



Web Application Security Trends Report Q1-Q2, 2010

Proprietary Notice

The information in this document is the property of Cenzic, Inc. and cannot be reproduced or redistributed for commercial purposes, without prior written consent from Cenzic, Inc. except as specified below.

We encourage you to share this report with others via linking or attribution. Information can also be used in any articles – online or print, whitepapers, or journals when cited with the following attribution Source: Cenzic Web Application Security Trends Report – Q1-Q2, 2010, Cenzic Inc.

© Copyright 2010 Cenzic, Inc.

Table of Contents

Contributors.....	3
Executive Summary	4
Top 10 Vulnerabilities of Q1-Q2, 2010.....	6
Vulnerabilities in Web Applications for Q1-Q2, 2010	7
Vulnerability Breakdown.....	9
Web Browser Vulnerabilities	11
Detailed Trends from Enterprise Proprietary Applications	13
Interesting Web Attacks for Q1-Q2, 2010	19
About Cenzic.....	21

Contributors

We'd like to thank everyone who contributed to the Q1-Q2, 2010 Trends Report.

Project Lead and Writer

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

Executive Editor

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

Additional Contributors

- Sameer Dixit, Cenzic ClickToSecure
- Strategic Data Command
- Kulesa Faul, Inc.
- Erin Swanson, Sr. Director, Product and Strategic Marketing

Key Sources

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

Executive Summary

Russian, Turkish, Iranian, Chinese, and other International hacker groups joined the ranks of various U.S. hacker organizations to cause havoc across many websites across the globe – most through websites exploiting vulnerabilities in Web applications during the first half of 2010. While there were many well publicized attacks, our estimate is that thousands of attacks probably stayed in the stealth mode where companies had no clue they had been infiltrated. Some of the interesting attacks during this period included exploitation of a SQL vulnerability to plant malware on over 100,000 pages, a session vulnerability attack leading to exposure of information of over 100,000 iPad users including the White House, exposure of 168,000 Netherlands travelers information, hacking of 100 cars through the Web, hacking of Baidu by the Iranian Cyber Army and many other attacks against commercial corporations, and government agencies. While the organized hackers are getting more sophisticated with their techniques, new hackers are finding it an easy play especially with crimerware kits like Zeus readily available, shortening their learning curve.

The Cenzic Q1-Q2, 2010 Trends Report saw a reduction in Web application related vulnerabilities as a percentage of total reported vulnerabilities in commercial products. Web vulnerabilities were at about 66 percent of total reported vulnerabilities of 4,019 that included Web, network and other infrastructure vulnerabilities. The good news is that this is a positive trend compared to second half of 2009 when Web related vulnerabilities comprised 82 percent of total vulnerabilities. However the bad news is that in absolute terms there were 2,645 Web vulnerabilities, almost identical to the previous period. More concerning is that 60 percent of these vulnerabilities still have no known fix available. Even more troubling, about 45 percent of the Web vulnerabilities have an exploit code publicly available which means any hacker can easily look it up and use it to attack Websites that have not patched these vulnerabilities. And, making it worse, almost 1000 Web related vulnerabilities that had no known solution had a public exploit available.

Among the published Web vulnerabilities in Commercial Off The Shelf (COTS) software, Cross Site Scripting and SQL Injection again topped the list with 28 percent and 20 percent respectively. These types of vulnerabilities have been known for a long time and it's extremely surprising that software companies continue to have these in spite of all the publicity, education, and known attacks that have exploited XSS and SQL vulnerabilities. Even some very large software vendors continue to report these two vulnerability types.

We also looked at the vulnerabilities in proprietary Web applications (developed by companies in-house either using internal resources or outsourced development organizations) that were assessed using Cenzic's managed service offering. We found Information Leaks vulnerabilities comprised the most at 49 percent followed by Authorization and Authentication at 21 percent and Cross Site Scripting at 16 percent. SQL Injection vulnerabilities came in low at 2 percent.

Once again, we observed that over 90 percent of all the proprietary applications we assessed were vulnerable with at least Information Leaks types of vulnerabilities. 80 percent of the applications had Authorization and Authentication vulnerabilities followed by Cross Site Scripting and Session Management vulnerabilities which were found in 68 percent of the applications.

As in the previous periods, we also looked at vulnerabilities in various browsers. Both Internet Explorer and Mozilla Firefox showed improvements in reported vulnerabilities. IE had 40 vulnerabilities compared to 44 in the second half of 2009 and Firefox went down to 59 compared to 77 in the previous six months. What was unexpected was the dramatic increase in vulnerabilities in Apple's Safari that soared from 25 in the previous period to 83 in this period and Google Chrome which jumped to 69 from 25 in the second half of 2009. Opera also saw an increase but continue to have the least number of vulnerabilities among browsers. The spike in Safari and Chrome vulnerabilities can be attributed to vulnerabilities in the rendering engine shared by both called WebKit as well as iPhone and Droid related vulnerabilities. We want to acknowledge the tremendous work that all browsers have done in fixing these vulnerabilities quickly. Patching ranged from 78 percent to 92 percent depending on the browser.

We have also identified the Top 10 vulnerabilities for the first half of 2010 based on severity levels and impact of an exploit. These include a lot of the big players including Oracle, Microsoft, Cisco, and Adobe, Apple, and a few small ones.

We have also highlighted some of the interesting Web level attacks that took place in the first half of 2010. Most of the attacks continue to be either financially driven or politically motivated. Most organizations being hacked have no clue that they are actually being hacked. For every attack that is reported, there are hundreds of attacks that are not being reported. Billions of dollars' worth of damage is being caused by hackers every year through Website attacks. The trend is not likely to slow down. And, the worst is yet to come.

While more software vendors are getting conscientious about building security in the Software Development Lifecycle (SDLC), there's still much more work that needs to be done. With over 100 million Web applications out there, and over 95 percent still vulnerable, it's a long road ahead. Most organizations still haven't updated their applications to the available patches and with thousands of new vulnerabilities every year they'll continue to fall behind. Of course, one segment of the population likes this scenario. Hackers know their future is secure for a while. They are constantly circling in the virtual skies waiting for the right opportunity. And, it's not "if" but "when" will you get hacked. It's a lottery of the wrong kind.

Mandeep Khara
Chief Marketing Officer, Cenzic

Top 10 Vulnerabilities of Q1-Q2, 2010

Cenzic classified the following Web application vulnerabilities disclosed during the first half of 2010 as the most severe. These are not listed in any specific order.

1. Oracle Java Deployment Toolkit Java Web Start Argument Injection Arbitrary Program Execution

An unspecified vulnerability in the Java Deployment Toolkit component in Oracle Java SE and Java for Business JDK and JRE 6 Update 10 through 19 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.
CVE-2010-0886

2. TANDBERG Video Communication Server Admin Web Console secure.php Crafted HTTP

The administrative web console on the TANDBERG Video Communication Server (VCS) before X4.3 uses predictable session cookies in (1) tandberg/web/lib/secure.php and (2) tandberg/web/user/lib/secure.php, which makes it easier for remote attackers to bypass authentication, and execute arbitrary code by loading a custom software update, via a crafted "Cookie: tandberg_login=" HTTP header.
CVE-2009-4509; CWE-94

3. Cisco Digital Media Player Unspecified Remote Display Content Injection

Unspecified vulnerability on the Cisco Digital Media Player before 5.2 allows remote attackers to hijack the source of (1) video or (2) data for a display via unknown vectors, related to a "content injection" issue, aka Bug ID CSCtc46024.
CVE-2010-0573

4. Microsoft IE Dynamic OBJECT Tag Cross-domain Arbitrary File Access

Microsoft Internet Explorer 5.01 SP4, 6, 6 SP1, 7, and 8 does not prevent rendering of non-HTML local files as HTML documents, which allows remote attackers to bypass intended access restrictions and read arbitrary files via vectors involving JavaScript exploit code that constructs a reference to a file:///127.0.0.1 URL, aka the dynamic OBJECT tag vulnerability, as demonstrated by obtaining the data from an index.dat file, a variant of CVE-2009-1140 and related to CVE-2008-1448. An attack would involve malicious web content navigating a victim's browser to a UNC path referencing index.dat on the local filesystem. Script planted within index.dat would then be able to read data from other local files on the machine. The attacker could then access files in predictable paths assuming the files were not locked for read or otherwise inaccessible. Allows remote attackers to bypass the Same Origin Policy.
CVE-2010-0255; CWE-264

5. Linksys WAP54Gv3 firmware

Linksys WAP54Gv3 firmware 3.04.03 and earlier allows remote attackers to execute arbitrary commands via shell metacharacters in the (1) data2 and (2) data3 parameters to (a) Debug_command_page.asp and (b) debug.cgi.
CVE-2010-0255; CWE-264

6. Joomanager Component for Joomla! index.php catid Parameter SQL Injection

Joomanager Component for Joomla! contains a flaw that may allow an attacker to carry out an SQL injection attack. The issue is due to the 'index.php' script not properly sanitizing user-supplied input to the 'catid' parameter. This may allow an attacker to inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data.

CVE-2010-2622; CWE-89

7. Newsfeeds Component for Joomla

Newsfeeds Component for Joomla! contains a flaw that may allow an attacker to carry out an SQL injection attack. The issue is due to the 'index.php' script not properly sanitizing user-supplied input to the 'feedid' parameter. This may allow an attacker to inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data.

CVE-2010-1739; CWE-89

8. Stack-based buffer overflow in the WebDAV implementation in webservd in Sun Java System Web Server

Stack-based buffer overflow in the WebDAV implementation in webservd in Sun Java System Web Server (aka SJWS) 7.0 Update 7 allows remote attackers to cause a denial of service (daemon crash) and possibly have unspecified other impact via a long URI in an HTTP OPTIONS request.

CVE-2010-0361; CWE-119

9. Use-after-free vulnerability in Adobe Flash Player 6.0.79

Use-after-free vulnerability in Adobe Flash Player 6.0.79, as distributed in Microsoft Windows XP SP2 and SP3, allows remote attackers to execute arbitrary code by unloading a Flash object that is currently being accessed by a script, leading to memory corruption, aka a "Movie Unloading Vulnerability."

CVE-2010-0378

10. Safari on Apple iPhone OS 3.1.3 for iPod touch allows remote attackers to cause a denial of service (application crash)

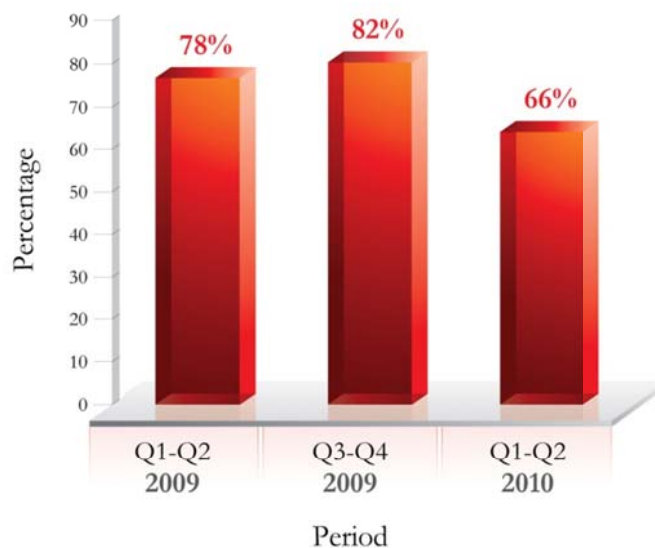
Safari on Apple iPhone OS 3.1.3 for iPod touch allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors involving document.write calls with long crafted strings.

CVE-2010-1177; CWE-94

Vulnerabilities in Web Applications for Q1-Q2, 2010

Cenzic analyzed all reported vulnerability information from various sources including MITRE, NVD, OSVDB, Security Focus, Security Tracker, as well as other third party databases for Web application security issues reported during the first half of 2010. We looked at the total vulnerabilities and vulnerabilities specifically associated with Web technologies. For this period, roughly 66 percent of all vulnerabilities pertained to Web applications and related technologies, which is lower than the last two periods, albeit still very high. 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. We have shown the breakdown of vulnerabilities in proprietary applications further down in this report.

Web Application Vulnerabilities
(as a percentage of total)

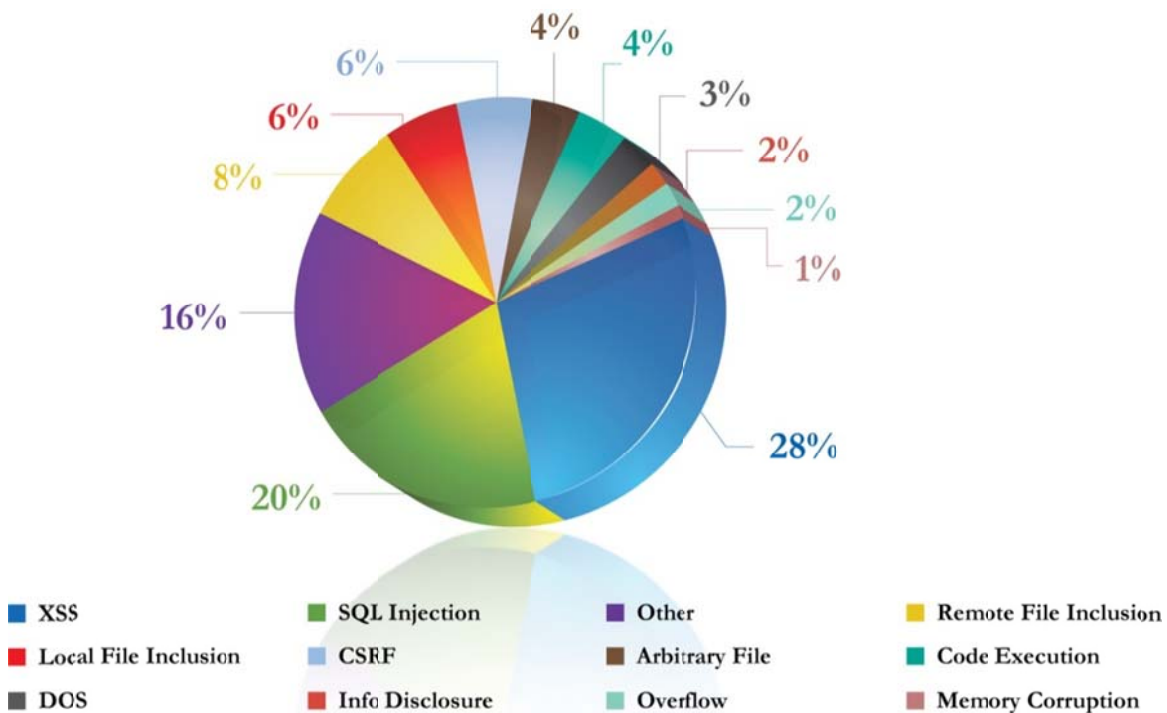


Vulnerability Breakdown

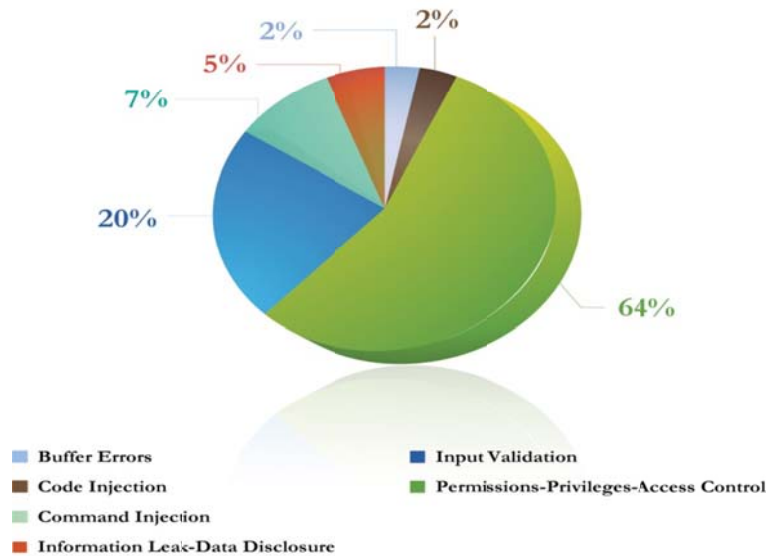
The Q1-Q2 2010 reported vulnerability information reveals that 66 percent of the reported vulnerabilities were in Web applications. We have analyzed these vulnerabilities based on type and class in more detail below.

Once again, critical application-layer injection flaws, such as Cross Site Scripting (XSS), and SQL Injection, continue to dominate. Cross Site Scripting jumped to 28 percent of total Web vulnerabilities, one of the highest percentages ever and significantly higher than 19 percent in the second half of 2009. SQL Injection was also higher at 20 percent compared to 16 percent in the second half of 2009. These high numbers are surprising since these two vulnerability types have been known for a while and even some of the largest commercial software vendors had these types of vulnerabilities. Remote File Inclusion, Local File Inclusion, and CSRF were some of the other ones that comprised a reasonable percentage of the total. We have also broken down below the miscellaneous category, which comprised 16 percent of total Web vulnerabilities and includes other vulnerabilities like Information Leaks, Authentication, and Command Injection etc.

Web Vulnerabilities by Class (commercial applications)

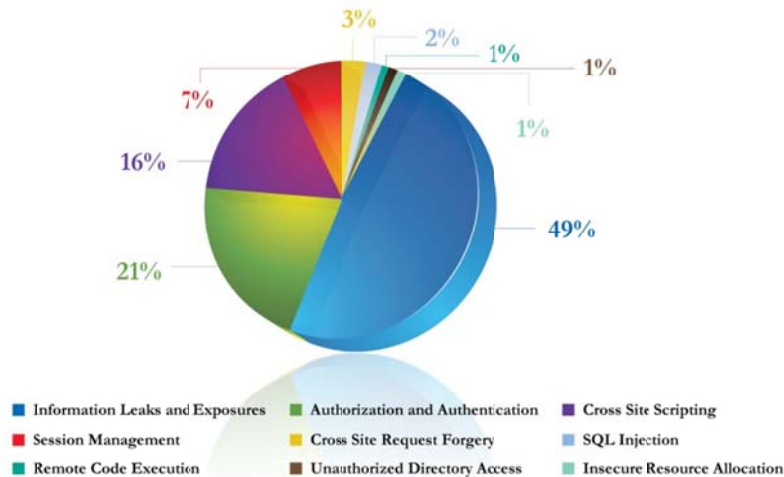


Web App Other Category



Vulnerability percentages mentioned above 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 below.

Web Vulnerabilities by Class (proprietary applications)

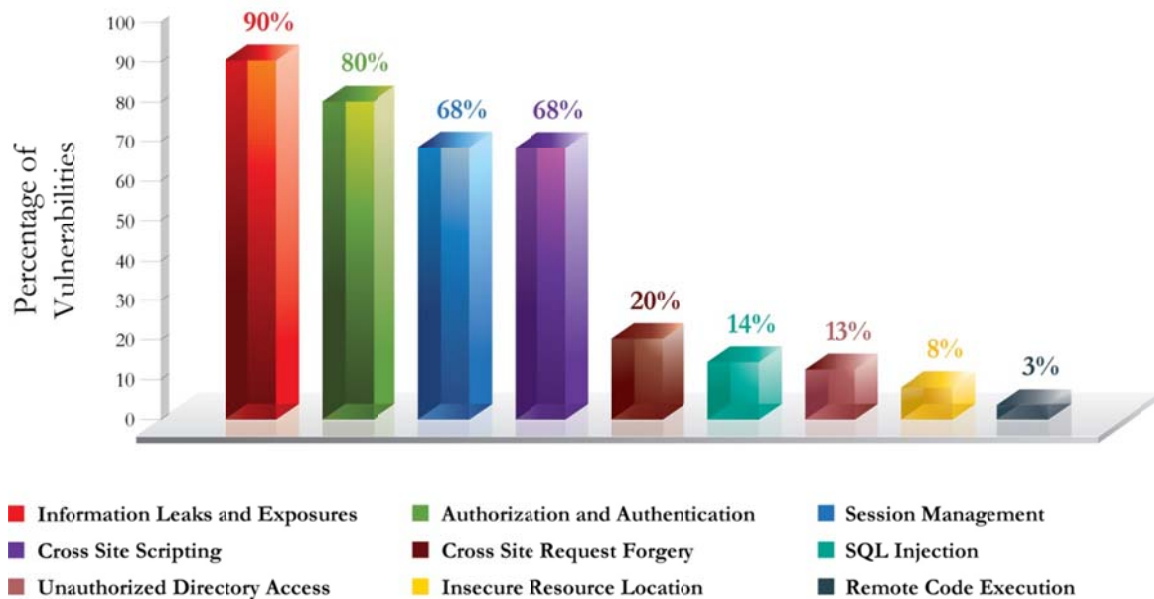


These findings in the chart above are from assessment of actual Web applications that are proprietary, from ClickToSecure Managed, Cenzic's managed service involving remote assessments performed by Cenzic experts for the customers using Cenzic products. Trends of individual vulnerabilities for proprietary applications are provided in

the last section of the report. The largest number of vulnerabilities is in the Information Leaks category at 49 percent which includes vulnerabilities like Application Exception, HTML/Javascript comments etc. Authorization and Authentication is the second highest category with 21 percent followed by Cross site scripting vulnerabilities comprising 16 percent.

Another way to look at the state of applications is by reviewing the percentage of applications that are susceptible to specific vulnerability types. The chart below shows that over 90 percent of applications are vulnerable to Information Leaks and Exposures. Hackers can use this information to come up with attack plans. Authorization and Authentication vulnerabilities were found in 80 percent of the applications, Session Management and Cross Site Scripting vulnerabilities in 68 percent of the applications.

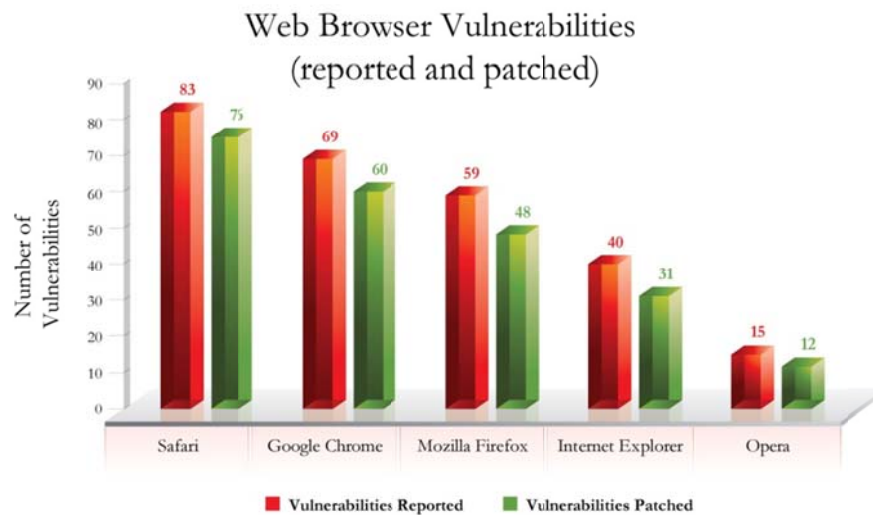
Percentage of Applications with Vulnerability Type
(proprietary applications)



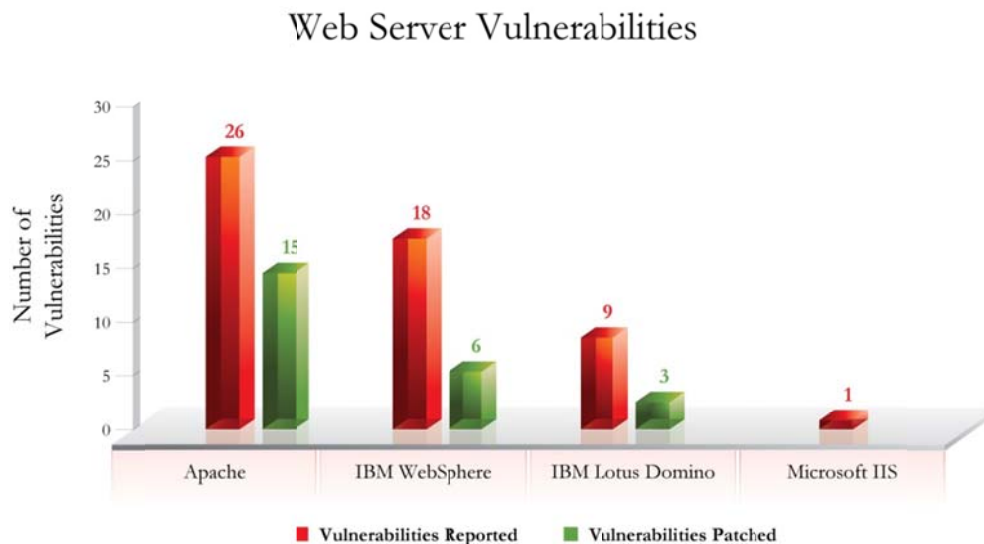
Web Browser Vulnerabilities

In terms of vulnerabilities in Web browsers, we observed some interesting behavior in the first half of 2010. Both Mozilla Firefox and Internet Explorer showed improvements in vulnerabilities found compared to the previous period. Firefox had 59 reported vulnerabilities compared to 77 in the second half of 2010. Internet Explorer had 40 reported vulnerabilities compared to 40 in the previous period. What is surprising this time around is vulnerabilities in Safari, which sky rocketed to 83 from 25 before and Google Chrome jumped to 69 from 25. Opera continued to stay low at 15 however it also had significantly more vulnerabilities compared to the 3 vulnerabilities reported in the

second half of 2009. But, we should acknowledge that this is after all software and as functionality expands, so will the number of vulnerabilities. The key is to fix these vulnerabilities quickly. What impressed us in the first half of 2010, all browser companies did a great job of fixing majority of their vulnerabilities ranging from 78 percent to 92 percent patching ratio. So, the development teams focused on these browsers deserve recognition for taking security seriously.



In the case of Web servers, Apache had the most vulnerabilities with 26, followed by IBM Websphere at 18, Lotus Domino at 9, and Microsoft IIS with 1 vulnerability. Microsoft IIS was the most improved from the second half of 2009. Apache was the quickest in fixing its vulnerabilities.



Detailed Trends from Enterprise Proprietary Applications

Cenzic ClickToSecure Managed is a leading-edge application security assessment and penetration testing managed service that identifies vulnerabilities and provides remediation to allow organizations to stay ahead of hackers. This service leverages the power of 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 coverage without adding resources.

During the first half of 2010, the Cenzic ClickToSecure Managed 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, 2010 findings are for the most part consistent with the findings revealed for the last couple of years. However, we did see an improvement in terms of fewer applications with critical vulnerabilities like Cross Site Scripting and SQL Injection. It's hard to tell if it's a trend or if we happened to have tested more secure applications in this period. Cenzic found that 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.

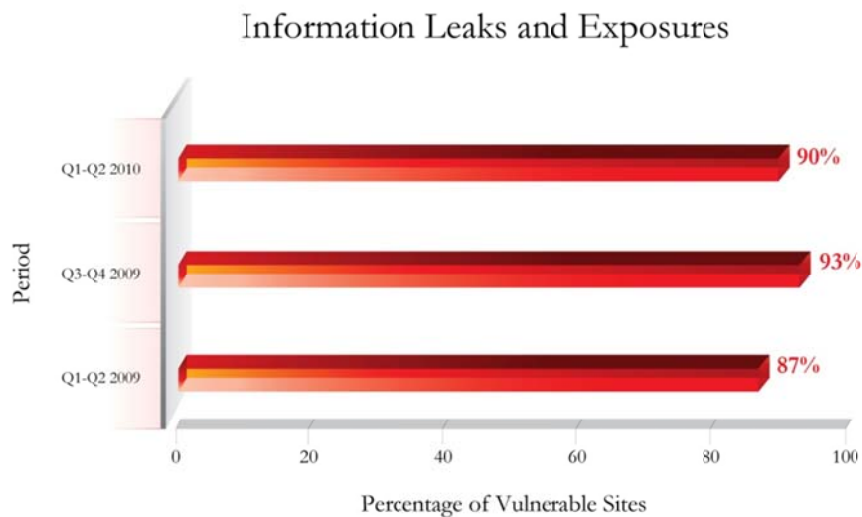
Authorization and Authentication flaws were found in 80 percent of all the Web applications we tested. These types of vulnerabilities continue to be common across many applications. Cross Site Scripting and Session Management came in high as well with 68 percent of applications having those types of vulnerabilities. Fortunately, we saw a decline in percentage of applications with SQL injection vulnerabilities.

Vulnerabilities Breakdown

Cenzic ClickToSecure found the following percentages of sites with vulnerabilities as belonging to each of the categories below during Q1-Q2 2010. 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 2010 data and previous quarters going back twelve months.

Information Leaks and Exposures (90%)

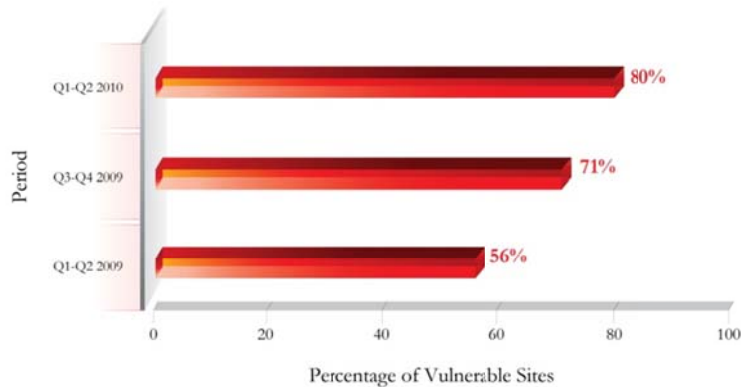
Transactions during ordinary use of a Web application can reveal sensitive information belonging to other users. It may also be possible to generate application errors by supplying various malformed character sequences, which can contain sensitive information. HTML comments are another example of an information leak, as these comments may assist an attacker in gathering information about the application. In the first half of 2010, we saw a slight decline from the previous period but still very high.



Authorization and Authentication Flaws (80%)

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 once again saw a jump from 2009.

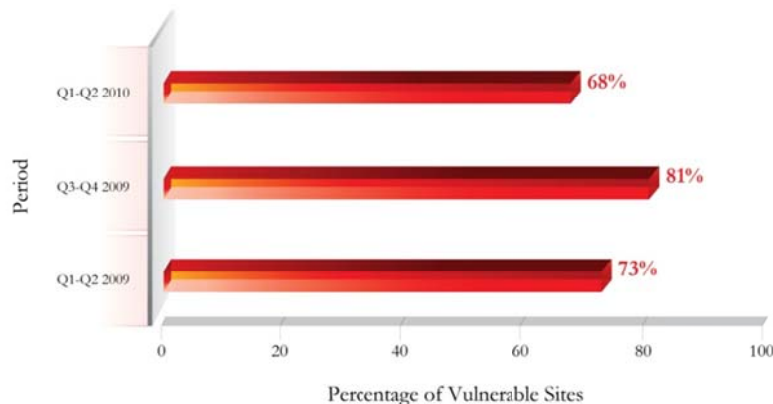
Authorization and Authentication Flaws



Cross Site Scripting (68%)

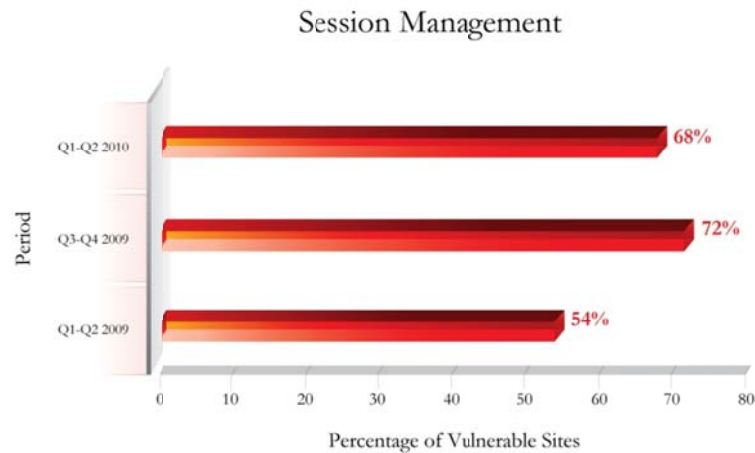
Cross Site Scripting attacks allow a remote attacker to corrupt the integrity of an application's code by inserting malicious scripts into the application itself, often directly into the database. Cross Site Scripting attacks may allow an attacker to steal users' session cookies, spoof content, or redirect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

Cross Site Scripting



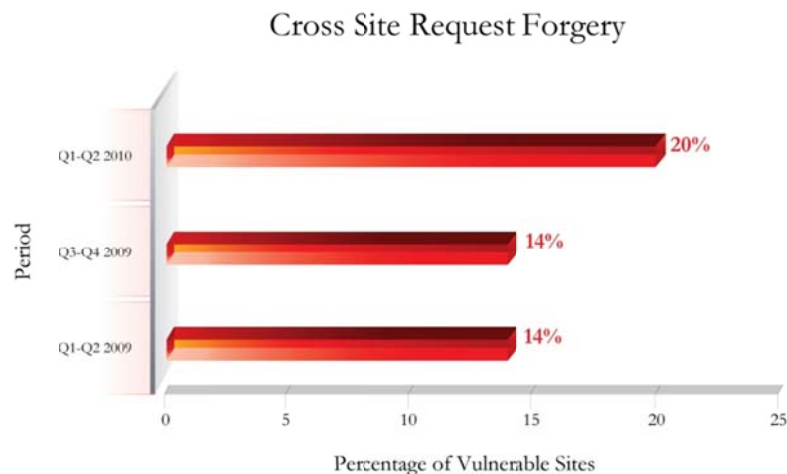
Session Management (68%)

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. We saw number of applications with Session Management vulnerabilities go down compared to the last period.



Cross Site Request Forgery (20%)

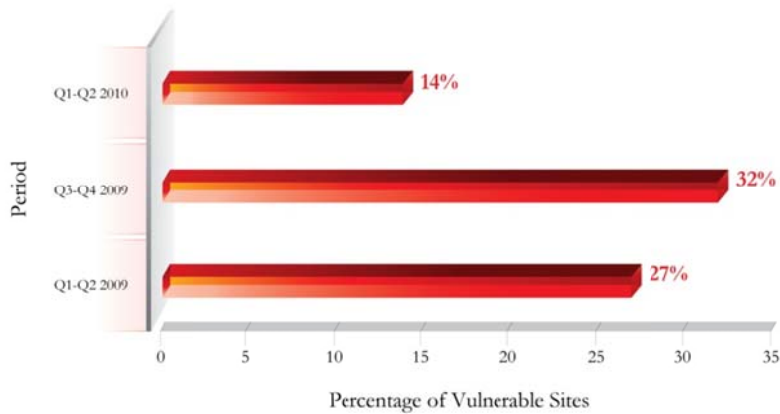
Cross Site Request Forgery (CSRF) is an attack that tricks the victim into loading a page that contains a malicious request. It is malicious in the sense that it inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf, like change the victim's profile, send an email to third party on his behalf, or purchase something. It exploits the trust a Web site has for the user. The percentage of applications with this vulnerability went up compared to the last period.



SQL Injection Attacks (14%)

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 major decline in applications with SQL injection vulnerabilities which is a great sign and hopefully this trend will continue.

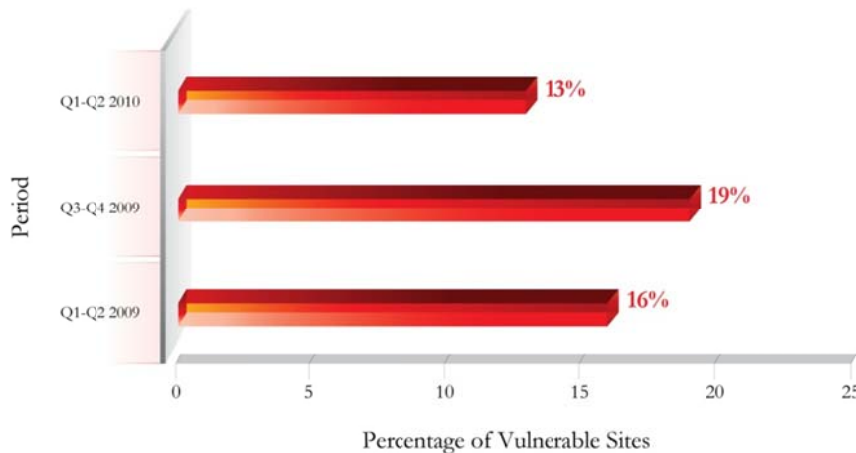
SQL Injection



Unauthorized Directory Access (13%)

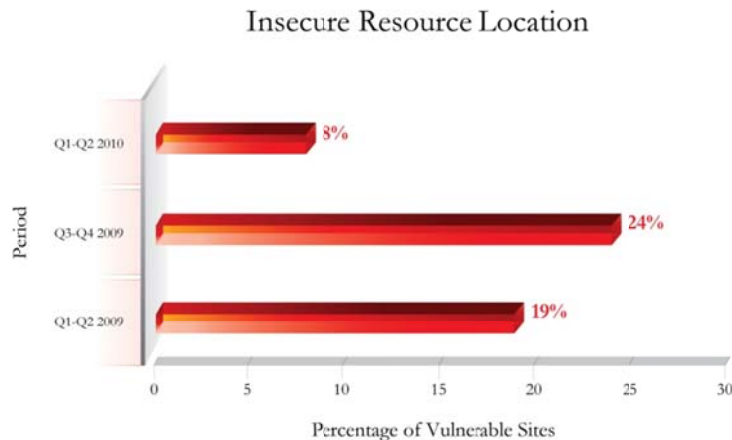
Insecure permissions on directories can allow an attacker to access areas of a Web site or Web application that should otherwise be protected. In other cases it is possible to directly browse the contents of a directory and enumerate all of the resources it contains. These types of vulnerabilities help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

Unauthorized Directory Access



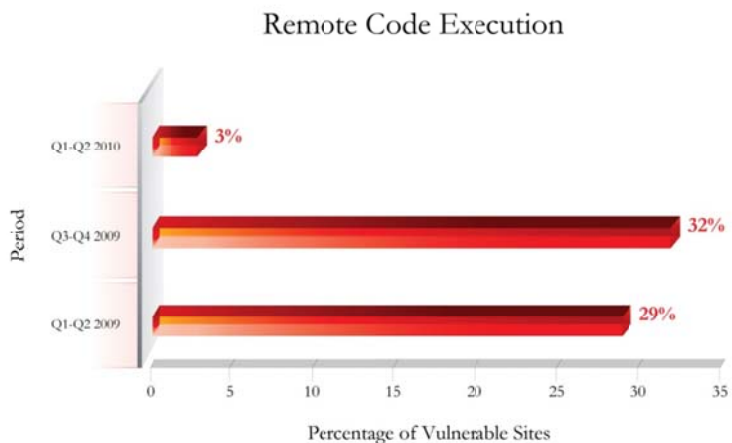
Insecure Resource Location (8%)

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 significant decrease in applications with this vulnerability.



Remote Code Execution (3%)

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 significant decline in applications with this vulnerability.



Interesting Web Attacks for Q1-Q2, 2010

While the percentage of vulnerabilities continue to be very high for Web applications, it's hard to pin down the number of attacks through Web applications. Since most hackers are now driven by either financial motivation or for political reasons, they are not likely to announce their presence even when they are actively hacking your site. In most cases, companies don't know for months and sometimes years that they were being hacked. Estimates range from 65 percent to 90 percent in terms of attacks at the Web application layer. Millions of hacking attempts are being made every day against corporations, universities, and government agencies. It simply makes sense. Hackers go where the vulnerabilities are. And, most of those holes are in Web applications.

We have listed some of the interesting and visible Web application related attacks from the first half of 2010. These are not in any particular order.

- **Hackers exploit SQL vulnerability on thousands of sites – June, 2010**
 - More than 100,000 webpages, including victims as diverse as The Wall Street Journal, TomTom, and the UK's Strathclyde police were hit by an attack that redirected visitors to a website that attempted to install malware on their machines. The sites were infected using SQL injection exploits, which allow attackers to tamper with a server's database by typing commands into user-input fields. The hackers used the exploit to plant iframes in the compromised sites that redirected visitors to robint.us. Malicious javascript on that site attempted to infect end users with malware dubbed Mal/Behav-290.

- **Session Management vulnerability exploited to gain iPad users' information – June, 2010**
 - A security flaw in AT&T's network exposed the e-mail addresses of more than 100,000 owners of Apple's 3G iPad. The security hole was uncovered by Goatse Security, a group known among security experts as hackers who enjoy pulling Web pranks. The group exploited a session prediction vulnerability which allowed the hackers to write a script to predict the iPad owners' unique identification numbers to obtain their e-mail addresses. The list of exposed owners included New York Mayor Michael Bloomberg, White House Chief of Staff Rahm Emanuel and other powerful figures in finance, media and politics.

- **Cross Site Scripting (XSS) Vulnerability on Twitter exploited by Turkish Hackers – June, 2010**
 - A persistent XSS vulnerability was exploited by Turkish hackers to post a rogue status "Hacked by Turkish Hackers".

- **SQL Injection exploited to gain information on 168,000 Netherlands travelers – May, 2010**
 - The website created to encourage the use of smart cards for public transportation had a serious SQL injection flaw. The flaw was exploited by

a hacker with apparently good intentions to expose the weakness. As a result though names, addresses, and phone numbers of 168,000 travelers were publicly available.

- **Using Bruteforce, Turkish hackers attacked Armenian Sites – April, 2010**
 - Turkish hackers attacked several Armenian websites ahead of annual commemorative remembrances of the Armenian Genocide. On April 12th, more than 250 sites were impacted when cyber terrorists attacked a server hosting sites - ArmeniaChat.com, and ArmeniaSearch.com.

- **Exploiting an authorization vulnerability, hacker disables 100 cars remotely – March, 2010**
 - An ex-employee Ramos-Lopez's account had been closed when he was terminated from Texas Auto Center in a workforce reduction, but he allegedly got in through another employee's account. At first, the intruder targeted vehicles by searching on the names of specific customers. Then he discovered he could pull up a database of all 1,100 Auto Center customers whose cars were equipped with the device. He started going down the list in alphabetical order, vandalizing the records, disabling the cars and setting off the horns.

- **Credit Card Information of Customers of an electronic retailer exposed – February, 2010**
 - Credit Card information of 3000 customers of an electronics e-retailer was exposed after hackers exploited a SQL Injection vulnerability in its e-commerce system.

- **Baidu hacked by Iranian Cyber Army – January, 2010**
 - The attack was used to show a message from the Iranian Cyber Army appear on the Baidu home page. Here's how Baidu alleges the hacker got access to one of the world's most popular web sites domain name account in under an hour: 1. Hacker starts online chat session with Register.com representative, claiming to be an agent of Baidu. 2. Register.com representative asks hacker to provide verification information. Hacker provides invalid information, but Register.com goes ahead and e-mails a security code to the email address it has on file for Baidu anyway. 3. The hacker doesn't have access to that e-mail address, so he/she relays a bogus security code to the Register.com representative via chat. Baidu claims the representative didn't bother to compare the code to the actual one. 4. Hacker asks Register.com representative to change email address on file to antiwahabi2008@gmail.com, and representative does. 5. Hacker now uses "forgot password" link at Register.com to request the username and password to the account. Hacker can then log in and change the name servers.

About Cenzic

Winner of numerous awards and independent product reviews, Cenzic, a trusted provider of software, managed service, and cloud security products, helps organizations secure their websites against hacker attacks, serving organizations across all industries. Cenzic focuses on Web Application Security, automating the process of identifying security defects at the Web application level where more than 75 percent of hacker attacks occur. Our dynamic, black box Web application testing is built on a non-signature-based technology that finds more “real” vulnerabilities as well as provides vulnerability management, risk management, and compliance for regulations and industry standards such as PCI. Cenzic solutions help secure the websites of numerous Fortune 1000 companies, all major security companies, leading government agencies and universities, and hundreds of SMB companies -- overall helping to secure trillions of dollars of e-commerce transactions. The Cenzic solution suite fits the needs of companies across all industries, from testing remotely via our cloud service (ClickToSecure Cloud™) to our managed service (Cenzic ClickToSecure® Managed), to a full enterprise software product (Cenzic Hailstorm® Enterprise ARC™) for managing security risks across the entire company.

Cenzic Product Suite

Software	SaaS	Professional Services
<p>Cenzic Hailstorm Enterprise ARC Enterprise software product that tests Website security. Supports security risk management throughout the SDLC using a role-based & scalable architecture, with results via a Web dashboard.</p>	<p>Cenzic ClickToSecure Managed Managed service offering where Cenzic security experts remotely perform full vulnerability testing on your Website. Ideal solution for companies with limited budget and/or resources.</p>	<p>Assessment Methodology Get an assessment of your Web application security processes in just 3 days from Cenzic’s highly skilled security team.</p>
<p>Cenzic Hailstorm Professional Desktop version of our software suite that’s designed for the power user to run their own Website security assessments.</p>	<p>Cenzic ClickToSecure Cloud Full SaaS offering that allows users to test their own Websites for basic attacks & receive actionable results all within their own Web portal. No security experts needed.</p>	<p>Training Product and application security training courses for both introductory and intermediate levels. Classes are taught as instructor-led or self-paced via CBT.</p>
<p>Hybrid Solution The combination of both software and SaaS offerings allow customers to run their own vulnerability assessments (using software) as well as leverage Cenzic’s security experts (using ClickToSecure Managed SaaS) to perform additional tests when volume increases.</p>		

Recent Awards

- Network Products Guide (Best Security Testing, Best Web 2.0 Security)



- Stevies 2010 Finalist (Most Innovative Company)



- AlwaysOn Top 100 (Cloud Security)



- SC Magazine Finalist (Best Security Software Development Solution)



- InfoSecurity Products Guide (Best Managed Security Solution)



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