



## **Cenzic for Government**

Cloud, Mobile and Web Application Security  
to Protect Online Services



## Table of Contents

Executive Summary .....	3
Why Web Application Security Is Important.....	3
Risk Management.....	4
The Application Security Link in the Compliance Chain .....	5
Cenzic’s Application Security Solutions for Assisting in Compliance .....	5
About Cenzic .....	6



## Executive Summary

The President's office is dedicated to providing technology leadership including rolling out more online services to citizens. New CIO and CTO positions and other initiatives laid down by the administration are bound to produce positive results. Unfortunately openness of the Web attracts more threats and attacks against our infrastructure. With over 75% of attacks happening through the websites, it's critical that the government agencies are prepared to defend their information assets appropriately. Hackers are not relenting. Whether it's politically motivated and funded attacks like the ones from North Korea, or financially motivated attacks from Russia, Ukraine, China, and other countries, there is a continuous stream of attacks. Many of these attacks have been successful causing major damages. According to President's office, over \$1 trillion worth of intellectual Property was stolen last year alone. There are about 24,000 U.S. Government websites that are exposed and ripe for hackers. The Nation is not even close to prepared to thwart attacks from professional hackers and other governments in proxy cyber wars. Cyber security needs to be integral part in the Government 2.0 world.

Senior IT and security managers at government agencies have a huge challenge in addressing various security issues to protect their cyber infrastructure. Most agencies are significantly behind in understanding issues around their websites, which have become the weakest link in the cyber war. Not only are they responsible for ensuring that there are no breaches, they have to ensure compliance with the many regulations, including the Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), Section 508 and others. While most agencies, including Department of Defense (DOD), Department of Homeland Security (DHS), and others, have done a reasonable job of ensuring security at the network layer with network firewalls, anti-virus, and intrusion detection systems (IDSs), more work is required on protecting their applications.

Application security and automated tools to assess application security vulnerabilities protect computerized information accessible through Web-enabled applications. Accordingly, application security tools are crucial for preventing unauthorized access, destruction, use, modification, or disclosure of personal information available through Web applications, as required by various regulations. Cenzic's application security solutions help agencies comply with various government regulations, by allowing them to use automated processes to assess risk, check for vulnerabilities, test code and controls during software development for the purpose of preventing unauthorized access, destruction, use, modification, or disclosure of personal information.

## Why Web Application Security Is Important

While various network security technologies are good at protecting the network layer, hackers now target the Web application layer by injecting attacks through the forms and fields that are open to citizens.

What is a Web application? Most citizens and even a lot of IT professionals don't realize that websites that allow users to do communicate and conduct business transactions online are powered by Web applications. And, in some cases there are hundreds or even thousands of these applications acting as the engine for websites. Simply put, a Web application is a software program that's written in a browser supported language like HTML, and is accessed over the browser. This is different from the older ways of an application that used to have a fat client which accessed the server.

Technically, the fact that these Web applications are vulnerable is not a new phenomenon. The fact is that they have always been vulnerable since the early days of Web in the late 90s. However, hackers started exploiting these vulnerabilities in the early 2000s as networks got more secure and hackers realized that most websites were wide open for hacking.

So, how did these applications get deployed with so many vulnerabilities? First, most developers were not trained to think about security when developing applications. During the client-server era, there weren't any public facing applications so no one thought it would be a big issue. The Web made everything open which was great for business but with everything good comes something bad. In this case, we got the hackers. Secondly, even developers who were trained in security and

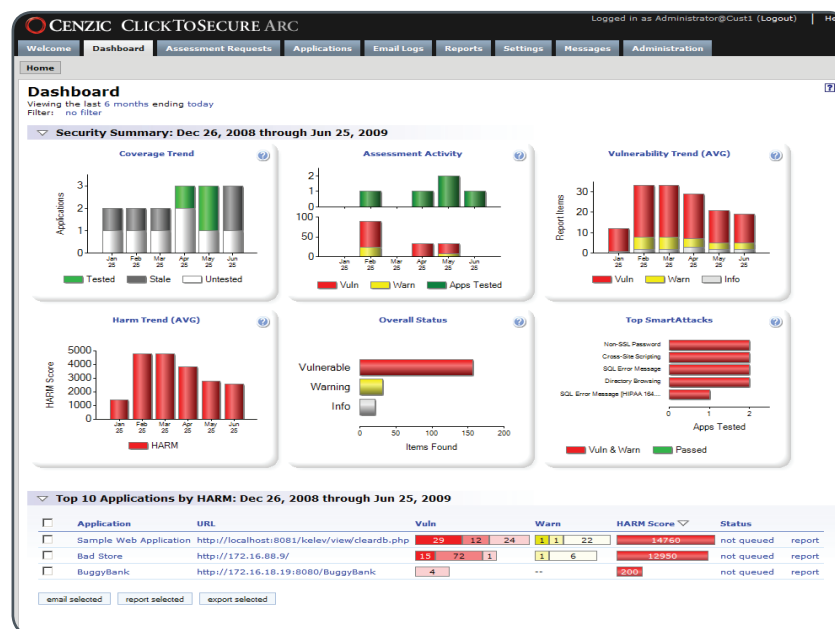


really understood security issues suffer from lack of time. Most developers are extremely busy and under a time crunch to get the applications out in a timely fashion. They don't have time to even do unit testing, let alone security testing.

For many government agencies, Web applications have even more significance due to the vast amount of sensitive intelligence information relating to our nation's intellectual property as well as confidential information pertaining to citizens. Hackers, both domestic and foreign, realize the importance of the information and are making these Web applications a prime target to attack penetrating these many times already. Custodians of these Web applications within these agencies have to figure out how to quickly start the process of finding the holes and putting a plan together to remediate before more significant damage is done.

## Risk Management

Web application security is all about risk management. You have to know which Web applications you have, where they are, which ones have been tested vs. not, what vulnerabilities do you have, how to prioritize them, and how to monitor the progress on an ongoing basis. Cenzic's application security solutions provide a comprehensive management console that provides answers to these questions and more. With an easy-to-use interface, users can quickly run assessments on websites to find all the vulnerabilities. The management dashboard provides dynamic decision support information at your finger tips so you can start acting on the results immediately.



Cenzic Application Assessment Dashboard

Specifically, Cenzic can help government agencies:

- Run assessments and find vulnerabilities
- Provide actionable decision-support information with remediation tips
- Help prioritize vulnerabilities based on a quantitative metric
- Identify risks in various functions and subgroups



## The Application Security Link in the Compliance Chain

Government agencies, with Web applications, see the compelling opportunity to reach citizens and increase their exposure through the Internet. However, they also want to avoid the fate of organizations that got hacked. This means that securing applications has become a top priority.

Securing applications involves performing a risk assessment to identify the universe of possible security threats in a rapidly-changing environment. In particular, agencies will want to know whether their Web applications have vulnerabilities and what those vulnerabilities are. Whether agencies procure Web applications or develop them in-house, they will likely be judged on the efforts they take to ensure that they have minimized security risks affecting their applications.

Government regulations like FISMA and NIST place a large premium on preventing unauthorized access to personal information. Nonetheless, application security controls cannot be a mere afterthought, added just before moving a code base to production systems. Rather, application security should be part of the design, and security should be checked during development by QA engineers or information security professionals.

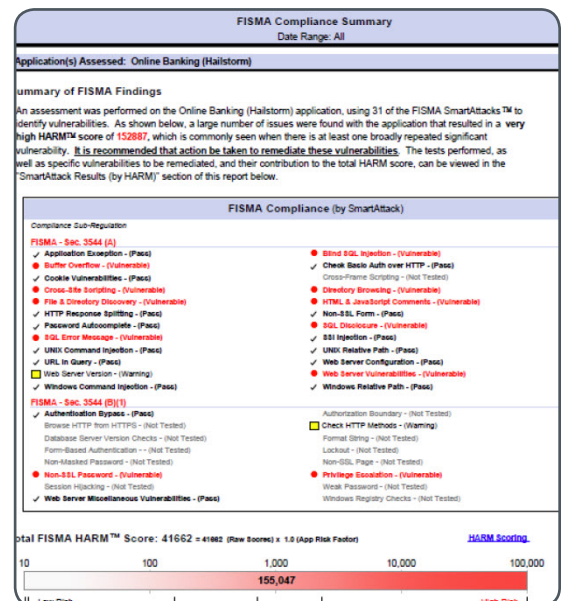
Following the implementation of a Web application on production systems, regular retesting is important to ferret out vulnerabilities that can only be seen in the application's operating environment and identify new vulnerabilities. Some vulnerabilities are apparent only when the Web application is in run time. For instance, session hijacking techniques pose a threat of unauthorized access to an application user's data and may permit a hacker to perform operations to misuse data as if the hacker were the user. Since these regulations require government agencies to prevent unauthorized access to or misuse of personal information, agencies hosting Web applications making use of personal information must check for vulnerabilities to threats, like session hijacking.

## The Cenzic's Hailstorm Solution for Assisting in Compliance

Cenzic's application security solutions provide a solution to businesses seeking to secure Cloud, Mobile or Web applications in an automated fashion with limited staff and time to perform testing. Cenzic's Hailstorm technology uses a Stateful Assessment™ approach. Businesses implementing Cloud, Mobile or Web applications can use Cenzic's solutions to perform automated security quality assurance checks on their applications. In addition, it can make use of user-defined tests for detection of vulnerabilities to attacks, such as phishing, circumvention of access controls and code injection.

Cenzic has created categories of attacks addressing NIST, FISMA and other regulations. It checks for vulnerabilities associated with unauthorized access or disclosure of sensitive data, such as personal information and thousands of other vulnerabilities that can be exploited by hackers to compromise government systems. By simply selecting a regulation category, government agencies can identify which sections of the regulation they are not in compliance with and take necessary correction action.

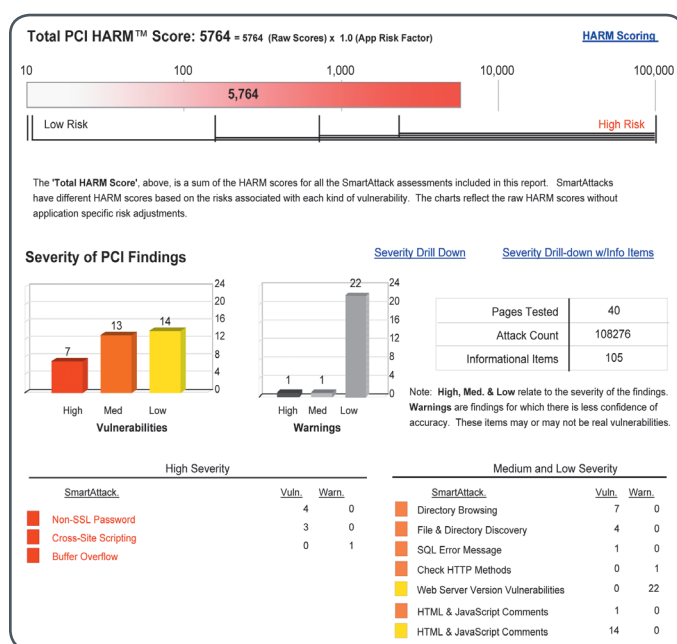
In addition to facilitating compliance, Cenzic provides crucial benefits for agencies deploying Web applications. Most importantly, Cenzic allows agencies with Web applications to obtain the results of manual penetration testing at a fraction of the cost. With hundreds of attacks in multiple categories, Cenzic's application security solutions ensure strong application security measures.





Automated checking permits developers, Q.A., and InfoSec teams to test for vulnerabilities more frequently throughout the software development lifecycle in a more closely controlled manner. Not only can checking be done more frequently, Cenzic makes it more practical to test earlier in the development lifecycle, saving development and testing costs.

Even after development or procurement, and the Web application goes live on production systems, Cenzic makes it possible to conduct ongoing assessments, of the live application, to check for security vulnerabilities in the production environment. Any new vulnerabilities uncovered can inform changes in security policies for appropriate responses, can motivate code changes, and can help in the design of new tests for additional future assessments. The Cenzic Intelligence Lab (CIA) continually develops new attack objects. Cenzic provides these objects to customers as updates on a regular basis. Because 400+ new application vulnerabilities appear every month, the updates from Cenzic's CIA permit customers to stay ahead of new developments.



## About Cenzic

Cenzic provides an application security intelligence platform to continuously assess Cloud, Mobile and Web vulnerabilities. This helps brands of all sizes protect their reputation and manage security risk in the face of malicious attacks. Today, Cenzic secures more than half a million online applications and trillions of dollars of commerce for Fortune 1000 companies, all major security companies, government agencies, universities and SMBs.



## Cenzic Products

Cenzic Enterprise	Cenzic Enterprise is a 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 customized views for other users from a Web-based dashboard.
Cenzic Desktop	Cenzic Desktop is a single-user version of 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 their own Web portal – 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’s expert security services team.
Cenzic Mobile	Cenzic Mobile service is delivered as a managed service. Cenzic’s security experts remotely perform full vulnerability testing on mobile applications. All testing is managed from a Web-based dashboard where users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
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.