CENZIC

NOW PART OF TRUSTWAVE

Application Vulnerability Trends Report : 2014

Table of Contents

2 Introduction

3 96% of Tested Applications Have Vulnerabilities

4 Cross Site Scripting Tops the List of Vulnerabilities Detected

5 Web Application Vulnerabilities Found - Trends

6 Probability of Vulnerability Type in any Given Application - Trends

7 Mobile Application Vulnerabilities

7 Prevention, Detection and Remediation

8 Common, Detectable Application Vulnerabilities

9 Products and Services

10 Conclusion

10 About Cenzic

Introduction

In 2013, Cenzic's Managed Services Team saw the world of online applications continue to grow more complex. We saw the emergence of people using any device in any location connecting to applications that could run on SaaS, private cloud and hybrid cloud infrastructures. Malicious hackers continue to exploit security gaps in applications created by vulnerabilities in order to breach sensitive information. In the course of scanning thousands of applications for our customers, we were able to gather many insights and data which went into this report.

While the benefits of web applications are rich, the risks to your organization, brand, and data are more costly than ever. Every day there are new reports of highly organized cyberattacks on leading websites. High profile victims have acknowledged breaches of their systems resulting in theft, espionage, and service interruption. The total number of reported security breaches in 2013 was 619 compared to 637 in 2012 according to the Identity Theft Resource Center.

The cost of cybercrime for 2013 for the US economy was more than $100 billion and $300 billion globally according to the Center for Strategic and International Studies (CSIS). Nearly 400 million credit card numbers, social security numbers and other personal information were stolen. The toll on IT and security teams after a breach is significant. There is a rush to investigate, analyze and remediate the damage.

We continue to see efforts to manage the security of BYOD mobile devices. It is clear that the prevalence of BYOD shifts more of the security burden to enterprise application owners to limit attack surfaces within the applications. Insecure mobile applications may result in unauthorized access to data. Quite often, customers are asking us how BYOD will affect their data security and what measures can they take before becoming a victim of cybercrime?

Hackers are continuously evolving their recon, mapping and exploitation efforts to gain access to back end servers that applications connect to while bypassing the traditional security perimeter of Firewalls, Intrusion Detection and Intrusion Prevention Systems. It is with this awareness that we present our findings on evolving web and mobile application vulnerability trends.

Please use this document to understand the current vulnerabilities and risk landscape. And more importantly, use it as a motivation to improve your application security posture.

96% of Tested Applications Have Vulnerabilities

The application layer continues to be a soft target with increasing cyberattacks. 96% of all applications tested in 2013 have one or more serious security vulnerabilities. The median number of vulnerabilities per app has elevated to (14) from last year's count of (13).

What explains this?

CISOs often tell us that they struggle to hire, train and retain web application security experts. Application developers often tell us they struggle with development timelines and more of their compensation is tied to feature completion rather than security certification. With thousands of known vulnerabilities and hundreds more discovered in any given month, minimizing application vulnerabilities is a serious challenge.

The security implications of these statistics are profound. Applications have become the soft target in the IT infrastructure. With so many vulnerabilities to choose from, hackers can easily breach the increasingly valuable data that applications access.

How do organizations respond today?

Many of these vulnerabilities are relatively easy for application security teams to detect, block and fix during every phase of the application development life cycle. Technologies and processes for reducing application vulnerabilities include secure coding standards, vulnerability scanning, web application firewalls and intrusion detection, among others. The best results come from a multi-layered and coordinated approach that includes technology, processes, employees and a security-oriented corporate culture.

The changes required to improve your risk profile may be possible with currently available security tools and your existing engineers. While the worldwide shortage of experienced web development engineers may impact the pace of development of new applications, it is a barrier that can be overcome.

Automated scanning tools, and managed services can shore up short-handed Development and Security teams. Best practices continue to evolve for making the most out of existing resources. For example, using quantitative risk metrics for application vulnerabilities allows for more efficient prioritization. This allows for highly effective processes for prioritization and improvement of real-world security within the constraints of available resources.

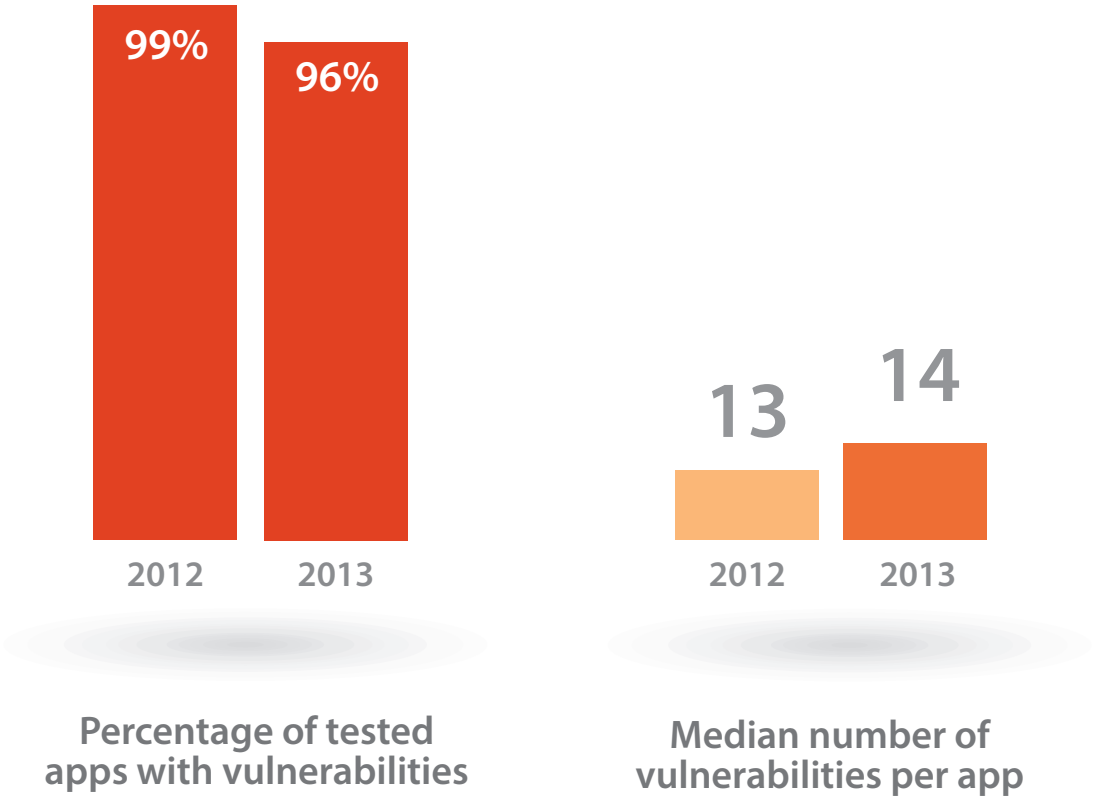

Figure 1: 2012-2013 Summary Statistics: Application Vulnerabilities

Cross Site Scripting Tops the List of Vulnerabilities

As Cenzic has gained visibility into more companies, our ability to track vulnerabilities in development, production and supply chain applications has improved. In multiple instances during 2013, Cenzic found major Cross Site Scripting (XSS), Information Leakage, Authentication and Authorization vulnerabilities across all vertical markets.

At 25% of the total, XSS was the most frequently found vulnerability in apps tested in 2013. A substantial percentage of tested apps have multiple XSS exposure points to remediate and many of them create severe security risks.

While XSS leads the list in terms of frequency of occurrence, the list is significant. Information Leakage (23%), Authentication and Authorization (15%), Session Management (13%), SQL Injection (7%), Cross Site Request Forgery (CSRF) (6%), and other (11%) round out the list of the total vulnerabilities found.

Why CISOs are concerned?

As application security professionals, we sometimes wonder why well-known and long-recognized vulnerabilities such as SQL injection still make the list. Shouldn't SQL injection be like small pox and be nearly extinct?

Nonetheless, this year's data paints a more nuanced picture. Even as application developers and the common modules and frameworks they use reduce the prevalence of some vulnerabilities such as CSRF, others such as information leakage appear to be growing in frequency.

Default and weak passwords, database misconfigurations, and missing security patches are consistent trends that provide easy avenues of attack to the seasoned hacker.

In a recent survey from OWASP, CISOs see more than 51% of their security risk coming from application security. Exploitation of web applications is the leading threat haunting CISOs and yet they have difficulties allocating head count and budget needed to detect and correct application vulnerabilities.

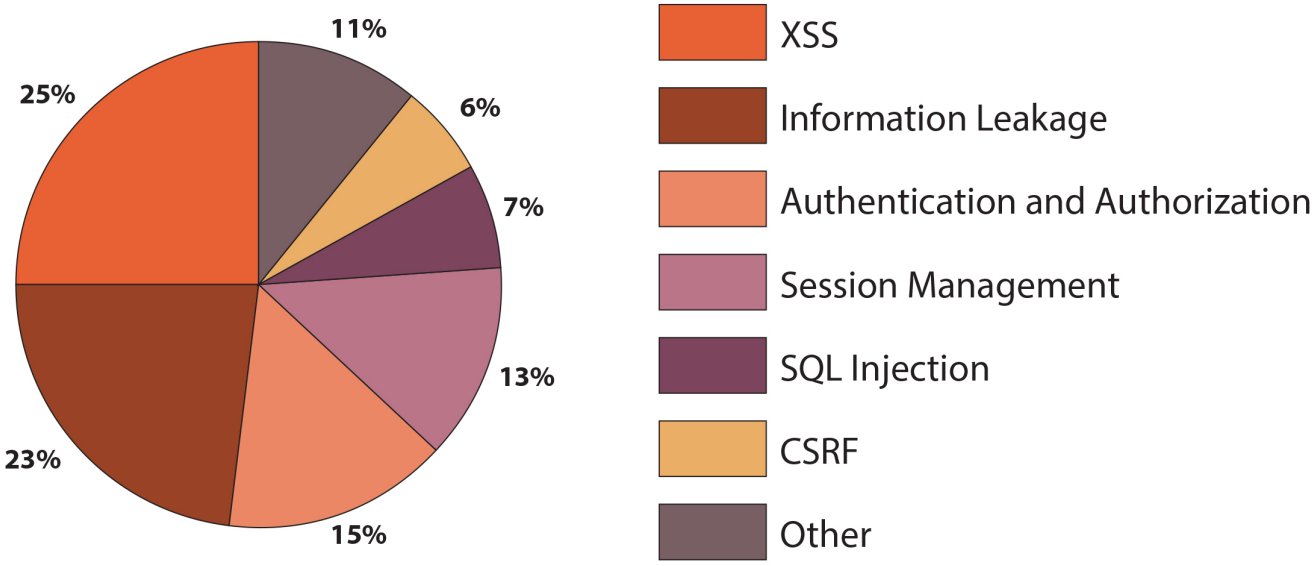

Figure 2: 2013 Web Application Vulnerabilities Found Trend

Web Application Vulnerabilities Found Trends

"25% of Vulnerabilities Found Involve Cross-Site Scripting"

The chart below shows the relative share of vulnerability types found and the sum equals 100%. Out of all vulnerabilities discovered XSS and Information Leakage are the largest share because they occur often and in some cases multiple times per application. Information leakage has the highest percentage increase which is up 7% from the 2012 level of 16% of detected vulnerabilities.

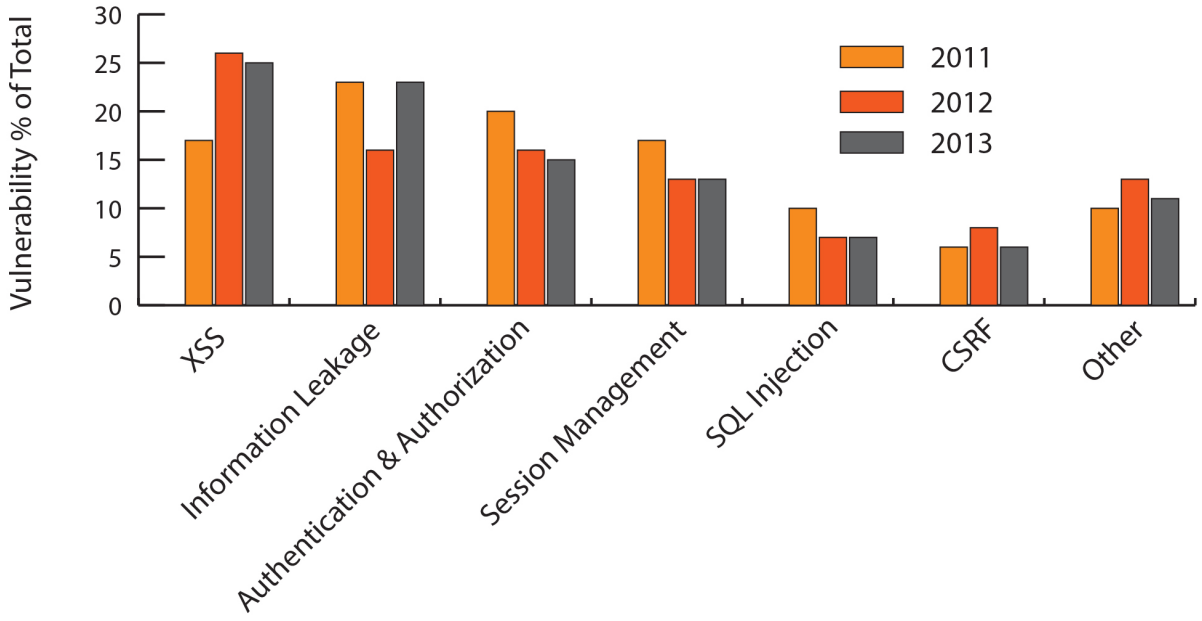

Figure 3: 2013 vs. 2012 and 2011 Web Application Vulnerabilities Found Trends

Figure 3 shows that three out of seven categories of vulnerabilities declined in 2013 compared to 2012, while one category increased and the remainder were essentially unchanged. Using the categories described above it was possible to identify areas within web applications that caused the highest number of vulnerabilities during the period of study. In all three years, session management, cross-site scripting, information leakage, authentication & authorization accounted for the highest number of vulnerabilities identified.

None of the categories saw consistent increases each year. Information leakage had the biggest percentage increase which nearly doubled in 2013 compared to 2012. This is likely due to accidental leakage of sensitive information through data transmission or error messages.

Authentication & authorization saw a third year in a row of decline, albeit modestly. Whether this is because Authentication & Authorization are actually shrinking, or simply because other vulnerabilities are becoming more common is less clear.

General awareness within IT organizations about the importance of application security is growing. We see more of them demanding that their vendors also take application security seriously. In the past, it was common to see vendors postpone security fixes in favor of releasing new versions of their software with new functionality and unpatched vulnerabilities.

The trend of consistent scanning, monitoring and correcting vulnerabilities is a process that many companies have implemented to reduce online risk. Information security teams who use remediation data that integrates into Security Information and Event Management (SIEM) devices or Web Application Firewalls (WAF) can quickly patch vulnerabilities.

While these trends are modestly good news, it is important to remember that vulnerabilities still exist across all categories. They exist in legacy applications and new applications. The threats from these vulnerabilities continue to evolve as cybercriminals experiment with new and different attack strategies.

Probability of Vulnerability Type in any Given Application

"Session Management Vulnerabilities Appear in 79% of Applications"

Below is a breakdown of the likelihood of finding at least one such vulnerability class in any given application. Numbers will not add up to 100% as each application can have multiple classes of vulnerabilities.

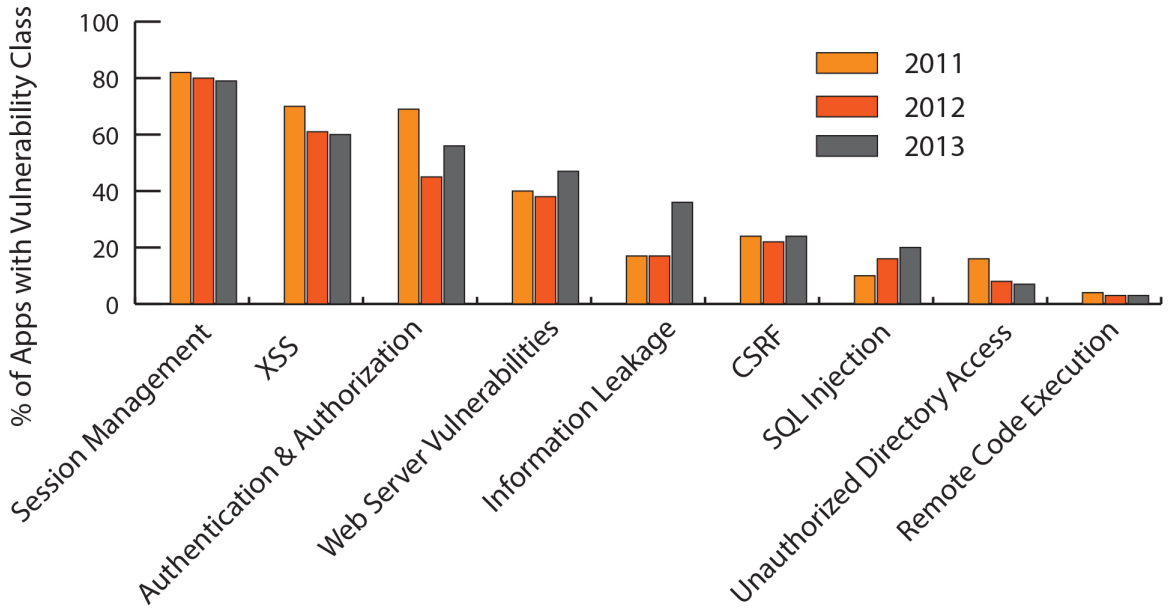

Figure 4: 2013 vs. 2012 and 2011 Probability of Vulnerability Type in any Given Application

Figure 4 shows that most apps have several common categories of vulnerabilities. This makes remediation more labor intensive, as each kind of vulnerability has its own particular technique for fixing the issue.

Session Management vulnerabilities were detected in (79%) of applications tested in 2013, more than any other application vulnerability class. It also shows that XSS vulnerabilities appear in (60%) of applications, followed by Authentication and Authorization (56%), Web Server Vulnerabilities (47%), Information Leakage (36%), CSRF (22%), SQL Injection (20%), Unauthorized Directory Access (8%) and Remote Code Execution (3%).

Six vulnerability categories increased and three decreased in 2013 versus 2012, suggesting that application and security teams are still leaving holes that can be exploited. The increase in detection of SQL Injection vulnerabilities may be due to improvements in the detection techniques more than from new deficiencies in security practices. The possible security ramifications range from authentication bypass to information disclosure to enabling the distribution of malicious code to application users.

Even when applications are operating effectively and securely, they are constantly under scrutiny by attackers looking for vulnerabilities or points of entry. Enterprises should be persistent and continuously test their applications, monitor their status, and report on potential production problems in real time. Regular assessments help to ensure that applications are clear of vulnerabilities, and help mitigate the risk of a major breach.

It's worth noting that well-known vulnerabilities such as SQL injection appear in a small percentage of applications, yet are responsible for a significant portion of the data stolen or compromised. SQL Injection is one of the most effective exploits for stealing large amounts of data. Some experts estimate as much as 80% of the data stolen is because of SQL injection.

The take away here is that prevalence data such as figure 4 above must be coupled with objective risk scores, such as Cenzic's HARM™ Score, to optimally prioritize and reduce risk.

Mobile App Vulnerabilities

As more data is made available to mobile devices, mobile application security grows in importance. The Cenzic Managed Services team has discovered the following vulnerabilities during 2013:

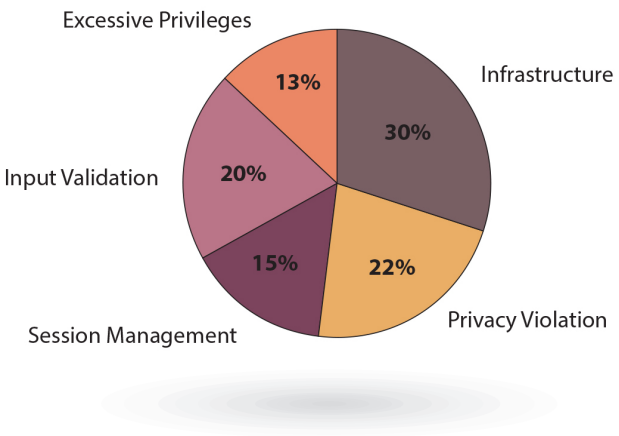

Figure 5: 2013 Mobile Application Vulnerability Population

It is important to note that the largest category of risk (30%) comes from server configuration and patch level (Infrastructure), rather than the mobile application code itself. Web services must be secured.

Mobile developers should consider focusing their attention on how data is transferred to and stored on mobile devices as Input Validation (20%), Session Management (15%) and Privacy Violation (22%) combine to account for (57%) of mobile vulnerabilities. Storing unencrypted data on mobile devices is a significant cause for concern.

In the chart below we see that five vulnerability categories are extremely common in mobile applications. Privacy is not always seen as a security issue for the enterpise, though it may be for the user. Excessive privileges stems from developers giving their apps more power than is necessary to complete its function. Session termination is far too often an after thought.

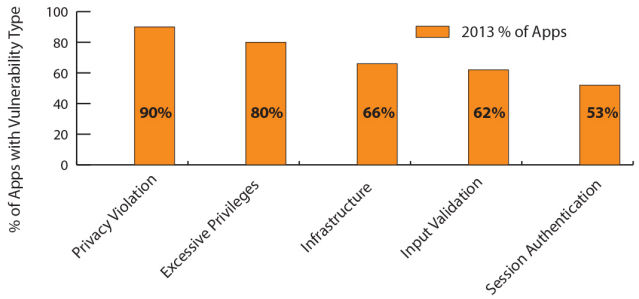

Figure 6: Probability of Vulnerability in a Given Mobile App

Prevention, Detection and Remediation

Proactive and consistent application risk mangement generally involves efficiently preventing, detecting and remediating vulnerabilities across the entire application ecosystem. In general, early detection is more efficient but with some notable exceptions. In theory, prevention would be the most efficient way to reduce vulnerabilities...except that no human developer can keep track of the 6,000+ known vulnerabilities. Nonetheless, coding best practices certainly help reduce vulnerabilities early on.

Static Application Security Testing (SAST) tools can identify vulnerabilities in early-stage development. There are pros and cons to SAST. SAST tools can identify vulnerabilities at the earliest possible moment, when the developer is actively working the project, and identify the specific line of code in need of remediation. This helps save time. Unfortunately, SAST may create some superfluous information and has an inherently higher false positive rate than Dynamic Application Security Testing tools (DAST). Some vulnerabilities simply cannot be seen until they are in a run-time environment. DAST tools look at code behavior, and hence tend to be much more accurate. As a result, many developers prefer to compile their code and dynamically test it in a run-time environment iteratively. Since some vulnerabilities only appear in a run-time environment, there must be a DAST scan prior to an application launch. We recommend scheduling and automating regular scans after going into production.

Remediation can follow several paths. SAST solutions tend to point out each specific instance of a vulnerability and offer great precision. DAST solutions are stronger at identifying global problems where a single high-level code fix may remediate many specific instances of a given vulnerability. Some developers prefer to run DAST scans first, make global repairs, and then use SAST to focus on any remaining code sections.

While it is often more efficient for developers to modify code while the project is still ongoing, that is not always the most efficient way to address a vulnerability. Web Application Firewalls (WAF) can create virtual patches to block vulnerabilities, sometimes in seconds. Given that new vulnerabilities are often discovered after the application goes into production, WAFs have a variety of advantages over the long haul.

Server Configuration incorporates aspects of prevention, detection and remediation. Some vulnerabilities disappear when the server is brought up to the proper patch level and configuration specifications.

A mature risk management model, whether it incorporates enterprise scanning software or managed services, provides both real time snap shots and trend data of your security posture over time. This allows both proactive and, if needed, crisis management capabilities. This is crucial not only to speed security response but to optimally reduce risk with inevitably limited resources.

Common Detectable Application Vulnerabilities

Vulnerability	Description
Cross Site Scripting (XSS)	An application allows attackers to send malicious scripts by relaying the script from an otherwise trusted URL. **Detection:** web application security scanner **Block/Fix:** coding standards, web application firewall
Information Leakage	An application inappropriately discloses sensitive data, such as technical details of the application, environment, or user-specific data. **Detection:** web application security scanner **Block/Fix:** coding standards, web application firewall
Session Management	An application inappropriately allows attackers to interject themselves as valid website users. **Detection:** web application security scanner **Block/Fix:** coding standards
Authentication & Authorization	An application does not properly ensure for unbreachable and unreplayable authentication, and/or authorized access to data and capabilities is not properly enforced on the server side of the application. This includes enforcement of proper encrypted communication of credentials, password standards enforcement, feature and data access ACL enforcement, etc. **Detection:** web application security scanner **Block/Fix:** server configuration, coding standards
Cross Site Request Forgery (CSRF)	CSRF inappropriately leverages a current authenticated browser session and uses unauthorized commands with credentials that the application trusts. **Detection:** web application security scanner **Block/Fix:** Coding practices, web application firewall
SQL Injection	An attacker inputs SQL database commands into a data entry field, and tricks the application into delivering user data, destroying user data, planting malicious data, extracts infrastructure information, drops tables, removes users or can dump a database. **Detection:** web application security scanner **Block/Fix:** coding standards, web application firewall
Web Server Version	Exploits applications, servers and databases through unpatched versions of server software with known security issues. **Detection:** web application security scanner **Block/Fix:** server configuration
Remote Code Execution	An application allows any arbitrary commands to execute on a vulnerable device. Successful exploitation could result in an attacker both inappropriately controlling/executing commands on the device, and being able to do so with the same privileges as the logged in user. **Detection:** web application security scanner **Block/Fix:** Coding practices, server configuration
Web Server Configuration	Attackers exploit misconfigured servers or access to server configuration files, enabling further, more sophisticated attacks. **Detection:** web application security scanner **Block/Fix:** server configuration
Unauthorized Directory Access	Access to directory listings should be restricted. Unsecured directories can be traversed, accessed and viewed by an attacker who may be able to access or view the contents of files. **Detection:** web application security scanner **Block/Fix:** server configuration

Products and Services

Cenzic application security solutions are powered by Cenzic Hailstorm™ and enable organizations of all sizes to continuously assess Cloud, Mobile and Web applications to manage online risk and contain breaches.

Products	Description
Cenzic Enterprise	Cenzic Enterprise is a multi-tier software solution that assesses the security of Cloud and Web applications and supports security risk management throughout the software development lifecycle. Cenzic Enterprise provides a company-wide view of security vulnerabilities and status to executives as well as customizable role-appropriate views and assessment capabilities for each member via a Web-based dashboard.
Cenzic Desktop	Cenzic Desktop is a single-user version single-user version of the same core assessment technologies used by Cenzic Enterprise. It is designed for the power user that wants to run their security assessments on Cloud and Web applications from a single system.
Cenzic Managed Cloud	With Cenzic Managed Cloud, Cenzic's security experts remotely perform full vulnerability testing on Cloud, Mobile and Web applications. From a Web-based dashboard, users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
Cenzic Cloud	Cenzic Cloud allows users to test their own Cloud and Web applications for basic attacks and receive actionable results all within an account on our online hosted SaaS security solution. No security experts needed.
Cenzic Hybrid: Software + Cloud	Cenzic Hybrid provides access to both Cenzic Enterprise software and Cenzic Managed Cloud services. Vulnerability testing can be done either by using the software on premise or by leveraging Cenzic expert security services team.
Cenzic Mobile	Cenzic Mobile is a managed service to conduct full vulnerability testing and business risk analysis on mobile applications. All testing is managed from a Web-based dashboard where users can request assessments, view results, run reports, analyze trends and request re-tests of applications to verify remediation efforts.
Cenzic PASS™	The Cenzic Partner-Application Security Scanning (Cenzic PASS™) service helps enterprises reduce online risk stemming from integrated third-party applications, such as supply chain, COTS vendors, and partners, in an efficient, effective and prudent manner.
Cenzic Services	Cenzic services and training help those responsible for Cloud, Mobile and Web application security to implement best practices and procedures to protect data from hacker attacks.

Conclusion

- 96% of applications have vulnerabilities with a median of 14 per application
- Vulnerabilities per application is steady over the last three years
- XSS, Leakage, Authentication and Session Management are most common
- Privacy Violation and Excessive Privileges appear in over 80% of mobile apps
- Enterprise software and managed services can make most efficient use of existing headcount

While the majority of corporations have the important security building blocks, such as firewalls and intrusion protection systems needed for their security infrastructure, not enough organizations have comprehensive tools and practices in place for securing applications. The result is that hackers are increasingly focusing on and are succeeding with layer 7 attacks.

Application developers tend to focus on adding features rather than rooting out all application vulnerabilities. This combined with the daunting task of preventing, detecting and eliminating application vulnerabilties explains part of the continued widespread discovery. Prevelance data should be coupled with objective risk scores, such as Cenzic's HARM™ Score, to optimally prioritize and reduce risk.

A shortage of skilled application security professionals remains a major issue across the global business landscape. This is likely to continue and lead to the growth in managed security services as companies look to bring in specialists to augment their overextended teams. Ultimately this will lead to better protection for web, cloud and mobile applications.

About Cenzic

Cenzic, now part of Trustwave, provides the leading application security intelligence platform to continuously assess Cloud, Mobile and Web applications to reduce online security risk. Our solutions scale from a single application to enterprise-level deployments with hybrid approaches that enable testing of all applications at optimal levels. Cenzic solutions are used in all parts of the software development life cycle, and most importantly in production, to protect against new threats even after the application has been deployed. Our patented Hailstorm platform has an architecture designed to monitor and detect web, cloud and mobile applications for vulnerabilities across 120 threat vectors. We help brands of all sizes protect their reputation and manage security risk in the face of malicious attacks. Today, Cenzic solutions help secure more than half a million online applications and trillions of dollars of commerce for Fortune 1000 companies, government agencies, universities and SMBs.

www.cenzic.com