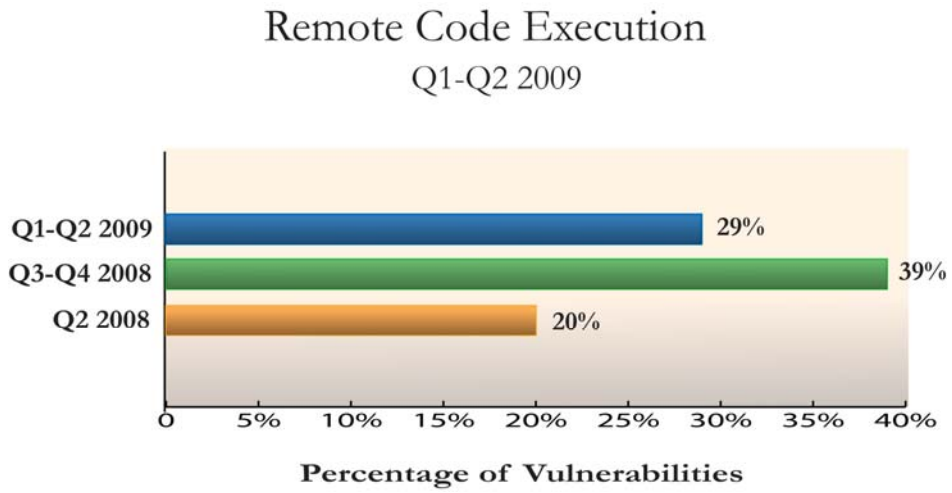
Web applications manage user sessions for the purpose of tracking a user's state and position within a Web application. Vulnerabilities in session management can allow an attacker to take over a user's session by guessing a valid session ID or session token, or by reusing session IDs cached by intermediate 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.

We saw number of applications with Session Management vulnerabilities go up significantly in this period.



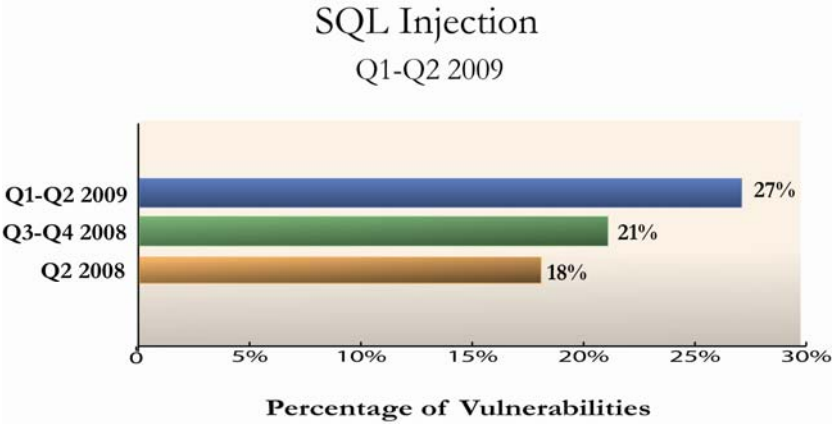
Remote Code Execution (29%)

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. We saw a decline in applications with this vulnerability.



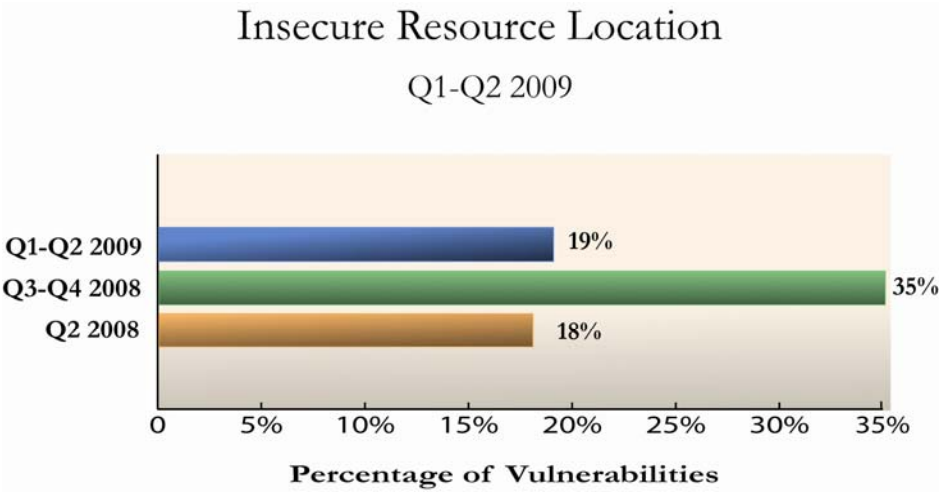
SQL Injection Attacks (27%)

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. We saw a significant jump in applications with SQL injection vulnerabilities.



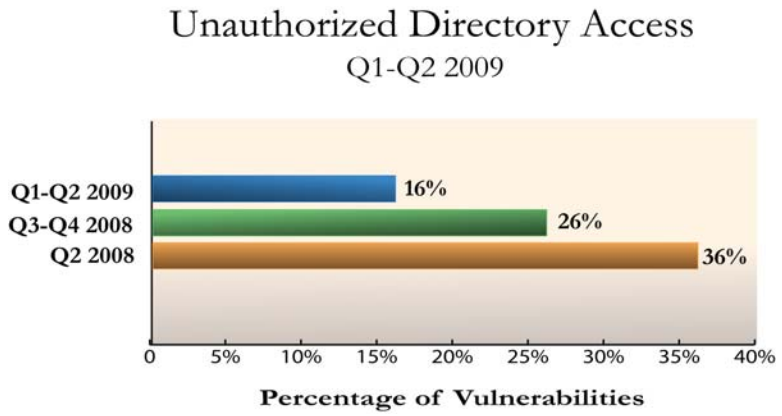
Insecure Resource Location (19%)

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. We saw a decline in applications with this vulnerability.



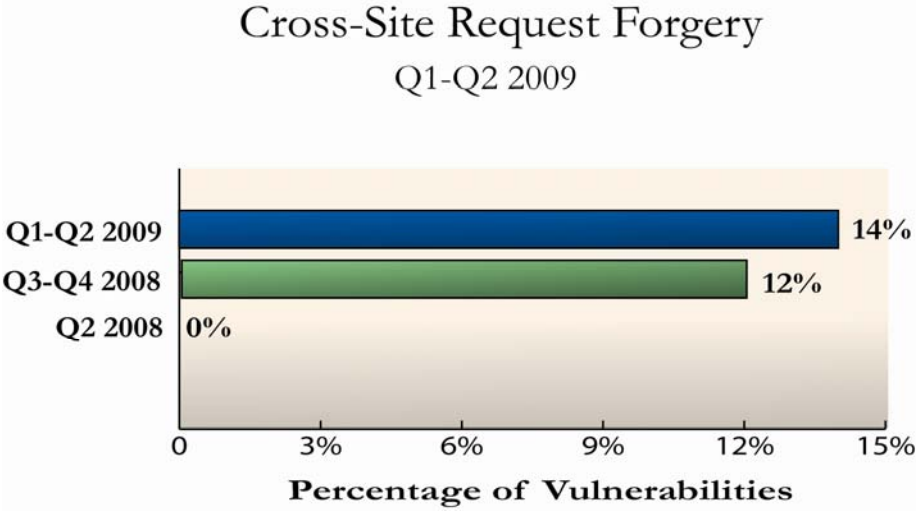
Unauthorized Directory Access (18%)

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. We saw a decline in applications with this vulnerability.



Cross-Site Request Forgery (14%)

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. We saw a slight increase in applications with this vulnerability.



About Cenzic

Cenzic provides **software** and **SaaS** products to protect Websites against hacker attacks. Unlike network security and SSL solutions, Cenzic tests for security defects at the Web application level where over 75% of attacks occur. Our dynamic, black box testing of Web applications is built on a non-signature-based technology that enables us to find more "real" vulnerabilities.

Cenzic Product Suite

Software	SaaS	Professional Services
Hailstorm Enterprise ARC Flagship product for securing applications, accessible over the Web and used by the entire organization.	**ClickToSecure** SaaS / managed service that tests Websites remotely. Ideal solution for limited budget and resources. No software. No hardware. No installation. Just fast results.	**Assessment Methodology** Get an assessment of your security processes in just 3 days from Cenzic's security experts.
Hailstorm Professional Desktop software product for the power user that tests Website security.		**Training** Product & application security training including best practices.

Hybrid
Hybrid Model Combination of both software and SaaS / managed service offerings. Use the software to perform your own vulnerability assessments, and leverage Cenzic's security experts to run additional tests when volume increases.

Awards

- Tomorrow's Technology Today Award (Info Security Products Guide)
- Top Hot Companies Award (Network Products Guide)
- Best Buy Award (Information Security Magazine)
- Global Excellence Award Winner (Info Security Product Guide)

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).